

FNBDT 210 (Future Narrow Band Digital Terminal)'in IP Ağları Üzerinde Uygulaması

O. DİLLİ, M.MERT, M. KOYUNCU, S.NAZLIBİLEK ve N.AKÇAM

Özet — Teknolojideki hızlı değişim her alanda olduğu gibi haberleşme sistemlerinde de yaşanmaktadır. Geliştirilen farklı sistemler veya cihazlar zaman kaybedilmeden kullanıma sunulmaktadır. Söz konusu değişim genelde olumlu olmakla birlikte bazen olumsuz sonuçlara yol açabilmektedir. Bu olumsuz sonuçlardan bir tanesi, ISDN, PSTN ve IP tabanlı haberleşme cihazlarının birbirleriyle uçtan uca güvenli olarak haberleşme yapamamasıdır. Gelişmiş ülkeler tarafından söz konusu sıkıntının farkına varılmış ve çözüm bulma gayretleri 20. Yüzyılın sonlarında başlamıştır. Bu konuda en dikkat çekici çalışma, ABD tarafından başlatılan FNBDT 210 (Future Narrow Band Digital Terminal) çalışmasıdır. Bu çalışma, farklı şebekelerde haberleşme yapan cihazların birbirleri ile emniyetli haberleşme yapabilmesini amaçlamıştır.

Anahtar Kelimeler — FNBDT, Uçtan Uca Güvenli Haberleşme

Abstract — Fast progress in technologies affects all the domains as well as the communication systems. Different types of systems or devices are developed and given to the services without losing time. Although these progresses, in general, have positive effects sometimes they may cause some problems. One of these problems is that the different terminal devices based on ISDN, PSTN and IP cannot communicate end-to-end with each other in a seamless secure way. Some developed countries were become aware of the problem and started some studies at the end of the 20 century. The most important study on this problem was FNBDT 210(Future Narrow Band Digital Terminal) Project. The aim of the project was to achieve end-to-end secure communication of different terminal devices communicating on different networks.

Index Terms— FNBDT, End-to-End Secure Communication.

I. GİRİŞ

FNBDT 210 protokolü, farklı şebekelerde haberleşme yapan cihazların birbirleri ile emniyetli haberleşme ihtiyacından doğmuş bir protokoldür. Protokolün çalışması için temel olarak, FNBDT 210 destekli terminal cihazları ile şebekeler arasında altyapı dönüşümü yapan IWF (Interworking Function-Gateway) birimlerine ihtiyaç vardır.

FNBDT 210'un farklı network ağları üzerinde uygulama alanı bulunmaktadır. Bu çalışmanın IP Ağları üzerinden yapılmak istenmesinin nedenleri;

- IP Ağ uygulamalarının hem taktik hem de stratejik alanda çok yaygın olması,
- Haberleşme alanında IP ağlarının gelecekte daha da yaygın olarak kullanılacak olması,

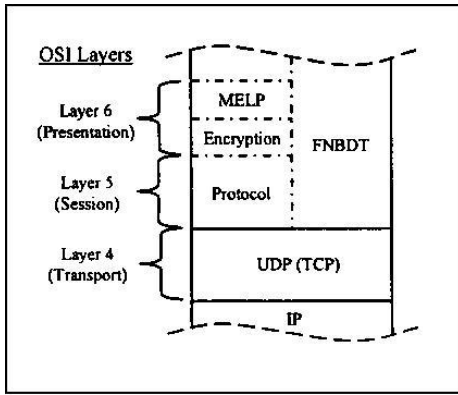
- FNBDT 210'un IP ağları üzerinden G.711 (64 kbps), G.729 (8 kbps) gibi yüksek bant genişliği tahsis yapan ses kodeklerini kullanmaksızın, Stanag 4591 Standartına uyumlu 2,4 kbps hızında MELP ses kodeğini kullanarak az bir bant genişliği tahsis yapması olarak belirtilebilir.

IP dünyasında paket kayıpları fazla miktarda olabilmektedir. Fakat gerçek zamanlı uygulamalarda ses paketlerinin kaybolması ses haberleşmesini ciddi ölçüde etkilemektedir. Bu çalışma, IP altyapısında FNBDT 210 haberleşme davranışlarının değişik durumlar altında gözlenmesi maksadıyla yapılmıştır. IP ortamında FNBDT 210'un nasıl davranacağı bilinmediğinden birtakım test verilerinin alınması gelecekte FNBDT 210 ile ilgili IP ağları üzerinde çıkabilecek olan sorunlara çözüm yolu sağlayacak ve referans olabilecektir. Bu çalışma bu alanda yapılan ilk uygulama olması ile dikkat çekmektedir. Bu çalışma ile, çağrı kurma ve farklı modlarda haberleşmede çok önemli yeni veriler elde edilmiştir. Bu veriler, bu alanda yeni ve farklı çalışmalar yapacaklara, ışık tutacak ve elde edilecek veriler ile karşılaştırılabilecektir.

II. FNBDT 210 SİNYALLEŞMESİ

FNBDT 210 Protokolü, Şekil 1'de görüldüğü gibi UDP protokolü üzerinde çalışmaktadır. Kriptolama işlemi Layer 6 ve üzerinde yapılmaktadır. IP paketleri ve UDP paketleri kriptosuz gönderilmektedir. Bu sayede Layer 3 ve 4 kapsamında Header Compression yapılabilmektedir [1].

FNBDT 210 sinyalleşmesi esas olarak bağlantı kurma ve kontrol sinyalleşmelerinden oluşmaktadır. Bağlantı Kurma Sinyalleşmesi, Yetenekler, Parametre/Sertifika, F(R) ve Kripto Senkronizasyon (CryptoSync); Bağlantı Kontrol Sinyalleşmesi ise İhbar İşlemleri (Notification), Mod Değiştirme ve Senkronizasyonu Tekrar Kurma konularını içermektedir.



Şekil 1. FNBDT/FNBDT 210 Protokol Altyapısı [2]

FNBDT 210 sinyalleşmesi, sekiz baytlık Start of Message (SOM) ile başlayıp sekiz baytlık End of Message (EOM) ile sonlanmaktadır.

SOM ve EOM arasında gönderilen çerçeveler “çerçeve grubu (superframe)” olarak tanımlanmaktadır. Her çerçeve grubu gönderme yönünde hata düzeltimi (FEC) ve çevrimsel artıklık denetimi (CRC) ile korunan çerçevelerden meydana gelmekte; FEC ile düzeltilemeyen hataların ortadan kaldırılması içinse olumlu veya olumsuz onay verme mekanizmaları (ACK ve NACK) kullanılmaktadır.

Her bir çerçeve, 1 çerçeve numarası, 13 mesaj, 4 FEC ve 2 CRC olmak üzere 20 bayttan oluşmaktadır. Bu çerçevelerden oluşan ve Mesaj Başlangıcı (SOM) ile başlayıp Mesaj Sonu (EOM) ile sonlanan her çerçeve grubu en az bir en çok 127 adet çerçeveden oluşmaktadır.

EOM alındığında öncelikle son alınan çerçevenin ESCAPE veya REPORT olup olmadığına bakılır, eğer değilse o ana kadar alınmış çerçeveler için rapor hazırlanır ve gönderilir. ESCAPE mesajı band genişliği kullanımı, REPORT mesajı ise gelen çerçevelerin hata oran onayları ile ilgili kavramlardır.

Benzer şekilde FNBDT 210 sinyalleşmesinde karşılaşılabilecek mesaj türlerinden diğer bir tanesi RESET mesajıdır ki bu mesaj gerekli durumlarda iletim katmanını yeniden senkron hale getirmek için kullanılır. RESET mesajı çerçeve numaralarını sıfırlar ve bir SOM ve EOM arasında yalnızca bir RESET mesajı gönderilir.

FNBDT 210 sinyalleşmesinde, bağlantı kurma sinyalleşmesinin ilk adımı olarak terminaller birbirlerine Yetenekler Mesajını (Capabilities Message) göndermektedirler. Bu mesaj sayesinde terminaller birbirleriyle uyumlu olarak ne şekilde çalışabileceklerini (açık veya kapalı modlar) belirli bir esasa bağlamakta ve güvenli modda haberleşilecek ise uygun anahtar listesinin seçilmesi de bu sayede mümkün olmaktadır. Yetenekler Mesajı gönderildiği anda ilk mesaj zamanlayıcısı başlamakta, bu zamanlayıcı karşı taraftan FNBDT 210 uyumlu mesaj gelmemesi halinde bağlantının zaman aşımına uğramasını temin etmektedir. Zaman aşımı sonunda Boş Bağlantı haline dönlür.

İlk mesajlaşma sonunda eğer güvenli haberleşme kararı verildiyse FNBDT 210 bağlantısı kurulabilmesi maksadıyla trafik anahtarını oluşturabilmek için karşılıklı sertifikaların ve F(R)’ların değiş tokuş yapılması gerekmektedir. Bunlardan

sertifikanın gönderilmesi Parametre/Sertifika mesajı ile olur.

F(R) mesajı anahtar takımı ile ilgili bir takım bilgiler (anahtarın tip, uzunluğu vb.), F(R) uzunluğu ve F(R)’ın kendisini kapsayan bir mesajdır. F(R) mesajı iletilmeden önce mutlaka parametre/sertifika mesajı iletilmiş olmalıdır.

FNBDT 210 bağlantısı kurmada diğer bir adım kriptosenkronizasyon mesajlarının değişimidir. Değişimi yapılan sertifika ve F(R) bilgileri ile trafik anahtarı oluşturulmakta, bu anahtar ile test paketi şifrlenip Kripto Senkronizasyon Mesajı haline getirilmektedir.

Bağlantı kurma sinyalleşmesinden sonra kurulan bağlantının değişikliklere tabi tutulmasıyla ilgili bir takım sinyalleşme tanımları mevcuttur. Bağlantı kontrol sinyalleşmesinin amacı; herhangi bir sebeple bağlantıyı sonlandırmak, mevcut uygulamayı değiştirmek, diğer terminali ikaz etmek ve/veya kriptosenkronizasyonunu baştan sağlamak olabilir. Bağlantı kontrol sinyalleşmesinde dört farklı mesaj vardır. Bunlar İhbar (Notification), Mod Değişim İsteği (Mode Change Request), Mod Değişim Yanıtı (Mode Change Response) ve Kripto Senkronizasyon (CryptoSync) olabilir.

Mod değiştirme işlemi; talep ve buna verilen yanıt şeklinde iki türdür ve sadece her iki terminal de güvenli uygulama trafiğinde iken mümkün olabilir.

Güvenli Ses için beş farklı çağrı mevcuttur. Bunlar [2];

- Güvenli 2,4 kbps MELP kodlu Ses – Blank & Burst (DTX),
- Güvenli 2,4 kbps MELP kodlu Ses – Blank & Burst (FCT),
- Güvenli MELP kodlu Ses –Burst w/o Blank (DTX),
- Güvenli MELP kodlu Ses –Burst w/o Blank (FCT),
- Güvenli, Gelişmiş Çoklu-Band Uyarımı (AMBE).

FNBDT 210’da Blank & Burst uygulamalı MELP ve Burst w/o Blank olmak üzere iki tip güvenli ses çağrısı yapılabilmektedir.

FNBDT 210 uyumlu bir terminalde, kriptosenkronizasyonunun sürekliliği için belirli periyotlarla terminal tarafından 2,4 kbps’de üretilen MELP kodlu ses bilgisinin üzerine kriptosenkronizasyon bilgisi yazılır. Bu işleme “B&B” (Blank and Burst) protokolü denilmekte ve bu uygulamada zaman zaman ses bilgisi silinerek yerine kriptosenkronizasyon bilgisi yazılmasından dolayı ses kalitesinde ufak çapta düşüşler yaşanmaktadır.

Blank & Burst çerçeve grubu 24 çerçeveden oluşmasına karşın, Burst w/o Blank uygulaması 25 çerçeveden oluşmaktadır. Dolayısıyla Burst w/o Blank uygulaması için gerekli kanal kapasitesi 2,4 kbps’den fazla (overhead) olmaktadır. Aynı zamanda, MELP kodlanmış ses bilgilerinin üzerine kriptosenkronizasyon bilgisi yazılmadığı için ses kalitesi B&B’ye göre daha iyidir.

Açık MELP ses çağrı hizmeti görüşmesinde de ortaya çıkan yapı tıpkı B&B’de olduğu gibidir. Mesaj yine, biri SM çerçevesi olmak üzere toplam 24 çerçeveden oluşan çerçeve gruplarıyla yapılır. Ancak burada kriptolama yapılmadığından SM çerçevesinin başlık kısmından sonrası sıfır ile doldurularak mesaj gönderilir.

Ayrıca ister güvenli isterse açık olarak görüşen tüm FNBDT

210 uyumlu terminallerin DTX ve FCT durumları desteklemesi beklenmektedir. Bunlardan DTX; bir ses çağrısı sırasında, terminalin kullanıcısı konuştuğu sürece çerçeve gruplarının oluşturularak gönderilmesi, kullanıcı sustuğunda ise gönderme yapmanın kesilmesi prensibini; FCT ise; ses çağrısı sırasında terminalin kullanıcısının sustuğu sürede de çerçeve gruplarının oluşturularak karşı terminale iletilmesi yani MELP kodlayıcı biriminin sürekli çalışmasını ifade etmektedir.

FNBDT 210, veri haberleşmesinde ise iki veri hizmetini desteklemektedir. Bunlar “Güvenli Aktarım (Reliable Transport-RT) Asenkron Veri Hizmeti” ve “Garanti İş (Guaranteed Throughput-GT) Asenkron Veri Hizmetleridir. RT Asenkron Veri hizmetinde, güvenli ses hizmetinde kullanılan sinyalizasyon mekanizmalarının aynısını kullanarak veri çağrısı başlatılır ve kanal kapasitesi %70 verimlilikle kullanılır. GT Asenkron Veri hizmeti ise kanal kapasitesinin tamamının kullanıldığı bir servistir [3, 4].

III. UYGULAMADA GEÇEN KAVRAM VE TANIMLAR

FNBDT 210 Simulâtör: Laboratuvar ortamlarında cihazların karşılıklı çalışabilirliğini değişik senaryolar ve durumlar dahilinde test eden ve bizim tarafımızdan yazılan bir uygulamadır.

FNBDT 210 Tester: FNBDT 210 Simulâtör Yazılımının bir parçası olarak olup ve yazılımı bizim tarafımızdan yapılan, terminaller arası FNBDT 210 haberleşmesinin takip ve kontrol edilmesi maksadıyla kullanılmaktadır. Modülün içerisinde sürece etki edilebilmesini (bozma, karıştırma, geciktirme vb.) sağlayan fonksiyonlar mevcuttur.

Bit Hata Oranı (Bit Error Rate-BER) : Belli bir zaman aralığında iletilen veri bitlerinden hatalı olanların, aktarılan toplam bit sayısına oranı olarak tanımlanmaktadır.

Veri Kaybı (Data Loss): Bit veya Bayt olarak hatalı aktarılan veri miktarının toplamda aktarılan veriye oranıdır. Uygulamada kanal simülâtörü tarafından yaratılan bu durumda bit kayıpları için bitler, bayt kayıpları içinse sekizli bit gruplarının rastlantısal olarak iletilmesi engellenerek veri kaybına yol açılmaktadır.

Gecikme (Delay) : Aktarılan veride yaratılan sistematik zaman kaymaları bu başlık altında tanımlanmaktadır.

IV. UYGULAMA İÇİN KURULAN AĞ

FNBDT 210 protokolünün IP ağlar üzerindeki davranışını incelemek amacıyla IP test düzeneği laboratuvarlarında gerçekleştirilmiş, gerekli parametre değişiklikleri yapılarak gerekli ölçmeler rahatlıkla yapılabilmiştir. ;

- Çağrıyı başlatan (Yazılımını kendimiz yazmış olduğumuz FNBDT 210 destekli test cihazımız),
- Haberleşme ortamını test eden (FNBDT 210 destekli yazılımını kendimiz yazmış olduğumuz test cihazımız),
- Çağrıyı cevaplayan (FNBDT 210 Terminal),

• Router-1, Router-2 ve Router-3 ile oluşturulmuş 3 adet yerel alan ağından (YAA) oluşmaktadır. Bu uygulamada FNBDT 210 Terminali olarak FNBDT 210 Simulator programımız (yazılımını kendimizin geliştirmiş olduğu program) ve Haberleşme ortamını test eden olarak FNBDT 210 Test Tool (yazılımını kendimizin geliştirmiş olduğu program) programı kullanılmıştır. FNBDT 210 Test Tool programımız sayesinde farklı senaryolara göre, Bit Hata Oranı (Bit Error Rate-BER), Veri Kaybı (Data Loss) ve Gecikme (Delay) durumları yaratılmıştır.

Uygulama esnasında ağ üzerinde FNBDT 210 uygulamasını etkileyecek yoğun bir trafik olmamıştır. Dolayısıyla uygulama esnasında ağ üzerindeki trafik etkisini en aza indirmek için Cisco'nun 3800 serisi Router'ları tercih edilmiş ve sisteme FNBDT 210 paketleri dışında hiçbir paket verilmemiştir.

V. UYGULAMA

Çalışma için ağ yapısı özel olarak tesis edilmiş ve çalıştırılmıştır. Çalışma esnasında yapılan testler; tekrarlanmak suretiyle elde edilen verilerin ve test ortamının güvenilirliği, mümkün olduğu kadar uzun tutulmak suretiyle de verilerin geçerliliği sınanmıştır.

FNBDT 210 sinyalleşmesinin kritik evrelerini teşkil etmeleri nedeniyle çalışmada daha çok FNBDT 210 sinyalleşmesinin “Çağrı Kurma” ve “Güvenli Veri Aktarımı” bölümlerindeki denemeler yoğunluk kazanmıştır. Bununla beraber “Güvenli Ses Haberleşmesi” konusunda da çalışmalar yürütülmüş ve bir takım sonuçlara ulaşılmıştır.

Genel olarak çalışma, Çağrı kurma (Call Setup), B&B Güvenli Ses, B w/o B Güvenli Ses, RT Asenkron Güvenli Veri, GT Asenkron Güvenli Veri, olmak üzere beş ana başlık ve her ana başlığın altında Bit Hata Oranı ve Veri Kayıpları durumlarının değerlendirildiği iki alt başlık altında yapılmıştır.

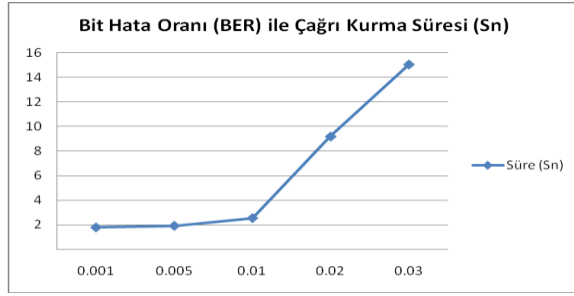
A. Çağrı Kurma Uygulamaları

1) Normal Hallerde Çağrı Kurma:

FNBDT 210 Çağrı Kurma Sinyalleşmesi'nin ilk mesajı SOM (Start of Message) ile başlamakta ve ses veya veri haberleşmesinin başlayabileceğine işaret eden START mesajı ile çağrı kurma sinyalleşmesi tamamlanmaktadır. Laboratuvar ortamında yapılan deneysel testler sonucunda çağrı kurma işleminin $1,818 \pm 0,057$ saniyelik bir zaman diliminde gerçekleştiği saptanmıştır. Bu sonuç sonraki aşamalarda alınan sonuçların değerlendirilmesinde bir kıyas noktası olacağından önemlidir.

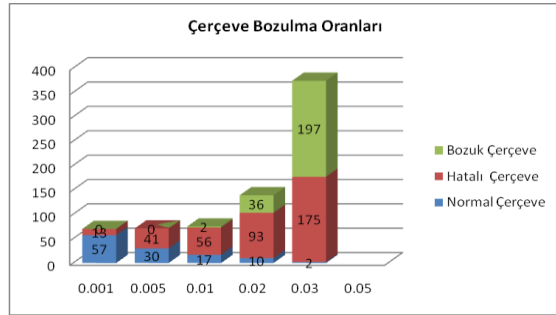
2) Bit Hata Oranı (BER) ile Çağrı Kurma

Bu denemeler esnasında Haberleşme ortamını test eden FNBDT 210 Test Cihazı tarafından iletişim kanalına belirli oranlarda bit hataları verilerek sonuçları gözlenmiştir. Küçük bit hata oranlarından başlanarak hata oranları gittikçe artırılmış ve 0.03 lük Bit Hata Oranına kadar FNBDT 210 bağlantı kurma işleminin mümkün olabileceği tesbit edilmiştir.



Şekil 2. Bağlantı Kurma (BER) Zaman Grafiği

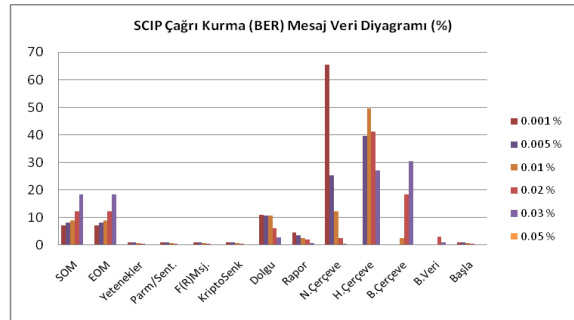
Şekil 2'deki grafikte görüldüğü gibi, Bit Hata Oranı arttırıldıkça, Çağrı Kurma Süresinin de arttığı tespit edilmiştir. Çağrı Kurma süresi, özellikle 0.01 Bit Hata Oranından sonra daha büyük artışlar göstermiştir.



Şekil 3. Çerçeve Bozulma Oranları

Şekil 3'de, Bit Hata Oranının çerçevelere etkisi görülmektedir. Bit Hata Oranı arttıkça, çerçevelerin neredeyse tamamının Hatalı ve Bozuk Çerçeve olarak iletildiği, toplam çerçeve sayısında ciddi artış saptandığı ve rapor mesajlarının eksik olarak iletildiği gözlenmiştir. 0.03 Bit Hata Oranında, tüm çerçevenin bozuk ve hatalı olduğu, çerçeve sayısında ise 0.02 Bit Hata Oranına göre iki kattan fazla artış olduğu tespit edilmiştir.

Burada Hatalı Çerçeve, FEC ve CRC hata düzeltme algoritmalarıyla düzeltilmesi mümkün olan veri çerçevelerini, Bozuk Çerçeve ise, düzeltilmesi mümkün olmayan veri çerçevelerini ifade etmektedir.



Şekil 4: FNBDT 210 Çağrı Kurma (BER) Mesaj Veri Diyagramı (%)

Şekil 4, FNBDT 210 Çağrı Kurma esnasındaki verilerin % olarak değişimini göstermektedir. Şekilde görüldüğü gibi Bit Hata Oranı arttıkça Normal çerçeve sayısı ve yüzdesinin

azaldığını, diğer taraftan SOM, EOM, Hatalı ve Bozuk çerçeve miktarlarında artma olduğu tespit edilmiştir.

2) Veri Kaybı Durumlarında Çağrı Kurma

A) Eksik Bit Oranı (Drop Bit Rate)

Çalışmanın bu kısmında mesaj iletimi, FNBDT 210 Test Cihazı tarafından bit bazında veri kaybına uğratarak sonuçları değerlendirilmiştir. Çizelge-1'de değişik Eksik Bit Oranları için mesaj miktarları ve bağlantı kurma süreleri verilmektedir.

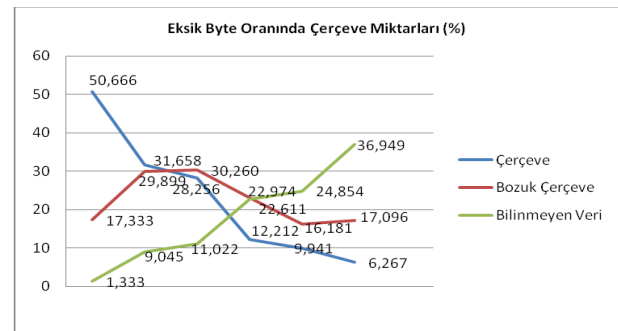
Çizelge 1. Eksik Bit Oranı Mesaj Verileri

Eksik Bit Oranı	0.001	0.005	0.01	0.02
SOM	60	287	434	999
EOM	60	287	434	999
Hatalı Çerçeve	18	99	161	208
Çerçeve	127	169	98	66
Bozuk Çerçeve	122	370	572	1101
Yetenekler Msj.	1	1	1	1
Parm./Sert. Msj.	1	1	1	0
Rapor	4	3	4	3
F(R) Msj.	1	1	1	0
Kripto Senk.	1	1	1	0
Dolgu	12	11	11	11
BAŞLA	1	1	1	1
Bilinmeyen Veri	7	91	177	564
Topl. Mesaj	404	1331	1919	4022
Bağ Sür (sn)	12,078	37,453	67,453	125,860

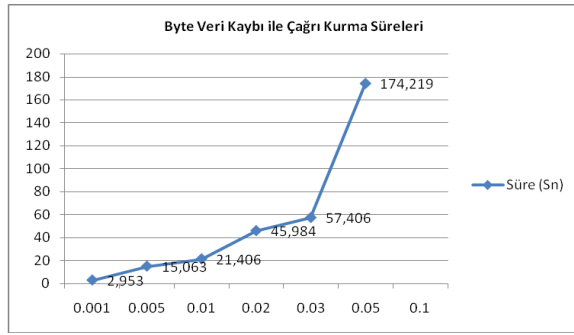
Çizelge 1'de de görüldüğü gibi FNBDT 210 bağlantı kurulması esnasında bit bazında veri kaybına uğratıldığında ciddi sorunlarla karşı karşıya kalınmış ve 0.03 Bit veri kaybında bile çağrı kurulması mümkün olmamıştır.

B) Eksik Bayt Oranı (Drop Byte Rate)

Eksik Bit Oranı test sonuçlarının aksine bu kısımda yapılan denemelerde, veri iletimi esnasında Bayt tabanlı kayıpların yüksek kayıp oranlarına çıkılana kadar büyük problemlere yol açmadığı görülmüştür. Sadece dikkate değer değişiklik gösteren mesajların yer aldığı Şekil 5'de, Hatasız Çerçevelerin Eksik Bayt Oranları arttıkça azaldığı, buna karşın özellikle Bilinmeyen Verilerin ters orantılı olarak arttığı tespit edilmiştir.



Şekil 5. Veri Kaybı Eksik Bayt Oranında Çerçeve Miktarları



Şekil 6. Çağrı kurma Süreleri, Bayt Veri Kaybı

0,05'lik bayt veri kaybının olduğu nokta FNBDT 210 çağrısının son olarak kurulabildiği değer olarak tespit edilmiştir. Bu noktada, Şekil 6'da görüldüğü gibi çağrı kurma süresi 174 saniyeye çıkarken iletilen verilerin %36,949 (Şekil 7) sistem tarafından Bilinmeyen Veri olarak algılanmıştır.

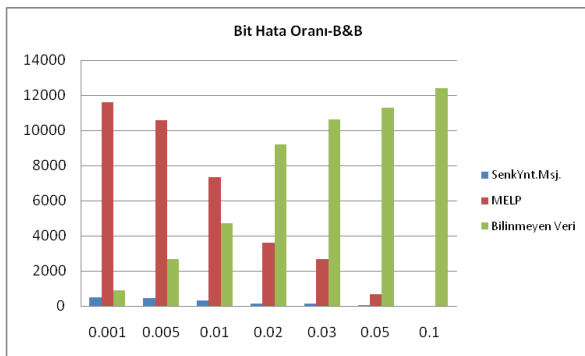
B. Blank&Burst Güvenli Ses Haberleşmesi Uygulamaları

Bu bölümdeki güvenli ses haberleşmesi FCT (Force Continuous Transmission) olarak gerçekleştirilmiştir. Güvenli ses haberleşmesinde de FNBDT 210 Test Cihazının yetenekleri çerçevesinde ölçüm ve denemeler yapılmıştır.

1) Bit Hata Oranı Etkileri

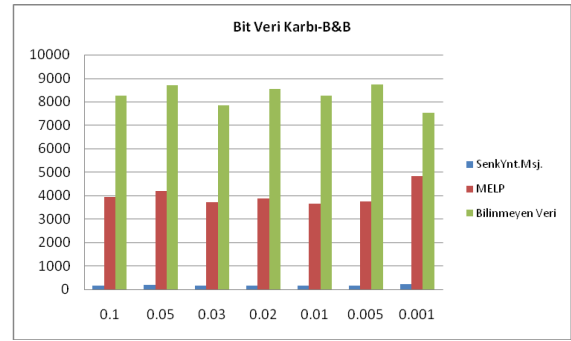
Bu kısımda, FNBDT 210 çağrısı kurulduktan sonra sisteme belirli bit hata oranları sırasıyla verilerek B&B FCT ses haberleşmesi üzerine yarattığı etkiler gözlenmiştir.

Şekil 7'da açıkça görüldüğü gibi, Bit Hata Oranı arttıkça, Bilinmeyen Verinin artmasına karşılık MELP ve Senk.Ynt.Mesajı azalmaktadır. Hatta Bit Hata Oranı 0.1 olduğunda hemen hemen tüm verilerin bilinmeyen olduğu tespit edilmiştir.



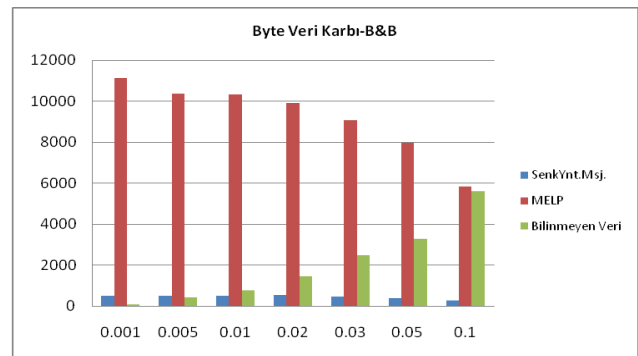
Şekil 7. B&B Ses Görüşmesinde Bit Hata Oranı

2) Veri Kaybı



Şekil 8. B&B Güvenli Ses Görüşmesi ve Bit Veri Kaybı

Şekil 8'de görüldüğü gibi Bit Veri Kaybının Ses görüşmesini etkilemediği, hata oran ne olursa olsun görüşmenin devam ettiği tespit edilmiştir.



Şekil 9. B&B Güvenli Ses Görüşmesi ve Bayt Veri Kaybı

Şekil 9'da sistem tarafından bayt veri kayıplarına verilen tepkiler görülmektedir. Bayt veri kayıplarında kritik eşik 0,1 ve üzeri orandaki kayıplar olarak tespit edilmiştir.

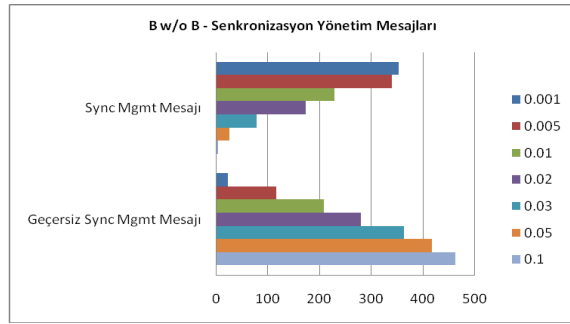
C. Burst w/o Blank (FCT) Güvenli Ses Haberleşmesi Uygulamaları

Bilindiği üzere B w/o B modunda MELP kodlu güvenli ses iletimi 24'lü MELP çerçeve grubuna ek 25'nci bir çerçeve olarak katılmaktadır. Bu sayede MELP çerçevelerinden biri eksilmediği için daha iyi ses kalitesine ulaşılabilirken, diğer yandan iletim hattında yarattığı ilave yük (overhead) ile daha yüksek band genişliklerine ihtiyaç duyulmasına sebep olmaktadır.

Denemelerin bu bölümünde B w/o B ses iletiminin karakteri gereği bir avantajlı tarafı daha ortaya çıkmaktadır. Bu avantaj, veri kaybı ve hatalı veri durumlarında sistemin direnç göstermesi, ses kalitesini oldukça muhafaza etmesidir.

1) Bit Hata Oranı Etkileri

Şekil 10'da görüldüğü üzere, Bit Hata Oranı arttıkça, Geçersiz Senkronizasyon Yönetim mesajlarının arttığı, Geçerli Senkronizasyon Yönetim mesajlarının ise azaldığı tespit edilmiştir.



Şekil 10. B w/o B - Senkronizasyon Yönetim Mesajları

2) Veri Kaybı

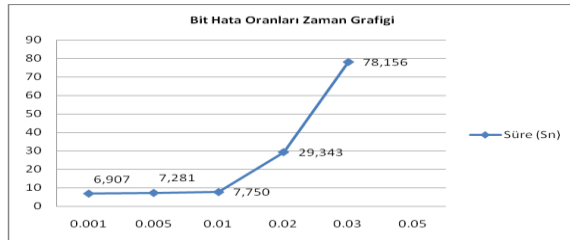
Byte veri kaybı testlerinde; Byte Veri Kaybı arttırıldıkça Geçersiz Senkronizasyon Yönetim Mesajlarının arttığı ve Senkronizasyon Yönetim Mesajlarının ise azaldığı tespit edilmiştir.

Bit veri kaybı testlerinde; Bit Veri Kaybı arttırılmasına rağmen Geçersiz Senkronizasyon Yönetim Mesajlarının ve Senkronizasyon Yönetim Mesajlarının sayısında ciddi bir değişiklik olmadığı tespit edilmiştir.

Ç. RT Asenkron Güvenli Veri Haberleşmesi

Bu tip güvenli veri iletiminde FNBDT 210 mesaj iletim mekanizması kullanılması dolayısıyla verilerin güvenli (Reliable) bir şekilde uzak uca ulaştırılması sağlanmış olur. Ayrıca bu iletim şeklinde Kripto Senkronizasyonu kayıpları olmadığından Senkronizasyon Yönetim Mesajı işlevleri görülmemektedir.

1) Bit Hata Oranı Etkileri



Şekil 11. Bit Hata Oranları Zaman Grafiği

RT Asenkron Güvenli Veri Haberleşmesinde veri aktarma sürelerinin Bit Hata Oranlarındaki değişimi Şekil 11'de grafik olarak verilmiştir. Görüldüğü gibi zaman ekseninde ilk büyük sıracama 0,01 bit hata oranında gerçekleşmiştir. Bununla beraber, 0,03 Bit Hata Oranının, RT Asenkron Güvenli Veri Aktarımı için son nokta olduğu tespit edilmiştir.

2) Veri Kayıpları

RT Asenkron Güvenli Veri Haberleşmesinde veri aktarımının Bit Veri Kaybına karşı çok hassas olduğu tespit edilmiştir.

A) Eksik Bit Oranı Veri Kayıpları

0,001'lik bit kayıp oranında bile veri aktarım süresinin fazla

olduğu tespit edilmiş olup bu bölümdeki çalışmalar 0,01'lik Bit Veri Kaybına kadar yapılabilmektedir.

B) Eksik Bayt Oranlı Veri Kayıpları

Çizelge 2'de, RT Asenkron Güvenli Veri Haberleşmesinde Byte Veri Kaybı Etkileri ayrıntılı olarak verilmiştir. Verilen sonuçlardan anlaşılabileceği üzere 0,02 Eksik Bayt Oranının aşıldığı noktadan sonra veri aktarımı mümkün olmamıştır. (*) işaretli sütunlar hata düzeltme mekanizmalarıyla düzeltilen mesajları temsil etmektedir.

Çizelge 2. Bayt Veri Kaybı Etkileri

Eksik Bit Oranı	0,001	0,005	0,01	0,02
SOM	203	787	1113	3474
SOM*	1	7	28	160
Çerçeve	1559	2421	2224	3705
Bozuk Çerçeve	423	1502	1953	4336
EOM	206	787	1113	3474
EOM*	1	7	28	160
Bilinmeyen Veri	43	460	820	4082
Süre (sn.)	30,438	72,765	95,296	258,25

D. GT Asenkron Güvenli Veri Haberleşmesi

GT Asenkron veri haberleşmesi ile her ne şartta olursa olsun asgari 2,4 kb/s veri aktarım hızı garanti edildiğinden önceki kısma göre verilerin daha çabuk uç terminale ulaşması beklenmelidir. Diğer bir konu ise bu yapıda da Senkronizasyon Yönetim Mesajları kullanılmaktadır. Fakat ses mesajlarında olduğu gibi aradan bir mesajın gözden çıkartılması mümkün değildir, dolayısıyla GT Asenkron veri haberleşmesi her zaman B w/o B şeklinde ve tam bant olmaktadır.

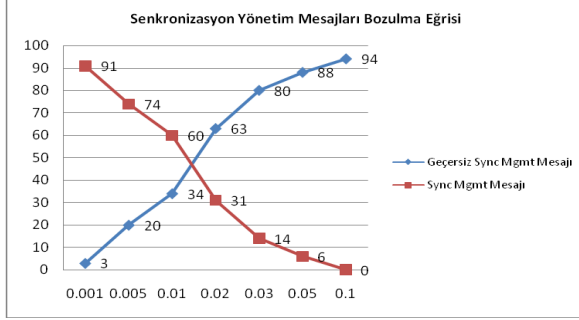
Çizelge 3'de de görüldüğü gibi, gerçekten de normal şartlarda yapılan denemelerden elde edilen sonuçlar aynı büyüklükteki verinin aktarım süresinin daha kısa olduğunu göstermektedir. RT Asenkron veri Aktarımında 6,698 sn. olan iletim süresi GT Asenkron veri Aktarımında 2,310 saniye olarak tespit edilmiştir.

Çizelge 3: Veri Aktarım Sürelerinin Karşılaştırması

Bit Hata Oranı (%)	Süre (Sn)	
	GT	RT
0.001	3,900	6,907
0.005	3,954	7,281
0.01	4,070	7,750
0.02	3,793	29,343
0.03	3,867	78,156

0.05	4,026	Başarısız
0.1	4,800	Başarısız

Şekil 12’de görüldüğü gibi, Bit Hata Oranları Geçersiz Senkronizasyon Yönetim Mesaj oranlarıyla doğru, Senkronizasyon Yönetim Mesaj oranlarıyla ise ters orantılı olarak artışı tespit edilmiştir.



Şekil 12. Bit Hata Senkronizasyon Yönetim Mesajları Bozulma Eğrisi

GT Asenkron Veri Haberleşmesinde Bit Hata Oranı üst değeri 0,02 olarak tespit edilmiştir. Veri kayıplarına gelindiğindeyse en küçük miktardaki veri kayıplarında bile bu aktarım modunda veri haberleşmesi yapmanın mümkün olmadığı, Bayt Veri kayıplarında 0,1’lik hata oranlarına kadar sistemin tahammül edebildiği görülmüştür.

VI. SONUÇLAR

Bu çalışmada, farklı haberleşme ağları üzerinde uçtan uca emniyetli haberleşmenin yapılması amacıyla geliştirilen FNBDT 210 protokolü, simülörümüz vasıtasıyla IP ağ üzerinde değişik açılardan test edilmiştir.

İcra edilen uygulama çalışması neticesinde değişik durum senaryoları için bir takım sınır değerlere ulaşılmıştır. Bu değerlerin ve sonuçların sonraki benzer nitelikteki çalışmalara, ışık tutacaktır.

Bu çalışma sonunda tespit edilen genel sonuçlar, olabilecek çözümler ve gelecekte yapılabilecek testler şu şekildedir:

- BER arttıkça çağrı kurma süresi artmakta ve normal çerçeve sayısı azalmaktadır. Normal çerçevelerin yerini hatalı ve bozuk çerçeveler almaktadır ve çerçeve miktarının genelinde bir artış olmaktadır. Çerçeve miktarının genelindeki artış SOM ve EOM mesajlarının artmasına neden olmaktadır. Bu yüzden de çağrı kurulum süresi artmaktadır. BER’in artırılmasına rağmen toplam çerçeve sayısı sabit tutulabilirse SOM ve EOM paketlerinin sayısı sabit tutulmuş olunur ve çağrı kurulum süresi belli bir BER değerine kadar artmaz sabit kalır. 0.03’lük BER değerinden sonra ise çağrı kurulamaz.

Çalışma, özellikleri ve içeriği bakımından konuyla ilgili yapılan ilk çalışma olması ve elde edilen test verilerinin müteakip çalışmalara girdi oluşturma olanakları sunması nedeniyle önem arz etmektedir.

KAYNAKLAR

- [1] Edward J. Daniel, Keith A. Teague, Robert Sleezer, Jerry Brewer, Josh raymond, William J. Beck, Joe Hershberger, "The Future Narrowband Digital Terminal," IEEE Magazine, pp. II-589-591, Stillwater, OK, 2002.
- [2] E. J. Daniel, K. A. Teague, "Performance of FNBDT and Low Rate Voice (MELP) Over Packet Networks," Proc.35th Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, California, Nov.4-7, 2001.
- [3] BOZOKLU, Oğuz. "Uyumlu ve Birlikte Çalışabilir Güvenli Muhabere Kapsamında NATO/FNBDT 210 Bünyesindeki Kripto Standartlarına Türkiye'nin Yaklaşımı" (Yüksek Lisans Tezi), Ankara, Kara Harp Okulu Savunma Bilimleri Enstitüsü, Haziran 2007.
- [4] ÖREN, Özgür. "Geleceğin Darband Sayısal Terminali" (Yüksek Lisans Tezi), Adapazarı, Sakarya Üniversitesi FEN Bilimleri ENSTİTÜSÜ, Haziran 2005.

Orkun DİLLİ (M’71) Elektrik-Elektronik Mühendisliği Bölümünden 1992 yılında mezun oldu, Yüksek Lisansını 2004 yılında tamamladı. 2005 yılında Gazi Üniversitesi Mühendislik Fakültesi, Elektrik-Elektronik Ana Bilim Dalında başladığı Doktora Eğitimine devam etmektedir. ISDN ve Uçtan Uca Güvenli Haberleşme konusunda araştırmaları bulunmaktadır.

Mesleğine bir Kamu Kuruluşunda, 1994 yılında, Ankara’da başladı. Önce ISDN konusunda ve daha sonraları, Gelecek Nesil Uçtan Uca Güvenli Haberleşme Cihazları konusunda yapmış olduğu araştırmalarını bildiri haline getirerek çeşitli ulusal ve uluslar arası katılımlı sempozyumlarda sundu.

Ülke Bilgi Güvenliği

Yılmaz VURAL, Şeref SAĞIROĞLU

Özet— Kişisel ve kurumsal düzeyde stratejik bilgileri içeren ülke bilgi sistemleri, güvenlik tehditlerine karşı korunmalıdır. Ülke bilgi sistemlerimizde bilgilerin üretilmesi, işlenmesi, iletilmesi, depolanması ve paylaşılmasına bağlı olarak oluşabilecek güvenlik ihlallerini en aza indirmek için kişisel ve kurumsal seviyede alınması gereken güvenlik önlemleri her geçen gün artmaktadır. Bu çalışmada, ülke bilgi güvenliğinin yüksek seviyede sağlanması için kurumsal ve kişisel bilgi güvenliğinin önemi, en zayıf halka olan insan faktörünün iyileştirilmesi için eğitimin önemi ve güvenlik süreçlerinin iyileştirilmesini sağlayan güvenlik testleri incelenmiştir. Son olarak ülke bilgi güvenliği hakkında genel değerlendirmeler yapılarak öneriler yapılmıştır.

Anahtar— Bilgi güvenliği, kişisel bilgi güvenliği, kurumsal bilgi güvenliği, güvenlik testleri, ülke bilgi güvenliği

Summary— National Information Systems that consist of strategic information at personal and enterprise level must be protected against threats. Personal and enterprise level security precautions are increasing day by day in order to decrease probable security threats that occur as a result of information being produced, processed, transferred, stored and shared on national information systems. In this paper, importance of personal and enterprise information security in order to provide national information security, importance of information security education and awareness in order to improve human factor which is the weakest link of security life cycle and security tests supplying improvements of security processes have been examined. Finally some evaluations about national information security have been performed.

Keywords— Information security, enterprise information security, personal security, security testing, national information security

I. Giriş

Bilgi sistemlerinin kurumsal veya kişisel düzeyde kullanımının yaygınlaşması sonucunda hayatımız kolaylaşırken güvenliği yüksek seviyede sağlanan bilgi sistemlerine duyulan ihtiyaçlar da aynı oranda artmaktadır [1]. Ağ destekli bilgi sistemleri üzerinden haberleşen, sayıları hızla artan ve geniş kitlelerce ülke çapında kullanılan uygulamalar üzerinde tutulan bilgilerin değeri düşünüldüğünde bilgi güvenliğinin sağlanmasının önemi daha iyi anlaşılacaktır.

Ş. SAĞIROĞLU, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Ankara, ss@gazi.edu.tr

Y. VURAL, STM A.Ş., Ankara, yvural@stm.com.tr

Ayrıca geliştirilen yeni uygulamaların da beraberinde yeni güvenlik tehditlerini getirdiği düşünüldüğünde bilgi güvenliğinin sağlanmasının her geçen gün daha da zorlaştığı anlaşılabacaktır.

Kamu veya özel kuruluşlara ait ağ destekli bilgi sistemlerinin birbirleriyle etkileşimi her geçen gün artmakta ve bu sistemler ülke bilgi sistemlerinin altyapısını oluşturmaktadır. Ülke bilgi sistemleri ülke güvenliği açısından önemli olan stratejik ülke bilgilerinin, ilgili kurumların kendi içinde veya başka kurumlar arasında paylaşılmasını ve kullanılmasını sağladığından ülke bilgi sistemlerinin güvenliğinin yüksek seviyede sağlanması ülke güvenliği açısından önemlidir.

Kişilerin ve kurumların sahip oldukları önemli bilgilerin yer aldığı ülke bilgi sistemleri istihbarat veya terör amaçlı yapılabilecek siber saldırılara karşı yüksek seviyede korunması gerekmektedir. Ülke bilgi güvenliğini tehdit eden unsurlar sadece elektronik ortamlarda yapılan saldırılarla sınırlı değildir. İnsan hataları, yangın, sel, deprem, terör saldırıları, sabotaj gibi istenmeyen olaylar veya doğal felaketler sonucunda da bilgiler ve bilgi sistemleri tamamen ya da kısmen zarar görmektedir. Ayrıca korunmasızlığın yanında korunma seviyesinin iyi belirlenememesi ve etkin güvenlik önlemlerinin alınamaması da beraberinde maliyet, performans ve verimsizlik gibi önemli diğer sorunlara yol açmaktadır.

Günümüzde elektronik ortamlarda meydana gelen güvenlik ihlallerinden hemen hemen her gün bahsedilmektedir. Bu ihاللerden bir tanesi olan ve ülke bilgi güvenliği açısından önemli bir örnek olan “Estonyanın ülke bilgi sistemlerine karşı yapılan dağıtık temelli hizmet aksattırma saldırıları” sonucunda 1,3 milyonluk nüfusa sahip Estonya’daki kamu, banka ve medya internet siteleri, Rusya kaynaklı yüz binlerce bilgisayardan yapılan geniş kapsamlı, eşgüdümlü ve uzun süreli saldırılar sonucu çöktürülmüş ve Estonyada hayat durma noktasına gelmiştir [2]. Bu saldırı devletler arasında yaşanan ilk siber soğuk savaş olarak tarihe geçmiştir.

İnternet güvenlik şirketi McAfee firmasının 2007 yılı sonunda hazırladığı raporda gelecek on yılda dünyada güvenliğe ilişkin en büyük tehditlerden birinin, ülkeler arasında bilgi sistemleri üzerinde yaşanacak siber soğuk savaşların olduğu belirtilmiştir. Raporda yaklaşık 120 ülkenin, mali piyasalar, resmi bilgisayarlar sistemleri ve kamu hizmetleri alanında interneti kullanmak için çözümler geliştirdiğini ve istihbarat örgütlerinin diğer devletlerin ülke bilgi sistemlerini sürekli sınyarak zayıf noktalarını bulmak için yeni teknikler geliştirildiği vurgulanmıştır [3].

Bu ve benzeri siber tehditlerden ülke düzeyinde etkilenmeyi

en aza indirmek için kurumsal ve kişisel düzeyde alınması gereken önemli güvenlik tedbirleri vardır. Ülke bilgi güvenliğinin aşamalarını oluşturan kurumsal ve kişisel bilgi güvenliğinin yüksek düzeyde sağlanması, ülke bilgi güvenliği politikalarının oluşturulması, yapılması gerekenler arasında ilk sırada gelmektedir. Kullanıcıların kişisel bilgi güvenliği konusunda bilinçli olmaları gerekirken, kurumların kurumsal bilgi güvenliği konusunda önlemler almaları ise yapılması gereken önemli görevler arasındadır [4].

Bu çalışmada takip eden bölümlerde stratejik ülke bilgilerinin yer aldığı ülke bilgi sistemleri açıklanmış, ülke bilgi sistemlerinin güvenliğinin sağlanmasında önemli aşamalar olan kişisel ve kurumsal bilgi güvenliği konuları ayrı başlıklar altında ele alınmış ve takip eden bölümlerde güvenlik testleri ve eğitimin önemi üzerinde durulmuştur. Son olarak ülke bilgi güvenliği konusunda değerlendirmeler yapılmış ve öneriler sunulmuştur.

II. ÜLKE BİLGİ SİSTEMLERİ

Bilgi genellikle, bireyler veya kurumlar tarafından bir sorunun çözümü, herhangi bir çalışmanın başlatılması ya da bitirilmesi gibi faaliyetler sonucunda ortaya çıkarılan anlamlandırılmış verilerin bütünüdür ifade etmektedir. Bilgi kelimesinin menşei, Latince'deki herhangi bir şeye şekil vermek anlamına gelen "informare" kelimesinden gelmektedir [5]. Sözlük anlamıyla bilgi; "Öğrenme, araştırma ve gözlem yoluyla elde edilen her türlü gerçek, malumat ve kavrayışın tümü" olarak tanımlanmaktadır [6]. Bilgi sistemleri donanımlar, yazılımlar, iletişim teknolojileri ve insan gibi alt bileşenlerden meydana gelmektedir. Bilgiler, bilgi sistemleri aracılığıyla üretilmeye, işlenmeye, taşınmaya ve depolanmaya başladıkça güvenlik tehditleri ve alınması gereken önlemler ise artarak farklılık göstermeye başlamıştır.

Ülke bilgi sistemleri bireylerden kurumlara kadar değişik seviyelerde ağ destekli ortamlarda bilginin yönetilmesi, iş verimliliğin ve bilgi akışlarının hızlandırılması, bireyler ve kurumlarla daha hızlı iletişimin kurulabilmesini sağlayan ulusal ve uluslararası kullanımı olan sistemlerdir [7]. Ülke Bilgi Sistemleri sayesinde ağ destekli ortamlarda bilginin üretilmesi, işlenmesi, taşınması ve saklanması sağlanarak bilgiye mekândan bağımsız olarak istenilen ortamlardan erişilmesi ve paylaşılması sağlanmıştır. Nüfus Vatandaşlık İdaresi MERNİS, Maliye İnternet Vergi Dairesi, Sosyal Güvenlik Kurumu Bilgi Sistemi, Meteoroloji Bilgi Servisleri, Coğrafi Bilgi Sistemleri ve Banka Bilgi Sistemleri ülke bilgi sistemlerimize ilk bakışta örnek olarak gösterilebilir.

Ülke bilgi sistemlerimizin birlikte çalışabileceği Ulusal Bilgi Sistemi ile ilgili çalışmalara ülkemizde devam edilmektedir. Ulusal Bilgi Sistemi ülke yönetimine yönelik stratejik bilgilerin ilgili kurumlar arasında ilişkilendirilmesi, paylaşılması ve yönetilmesini amaçlayan ülke bilgi sistemleri topluluğudur [8]. Ulusal Bilgi Sisteminin kurulmasıyla birlikte kurumsal bilgi sistemleri sistemlerin sistemi yaklaşımıyla ağ

destekli bir ortamda birlikte çalışabilirlik kabiliyeti kazanacaktır.

Sistemlerin sistemi, birbirinden farklı sistemlerin tek başlarına gerçekleştiremeyecekleri işlevleri yapabilmek için ağ destekli ortamları kullanarak birbirleriyle uyumlu ve etkin şekilde çalışabilmesiyle oluşan sistemler kümesi olarak tanımlanmaktadır [9]. Sistemlerin sistemine verilebilecek en güzel örnek İnternet'dir. İnternet yıllar içinde gelişmiş, yaygınlaşmış ve günümüzde dünyaya yayılmış bir bilgi sistemleri topluluğu haline gelmiştir.

Ulusal bilgi sisteminin bu yaklaşım çerçevesinde oluşturulması sonucunda kazanılacak bir çok olumlu kabiliyetin yanında güvenlik, performans ve yönetim gibi temel sorunlarında dikkate alınması ve çözülmesi gerekmektedir. Tüm bu sorunların çözümünde ise bilgi güvencesi (information assurance) kavramı ön plana çıkmaktadır.

Bilgi güvencesi bilginin güvenliği, performansı ve yönetimi gibi temel konuların birlikte çözülmesini sağlayan çözümler kümesi olarak tanımlanmaktadır [10]. Bilgi güvencesi sayesinde ülke bilgi sistemlerinin ağ ve bilgi altyapılarının bütünleşmesi sağlanacaktır. Bilgi güvencesi kurumsal bilgi sistemlerinin birlikte çalıştığı ülke bilgi sistemlerinin tamamında sağlanmalıdır. Ülke bilgi güvenliğinin yüksek seviyede sağlanabilmesi için kurumsal bilgi güvenliğinin ülke genelinde yeterli koruma seviyesinde sağlanması önemlidir. Bundan dolayı takip eden bölümde kurumsal bilgi güvenliğinin yüksek seviyede sağlanmasına yönelik açıklamalar yapılmıştır.

III. KURUMSAL BİLGİ GÜVENLİĞİ

Kurumsal bilgi, kurum içinde üretilen veya kuruma dışarıdan gelen, o kurumla ilgili kayıtlı ya da kayıtsız her türlü bilgiyi ifade etmektedir. Kurumsal bilgi, bireysel bilgilerin toplamının yanı sıra, diğer kurumlar tarafından kolayca taklit edilemeyecek şekilde insan, teknoloji ve yönetim ilkeleri arasında üretilen bilgi kaynaklarını ifade etmektedir [11].

Bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci bilgi güvenliği olarak tanımlanmaktadır [12]. Kurumsal bilgi güvenliği ise, kurumların bilgi varlıklarının tespit edilerek zafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerinin alınması ve güvenlik süreçlerinin standartlara göre yönetilmesidir [13].

Kurumsal bilgi güvenliği, ülke bilgi güvenliğinin sağlanmasında önemli bir aşamadır. Kurumsal bilgi güvenliği sağlanmadıkça, ülke bilgi güvenliği sağlanamayacaktır. Kurumsal Bilgi güvenliğinin sağlanması, planlanması, tasarlanması, gerçekleştirilmesi, işletilmesi, izlenmesi, denetlenmesi, sürdürülmesi ve geliştirilmesi için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası

Kurumsal Bilgi Güvenliği Yönetim Sistemi (KBGYS) olarak tanımlanmaktadır [14].

Kurumlar açısından önemli bilgilerin ve bilgi sistemlerinin korunabilmesi, risklerin en aza indirilmesi ve sürekliliğinin sağlanması, KBGYS'nin kurumlarda hayata geçirilmesiyle mümkün olmaktadır. KBGYS'nin kurulmasıyla; olası risk ve tehditlerin tespit edilmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun yöntemlerin geliştirilmesi, örgütsel yapılar kurulması ve yazılım/donanım fonksiyonlarının sağlanması gibi bir dizi denetimin birbirini tamamlayacak şekilde gerçekleştirilmesi anlamına gelmektedir.

Sadece teknik önlemlerle (güvenlik duvarları, atak tespit sistemleri, antivirüs yazılımları, anticasus yazılımlar, şifreleme, vb.) kurumsal bilgi güvenliğinin sağlanması mümkün değildir. KBGYS; insanları, süreçleri ve bilgi sistemlerini içine alan ve üst yönetim tarafından desteklenen bir yönetim sistemidir. Kurumsal bilgi güvenliği insan, eğitim, teknoloji gibi birçok faktörün etki ettiği yönetilmesi zorunlu olan karmaşık süreçlerden oluşmaktadır.

Kurumsal Bilgi Güvenliği sadece teknoloji problemi olarak değil aynı zamanda insan ve yönetim problemi olarak değerlendirilmelidir [15]. Kurumlarda insan ve yönetim hatalarından kaynaklanan güvenlik ihlallerinin sebeplerine bakıldığında son kullanıcılardan üst yönetime kadar farklı kademelerde çalışan insanların ortak eksikliklerinin eğitim ve bilinçlendirme olduğu görülür. Kurumun stratejik hedeflerini belirleyen en üst seviyedeki yönetim kademelerinin kurumsal bilgi güvenliğinin sağlanması için verecekleri destek çok önemlidir. Bilgi güvenliğinin sağlanması için gerekli olan idari ve mali kararların verilebilmesi amacıyla yönetim tarafından bilgi güvenliği birimi kurulmalıdır. Bu birim tarafından güvenlikle ilgili stratejik kararlar zamanında ve doğru bir şekilde alınmalıdır. Yönetim tarafından bilgi güvenlik biriminin kurulması ve etkin bir yapıda çalışması yönetimin kurumsal bilgi güvenliğini sahlendirdiğinin ve desteklediğinin önemli bir göstergesidir.

Kurumsal bilgi güvenliğinin üst seviyede sağlanmasına yönelik süreçlerinin oluşturulması, yönetilmesi ve yapılandırılması amacıyla yapılan standartlaşma çalışmaları dünyada ve ülkemizde hızla sürmektedir. Standartlaşma konusuna öncülük eden İngiltere tarafından geliştirilen BS-7799 standardı, ISO tarafından kabul görerek önce ISO-17799 sonrasında ise ISO-27001:2005 adıyla dünya genelinde bilgi güvenliği standardı olarak kabul edilmiştir [16].

Kurumsal bilgi güvenliğinin sağlanması ülke bilgi güvenliğinin yüksek seviyede sağlanması için önemli bir aşama olmasına rağmen tek başına yeterli değildir. Ülke bilgi güvenliğinin yüksek seviyede sağlanması için ülke bilgi sistemlerini kullanan son kullanıcıların güvenliği yani kişisel bilgi güvenliği de sağlanmalıdır. Bundan dolayı takip eden bölümde kişisel bilgi güvenliğinin yüksek seviyede sağlanmasına yönelik açıklamalar yapılmıştır.

IV. İNSAN FAKTÖRÜ (KİŞİSEL BİLGİ GÜVENLİĞİ)

Çalışma kapsamında incelenen, bilgi güvenliğiyle ilgili yapılan raporlar, anketler, kitaplar ve makalelerde bilgi güvenliğinin sağlanmasındaki en zayıf halkanın insan faktörü olduğu gösterilmiştir [17-23].

İnsan faktöründen kaynaklanan zafiyetlerin saldırganlar tarafından kullanılması, teknolojik olarak tüm güvenlik tedbirlerinin alınmasına rağmen bilgi güvenliği ihlallerinin yaşanmasına neden olacaktır. Bu ihlaller ülke bilgi güvenliği açısından önemli sorunlara yol açacaktır.

Kişisel bilgi güvenliğini tehdit eden, insan faktöründen kaynaklanan hatalar ve alınması gereken önlemlerden bazıları aşağıda başlıklar halinde özetlenmiştir.

Güvenlik politikaları ihlali: Bilgi Sistemlerindeki bilgilere erişim hakkı olan her kullanıcının yöneticiler tarafından onaylanan Bilgi Güvenliği politikalarına uyması gerekmektedir. Güvenlik politikaları son kullanıcılar tarafından çoğu zaman bilerek veya bilmeyerek ihlal edilmektedir. Güvenlik politikalarının ihlal edilme sebeplerinin başlıcaları, kullanıcı alışkanlıkları, uygulanamayacak yaptırımlar, bilinçsizlik olarak tespit edilmiştir. Politika ihlallerinin önüne geçebilmek için kullanıcıların genel bilgi güvenliği konusunda eğitilmesi ve güvenlik politikalarının uygulanabilir ifadeler içermesi gerekmektedir.

Bilgi aktarımı: İnsanlar genellikle tanımadıkları kişilere sohbet esnasında birçok önemli bilgiyi farkında olmaksızın iletmektedir. Hiçbir kullanıcı ortam fark etmeksizin (e-posta, telefon, faks, yüzyüze, vb.) kimliğinden emin olmadığı kimselere hiçbir konuda bilgi vermemelidir. Örneği hiçbir teknoloji kullanılmadan bir kurum çalışanlarından alınacak bilgilerle tüm kurumsal bilgi güvenliği kontrollerinin aşılabileceği hiçbir zaman unutulmamalıdır. Başlangıçta önemsiz gibi görünen küçük bilgiler bir araya geldiğinde, içinde gizli bir bilgiyi barındıran ciddi bir güvenlik açığına dönüşebileceğine dair örnekler her geçen gün artmaktadır. Bilinmeyen kişilere bilgi aktarılması için kullanıcıların özellikle sosyal mühendislik konusunda eğitilmesi gerekmektedir.

Şifrelerin kâğıtlara yazılması: Şifreleme politikaları, kırılması güç olan şifrelerin kullanıcılar tarafından kullanılmasını ve düzenli aralıklarla bu şifreleri değiştirilmesini zorunlu kılmaktadır. Şifrelerin güçlü olması, içerdiği karakterlerin karmaşıklığıyla doğru orantılıdır. Güçlü şifrelerin kullanılmasıyla birlikte kullanıcıların bu şifreleri hatırlama problemleri ortaya çıkmaktadır. Kullanıcılar, bu durumda şifrelerini hatırlayabilmek amacıyla görebilecekleri bir yere şifrelerinin yazılı olduğu kâğıdı asmaktadır. Bu durum ilgili kullanıcı şifresinin kötü niyetli başka bir kişi tarafından okunarak kullanılmasıyla güvenlik ihlalinin oluşmasına sebep olacaktır. Bu durumların meydana gelmemesi için kullanıcılara şifre seçimi ve hatırlanmasıyla ilgili eğitimler verilmelidir.

Güvenilir olmayan yazılımların kullanımı: Güvensiz yazılımlar illegal olarak kopyalanmış veya internetteki

güvenilir olmayan sitelerden indirilmiş, lisanssız yazılımlar olup içerisinde bilgisayara zarar verebilecek virüs, truva atı, tuş kaydedici ve her türlü kötü amaçlı yazılımları barındırabilen programlardır. Güvenilir olmayan yazılımlar, ziyaret edilen web sitelerinin kayıtlarını tutarak başkalarına gönderen, istenmeyen reklâm pencerelerinin gelmesini sağlayan, bilgisayar içerisinde yer alan kişisel dosyaları başkalarına gönderebilen, bilgisayarın performansını düşüren ve internet erişimini gereksiz yere meşgul eden istenmeyen yazılımlardır. Güvenilir olmayan yazılımların kullanımı sonucunda, birçok güvenlik ihlali meydana gelmektedir. Bu tür ihlallerin önüne geçebilmek için kullanıcılara güvenilir olmayan yazılımların ne olduğu ve bu yazılımlardan nasıl korunulacağı konusunda eğitimler verilmelidir.

Bilgisayarların fiziksel güvenliğinin sağlanmaması: Genellikle kullanıcılar koruma önlemi almaksızın bilgisayarlarının başından ayrıldığında kötü niyetli insanlar bu durumu değerlendirerek bilgisayarı zararlı amaçlar için kullanmakta ve güvenlik ihlalleri meydana gelmektedir. Fiziksel güvenlik zafiyetinden faydalanarak bilgisayarı kullanan kötü niyetli kişi gizli bilgiler içeren dosyaları dışarıya e-posta aracılığıyla gönderebilir, bilgisayar üzerindeki bilgileri silebilir, değiştirebilir ve o anki kullanıcının yetkisi ölçüsünde birçok işlemi kötücül amaçlar için yapabilir. Bilgisayarların fiziksel güvenliğinin sağlanmasıyla ilgili olarak; kullanıcılar bu konuda bilinçlendirilmeli bilgisayarların başından ayrılan kullanıcıların en azından parola korumalı ekran koruyucusu kullanmaları bilgisayarlara fiziksel olarak yapılabilecek saldırıların en aza indirgenebilmesi açısından önem arz etmektedir.

Bilgisayarların yönetici hakkıyla açılması: Kullanıcılar kurum içerisinde kendilerine tahsis edilmiş olan kişisel bilgisayarlarını, herhangi bir kısıtlama almaksızın kullanmak amacıyla genellikle yönetici haklarına sahip olan hesaplarla kullanmaktadırlar. Bu durum, bilgi güvenliğinin sağlanmasında önemli ilkelerden biri olan “en az yetki” prensibinin (principle of least privilege) ihlali anlamına gelmektedir. Yönetici haklarına sahip bir hesapla bir kullanıcının bilgisayarında oturum açılması, güvenlik ihlali meydana geldiğinde bilgisayar üzerinde yönetici işlemlerini yapma yetkisine sahip olacağından güvenlik ihlalinin etkisi çok daha büyük olacaktır. Bu tür ihlallerin etkisini azaltmak için kullanıcıların ihtiyaçlarını karşılayacak kısıtlı haklara sahip olan hesaplar tanımlanmalı ve bu hesaplarla kullanıcıların oturum açmaları zorunlu hale getirilmelidir. Bu önleme ek olarak kullanıcılara yönetici haklarına sahip hesaplarla oturum açmalarının gereksizliği ve zararları anlatılarak, kısıtlı haklara sahip olan hesapları kullanmaları yönünde özendirici ve bilgilendirici eğitimler verilmelidir.

Bilinçsiz e-posta kullanımı: Kurum çalışanları tarafından kullanılan iletişim araçlarının başında e-posta gelmektedir. Günümüzde kötücül yazılımlar çoğunlukla e-postalar aracılığıyla yayıldığından, e-posta kullanımının önemi artmıştır. Bilinçsiz e-posta kullanımı sonucunda bilgi güvenliği ihlalleri meydana gelmektedir. Kullanıcıların tanımadığı kişilerden gelen şüpheli e-postaları açmaması, e-

posta eklerini virüs taramasından mutlaka geçirmesi, e-posta aracılığıyla kişisel gizli bilgilerini (internet bankacılığı hesap bilgilerini, kimlik bilgileri, kullanıcı hesap bilgileri) kimseye vermemesi gibi e-posta kullanımında dikkat edilmesi gereken hususlar konusunda kullanıcılar bilinçlendirilmeli ve eğitilmelidir. Bu eğitimler sonucunda e-posta kullanımından kaynaklanacak zafiyetler en aza indirgenecektir.

Genel anlamda bilgi güvenliğinin sağlanmasında en zayıf halka olan insan faktöründen meydana gelen zafiyetlerin giderilmesinde eğitim önemli bir rol oynadığından ülke bilgi güvenliğinin sağlanmasında eğitimin önemi ayrıntılı olarak takip eden bölümde incelenmiştir.

V. EĞİTİM

Ülke bilgi güvenliğinin sağlanması açısından önemli olan eğitimler ve bilinçlendirmeler farklı yöntemlerle ülke bilgi sistemlerini her seviyede kullanan kişilere düzenli olarak verilmelidir. Bu yöntemler bilinçlendirmeler, toplantılar, web üzerinden eğitimler, e-posta yoluyla kullanıcılara bildirimler, yazılar ve duyurular, seminerler, bültenler ve güvenlik posterleri şeklinde olabilir.

İnsana bağlı güvenlik riski hiçbir zaman tamamen yok edilemese de iyi planlanmış bilgi güvenliği eğitimleri riskin kabul edilebilir bir seviyeye indirilmesine yardımcı olacaktır. Farklı bilgi seviyesindeki insan gruplarının, bilgiyi ve bilgi kaynaklarını koruma konusunda üzerilerine düşen sorumlulukları anlaması ve yerine getirmesi, bilgi güvenliğinin sağlanması ve insan faktöründen kaynaklanan zafiyetlerin en aza indirgenmesi açısından kritik bir öneme sahiptir.

Bilgi güvenliği eğitimlerinin temel hedefi, bilgi kaynaklarının gizlilik, bütünlük ve erişilebilirliğin sağlanması konusunda yapması gereken görev ve sorumluluklar konusunda insanları eğitmektir. Bilgi güvenliği eğitimleriyle insanlar sadece bilginin korunması konusunda nasıl katkı sağlayabileceklerini değil aynı zamanda bilginin neden korunması gerektiğini de öğrenmelidir. Çalışanlar hatalı davranışlarının ülke bilgi güvenliği üzerinde yaratabileceği etkiyi eğitimler aracılığıyla açıkça anlamalıdır. Kullanıcı bilinçlendirme çalışmaları, güvenlik ihlallerinin maliyetini azaltmaya ve kontrollerin kurumun tüm bilgi kaynakları üzerinde dengeli uygulanmasına yardımcı olacaktır.

Güvenlik farkındalık eğitimlerinin amacı, güvenlik ve güvenlik kontrollerinin önemi hakkında ülke bilgi sistemleri kullanıcılarında ortak bir bilinç oluşturulmasıdır [24]. Bilinçlendirme mesajları basit ve açık olmalı, bilinçlendirme eğitimleri insan gruplarının anlayabileceği basit bir formatta verilmelidir.

Çoğu kurumda güvenliğin sağlanması için yapılması gereken kısıtlamaların kullanıcıların alışkanlıklarıyla ters düşmesinden dolayı güvenlikle ilgili yaptırımların uygulanmasında geç kalınmaktadır. Güvenlik uygulamaları başından itibaren uygulanmadığından zamanla her kullanıcının, güvenliğe dikkat etmeksizin farklı kullanım alışkanlıkları edindiği görülmüştür. Bu durum bilgi güvenliği

bilinçlendirme eğitiminin uygulanmasını zorlaştırarak, kullanıcılarda güvenlik uygulamalarına karşı direnç oluşmasını sağlamaktadır. Çünkü sadece kullanıcıları eğitmek değil aynı zamanda eski alışkanlıklarından kurtarmak gerekmektedir.

Kullanıcılara göre kurum güvenlik önlemleri olmaksızın bugüne kadar gayet iyi çalışmıştır ve hiçbir sorunla karşılaşmamıştır. Yeni güvenlik önlemleri hayatı zorlaştırıcı gereksiz değişiklikler olarak görülür. Bilinçlendirme eğitimleri güvenlikle ilgili bilgi vermenin yanında kullanıcı alışkanlıklarından nasıl kurtarılacağı göz önüne alınarak hazırlanmalı akıcı ve eğlenceli bir içerikle kullanıcılara sunulmalıdır.

Çalışma kapsamında yapılan araştırmalarda çoğu kurumda güvenlik bilinçlendirme programının olmadığı görülmüş, olan kurumlarda ise genellikle kullanıcıları bilgi güvenliğinin neden önemli olduğu konusunda eğitmeyi başaramadığı tespit edilmiştir. Eğitimin başarılı olabilmesi için kullanıcıların kafasındaki neden sorusunun cevabı kullanıcıyı ikna edecek şekilde verilmelidir. Başarılı bir eğitim sonrasında kullanıcıların şifreleme politikasına sahip çıkarak yeni politikanın uygulanmasında gayretli olacakları görülecektir. Pek çok kullanıcı, bilgi ve bilgi kaynaklarının korunmasının önemi konusunda yeterli bilgiye sahip değildir. İyi tasarlanmış ve sonuçlandırılmış bilinçlendirme ve eğitim çalışması güvenlik zincirinin en kırılgan halkası olan insan faktörünün güçlendirilmesine büyük katkı sağlayacaktır.

Ülke Bilgi Güvenliğinin sağlanmasındaki kurumsal ve kişisel bilgi güvenliği aşamalarından sonra insan faktöründen kaynaklanan zafiyetleri en aza indirgeyen eğitim unsuru üzerinde durulmuştur. Ülke bilgi güvenliği süreçlerinin işlerliğinin kontrol edilebilmesi için güvenlik testlerine ihtiyaç duyulduğundan güvenlik testleri takip eden bölümde açıklanmıştır.

VI. GÜVENLİK TESTLERİ

Ülke Bilgi Güvenliğinin sağlanmasında temel unsurlar olan insan faktörü ve eğitim önceki bölümler içerisinde alt başlıklar halinde incelenmiştir. Bilgi güvenliğine etki eden unsurların bir bütün olarak saldırgan gözüyle sınanması, zafiyetlerin tespit edilerek giderilmesi için yapılacak düzeltmelerin ve sıkılaştırmaların belirlenmesi, güvenlik testlerinin ülke bilgi güvenliğinin sağlanmasındaki önemini özetlemektedir.

Güvenlik testleri, bilgi sistemlerinin başına olumsuz bir durum gelmeden önce, sistem açıklarını sınyarak belirlemek ve alınabilecek karşı tedbirlerin önceden düşünülmesinde kullanılan önemli bir erken uyarı sistemidir. Güvenlik testlerinin başarılı olabilmesi için bilgi sistemlerinin güvenliğine etki eden faktörlerinin ağırlıkları dikkate alınarak sistemlere özgü farklı senaryolar geliştirilmesi gereklidir. Güvenlik testleri için geliştirilen senaryolar kullanılan teknolojilere, kullanıcıların bilgi düzeylerine, bilgi güvenliği seviyesine, bilgi güvenliği bileşenlerinin dozuna göre farklılık gösterebilir.

Bilgi güvenliği ihlallerinin kontrollü bir şekilde tespit

edildiği teknik testlere ek olarak teknik olmayan testler de yapılmalıdır. Teknik olmayan güvenlik testlerinin başında sosyal mühendislik testleri gelmektedir. Sosyal mühendislik, yalan söyleme ve ikna etme üzerine kurulan inandırma ve bilgi toplama sanatıdır [25]. Sosyal mühendislik testlerinden sonuç alabilmek için farklı yöntemler kullanılmaktadır. Bu yöntemlerden en çok kullanılanı telefon yoluyla taklit ve ikna yöntemidir.

Güvenlik testlerinin yapılmasında dünyada yaygın olarak bilinen birçok açık kaynak standart ve kılavuzlar (OSSTMM, NIST, OWASP, v.b.) vardır. Güvenlik testleri yapılırken bu kaynakların kullanılması güvenlik testlerinin başarısı açısından önemlidir.

Bu çalışmada ülkemizde güvenlik testlerinin henüz yaygınlaşmadığı ve kurumlar tarafından kurumsal bilgi güvenliğinin sağlanmasında önemli bir bileşen olduğunun bilinmediği tespit edilmiştir. Bu durum güvenlik testlerinin kurumlara katkılarının, sağlayacağı farkındalığın ve güvenlik seviyesinin artırılmasına katkısının ülkemizde pek bilinmediğinin ve yeterince önem verilmediğinin göstergesidir.

VII. SONUÇLAR VE DEĞERLENDİRMELER

Ülke bilgi sistemleri, e-devlet uygulamaları aracılığıyla kişisel veya kurumsal ihtiyaçlar doğrultusunda kurumsal bilişim altyapılarını kullanarak hizmet vermektedir. Geçmiş yıllarda saldırılar hedef gözetmeksizin yapılmaktayken günümüzde nokta hedefi gözeten ve ülke bilgi sistemlerini hedef alan bilinçli saldırılar yapılmaktadır. Ülke bilgi güvenliğini zaafa uğratmaya hatta yıkmaya çalışan, bireyler ve kurumlar üzerinde maddi manevi büyük zararlara yol açan bilgi güvenliği tehditlerinin engellenmesi için kişisel ve kurumsal seviyede bilgi güvenliği sağlanmalıdır. Ülke bilgi sistemlerinin bilgi güvenliği süreçleri uluslararası standartlara göre yönetilmelidir.

Ülke bilgi sistemleri ülkeler açısından kritik bilgiler barındırmaktadır. Bu kritik bilgilerin bilgi güvenliğinden kaynaklanan zafiyetlerden dolayı siber saldırılara uğraması sonucunda ülkeler açısından telafisi mümkün olmayan durumlarla karşılaşılabilir. Bir barajın kapaklarının yetkisiz bir şekilde istenmeyen bir zamanda açılması, sivil veya askeri haberleşme sistemlerinin aksatılması, elektrik ve doğalgaz santrallerinin kullanılmaz hale getirilmesi, bankacılık, sağlık ve eğitim sektörlerine ait bilgi sistemlerinin çökertilmesi ülke güvenliğini tehdit eden bilgi sistemleri odaklı saldırılara örnek olarak gösterilebilir. Ülke güvenliğini tehdit eden bilgi sistemleri odaklı saldırılardan korunmak için ülke güvenlik politikaları oluşturulmalı ve bu politikalara göre ülke bilgi güvenliği sağlanmalıdır.

Bilginin gizliliğine, bütünlüğüne, erişilebilirliğine karşı yapılan saldırılar ciddi ve giderilemeyecek kayıplara yol açmaktadır. Bu kayıpları tamamen yok etmek mümkün değildir. Ancak yapılacak güvenlik testleriyle kayıpları en aza indirmek mümkündür. Ülke bilgi sistemlerine yönelik yapılacak güvenlik testlerinin ulusal bir otorite tarafından

oluşturulan güncel ulusal güvenlik politikalarına uygun olarak yapılması gerekmektedir. Ülkemizde güvenlik testlerini ücretsiz yapan devlet destekli merkezler oluşturulmalı ve güvenlik testlerine yönelik milli yazılımlar geliştirilerek kullanılmalıdır.

Bilgi güvenliğinde “güvenliğiniz en zayıf halkanız kadardır” ilkesi gözönüne alındığında ülke bilgi güvenliğini oluşturan halkalar içerisinde en zayıf halka olan insan faktöründen kaynaklanan zafiyetlerin giderilmesi için bilgi güvenliği eğitimi ve bilinçlendirmesi, ilköğretimden üniversiteye kadar eğitimin her aşamasında verilmelidir. Burada özellikle sivil toplum kuruluşlarına, Milli Eğitim Bakanlığına ve üniversitelere büyük görevler düşmektedir.

Ülke güvenliğini tehdit eden siber saldırıların bilinmesi, bilgi güvenliğinin sağlanmasına yönelik ülke stratejilerinin geliştirilmesinde önemli bir role sahiptir. Bilgi sistemlerine yönelik olarak yapılan planlı saldırılar incelendiğinde; saldırıların kişi düzeyinden ülke düzeyine kadar çok geniş bir yelpazede gelişmiş teknikler kullanılarak yapıldığı tespit edilmiştir. Ülke bilgi güvenliğinin sağlanması amacıyla, saldırı türlerinin takip edilmesi, saldırganların kullandığı gelişmiş yöntemlerin saptanması, ülkemizde ve dünyada bu konuda yapılan araştırmaların, raporların ve çalışmalar ile tespit edilen açıkların yakından takip edilmesi ve zamanında giderilmesi gerekmektedir.

Sonuç olarak; ülke bilgi güvenliğinin sağlanmasına yönelik yapılan çalışmaların ve alınması gereken önlemlerin yeterli olmadığı, kişisel ve kurumsal düzeyde bilgi güvenliği bilincinin ve eğitiminin toplumumuza tam olarak yerleşmediği ve ülkemizde yüksek seviyede ülke bilgi güvenliğinin sağlanamadığı dikkate alındığında, bu çalışmada sunulan hususlara dikkat edilmesi ve yapılan önerilere uyulması gerekmektedir.

KAYNAKLAR

- [1] Thow-Chang, L., Siew-Mun, K., and Foo, A., “Information Security Management Systems and Standards” Synthesis Journal, 2(2):5,8 (2001).
- [2] Sandham, D., “News”, Communications Engineer Publication 5(4):3-8, (2008).
- [3] İnternet: “McAfee Virtual Criminology Report” http://www.mcafee.com/us/research/criminology_report/default.html (09.11.2008)
- [4] Vural, Y., “Kurumsal Bilgi Güvenliği ve Sızma Testleri”, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 15-20, (2007).
- [5] Rocha, L. M., Schnell, S., “The Nature of Information-Lecture Notes”, Indiana University, Bloomington, 1, (2007).
- [6] İnternet: Türk Dil Kurumu “Güncel Türkçe Sözlük” <http://www.tdk.gov.tr/TR/SozBul.aspx?F6E10F8892433CFFAA6AA849816B2EF4376734BED947CDE&Kelime=bilgi>
- [7] İnternet : “National Information Systems Advisory Panel- Computer-Based National Information Systems” http://govinfo.library.unt.edu/ota/Ota_5/DATA/1981/8109.PDF (09.11.2008).
- [8] İnternet: “Türkiye Ulusal Bilgi Sistemi:Genel Esaslar” www.hssgm.gov.tr/stratejikonetim/egitim_dokumanlari/turkiye_ulusal_bilgi_sistemi_esaslari.pdf (09.11.2008)
- [9] Krygiel, J., “Behind the Wizards Curtain: An Integration Environment for a System of Systems” DoD C4ISR Cooperative Research Program, Washington, 9-11 (1999).
- [10] İnternet: Wikipedia, “Information Assurance”, http://en.wikipedia.org/wiki/Information_assurance (09.11.2008)

- [11] Bhatt, G. D., “Knowledge Management in Organizations: Examining the Interaction between Technologies, Techniques and People”, Journal of Knowledge Management, 5 (1):71, (2001)
- [12] Vural, Y., Sağiroğlu, Ş., Kurumsal Bilgi Güvenliği: Güncel Gelişmeler, ISC Turkey Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara, 191-199, Aralık 2007
- [13] Vural, Y., Sağiroğlu, Ş., Gazi Üniv. Müh. Mim. Fak. Der. 23(2), 507-522, (2008)
- [14] Türk Standartları Enstitüsü, “Bilgi güvenliği yönetim sistemleri”, TSE-TS 1779- 2, Ankara, 3, (2005).
- [15] Mitnick, K. D., Simon, L. W., Wozniak, S., “The Art of Deception: Controlling the Human Element of Security”, Wiley Publishing, New York, 17-18 (2003)
- [16] İnternet: Wikipedia, “ISO/IEC 27001”, http://en.wikipedia.org/wiki/ISO_27001 (09.11.2008)
- [17] İnternet: CERT “Historical Statistics” <http://www.cert.org/stats/historical.html> (09.11.2008)
- [18] Dunlevy, J. C., “Information Security Strategies: A New Perspective”, CERT, Pittsburgh, 15, (2006)
- [19] İnternet: World Stats “Top 20 Countries With The Highest Number Of Internet Users” <http://www.internetworldstats.com/top20.htm> (17.03.2007)
- [20] Symantec Corp., “Symantec Internet Security Threat Report Trends for July–December 07” Symantec Volume XII, Cupertino, 24-64 (2008).
- [21] Gordon, L. A., Loeb, M. P., Lucyshyn, W., Richardson, R., “CSI/FBI, Computer Crime and Security Survey”, FBI Computer Security Institute, 1- 26, (2005).
- [22] Koç.net Haberleşme Teknolojileri ve İletişim Hizmetleri A.Ş., “Türkiye İnternet Güvenliği Araştırma Sonuçları 2005”, Koç.net, İstanbul, 5- 12, (2005)
- [23] İnternet: “Information Security Awareness” <http://www.massachusetts.edu/SecurityAwareness/securityawareness.html> (9.11.2008)
- [24] Morales, L., Dark, M., “Information Security Education and Foundational Research”, System Sciences, HICSS 2007. 40th Annual Hawaii International Conference, Hawaii, 269 (2007).
- [25] Mitnick, K. D., Simon, W. L., “Aldatma Sanatı”, Nejat Eralp Tezcan, ODTÜ Yayıncılık, Ankara, 303, (2006).

Eşler Arası Anonim Dosya Paylaşımı İçin Açık Anahtarlı Bir Kerberos Kimlik Denetimi Uygulaması

Tuğkan TUĞLULAR, Can Arda MÜFTÜOĞLU, Özgür KAYA

Özet—Bu çalışmada anonim dosya paylaşımı gereksinimine çözüm olarak anonim vekil önerilmektedir. Anonim vekil yetkisi olan eşleri dosya paylaşım grubuna eklemektedir. Kimlik denetimi için Kerberos kimlik denetimi mekanizmasının açık anahtarlı şifreleme ile güçlendirilmiş sürümü kullanılmıştır. Bilet sağlama sunucusunun katılımı ile oluşturulan model bir uygulama haline getirilmiş ve farklı eş sayıları altında denenmiştir.

Anahtar Kelimeler— Açık Anahtarlı Şifreleme, Anonim Dosya Paylaşımı, Eşler Arası, Kerberos Kimlik Denetimi.

I. GİRİŞ

ANONİM dosya paylaşımı İnternet üzerinde bir gereksinim olarak karşımıza çıkmaktadır. Bu gereksinimi karşılayacak çözüm yaklaşımlarından birisi güvenilir bir otoriteyi vekil olarak kullanmaktır. Anılan vekile, kendisi anonim olmamakla beraber anonimliği sağladığı için anonim vekil ismi verilmiştir.

Önerdiğimiz protokol, anonimlik derecesini, öncesinde gerçekleştirdiği Kerberos kimlik denetimi ile kuvvetlendirmeyi amaçlayarak, gruptan sorumlu bir vekil ile grup içi anonimliği sağlamaktadır. Bu konuda, dosya paylaşım isteğinin tüm eşlere gönderilmesi ve bu işlemin şifreli olarak yapılmasını [1], karmaşık bir matematiksel alt yapıya dayalı olarak şifreleme ağırlıklı bir anonimlik protokolü ile birlikte, paketlerin izleyeceği güzergahın da anonimlik kapsamında ele alınmasını [2], karşılıklı anonimlik sağlamak amaçlı “Gizli Paylaşım Tabanlı (Secret Sharing Based)” bir protokolün önerildiği, eşler arası mesajlaşmaların olmasına dayanan kimlik bilgilerinin, paket akışı takip edilerek açığa çıkarılmasının engellenmesini [3], eşler arası kişisel gizliliğin konu alındığı [4] ve karşılıklı anonimlikte en kısa yanıt protokolünün uygulandığı [5] çalışmalar bulunmaktadır.

Önerdiğimiz protokolde gruba katılan eşler, kimlik denetimi

sonrasında güvenilir alan içerisinde olduğu varsayıldığı için, dosya istek mesajlarını düz metin halinde yollamaktadır. Tüm dosya istek mesajları, direk olarak eşler arası iletmek yerine, anonim vekil üzerinden gerçekleştirildiği için, eşler arası karşılıklı gizlilik de anonim vekil tarafından sağlanmaktadır.

Bu çalışmada, bir grubu oluşturan eşlerin istedikleri zaman gruba bağlanıp dosya paylaşımını anonim vekil üzerinden gerçekleştirdikleri ortam modellenmiştir. Kimlik denetimi, gruba katılma ve dosya sorgulama gibi süreçler tasarlanmış ve detayları açıklanmıştır. Anılan süreçler kodlanarak bir uygulama haline getirilmiştir. Bu uygulama farklı sayıda eşten oluşan gruplar için laboratuvar ortamında çalıştırılmış ve operasyonel değerler elde edilmiştir.

Bildirinin içeriği şu şekilde düzenlenmiştir: İkinci bölümde eşler arası anonim dosya paylaşımı için açık anahtarlı Kerberos kimlik denetimi mekanizması açıklanmıştır. Üçüncü bölümde, geliştirilen uygulama anlatılmış ve bu uygulamaya ilişkin elde edilen operasyonel değerler izleyen bölümde ortaya konmuştur.

II. KİMLİK DENETİMİ VE GRUBA KATILIM

Önerdiğimiz modelde, her eş sadece anonim vekil ile iletişim içindedir ve diğer eşlerin kimliklerinden habersizdir. Anonim vekil, eşlerin kimliklerini elinde bulunduran tek otoritedir ve kimlik denetimi için Bilet Sağlama Sunucusu’ndan yardım alır. Bilet Sağlama Sunucusu kimlik denetimi için açık anahtarlı Kerberos kimlik denetimi protokolünü kullanır. Anonim vekil gruba katılmak isteyen eşin biletini kontrol eder ve eşi gruba dahil eder. Anonim vekil ayrıca, kendisine gelen istekleri gruba yayımlamanın yanı sıra, gruptan gelen cevapları alıp istek yapan eşi iletmekten de sorumludur.

A. Sürece Genel Bakış

Eşler için sonlu durum otomatu Şekil 1’de gösterilmiştir. Başlangıçta, eş grup dışında ve “Beklemede” durumundadır. Bilet Sağlama Sunucusu ile mesaj alışverişi sonucu aldığı bilet, gruba girerken Anonim Vekil tarafından kontrol edilir ve doğrulanır. Bileti doğrulanan eş, gruba katılır ve “Hazır” durumuna geçer. Gruba bulunduğu sürece, hazır durumundadır. Eş, kendisinin gönderdiği ve diğer eşlerden gelen istek veya cevap mesajlarını kuyruğa ekler. Kuyruқта

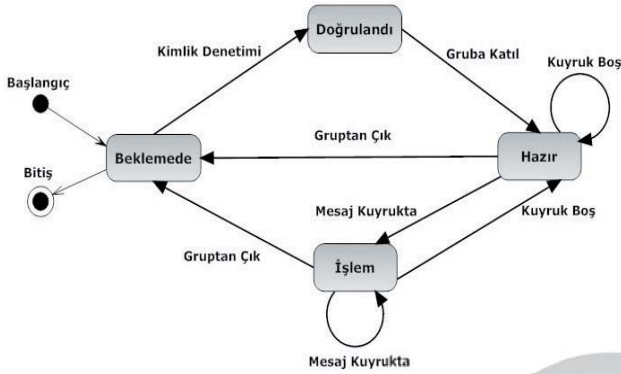
Manuscript received November 10, 2008.

Asst. Prof. Dr. Tuğkan Tuğlular is with the Department of Computer Engineering, İzmir Institute of Technology, İzmir, 35430 Turkey. e-mail: (tuğkantuglular@iyte.edu.tr).

Can Arda Müftüoğlu is with the Department of Computer Engineering, İzmir Institute of Technology, İzmir, 35430 Turkey. e-mail: (ardamuftuoglu@iyte.edu.tr).

Özgür Kaya is with the Department of Computer Engineering, Yasar University, İzmir, 35500 Turkey. e-mail: (ozgur.kaya@yasar.edu.tr).

bir mesaj olduğu zaman, eş, “İşlem” durumuna geçer ve kuyrukta mesaj olduğu sürece onu işlemek üzere, işlem durumunda kalır. Eş, kuyruk boşaldığı zaman, tekrar hazır durumuna geçer. Gruptan çıkma eylemini gerçekleştirdiğinde ise, eş tekrar beklemede durumuna geçer.



Şekil 1. Eş Sonlu Durum Otomatu.

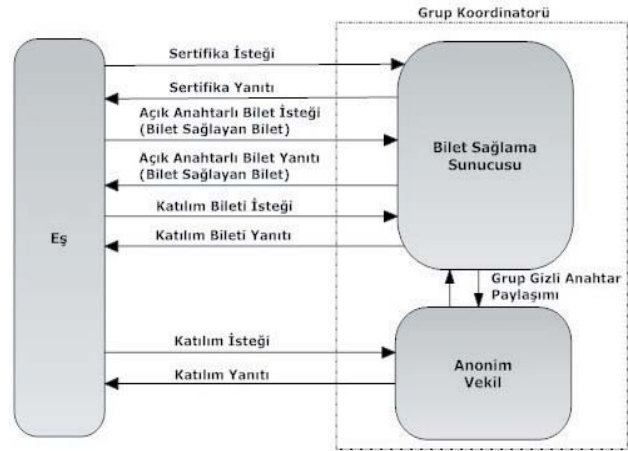
Önerimizde bir eşin, eşler arası dosya paylaşımı grubuna girmeden önce kimlik denetiminden geçmesi gerekmektedir. Bunun için Kerberos Kimlik Denetimi Protokolü kullanılır. Açık anahtar şifrelemesi, Kerberos Kimlik Denetimi'ne dâhil edilmiştir [6].

Her dosya paylaşım grubunda, kalıcı olarak çevrimiçi olan ve kimlik denetimi ve dosya paylaşımı işlemlerini yöneten bir grup koordinatörünün yer aldığı varsayılmıştır. Grup koordinatörü, açık anahtar şifrelemeli Kerberos kimlik denetimi işleminden sorumlu Bilet Sağlama Sunucusu(BSS) ve eşlerin grup içerisindeki kimlik gizliliğini sağlayan anonim vekilden oluşur. Bu iki servis aynı sunucu üzerinde olabileceği gibi farklı sunucular üzerinde de var olabilir. İki servisin hizmet verdiği kapılar birbirinden farklıdır.

[1]'deki öneriden farklı olarak, açık anahtar şifrelemeli Kerberos kimlik denetimine dayanan bir güvenlik sistemi kurulmuştur. Bilet Sağlama Sunucusu tarafından kimliği doğrulandıktan sonra gruba giren bütün eşler güvenilir kabul edilir. Bütün istekler anonim vekil üzerinden düz metin olarak iletilir.

B. Kimlik Denetimi

Anonim dosya paylaşımı için kimlik denetimi Şekil 2'de gösterildiği şekilde gerçekleştirilir. Bir eş ilk olarak, eşler arası dosya paylaşım grubuna girebilmek için Bilet Sağlama Sunucusu'na başvurur. Eşler isteklerini açık anahtar yetkili Bilet Sağlama Sunucusu'na göndermektedir. Geleneksel Kerberos kimlik denetimi protokolüne iki adım daha eklenerek, açık anahtarlı şifrelemenin Bilet Sağlama Sunucusu'na uygun hale gelmesi sağlanmaktadır [7]. Eş geleneksel bir Bilet Sağlayan Bilet(BSB) ve eşler arası dosya paylaşımı grubuna giriş için gereken erişim bileti alabilmek için ortak anahtar yetkili Bilet Sağlama Sunucusu ile iletişime geçer. Kimlik denetimi adımları ve mesajlaşmalar, eş ile Grup Koordinatörü'nün Bilet Sağlama Sunucusu arasında gerçekleşir.



Şekil 2. Kimlik Denetimi Etkinlik Şeması.

Kerberos Bilet Sağlama Sunucusu'na yetkilendirilmeden önce, eş kimlik denetiminin başlangıcı olarak açık anahtar sertifikası isteğinde bulunur. Bilet Sağlama Sunucusu'nun açık anahtarını kullanarak “Açık Anahtarlı Bilet İsteği” mesaj paketini şifrelemek için gereken anahtar bu adımda sağlanır. Sertifika İsteği Mesajı, Bilet Sağlama Sunucusu'nun kimlik bilgisini içerir. Bu ve sonraki kimlik denetimi mesajları grup koordinatörünün belirlediği kapı üzerinden sağlanır. Sertifika isteğine karşılık olarak, Bilet Sağlama Sunucusu, kendi açık anahtarını içeren sertifika cevap mesajını istekte bulunan eşe gönderir. Eş arzu eder ise Bilet Sağlama Sunucusu'na ait sertifikanın doğrulanması için bir Sertifika Otoritesi'ne başvurabilir. Ancak bu adım, önerimize ait gerçekleştirdiğimiz uygulamaya katılmamıştır.

Kimlik denetiminin bir sonraki aşamasında, eş Bilet Sağlama Sunucusu'ndan Bilet Sağlayan Bilet temin etmek için bir istekte bulunur. Oluşturduğu mesaj, eşin gizli anahtarıyla sayısal olarak imzalanır ve sunucunun açık anahtarıyla şifrelenir. Ayrıca, gönderilen bu mesaj, kimlik denetimi isteğinin gönderildiği kimlik denetimi başlangıç zamanı, eşin Bilet Sağlama Sunucusu'nun açık anahtarıyla şifrelediği rastgele üretilmiş bir K sayısını içerir [6]. Bu sayede, sadece Bilet Sağlama Sunucusu eşin kimliğini doğrulayabilir ve eşleşen gizli anahtarı olan sunucu bu mesajı deşifre edip geçerli bir yanıt oluşturabilir.

Eşin sahip olduğu sertifika ve kimliği, kimlik denetimi veri alanının içinde, bir kerelik rastgele üretilen anahtar, Bilet Sağlama Sunucusu'nun kimliği, Bilet Sağlama Sunucusu'nun ortak anahtarı, eşin gizli anahtarıyla imzaladığı kimlik denetimi zamanı yer alır. Kimlik denetimi veri alanı, “Kriptografik Mesaj Sözdizimi Standartları (Cryptographic Message Syntax Standards PKCS #7)”[8] sözdizimi standartlarına göre oluşturulmuştur. Üretilen rastgele sayı, istek mesajının şifrlenmesinde kullanılır. Eşin kimliğinin düz metin halinde gönderildiği Bilet Sağlama Sunucusu'nun sözdizimi kurallarının aksine, “Açık Anahtarlı Bilet İsteği” mesajı, bu alanda eşin kimliği şifreli halde gönderilir.

Bilet Sağlama Sunucusu'nun, “Açık Anahtarlı Bilet İsteği”

mesajına cevap olarak, düz metin halinde Bilet Sağlama Sunucusu'nun kimliğini, eş ve Bilet Sağlama Sunucusu arasında paylaşılan anahtar, eşin kimliğini ve kimlik denetimi istek zamanını zaman damgası halinde, sadece Bilet Sağlama Sunucusu tarafından bilinen simetrik bir anahtar ile şifreleyerek oluşturulan veri alanlarından oluşan, servis bileti görevini üstlenen Bilet Sağlayan Bilet gönderir. Bu şifreleme, eşin aldığı biletin içeriğini değiştirmesini engeller.

Eş ve Bilet Sağlama Sunucusu arasında paylaşılan oturum anahtar, tek kullanımlık rastgele oluşturulmuş anahtar 112 bit “Üçlü Veri Şifreleme Standardı (Triple DES)” ile şifrelenir. Eş tarafından rastgele üretilen anahtar tek kullanımlık bir anahtardır ve bu anahtar ayrıca rastgele sayı görevini de üstlenir.

Bilet Sağlayan Bilet aldıktan sonra, dosya paylaşım grubuna erişimi sağlayan gerçek bileti almak için eş, grup adını ve Bilet Sağlayan Bilet'i içeren istek mesajını gönderir. Bilet Sağlayan Bilet, Bilet Sağlama Sunucusu'nun simetrik anahtarı ile şifrelenmiş olduğu için, Bilet Sağlama Sunucusu mesajı deşifre edip, eğer mesaj değiştirilmemişse, eşe gruba katılabilmesi için gereken bileti cevap olarak gönderir.

Gruba katılmak için eş, Anonim Vekil'den aldığı bilet ile erişim iznini talep eder. Anonim Vekil, eşten gelen bileti kontrol ederek eşin kimliğini doğrular ve gruba katılma iznini verir.

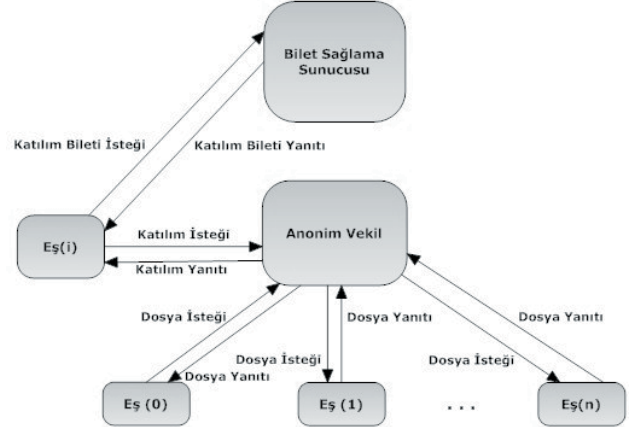
C. Eşler Arası Dosya Sorgulaması

Kimlik denetimi tamamlandıktan sonra eş, kimlik bilgileri saklı şekilde bileti (düz metin halinde bulunan koordinatörün kimlik bilgisi, eş ile koordinatör arasında paylaşılan anahtar, eşin kimlik bilgisi ve zaman damgası halinde kimlik denetimi istek zamanından oluşan) ile güvenilir bölge olarak ele alınan dosya paylaşım grubuna katılım isteği gönderir. Yanıt olarak koordinatör, eşin istenen gruba giriş iznini bildirir.

Eşin kimlik bilgisi, paylaşılan anahtar ile şifrelendiğinden anonimlik sağlanır. Bu adımda, anonim vekil, eşin kimlik bilgilerini kendi eş tablosuna yerleştirir. Her eşin kimliği sadece anonim vekil tarafından bilinir. Anonim vekil, gizliliği sağlamak için istekte bulunan ile alıcı taraf arasında bir aracı görevinde bulunur.

Gruba girdikten sonra, eş dosya adını belirterek dosya paylaşım grubuna bir dosya isteğinde bulunur. Bu istek mesajı, anonim vekil üzerinden diğer eşlere iletilir. Anonim vekil, kendisine gelen istekleri, her birine bir işlem numarası atayarak tanır ve bu isteği işlem tablosuna kaydeder.

Dosya istek mesajını alan eşler, istekte bulunulan dosya adıyla, dosya listelerinden arama yaparlar. Bu dosya kendilerinde mevcut ise, istek mesajına dosya adıyla yanıt verirler. Mevcut değilse, anonim vekil üzerinden olumsuz yanıt gönderilir. Anonim vekil bu mesajı alır, işlem tablosundan arama yaparak istek mesajını gönderen kişiyi bulduktan sonra yanıtı bu kişiye iletir ve ilgili kaydı işlem tablosundan kaldırır (Bknz Şekil 3).



Şekil 3. Eşler Arası Dosya Paylaşımı Etkinlik Şeması.

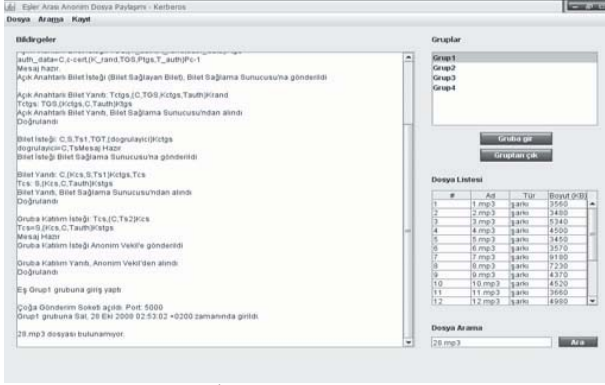
III. UYGULAMA

Önerdiğimiz modelin uygulaması Java programlama dilinde geliştirilmiştir. Uygulama, “Eş” ve “Koordinatör” olarak isimlendirilen iki ayrı projeden oluşur. Eş, gruba girmek isteyen ve kimlik denetiminden geçecek olan istemci, Koordinatör ise kimlik denetimini sağlayan Bilet Sağlama Sunucusu ile dosya istek mesajlarının anonim olarak gönderilmesine olanak sağlayan Anonim Vekil’den oluşur.

“Eş”, bir ana sınıftan ve ona bağlı sınıflardan oluşur. Uygulamada, tüm mesaj paketlerinin eklendiği bir kuyruk veri yapısı kullanılmıştır. Bu kuyruk, Koordinatör’den gelen ve Eş’in Koordinatör’e göndereceği mesaj paketlerini içinde barındırır. “Okuyucu” sınıfı aynı zamanda bir iş parçacığı sınıfı olup, Koordinatör’den gelen mesaj paketlerini kuyruğa eklemeye yarar. “İletici” sınıfı ise, Okuyucu sınıfı gibi bir iş parçacığı sınıfı olup, kuyruktaki mesajları “İşlemci” sınıfına girdi olarak verme işini yapar. İşlemci sınıfı da, mesajın içeriğine göre gerekli işlemi (gönderme, şifreleme, deşifreleme, yeni mesaj hazırlama vb.) yerine getirir. Bu işlemleri yaparken, açık anahtarlı ve simetrik şifrelemelerde “Sayısalİmza” ve “Anahtar” sınıflarını kullanır. Açık anahtarlı şifrelemede, “RSA” şifreleme algoritması, simetrik şifrelemede ise “Üçlü Veri Şifreleme Standardı (Triple DES)”, Java güvenlik kütüphanesinden kullanılmıştır.

Bunun dışında, Eş sınıfı başlangıçta bir XML konfigürasyon dosyasından, “XMLAyrıştırıcı” nesnesini kullanarak konfigürasyon parametrelerini dosyadan ayrıştırır ve lokal değişkenlerine atar. “Dosya Zinciri” nesnesini kullanarak eş, dosya listesini dosyadan okuyup, ayrıştırıp, bu nesnenin yaratılan bir objesinde saklar. “Grup” nesnesi ile eş, gireceği grubu belirledikten sonra bu grubun ip adresi ve port bilgilerini saklar. “MesajPaketi” nesnesi, mesaj paketlerinin gönderilip alınmasını ve ayrıştırılabilmesini sağlar. “SüreÖlçer” sınıfı ise, uygulamanın simülasyonu yapıldığında, belirlenen zamanları ölçmek ve bunları kaydetmek için kullanılır.

İstemcinin Şekil 4’de gösterildiği gibi bir arayüzü bulunur, ve bu arayüz ile seçilen gruba giriş veya gruptan çıkış,



Şekil 4. İstemci Kullanıcı Arayüz Ekranı

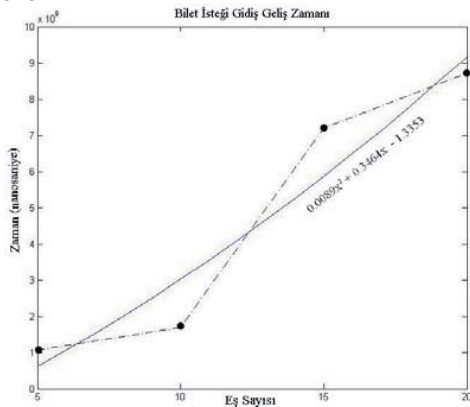
paylaşılan dosyaların listelenmesi ve yönetilmesi ve dosya arama gibi fonksiyonlar gerçekleştirilir. Arayüzün “Bildirgeler” bölümüne, alınan ve gönderilen mesaj içerikleri, gelen dosya istekleri, karşılaşılan hata mesajları gibi bilgilendirici mesajlar eklenir.

IV. DENEY

Önerdiğimiz model, bir yerel ağda denenmiştir. Protokol modelinde bahsedilen, kimlik denetimi için gönderilen ve alınan mesajların gidiş geliş süreleri ölçülmüş ve grafiklere aktarılmıştır. Bu deneyde sırasıyla 5, 10, 15, 20 eşten oluşan denek grupları kullanılmıştır ve her bir deney 100'er defa tekrar edilmiştir. Her tekrardan önce, uygulamalar yeniden başlatılmıştır ve komut satırından çalıştırılarak, istemci deney ortamına dahil edilmiştir.

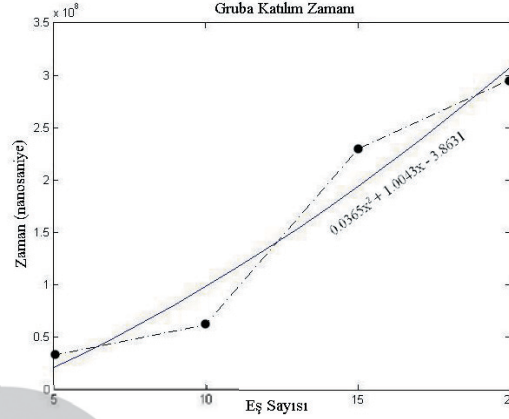
Önerdiğimiz modeli gerçekleyen uygulama Java programlama dilinin 1.6.0 sürümü ile kodlanmıştır. Modeli gerçekleyen program vasıtasıyla sonuçlar, deney bittikten sonra Microsoft Excel dosyasına yazdırılmıştır. Deney sonuçlarından elde edilen ortalama veriler kesikli çizgilerle grafiklerde gösterilmiştir. Matlab yazılımının 2006a sürümü kullanılarak 2. dereceden polinomlar oluşturulup, bu polinomlarla elde edilen eğriler ilgili grafiklerin üzerine çizilmiştir.

Şekil 5'te, sertifika isteği ile başlayan ve gruba katılım bileti yanıtının alınmasına kadar geçen kimlik denetim zamanının grafiği gösterilmiştir.



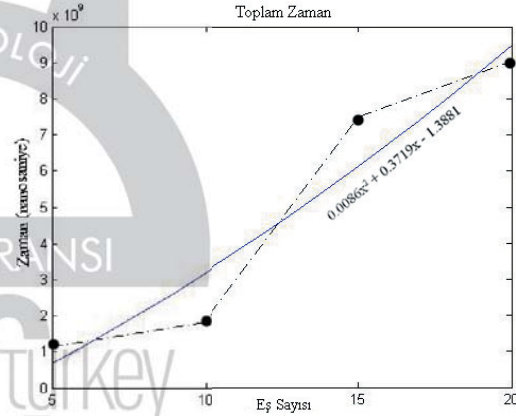
Şekil 5. Bilet İsteği Gidiş Geliş Zaman Grafiği.

Şekil 6'da, Anonim Vekil'e yapılan gruba katılım isteğinden, yanıt alınmasına kadar geçen zamanın grafiği bulunmaktadır.



Şekil 6. Gruba Katılım İsteği Gidiş Geliş Zaman Grafiği.

Şekil 7'de ise, sertifika isteği ile başlayıp, eşin gruba katılımına kadar geçen toplam zamanın grafiği gösterilmiştir.



Şekil 7. Toplam Zaman Grafiği.

Grafikler'de, eş sayısı ile zamanın birbirine doğru orantılı olarak arttığı görülmektedir. Ağ ve sunucu ortamındaki trafiğin artması, istek yanıtlarının gecikmesine, diğer bir deyiş ile gidiş geliş zamanlarının artmasına, dolayısıyla da grafiklerdeki eğrilerin bu artışlara bağlı olarak yükselmesine yol açmıştır.

V. SONUÇ

Anonim dosya paylaşımı için oluşturulacak gruplara yetkisi olup dahil olmak isteyen eşlerin kimlik denetimi için açık anahtarlı Kerberos kimlik denetimi yaklaşımı kullanılmıştır. Bu yaklaşım ile sayısal bilet alan eş gruba belirlenen politikalar doğrultusunda girebilecektir. Biletin varlığı değişik güvenlik ve paylaşım politikalarının uygulanmasına izin verdiği gibi zaman kısıtlarını da resme dahil edebilmektedir.

Açık anahtar yaklaşımı ile de anahtar yönetimi problemi konusunda önemli sorunlar aşılmış bulunmaktadır. Anılan avantajlar sebebiyle ortaya konan model bir Java uygulamasına dönüştürülmüş ve laboratuvar ortamında denenmiştir. Elde edilen sonuçlardan çıkarılan eğriler ile daha fazla eş sayısına sahip gruplar için yanıtlama zamanlarının tahmin edilebilir olmasına çalışılmıştır.

KAYNAKLAR

- [1] S. Krishnan, J. Uhlmann, "The design of an anonymous file sharing system based on group anonymity", *Information & Software Technology*, vol. 46, i. 4, pp. 273-278, 2004.
- [2] T. Chothia, K. Chatzikokolakis, "A Survey of Anonymous Peer-to-Peer File-Sharing", *IFIP International Symposium on Network-Centric Ubiquitous Systems* (NCUS 2005).
- [3] J. Han, Y. Liu, L. Xiao, R. Xiao, L.M. Ni, "A Mutual Anonymous Peer-to-Peer Protocol Design", *Parallel and Distributed Processing Symposium*, 2005. *Proceedings. 19th IEEE International*, vol., no., pp. 68a-68a, 04-08 April 2005.
- [4] R. Sherwood, B. Bhattacharjee, and A. Srinivasan, "P5: A Protocol for Scalable Anonymous Communication," in *Proceedings of IEEE Symposium on Security and Privacy*, 2002.
- [5] L. Xiao, Z. Xu, X. Zhang, "Low-cost and Reliable Mutual Anonymity Protocols in Peer-to-Peer Networks", *IEEE Transactions on Parallel and Distributed Systems*, 2003.
- [6] I. Cervesato, A. D. Jaggard, A. Scedrov, J. - K. Tsay, C. Walstad, "Breaking and Fixing Public-key Kerberos" in *ASIAC 2006*, LNCS, Springer Verlag, Available at <http://eprint.iacr.org/2006/009>.
- [7] M. Sirbu, J. Chuang, "Distributed Authentication in Kerberos Using Public Key Cryptography", *Symposium On Network and Distributed System Security*, pp. 78-85, 1997.
- [8] PKCS #7: Cryptographic Message Syntax Standard. Version 1.5, RSA Laboratories, 1998.

Single Transferable Electronic Voting Protocol for Elections with Barriers

Okan YÜCEL, Nazife BAYKAL

Abstract—A secure electronic vote protocol is proposed for the elections having the constraint of discarding the candidates that cannot exceed the barrier. The protocol prevents the loss of votes that remain under a certain threshold by making use of the concept of single transferable voting (STV) as a solution to the problem of exhausted votes. New protocol is very suitably applied to the ‘Prêt a Voter: All-In-One’ scheme proposed in 2007, with our modification in the tallying phase. We also give details of the cryptographic part and propose two modifications in the ballot construction phase of the ‘Prêt a Voter: All-In-One’ scheme, which enhances its security. ‘Prêt a Voter’ scheme, which provides voting receipts without any thread of coercion and ballot-selling is chosen in this work mainly because of its voter verifiability property.

Keywords —Electronic voting, public key encryption, single transferable voting, voter verifiability.

I. INTRODUCTION

LARGE scale elections are starting to be held increasingly by electronic means in various countries. Electronic voting over the Internet or closed networks accessible from voting booths has several advantages over paper based voting, especially in terms of voter verifiability. Arising new protocols for electronic voting are competing with each other and solving the earlier encountered problems such as the confliction between anonymity and voter verifiability.

Voter verifiability is a concept which does not exist in traditional paper-based elections but becomes an important issue of democracy in the electronic world. The idea is to endow each voter with the facility of *verifying that his vote is counted*. The first level of such a verification could be to verify that *his vote is cast correctly* and the second level is whether *his vote is counted (or tallied) correctly*. The check mechanism for the *correct count of the vote* can be provided by means of a voting receipt. On the other hand, whenever one has a receipt that serves to check the correct tallying of

the vote, it can also be used as the proof for the content of the vote used in the election. This may in turn lead to voter coercion and ballot-selling. Hence, previous versions of the electronic voting protocols have avoided giving receipts to the voters, and introduced the concept of *receipt-freeness* as an integral part of the voting system. On the other hand, the psychology of voters, who are traditionally used to paper based voting is much more on the side of having something touchable, like a paper in hand, rather than completely relying on the electronic media.

‘Prêt a Voter’ scheme is an electronic voting scheme, which responds to this psychological need of having the receipt. More importantly, the way that the receipt is constructed provides voter verifiability up to the second level, i.e., each voter can verify that his vote is cast correctly, by means of the receipt that does not tell anything about the content of the vote to anybody except for the voter himself. The second level of verifiability, i.e., the check of *correct tallying of each received vote* is managed by the *universal verifiability* of the overall system. In other words, the robustness, correctness and dependability of the overall system is provable. Prêt a Voter schemes have their origins in the scheme proposed by Chaum [1] in 2004 and developed by Ryan [2] in the same year.

Among different types of voting systems depending on the needs of the particular election, FPTP (First Past The Post), STV (Single Transferable Voting), Condorcet and Borda Count elections are the main ones to be mentioned. The ‘Prêt a Voter’ scheme proposed by Chaum, Ryan and Schneider [3] in 2005, PAV 2005, and its enhanced form PAV 2006 [4] are easily implemented for FPTP elections; however, they may be complicated for application to STV elections. On the other hand, ‘Prêt a Voter: All-In-One’ scheme [5] that we call PAV 2007, solves the problem of handling the STV elections efficiently.

In this work, we focus on STV elections and propose a protocol to be applied to large scale elections, in which political parties, whose votes remain below a certain barrier are eliminated. Our proposal prevents the loss of votes used for the eliminated parties and distributes them securely to the second choices of their voters. This protocol is then applied to PAV 2007 scheme, which we suitably modify to enhance the security of the ballot-construction and tallying phases.

In the original STV elections, voters give a preference ranking of the candidates (or political parties) rather than indicating a single choice on the ballot as in FPTP elections. In the first stage of tallying, only the first preference of each

Manuscript received November 10, 2008. This work is a part of the Ph. D. thesis presently being held at the Informatics Institute of Middle East Technical University.

O. Yücel is the co-founder of an information security company, Barikat Bilişim in Ankara (phone: 312-472-2055; fax: 312-472-2056; e-mail: okan.yucel@bigb.com.tr).

N. Baykal is a professor at the Informatics Institute of Middle East Technical University (e-mail: baykal@metu.edu.tr).

STV ballot is taken into account. If a candidate wins enough percentage of votes to achieve the winning quota, procedure terminates. If not, the votes of the candidate, who takes the least number of votes, are transferred to the other candidates. For that purpose, all ballots, on which the candidate having the least amount of votes are the first choices, are tallied again and the second choices on these ballots are distributed to the corresponding candidates. This procedure is repeated until one of the candidates achieves a vote percentage above the winning quota.

Some large scale elections have barriers (an example is the 10% barrier in Turkish Parliamentary elections), which eliminate the political parties that obtain a vote-percentage below a certain threshold. For preventing the problem of exhausted votes in such cases, we propose the following protocol in the tallying phase of STV elections: As in the original form, each voter indicates a preference ranking of the political parties on the ballot. The first step of tallying is the same, so in the first evaluation of ballots, only the first preference of each voter is taken into account. If all parties get enough votes to exceed the barrier, the tallying phase terminates. If not, in the second step, ballot tallying is repeated for all the voters whose first choice is a loser party that remains under the threshold. The second choice on these ballots is taken into account provided that it is a winning party above threshold. If the second choice is also a loser party, the successive choice on that ballot is used until one of the winner parties is encountered. Unlike the original STV elections, there is no need for repetition of tallying after this step. So, the election rule of eliminating the parties below the barrier is preserved, whereas no vote is exhausted. For the most suitable application, we suggest the use of PAV 2007, with our modification to enhance the security of the ballot-construction and tallying phases; and perhaps by adding blind signatures of all the observers of the parties entering the elections.

In Section II, we present a brief and comparative review of PAV 2005, PAV 2006 and PAV 2007 schemes. Section III discusses our modification in the STV protocol for elections with barriers and applies it to the tallying phase of PAV 2007. The security enhancement that we propose for the ballot construction phase of the PAV 2007 scheme is also given. In Section IV, we summarize our conclusions.

II. PRÊT A VOTER SCHEMES

We firstly describe the common properties of the Prêt a Voter schemes [3], [4] and [5] in part A; then give a comparative discussion in part B. Part C is devoted to the explanation of the cryptographic core used in ‘Prêt a Voter: All-In-One’ scheme [5], with vital details which cannot be found in the original reference.

A. Common Properties of ‘Prêt a Voter’ Schemes

Prêt a Voter schemes, PAV 2005 [3], PAV 2006 [4] and PAV 2007 [5] are all voter-verifiable electronic voting schemes, which provide voting receipts without any thread of coercion and ballot-selling. Ballots contain two columns as

shown in Fig. 1, say the left column including the candidate names in random order (or alphabetical order simply rotated by a random cyclic shift, say 2 downward shifts as in Fig. 1) and the right column having an encrypted number called ‘onion’ that is prepared as a function of the random order of candidates on this ballot. In the voting booth, voter marks his vote on the right column and the left column of the ballot on which the candidates are tabulated is removed after voting, as a part of the voting phase. The provided receipt includes only the right column that shows the marked vote and the onion; hence it is meaningless to anybody except the voter himself, who has seen the order of the candidates before the removal of the left column of the ballot.

Demet Diker	X
Efe Ersoy	
Ayşegül Ayaz	
Binnur Bulut	
Cihan Celasun	
	8HbWs6

Fig. 1. Ballot form used by original Prêt a Voter schemes (after voting but before removal of the left column).

There are k tellers (or clerks) of the mix network, each one having two sets of a public/private key pair. Ballots are prepared before the elections and the secret number, which indicates the candidate order on the left column of the ballot is encrypted one-after-another with $2k$ public keys of k tellers to form the onion. To decrypt this onion in the tallying phase, contribution of each teller is indispensable, because each layer of the encrypted onion can only be decrypted by one of the private keys of the corresponding teller. In order to preserve anonymity and break any linkage between the voter and decrypted vote, each teller randomly permutes the output list of ballots before submitting it to the next teller.

Voter verifiability is achieved by means of bulletin boards, which have universally accessible memory, and provide public communication, such that an election authority can write secured, unalterable and undeletable information on it and any other party can read. The receipt containing the right column with voter’s mark and the onion will be scanned after voting phase, and published onto the bulletin board by election authorities. Any voter can check for the existence and integrity of his receipt on the bulletin board and make an objection whenever any problem occurs. Perhaps the most attractive part of the Prêt a Voter schemes is that, although the receipts are publicized, nobody except the voter himself is able to understand the content of the vote, unless the onion is decrypted properly. However, decryption of the onion is distributed cleverly to k tellers, who also have to randomly shuffle the ballot lists that they receive, before submitting to the next teller; so that the link between the initial voter and the final tallied vote cannot be tracked unless all tellers are corrupted.

B. Differences Among 'Prêt a Voter' Schemes

Improvements brought by PAV 2006 over PAV 2005 are,

- i) preparation of ballot forms with two onions, the new-left onion on the left column being encrypted by the public key of the voting machine and decrypted by its private key whenever the voter casts his vote,
- ii) distributed generation of ballot forms, to enhance the security of ballot generation phase,
- iii) on demand-printing of ballots to resist the chain voting attack reported in [6],
- iv) size-independence of onion from the number of tellers,
- v) separation of shuffle and decryption phases to increase robustness, by first shuffling the received votes by a re-encryption mix network as suggested in [7].

The main improvement brought by PAV 2007 over PAV 2006 is its adjustment according to the needs of preferential elections, such as STV or Condorcet elections. Since each voter makes a ranking of the candidates in preferential elections, the order of the ballot candidate list needs to be totally randomized as in Fig. 2, instead of simply cyclically shifting the same alphabetically ordered list on each ballot. The implementation of previous PAV 2005 and PAV 2006 schemes may be complicated with this constraint, as compared to the implementation of the approval elections like FPTP or Borda Count. PAV 2007 takes care of this problem by treating the ballot as a whole in the ballot tallying phase. It makes use of the Paillier encryption [8] and exploits its homomorphic property in absorbing all ranked choices of the ballot within a single encrypted onion. Ballots are then shuffled by a re-encryption mix network composed of many tellers (or clerks).

Ayşegül Ayaz	5	dBOpTf
Efe Ersoy	3	66rdMv
Demet Diker	1	Abc123
Binnur Bulut	2	7YJLfN
Cihan Celasun	4	Vs68Hb

Fig. 2. Ballot form used by "Prêt a Voter: All-In-One" (PAV 2007) scheme (after voting but before removal of the left column).

C. Encryption and Decryption by Paillier Cryptosystem

Brief description of Paillier cryptosystem [8], [9] is needed at this point for making our contribution to "Prêt a Voter: All-In-One" (PAV 2007) scheme understandable. The Paillier algorithm has the additive homomorphic property; that is, an encryption of m_1+m_2 can be obtained from any encryption of m_1 and m_2 , as

$$E(m_1, r_1)E(m_2, r_2) \equiv E(m_1+m_2, r_1r_2). \quad (1)$$

In (1), the ciphertext $c = E(m, r)$ stands for the encrypted form of the plaintext m ,

$$c = E(m, r) = g^m r^n \pmod{n^2}, \quad (2)$$

r is chosen at random, n and g are fixed public elements defined by

- $n = pq$, the modulus where p and q are large primes
- $g \in \mathbb{Z}_n^*$, and a multiple of n

So, the pair (n, g) is the public key, and the pair (p, q) or equivalently $\lambda = \text{LCM}(p-1, q-1)$ is the private key of the Paillier's algorithm. As a consequence of (1), it is clear that

$$E(m, r)^k \equiv E(km, r^k). \quad (3)$$

Ballot Construction:

In Fig.2, the numbers on the rightmost are obtained as a result of successive encryptions performed by the clerks of the mix network. The order $\{1, 5, 4, 2, 3\}$ on the ballot shown in Fig. 2 of the candidates $\{1: \text{Ayşegül}, 2: \text{Binnur}, 3: \text{Cihan}, 4: \text{Demet}, 5: \text{Efe}\}$ is chosen randomly by the first clerk. First clerk also picks up the random numbers $r_1, r_2, \dots, r_5$ and prepares the encrypted numbers $c_1, c_2, \dots, c_5$ showing the candidate placed at each row, using (2) and the public key (n, g) . More specifically, the encrypted number that the first clerk prepares for the j 'th row is

$$c_j = E(M^i, r_j) = g^{M^i} r_j^n \pmod{n^2}, \quad (4)$$

where M is any integer greater than the number, v , of candidates, and $i=1,2,\dots,v$ shows the alphabetical order of the candidate corresponding to that row. Hence, for the example of Fig. 2, the candidate order $\{1, 5, 4, 2, 3\}$ is reflected directly to the exponents of M as follows

$$c_1 = E(M^1, r_1), \quad c_2 = E(M^5, r_2), \quad c_3 = E(M^4, r_3), \\ c_4 = E(M^2, r_4), \quad c_5 = E(M^3, r_5).$$

Each successive clerk of the mix network re-encrypts the numbers $c_1, c_2, \dots, c_5$ by multiplying them with the n 'th power of a random number t , so that the new value of the ciphertext becomes

$$\tilde{c}_j = c_j t^n = g^{M^i} r_j^n t^n = E(M^i, r_j t). \quad (5)$$

Equation (5) shows that, the plaintext M^i remains untouched while the random numbers picked by the first clerk are each time multiplied by a different random number t ; so that the first clerk, the only person who knows the candidate order, cannot trace the ballot. Since $\tilde{c}_j$ value of the j 'th row keeps the message M^i in encrypted form, the number i showing the alphabetical order of the candidate sitting at the j 'th row is always preserved and not affected by increasing number of re-encryptions. The numbers on the rightmost of the ballot in Fig. 2 are those $\tilde{c}_j$ values obtained by the last clerk at the end of the ballot construction chain.

Ballot Casting:

The voter casts his vote by ranking, i.e., filling up the numbers 1 to v in the right hand column; tears the ballot apart, destroys the left part and keeps the right part as the receipt after being scanned by the election authority at the voting booth. The scanned receipt is also announced at the web bulletin board for further checks demanded by the voter or any other party.

Ballot Tallying:

After the ballot is ranked by the voter, a single onion for each ballot having v candidates is calculated as follows:

$$E(m, r) = \prod_{i=1}^v E(M^i, r_i)^{k_i} = \prod_{i=1}^v \tilde{c}_i^{k_i}, \quad (6)$$

where k_i 's indicate the voter's ranking corresponding to the candidate, who is the i 'th one in alphabetical order. In the decryption of this onion, homomorphism of the Paillier algorithm leads to a very useful result:

$$\prod_{i=1}^v E(M^i, r_i)^{k_i} = E\left(\sum_{i=1}^v k_i M^i, \prod_{i=1}^v r_i^{k_i}\right). \quad (7)$$

The authority who has the private key (p, q) or equivalently $\lambda = \text{LCM}(p-1, q-1)$ corresponding to the public key pair (n, g) , extracts the useful message m in $E(m, r)$ given by (6). Because of the homomorphic property in (7),

$$m = \sum_{i=1}^v k_i M^i, \text{ and since } M > v, \quad (8)$$

retrieval of all choices of the ballot becomes possible. Because from (8) it is clear that (m / M^v) equals k_v , the $\{ \text{remainder of } m / M^v \}$ divided by M^{v-1} equals k_{v-1} ; and the remainder after dividing by M^{v-1} , again divided by M^{v-2} gives k_{v-2} and so on.

Example: In Fig. 2, the candidate order $\{1, 5, 4, 2, 3\}$ during the ballot construction is reflected to the subscript i of k_i 's, as $\{k_1, k_5, k_4, k_2, k_3\}$ and the voter's choice on the ballot shows that $k_1=5, k_5=3, k_4=1, k_2=2, k_3=4$.

If $M (>v=5)$ is chosen as 7, the following useful message m is obtained from (8).

$$m = \sum_{i=1}^v k_i M^i = 5 \times 7^1 + 3 \times 7^5 + 1 \times 7^4 + 2 \times 7^2 + 4 \times 7^3$$

So, m divided by 7^5 gives $k_5=3$, hence we understand that the alphabetically 5th candidate Efe is the third in the list of the voter,

$\text{Rem}\{m/7^5\}/7^4$ gives $k_4=1$,

which shows that the alphabetically 4th candidate Demet is the first choice of the voter,

$\text{Rem}\{\text{Rem}\{m/7^5\}/7^4\}/7^3 = k_3 = 4$, so Cihan is his 4th choice,

$\text{Rem}\{\text{Rem}\{\text{Rem}\{m/7^5\}/7^4\}/7^3\}/7^2 = k_2 = 2$, so Binnur is the

2nd, and finally, Ayşegül is the last choice of the voter since $\text{Rem}\{\text{Rem}\{\text{Rem}\{\text{Rem}\{m/7^5\}/7^4\}/7^3\}/7^2\}/7 = k_1 = 5$.

III. A NEW PROPOSAL

Large scale elections having vote-barriers such as the 10% barrier of Turkish Parliamentary elections eliminate the political parties, which obtain a vote-percentage below that threshold. People who vote for these parties feel a kind of injustice because of the invalidity and final loss of their votes.

On the other hand, STV elections in which each voter gives a ranked list of preferred political parties may be an excellent and democratic solution to the problem of exhausted votes. In the following, we propose an e-voting application for the elections having such barriers; first by modifying the STV protocol and then applying it to the "Prêt a Voter: All-In-One" (PAV 2007) scheme accordingly. Finally we propose two modifications in the ballot construction phase of PAV 2007, to enhance its security.

Modification of the STV Protocol:

Each voter gives a preference order (of say political parties entering the elections) on the ballot and the tallying phase of the applied voting scheme is modified as follows:

1) In the first evaluation of ballots, only the *first preference* of each voter is counted. If all parties get enough votes to exceed the barrier, the tallying phase terminates.

2) If not all the parties pass the barrier, calling the parties above the threshold *winners* and those below the threshold *losers*, ballot tallying is repeated for all the loser ballots having a loser party as the first choice. The choice on the ballot that is counted this time is the winner party, which is on top of all other winners in the voter's preference list. The new ballot-counts are added on the votes gained by *winners* in part (1) and the tallying phase terminates.

The above protocol preserves the election rule of eliminating the parties below the barrier, whereas no vote is exhausted and citizens are satisfied. The protocol should be accompanied by a secure control mechanism to publicly assure the robustness of the used scheme. To achieve this goal, observer teams assigned by each political party may play critical roles for increasing the robustness and accuracy of the voting scheme.

Application to "Prêt a Voter: All-In-One" (PAV 2007) Scheme and Enhancement of Its Security

The tallying phase of the PAV 2007 scheme [5], which is inherently very suitable for preferential elections can be easily modified according to the STV protocol suggested above. We strongly predict that such an e-voting scheme may become an indispensable alternative for paper-based elections, if the security of the overall system is enhanced. The weakest point in ballot-construction phase of the PAV 2007 scheme seems to be the over-dependence on the first clerk, who decides on the random candidate order of the ballots. He chooses this

random order, and encrypts it by using random seeds for each row of the ballot and the public keys of the election authority, who is responsible for tallying the votes. The re-encryptions performed by the following clerks in the network has the purpose of obscuring the path that the ballot follows. We propose at this point to enhance the security of the system by holding the first clerk in the chain more responsible of the encryption he performs, say by including his digital signature (or blind signature) as a part of the encrypted information, which may be checked whenever a need occurs. Such a modification increases the robustness of the scheme since any corrupted behavior is known to be traceable even in the future.

The second modification that we propose to enhance the security is in the re-encryption equation (5) that is used by the other clerks of mix network,

$$\tilde{c}_j = c_{j,t_j^n} = g^{M^i} r_j^n t_j^n = E(M^i, r_j, t_j) \quad (9)$$

in which we change the random number t by a row dependent random number t_j , so that each clerk in the network generates v (number of candidates and ballot rows) random numbers for each ballot, rather than a single one. The use of v random numbers by each clerk (or teller), will make the path more invisible and difficult to catch by the first clerk, who generates the crucial random ordering of the candidates on the ballot.

IV. CONCLUSION

The voter-verifiable e-voting scheme, ‘Prêt a Voter: All-In-One’ proposed in 2007 (so called PAV 2007 in this paper) [5], which supports single transferable voting (STV) seems to be a very suitable option for the elections having vote-barriers as in the Turkish Parliament elections. We modify STV elections protocol and the tallying phase of PAV 2007 accordingly. We then propose two modifications in the ballot construction phase of PAV 2007, to increase the security and the robustness of the overall system. The analysis we present for the cryptographic part of PAV 2007 is more detailed and inclusive than given in the original paper [5].

REFERENCES

- [1] D. Chaum, “Secret-Ballot Receipts: True Voter-Verifiable Elections,” *IEEE Security and Privacy*, 2(1): pp. 38–47, Jan/Feb 2004.
- [2] P. Y. A. Ryan, “A Variant of the Chaum Voter-Verifiable Scheme,” *Technical Report of University of Newcastle*, CS-TR:864, 2004. Also in *Workshop on Issues in the Theory of Security*, WITS 2005.
- [3] D. Chaum, P. Y. A. Ryan, and S. Schneider, “A practical, voter-verifiable election scheme,” *Technical Report of University of Newcastle*, CS-TR: 880, 2005.
- [4] P. Ryan, and S. Schneider, “Prêt a Voter with re-encryption mixes,” *Technical Report of University of Newcastle*, CS-TR:956, 2006.
- [5] Z. Xia, S. Schneider, J. Heather, P. Ryan, D. Lundin, R. Peel and P. Howard, “Prêt a Voter: All-In-One,” *LAVoSS Workshop On Trustworthy Elections (WOTE 2007)*, University of Ottawa, Ottawa, CANADA, June 20 - June 21, 2007.
- [6] P. Ryan and T. Peacock, “Prêt a Voter: a system perspective,” *Technical Report of University of Newcastle*, CS-TR:929, 2005.
- [7] C. A. Neff, “A verifiable secret shuffle and its application to e-voting,” in *Proc. 8th ACM Conference on Computers and Communications Security*, CSS’01, pp. 116–125, 2001.

- [8] P. Paillier, “Public-key cryptosystems based on discrete logarithm residues,” *Advances of Eurocrypt’99*, LNCS 1592, pp. 223–238, 1999.
- [9] P. Paillier, “Public key cryptosystems based on composite degree residuosity classes,” *Proc. Eurocrypt’99*, LNCS 1592, pp. 223–238, 1999.

An Intelligent and Automatic Eye Generation System from Only Fingerprints

Şeref SAĞIROĞLU, Necla ÖZKAYA

Abstract —Identifying people using body measurements has been devised and practised for a century. Although biometrics is a deeply studied field within the last three decades, relationships about biometrics have not been studied so far. In this study, we have focused on investigating the existence of any relationships between fingerprints and eyes. We have also strived to generate the eyes of a person using only fingerprint of the same person without knowing any information about eyes. Consequently, we have produced and introduced a new, automatic and intelligent system using a novel approach based on artificial neural networks to generate eyes from fingerprints among 0.4 % and 1.56 % absolute percent errors. Experimental results have shown that fingerprints and eyes are related to each other closely.

Keywords — information security, biometrics, artificial neural networks.

I. INTRODUCTION

THERE is an increased emphasis on the privacy and security of information recently. Biometrics is a marvellous technology that covers the unrealistic performance expectations compared with the existing alternatives like PINs and passwords. Biometric features are *reliable* as far as not being transferable easily, *peculiar* to individual as much as it represents him/her with his/her physical or behavioral attributes and *invariant* from beginning to end of the life. Since biometric based recognition systems has been largely investigated for 30 years, a lot of robust techniques and effective algorithms that present accurate security solutions are designed and proposed. In spite of all these developments in biometrics, there is no study on investigating relationships among the biometric features or obtaining one feature from another. We have noticed that most of the efforts in biometrics have been focused on how to improve the accuracy and processing time of the biometric systems, to design the more intelligent systems, and to develop more effective and robust techniques and algorithms [1], [2]. The scope of our study is intended to develop an

automatic and intelligent system capable of obtaining eyes from fingerprints without having any priori knowledge about eyes. In order to achieve that, an intelligent eye generation system from fingerprints (fingerprint to eyes: F2E) has been developed and introduced in this study. Although this research is in the biometrics field, it spans several disciplines such as image processing, pattern recognition, artificial intelligence, privacy and security, verification systems, soft computing and artificial neural networks.

This paper is organized as follows. Section 2 briefly describes background information on biometrics, automatic fingerprint identification and verification systems (AFIVSs), face recognition systems (FRSs) and artificial neural networks (ANNs) respectively. Section 3 highlights the novelty of the proposed technique, presents basic notation, definitions, performance metrics related to the F2E and explains the various steps of the new approach. Section 4 demonstrates our experimental results. Finally, the proposed work is concluded and discussed in Section 5.

II. BACKGROUND

Fingerprints are the most widely used biometric features due to their uniqueness, immutability and reliability [3]. The AFIVSs might be broadly classified as being *minutiae-based*, *correlation-based* and *image-based* systems [4]. A good survey about these techniques was given in [1]. In our study to get feature sets of the fingerprints a minutiae-based approach that relies on the comparisons for similarities and differences of local ridge attributes and their relationships to make a personal identification [5], [6], [7] has been preferred. Therefore details of the minutiae-based approach are given in this paper. The *minutiae-based approaches* attempt to align two sets of minutiae from two fingerprints and count the total number of matched minutia. In these approaches firstly it is extracted the minutiae from the fingerprint images correctly; then the comparison between two fingerprints is made using the two sets of minutiae parameters [4]. In general the comparison is based on representing two important attributes including *end points* and *bifurcations*. These main ridge characteristics are local discontinuities in a fingerprint image. The end point is defined as the point where a ridge ends suddenly. A bifurcation is defined as the point where a ridge separates or diverges into branch ridges [2], [5]. If these local attributes and their parameters are computed relative to the global attributes called singular points including core and delta points which are highly stable, rotation, translation and scale invariant, then these local attributes will also become

S. Sagioglu is with Gazi University, Engineering and Architecture Faculty, Computer Engineering Department, 06570 Ankara, Turkey. (corresponding author to provide phone: Tel: +90 312 2306503 Fax: +90 312 2306503; e-mail: ss@gazi.edu.tr).

N. Ozkaya is with Erciyes University, Engineering Faculty, Computer Engineering Department, 38039 Kayseri, Turkey. (phone: +90 352 4374901-32600, Fax: +90 352 4375784; e-mail: neclaozkaya@erciyes.edu.tr).

rotation, translation and scale invariant [8], [9]-[11]. Core points are the points where the innermost ridge loops are at their steepest. Delta points are the points from which three patterns deviate [10], [12], [13]. Many algorithms have been proposed to compute the singular points and orientation information of a fingerprint. The general methods to detect the singular points are Poincaré-based methods [14], intersection-based methods [10] or filter-based methods [15]. Ridge valley structure of a fingerprint image and local and global features which are used in minutiae-based AFIVSs are given in **Fig. 1**.

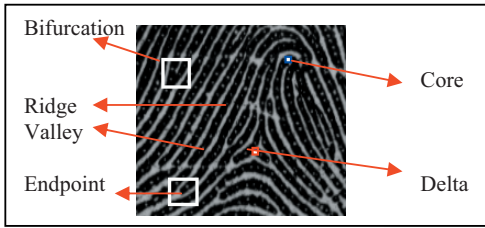


Fig. 1. Ridge valley structure and features of a fingerprint.

Main steps of the operations in minutiae-based AFIVSs are summarized as follows: selecting the image area, detecting the singular points, enhancing, improving and thinning the fingerprint image, extracting the minutiae points and calculating their parameters, eliminating the false minutiae, properly representing the fingerprint images with their feature sets, recording the feature sets into a database, matching the feature sets, testing and evaluating the system [16]. The performance of the minutiae-based techniques relies on the accuracy of all these processes. Especially the feature extraction and the use of sophisticated matching techniques to compare two minutiae sets often more affect the performance. *In the correlation-based AFIVS*, global patterns of the ridges and valleys are compared to determine if the two fingerprints align. The template and query fingerprint images are spatially correlated to estimate the degree of similarity between them. The performance of the correlation-based techniques is affected by non-linear distortions and noise present in the image. In general, it has been observed that minutiae-based techniques perform better than correlation-based ones [17]. *In the image-based approaches*, the decision is made using the features that are extracted directly from the raw image that might be the only viable choice when image quality is too low to allow reliable minutiae extraction [4].

Faces are probably the most common biometric characteristics used by humans to make personal recognition. Face recognition technology is well advanced. Because it is an active area of research with applications ranging from static, controlled mug-shot verification to dynamic, uncontrolled face identification in a cluttered background [5]. In general, a FRS consists of three main steps. These steps cover detection of the faces in a complicated background, localization of the faces followed by extraction of the features from the face regions and finally identification or verification tasks [18]. Face detection is a necessary first-step in face recognition systems, with the purpose of localizing and extracting the face region

from the background. It is a complex problem and many comprehensive face detection approaches have been proposed in the literature [19]. Face detection and recognition process is really complex and difficult due to numerous factors affecting the appearance of an individual's facial features such as 3D pose, facial expression, hair style, make up, etc. [20]. In addition to these varying factors, lighting, background, scale, noise and face occlusion and many other possible factors make these tasks even more challenging [18]. The most popular approaches to face detection and recognition [21] are based on either the location and shape of the facial attributes, such as the eyes, eyebrows, nose, lips and chin and their spatial relationships or the overall analysis of the face image that represents a face as a weighted combination of a number of canonical faces [22]. Also many effective and robust methods for the face recognition have been proposed [2], [5], [18]-[21], [23], [24]. As it has been mentioned before the aim of this study is establishing a relationship between eyes and fingerprints and generating the eyes from fingerprints with no knowledge about them. For this purpose to get the feature sets of the eyes a feature-based manual approach has been preferred [25] from the face recognition literature. We can explain the reason of this preference is that we used a minutiae-based approach to get the feature sets of the fingerprints. Actually minutiae-based approaches rely on the physical features of the fingerprints. Therefore it is reasonable that the feature sets of both fingerprints and eyes should be obtained in the same way. So, we decided to use feature-based approach to get the feature sets of the eyes. Cox et. al [25] used a template that was shaped from manually extracted 35 points for representing the each faces. They also used a dimensional feature vector computed from these points. We have increased the number of the eye reference points from 5 to 10 points for each eye for more accurate and sensitive representation. Also our eye feature sets are shaped from x-y coordinates of the eye reference points not distances or average measures as in [25]. Their method needs these modifications to use in our study. Because the feature sets do not contain enough information about eyes to re-generate the eyes properly. Therefore we have increased the number of the points and we used the coordinates of them simply. Our feature sets contain enough information about eyes for getting them again with high sensitivity.

III. PROPOSED INTELLIGENT AND AUTOMATIC EYE GENERATION SYSTEM FROM ONLY FINGERPRINTS

Fingerprint and face recognition topics have received significantly increased attention from both the academic and industrial communities as two of the few biometric methods that possess the merits of their reliability, performance and high accuracy. Proposed F2E that generates the eyes of a person from only fingerprint of the same person without having any information about the eyes will be very interesting innovation to the biometrics arena as a first step for an intelligent and automatic face generation system from only fingerprints. Also it will facilitate face recognition, security applications and police works. Implementation steps of the F2E to establish a relationship among fingerprints and eyes

(Fs&Es) can be mentioned as follows: A real multimodal database (MMDB) that includes Fs&Es belonging to 120 people was established. Fingerprint feature sets were obtained from the fingerprints. Enhancements, binarization, thinning, and feature extraction processes were applied to the acquired fingerprints to achieve this process. Eye feature sets were obtained from the eyes. The eyes were represented by 20 points. Training and test data sets were established to train and test the ANN predictors in the F2E. The training sets included pairs of Fs&Es while the test sets included only fingerprints. Eye feature sets of the test people were used in the evaluation process as the desired outputs. 80 data sets covering pairs of Fs&Es were used to train the ANN based F2E. The sizes of the input and the output vectors were 298 and 40, respectively. Suitable ANN structures and training algorithms were selected and parameters of them were determined. F2E was trained to generate eyes more realistically until achieving certain accuracy in learning. The ANN based system tested using 40 test sets covering only fingerprints. In order to test and evaluate the accuracy of the F2E, the test results were compared against to a variety of state-of-the-art methods [1].

F2E basically consists of a data enrolment module, a feature extraction module, an ANN module, a test & evaluation module and an eye reconstruction module. These modules are explained below. The first module of the system which is called the data enrolment module helps store biometric data of individuals into the biometric system database. During this process, Fs&Es of an individual have been captured to produce a digital representation of the characteristics. Two types of data are used in this study: Fs&Es. The second module of the system, extracts discriminative feature sets from the acquired data. Extracting local and global feature sets of fingerprints is achieved. This process includes fingerprint singularities, minutiae points and their parameters. Similarly feature sets of the eyes are obtained. The ANN module is used to analyze the existence of any relationship between Fs&Es. The ANNs have been applied to solve many problems [26]-[30]. Learning, generalization, less data requirement, fast computation, ease of implementation and software & hardware availability features have made the ANNs very attractive for biometric applications [23], [28]-[30]. Multilayered perceptron (MLP) is one of the most popular ANN architectures. Because of the MLP structure can be trained by many learning algorithms, it has been successfully applied to a variety of problems in the literature [27]. The ANN part of the system has been implemented with the help of the MLP structure that is trained with scaled conjugate gradient algorithm to find out any relationship between Fs&Es. The details of the scaled conjugate gradient algorithm can be found in [31], [32]. The ANN module can be encapsulated as an automatic and intelligent translator in which fingerprint images are converted to eye shapes efficiently. The ANN module is the most critical and important module of the system. Because, all modules of the system except the ANN module are on duty, either in pre-processing or post-processing of the main process that is done by the ANN module. So, if we investigate this module deeply, we can explain the working principles of the F2E properly.

Pre-processing steps include enrolling the Fs&Es to the system, extracting their feature sets in proper format, and arranging them in a suitable form that is convenient to the ANN module as an input or an output. Post-processing steps include the reconstruction of the eyes from feature sets which were obtained from the ANN and the evaluation process of the system. The ANN module operates its task in two stages: the training and the testing. In the training process, randomly selected input-output image sets covering Fs&Es belonging to the same people were used. The ANN structure and the training parameters were determined for achieving the training stage accurately. The training process is started with applying a person's fingerprint feature set to the system as an input and same person's eyes feature set as the desired output. The system achieves the training process with these feature sets according to the learning algorithm and the ANN parameters. Both Fs&Es feature sets are required in the training. Only fingerprint feature sets are used to obtain the eyes in the test. These fingerprints are unknown biometric data for the F2E. The outputs of the system for these unknown data indicate the success and reliability of the system. This success and reliability of the system must be shown clearly by evaluating the ANN outputs against to the proper metrics in proper way as it has been used in the literature. The block diagram of the ANN module is given in Fig. 2.

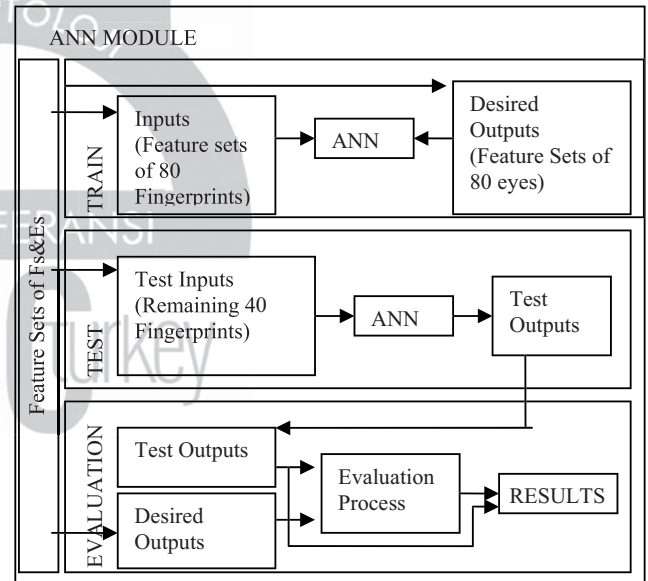


Fig. 2. The block diagram of the ANN module

In ideal situation, it is expected that a biometric-based recognition system will take the correct decision when a biometric feature is presented to the system. However in practice a biometric system can not be able to make perfect match decisions at all time. It can make two basic types of errors: (i) *False Match Rate (FMR)*: In the case of identification or screening, the biometric system incorrectly declares a successful match between the input pattern and a nonmatching pattern in the database. In the case of verification the pattern associated with an incorrectly claimed

identity. (ii) *False Non-match Rate (FNMR)*: In the case of identification or screening, the biometric system incorrectly declares failure of match between the input pattern and a matching pattern in the database. In the case of verification the pattern associated with the correctly claimed identity [33]. These traditional metrics of an ordinary biometric system are no longer appropriate to characterize the performance of the F2E. As it has been explained earlier, the aim of this study is to create eye shapes from only fingerprints without any information about eyes. Under these conditions, the system can not be evaluated properly with metrics of an ordinary biometric authentication system. So, we have decided to use appropriate performance metrics in this study. The results of the system may be evaluated by considering the following metrics: Mean squared error (MSE), sum squared error (SSE), average correlation, absolute percent error (APE) [34] and mean APE. In addition to these numerical evaluations a visual evaluation platform is created by drawing the ANN outputs and the desired outputs in the same sheets. Also another visual evaluation platform is presented by drawing the ANN outputs on the involved real face images of the test people. Consequently, for a more objective comparison, the performance and accuracy of the system have been evaluated and presented on the basis of the combination of these metrics for illustrating the qualitative properties of the proposed methods as well as a quantitative evaluation of their performance.

Eye reconstruction module facilitates the evaluation process, simplifies to comment on the results and presents to the users a comprehensive evaluation platform for visual sensing. In order to achieve these processes easily and efficiently, an automatic system has been proposed and a graphical interface that provides mechanisms for the system manager to manage the system properly is developed. This interface supplies all of the system parts to be controlled properly.

IV. EXPERIMENTAL RESULTS

The proposed eye generation system from fingerprints discussed in previous section is successfully implemented. The concept of generating eyes from fingerprints is a novel and challenging idea to biometrics technology. Dedicated software has been developed to conduct the experiments easily and efficiently. In our experiments, an MMDB having Fs&Es belonging to 120 people was established. In the training processes, 80 of 120 Fs&Es image sets were randomly selected from our MMDB. The remaining 40 image sets of Fs&Es were used for the test. The experimental image set used in the test process contains only fingerprint images of the test people and it is an unknown data for the system. The eye image sets of these test people are used for evaluation of the system performance. In the training process inputs and the outputs of the system were vectors sized 298 and 40, respectively. The feature vectors of fingerprints were computed using VeriFinger 4.1 SDK developed by Neuroteknologija. The reason of this preference is to establish an objective assessment for the F2E. This software is known as an effective, robust and reliable AFIVS in the field

of biometrics and uses a minutiae-based algorithm. Detailed explanation of algorithms, detailed information of fingerprint feature sets and their storage format are given in [35].

Producing the eyes as close to the real one as possible is critical for this study. In order to evaluate the performance of the system effectively, we have benchmarked our system against to the metrics MSE, SSE, APE, average APE, average correlation and human visual evaluation. The metrics MSE and SSE were computed before rescaling, while the other metrics MSE, SSE, average APE and average correlation were calculated after rescaling as $8.5079e-004$, 1.3613 , 28.6403 , $4.5825e+004$, 0.973047 and 0.997256 respectively.

These results indicate that the proposed system performs the tasks with high similarity measures to the desired values. For the purpose of more realistic and visual evaluation, test results achieved from only fingerprints were shown in Fig. 3. and Fig. 4. In order to compare the ANN outputs with their desired values, achieved test results and their desired values have been drawn on the same platform in Fig. 3. In a similar way 10 of 40 test results have been drawn on the real face images in Fig. 4. The APE values belonging to all test results were demonstrated in Fig. 5 for showing the overall system performance graphically.

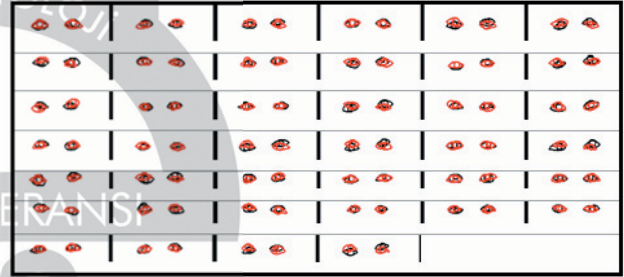


Fig. 3 Combined the ANN outputs and their desired values

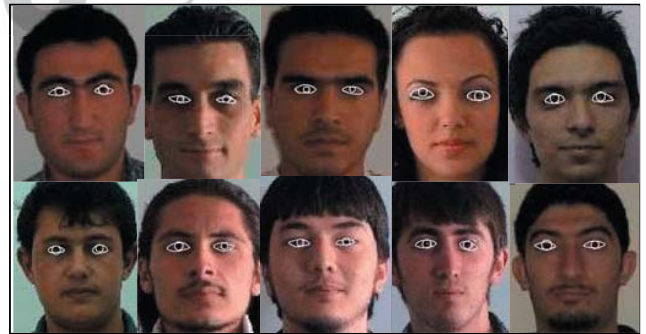


Fig. 4 The ANN outputs are drawn on the real face images

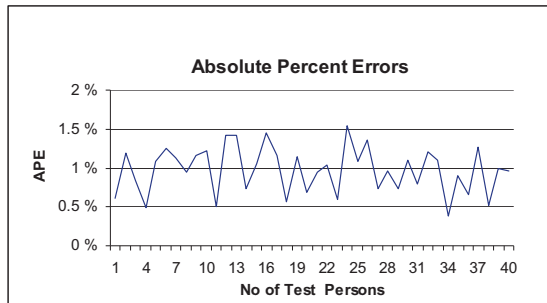


Fig. 5 APE values for all test results

Besides the numerical results indicate the system success clearly, graphical results also confirm this success as well. As it can be seen from Fig. 3, Fig. 4 and Fig. 5, the system is very successful in achieving eyes from fingerprints according to the evaluation metrics. Based on the observations, the proposed system can be used an intelligent and efficient translator that effectively converts fingerprints to eyes.

It is concluded that the fundamental novelty and diversity of the proposed approach over the most other studies in biometrics is that it is the first study that investigates the relationships between fingerprints and eyes. In addition it appropriately generates the eyes from fingerprints without any information about them.

V. CONCLUSION AND FUTURE WORK

The most important objective of this research is to investigate possible relationships between Fs&Es and to generate one using another. Consequently an intelligent F2E was designed, implemented and introduced for generating eyes from fingerprints without any need of eye information. In addition the relationships among Fs&Es are also experimentally shown. The results indicate for the first time that there are strong relationships among fingerprints and eyes. This is the first step of an automatic and intelligent system that is capable of accurately generating a face with all parts that include eyebrows, eyes, nose, mouth, ears and face border. The concept presented in this work would help to create some new research fields in biometrics in addition to being applied in many fields such as criminal applications. This approach also would lead to create new concepts, research areas and especially new applications in biometrics field.

REFERENCES

- [1] Maio, D., Maltoni, D., Jain A.K. and Prabhakar, S.: Handbook of fingerprint recognition, Springer-Verlag, New York, (2003)
- [2] Jain, L.C., Halici, U., Hayashi, I., Lee, S.B., Tsutsui, S.: Intelligent biometric techniques in fingerprint and face recognition, CRC press, New York (1999)
- [3] Kovács-Vajna, Z. M.: A fingerprint verification system based on triangular matching and dynamic time warping, *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, no. 11, pp. 1266-1276 (2000)
- [4] Lumini, A. and Nanni, L.: Two-class Fingerprint matcher, *Pattern Recognition*, vol.39, no.4, pp.714-716 (2006)

- [5] Hong L. and Jain, A.: Integrating faces and fingerprints for personal identification, *IEEE Transactions Pattern Analysis and Machine Intelligence*, vol. 20, no. 12, pp. 1295-1307 (1998)
- [6] Jain, A.K., Hong, L., Bolle, R.: On-line fingerprint verification, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 4, pp. 302-314 (1997)
- [7] Zhou, J., Gu, J.: Modeling orientation fields of fingerprints with rational complex functions, *Pattern Recognition*, vol. 37 no. 2, pp. 389-391 (2004)
- [8] Jain, A.K., Hong, L., Pankanti, S. and Bolle, R.: An identity authentication system using fingerprints, *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1365-1388 (1997)
- [9] Hsieh, C.T., Lu, Z.Y., Li, T.C., Mei, K.C.: An Effective Method To Extract Fingerprint Singular Point, *The Fourth International Conference/Exhibition on High Performance Computing in the Asia-Pacific Region*, pp. 696 -699. (2000)
- [10] Rämö, P., Tico, M., Onniva, V., Saarinen, J.: Optimized singular point detection algorithm for fingerprint images, *International Conference on Image Processing*, pp. 242-245 (2001)
- [11] Zhang, Q. and Yan, H.: Fingerprint classification based on extraction and analysis of singularities and pseudo ridges, *Pattern Recognition*, no. 11, pp. 2233-2243 (2004)
- [12] Wang, X., Li, J., Niu, Y.: Definition and extraction of stable points from fingerprint images, *Pattern Recognition*, vol. 40, no. 6, pp. 1804-1815 (2007)
- [13] Li, J., Yau, W.Y., Wang, H.: Combining singular points and orientation image information for fingerprint classification, *Pattern Recognition*, vol. 41, no. 1, pp. 353-366. (2008)
- [14] Kawagoe, M., Tojo, A.: Fingerprint pattern classification, *Pattern Recognition*, vol. 17, no. 3, pp. 295-303 (1984)
- [15] Nilsson, K., Bigun, J.: Localization of corresponding points in fingerprints by complex filtering, *Pattern Recognition Lett.*, vol. 24, pp. 2135-2144 (2003)
- [16] Ozkaya, N., Sagioglu, S., Wani, A.: An intelligent automatic fingerprint recognition system design, *5th International Conference on Machine Learning and Applications*, pp: 231 - 238 (2006)
- [17] Ross, A., Jain, A.K., and Reisman, J.: A Hybrid Fingerprint Matcher, *Pattern Recognition*, Vol. 36, No. 7, pp. 1661-1673 (2003)
- [18] Cevikalp, H., Neamtu, M., Wilkes, M. and Barkana, A.: Discriminative common vectors for face recognition, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 27, no 1, pp. 4-13 (2005)
- [19] Hjelmas, E., Boon K.L.: Face Detection: A Survey, *Computer Vision and Image Understanding*, vol. 83, pp. 236-274 (2001)
- [20] Bouchaffra, D. and Amira A.: Structural Hidden Markov Models for Biometrics: Fusion of Face and Fingerprint, In *Special Issue of Pattern Recognition Journal, Feature Extraction and Machine Learning for Robust Multimodal Biometrics*, Article in press, available online (2007)
- [21] Li, S.Z. and Jain, A.K.: *Handbook of Face Recognition*, NewYork: Springer Verlag (2004)
- [22] Jain, A.K, Ross, A. and Pankanti, S.: Biometrics: a tool for information security, *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125-143 (2006)
- [23] Yang, M.H., Kriegman, D.J. and Ahuja, N.: Detecting faces in images: a survey, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, No. 1, pp. 34-58 (2002)
- [24] Zhao, W., Chellappa, R., Phillips, P.J., and Rosenfeld, A.: Face recognition: a literature survey, *ACM Computing Surveys*, vol. 35, pp. 399-459 (2003)
- [25] Cox, I.J., Ghosh J. and Yianilos, P.N.: Feature-Based Face Recognition Using Mixture Distance, *Computer Vision and Pattern Recognition*, pp. 209-216 (1996)
- [26] Haykin, S.: *Neural Networks: A Comprehensive Foundation*, Macmillan College Publishing Company, New York, (1994)
- [27] Sagioglu, S., Beşdok, E., and Erler, M.: Artificial intelligence applications in Engineering I: artificial neural networks, *Ufuk publishing, Kayseri, Turkey* (2003)
- [28] Sagar, V.K., Beng, K.J.A.: Hybrid Fuzzy Logic And Neural Network Model For Fingerprint Minutiae Extraction, *International Joint Conference on Neural Networks*, pp. 3255 -3259 (1999)
- [29] Nagaty, K.A.: Fingerprints classification using artificial neural networks: a combined. structural and statistical approach, *Neural Networks*, Vol.14 pp. 1293-1305 (2001)

- [30] Maio, D. and Maltoni D.: Neural network based minutiae filtering in fingerprints, 14th International Conference on Pattern Recognition, pp. 1654 -1658 (1998)
- [31] The Mathworks, Accelerating the Pace of Engineering and Science, <http://www.mathworks.com/access/helpdesk/help/toolbox/nnet/nnet.htm?access/helpdesk/help/toolbox>, (2008)
- [32] Moller, M.F.: A Scaled Conjugate Gradient Algorithm. for Fast Supervised Learning, Neurall Networks, no.6, pp. 525-533 (1993)
- [33] Jain, A.K., Pankanti, S., Prabhakar, S., Hong, L., Ross, A. and Wayman, J.L.: Biometrics: A Grand Challenge, In Proceedings of the International Conference on Pattern Recognition, Cambridge, UK, August, vol. 2, pp. 935-942 (2004)
- [34] Novobilski, A. and Kamangar, F.A.: Absolute percent error based fitness functions for evolving forecast models, FLAIRS Conference, pp. 591-595 (2001)
- [35] Biometrical and Artificial intelligence Technologies, http://www.neurotehnologija.com/vf_sdk.html (2008)



RFID Sistemlerinin İncelenmesi ve Mikroişlemci üzerinde Güvenli Olacak Şekilde Gerçeklenmesi

Kaan BULUT, Berna ÖRS, İlker YAVUZ

Özet— Bu çalışmada, öncelikle muhtelif RFID sistemleri, sistem tasarım parametreleri açısından incelenmiş ve şifreleme açısından en uygun özelliklere sahip olan RFID sistemi türü belirlenmiştir. Daha sonra da bu RFID sistemi için güvenlik açısından en uygun kriptoloji algoritması belirlenmiş ve sistemde kimlik doğrulama için bu algoritma kullanılmıştır.

Bu çalışmada ilk önce RFID sistemlerinin ortak bir tanımı yapılmış ve bu sistemlerin sınırlamaları aktarılmıştır. Daha sonra RFID'nin alternatifi olan uzaktan tanıma sistemlerine kısa bir göz atılmıştır. Bunun ardından klasik bir RFID sisteminde olması gereken sistem elemanları tanımlanmış ve buradan sistem tasarımı sürecine geçilmiştir. Sistem tasarımı sürecinde RFID sistemleri değişik özellikleri açısından incelenmiştir. Bu kapsamda RFID sistemleri, çalıştıkları frekans, sahip oldukları menziller, sağladıkları güvenlik, harcadıkları bellek alanı ve güç açısından değerlendirilmiştir.

Son olarak RFID sistemlerinde kimlik doğrulamada kullanılmak üzere eliptik eğri kriptoloji sistemi seçilmiş ve mikroişlemci üzerinde gerçekleştirilmiştir.

Anahtar Kelimeler—RFID, Eliptik Eğri Kriptoloji Sistemi

I. GİRİŞ

Bu çalışmada radyo frekanslı kimlik doğrulama (RFID) sistemleri incelenmiştir. Bu sistemler içerisinde güvenlik için kimlik doğrulamaya uygun özellikte olanları belirlenmiştir.

RFID sistemlerinin günümüzde pek çok alanda birçok uygulamada kullanıldığı bilinen bir gerçektir. Bu uygulamalara örnek olarak kapı girişlerinde personel kartı okutma, mağaza çıkışlarında kurulan alarm sistemleri ve güncel bir örnek olarak da İstanbul'da Avrupa kıtasından Asya kıtasına geçerken köprüde kullanılan OGS ve KGS sistemleri gösterilebilir. Görüldüğü üzere bu sistemlerde karşılıklı bir bilgi aktarımı söz konusudur. Bu sebepten bu uygulamalar güvenlik açığına sahip olma tehdidiyle karşı karşıyadır. Bu güvenlik açığı ise istenmeyen kişilerin bu bilgileri ele geçirmesi veya değiştirmesidir. Bu istenmeyen durumun önüne geçilebilmesi için RFID sistemlerinin içerdikleri bilgiyi sadece doğru kişilere aktarmaları istenmektedir. Bunu sağlamanın

yolu ise bu sistemin alıcı ve verici olmak üzere iki tarafı arasında işleyen bir kimlik doğrulama protokolu oluşturmaktır. Bu çalışmada uygun bir açık anahtarlı kriptoloji sistemi kullanılarak bu doğrulama protokolu gerçekleştirilmiştir. Son bölümde istenen güvenlik hedeflerine uyup uymadığı belirlenerek bu sistemin gerçek bir sistem olarak uygulanabilip uygulanamayacağı tartışılmıştır.

II. RFID SİSTEMLERİNİN İNCELENMESİ

A. RFID Sistemlerinin Tanımı ve Sınırları

RFID sistemlerinin en temel özelliği sistem içindeki birimlerin birbirleriyle radyo frekansı aralığında haberleşmesidir [1]. Bu geniş frekans aralığında uygulamaya bağlı olarak uygun bir frekans seçilerek sistemin alıcı ve verici tarafı aynı frekansa ayarlanarak hava aracılığıyla uzaktan haberleşmeleri sağlanır. Bu frekanslar seçilirken uygulamanın tipi önemli olacağı gibi, yerel hukuki düzenlemeler de sınırlayıcı olmaktadır [2].

RFID sistemlerinin çoğunda istenen önemli bilgi aktarımı tek yönlüdür. Bilgiyi taşıyan ve istendiğinde karşı tarafa gönderen birime etiket, etiketi sorgulayıp bilgisini isteyen birime ise okuyucu denir. RFID etiketleri, ürün seri kodları gibi bilgileri saklayabilirler ve istendiğinde okuyucuya radyo frekansında elektromanyetik dalga üstünde gönderebilirler. En basit RFID sistemi bu iki birimin karşılıklı haberleşmesi ile oluşturulur.

B. RFID Sistem Elemanları

RFID sistemlerinde kullanılan elemanlar üç parçaya incelenebilir:

1. Veri taşıyıcı olan etiket
2. Veri sorgulayıcı olan okuyucu
3. Arka planda çalışan bir veritabanı

1) Etiket:

Etiket olarak adlandırılan parça, genel olarak istenen önemli veriyi taşıyan parçadır. Bu parça tipik olarak, veri saklamak amacıyla bir mikroişlemci ile bu veriyi istendiğinde radyo frekansında elektromanyetik dalgalar aracılığıyla okuyucuya göndermek üzere kullanılan bir antenden oluşur. Mikroişlemci ve anten ortak bir kılıfın içinde saklanırlar. Etiketlerin sınıflandırılmasında kullanılan en temel özellikleri kullandıkları gücün kaynağıdır. Bu özelliğe göre etiketler aktif, pasif ve yarı aktif olmak üzere üç sınıfa ayrılırlar.

Aktif etiketlerin üzerinde kendilerine ait bir güç kaynağı bulunur. Bu sayede aktif etiket dışarıdan herhangi bir

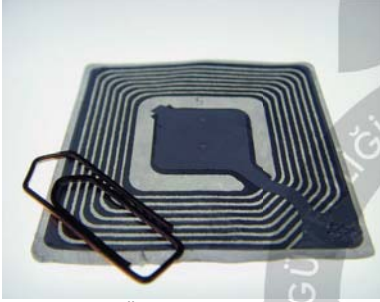
K. Bulut İstanbul Teknik Üniversitesi öğrencisidir.

B. Örs İstanbul Teknik Üniversitesi, Elektrik-Elektronik Fakültesi, Elektronik ve Haberleşme Mühendisliği Bölümü, 34469 Maslak, İstanbul'da Yardımcı Doçent Dr. olarak görev yapmaktadır. Tel: 0212 285 36 03, Fax: 0212 285 35 65, url: www2.itu.edu.tr/~orssi.

İ. Yavuz İstanbul Teknik Üniversitesi öğrencisidir. TÜBİTAK, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'nde görev yapmaktadır.

tetikleme gerekle kalmadan kendi işlemlerini başlatabilir. Bu işlemler arasında veri işleme, kriptografi işlemleri veya menzildeki diğer etiketlerle haberleşme gibi eylemler bulunur. Ayrıca aktif etiketler kendi ürettikleri işaretleri okuyucuya kendi kararları neticesinde gönderebilirler. Bunun yanı sıra aktif etiketler çok zayıf okuyucu sinyalleri ile de çalışabileceklerinden kullanılabilecekleri menzil daha geniştir ve bu da kullanıcıya daha fazla bir uygulama çeşitliliği sağlar. Aktif etiketler genelde okuyucudan yaklaşık 30 metre mesafeye kadar olan bir alanda işlem görebilirler [2]. Genelde mikroçipin içinde sahip oldukları verileri işleyebilmeleri için bir mikroişlemci, işledikleri verileri saklamak için bir oku-yaz bellek elemanı ve ne tür işlemler yapmaları gerektiğini bilmeleri için de etiketin işletim sistemini barındıran bir de sadece-oku bellek elemanı bulundurulur.

Aktif etiketler de enerji kullanımlarına göre ikiye ayrılırlar. Uyku moduna sahip olan etiketler, menzillerinde bir okuyucu olmadığı zaman uyku moduna geçerek enerji tüketimlerini sınırlandırılırlar. Bu özelliği olmayan aktif etiketler ise sürekli çalışma halindedirler ve bu sebepten dolayı, onlar da enerji tüketimlerini düşük tutmak için daha düşük veri iletim hızı ve bellek alanı kullanmayı tercih ederler. Şekil 1'de örnek bir etiket gösterilmiştir:



Şekil 1. Örnek bir RFID etiketi

Pasif etiketlerin ise, aktif etiketlerden en büyük farkları kendi içlerinde bir güç kaynağı bulundurmamalarıdır. Bu sebepten dolayı, okuyucudan kendilerine gönderilen elektromanyetik dalga tarafından beslenirler. Aynı zamanda okuyucuya geri veri göndermek gerektiğinde de okuyucudan gelen bu dalgayı kullanırlar ve geri-saçılım denilen bir yöntemle istenen bilgiyi okuyucuya geri gönderirler. Pasif etiket çok sınırlı bir güçle beslendiğinden iletebileceği veri çok sınırlıdır, en çok da seri numarası gibi kimlik bilgileri gönderilir. Bunun yanı sıra pasif etiketlerin menzili de oldukça sınırlıdır, çünkü ilettikleri veriyi kuvvetlendirecek güçleri yoktur, bu da gönderdikleri verinin belli bir mesafe sonra gürültüye karışıp kaybolacağını gösterir. Bu özelliklerinden ötürü pasif etiketlerin içlerinde mikroişlemci gibi çok güç harcayan birimleri barındırması mümkün değildir. Bunun sonucunda da kriptografi gibi bellek ve işlem gücü isteyen uygulamalarda kendilerine yer bulamazlar.

Aktif ve pasif etiketlerin yanı sıra bir de yarı aktif etiketler vardır. Bunlar pil yardımıyla etiketler de denir. Bu türdeki etiketler mikroçip devreleri içerisinde bir güç kaynağı barındırırlar ama bu güç kaynağını sadece kendi devrelerine güç vermek için kullanırlar. Okuyucu ile haberleşmek için ise gene pasif etiketlerde bahsedilen yöntemi kullanarak (geri-saçılım yöntemi) kendi güç kaynaklarını kullanmaktan

kaçınırlar. Bu tipteki etiketler kendi güç kaynaklarına dayandıklarından pasif etiketlerden çok daha fazla hesaplama gücüne sahiptirler ve pasif etiketlerden daha kısa bir sürede okuyucuya cevap vermeye hazır duruma geçerler, ancak daha fazla güç harcadıkları ve pahalı oldukları tahmin edilebilir. Ancak aktif etiketlerle kıyaslandıklarında okuyucuya kendi güçlerini kullanmadan cevap verdiklerinden daha az güç harcarlar ama aynı sebepten ötürü menzilleri daha kısadır.

2) Okuyucu:

Bir RFID sisteminde okuyucunun görevi, antenini kullanarak etiketleri uyarmak, etiketlerin içerdiği veriyi okumak ve bir ağ aracılığıyla bu veriyi bir sunucu bilgisayara göndermektir [4]. Okuyucular da belleğe sahip olup bu bellekte veri saklayabilirler. Bu açıdan okuyucu kavramı yanıltıcı olmamalıdır. Okuyucu, yapılan uygulamaya göre sabit ya da gezgin olabilir. Okuyucudan etikete giden kanala "ileri kanal", etiketten okuyucuya olan kanala ise "geri kanal" denir [3]. İleri kanalda okuyucu etikete elektromanyetik bir işaret göndererek, eğer etiket pasifse veya uyku modundaysa öncelikle onu uyandırır. Etiket pasif olması durumunda etiketin içeriğini ihtiva eden veri geri-saçılım yöntemiyle okuyucuya geri gönderilir ve okuyucu da bu veriyi ya kendi üstünde kaydeder ya da kendisine bağlı arka planda çalışan bir bilgisayarın veritabanına kaydeder. Etiket aktifse, etikette bir takım hesaplamalar yapılabilir ve oluşturulan veri okuyucuya geri gönderilir. Bu şekilde sürdürülen haberleşmede okuyucu yöneten bir konumdadır.

3) Veritabanı:

Okuyucu etiketin içeriğini alıp kendisine bağlı olan veritabanına yollar. Veritabanında bu veri kaydedilebilir veya bu verinin varlığı veri tabanında sorgulanabilir.

Ancak bu uygulamalarda unutulmaması gereken bir şey de veritabanı ile okuyucu arasındaki veri iletiminin mevcut durumda güvenli olmadığıdır. Etiket ile okuyucu arasındaki güvenliğin kriptolojik algoritmaları yardımıyla oluşturulabileceği önceden belirtilmişti, ancak veritabanı ile okuyucu arasındaki güvenliğin sağlanabilmesi için başka önlemlerin alınması gerektiği aşikardır.

C. RFID Sistem Ara Yüzü

RFID sisteminin elemanlarının birbiri ile olan haberleşmesi ve bu haberleşmede kullanılan yöntemler incelenecektir.

1) Etiket-Okuyucu Bağlantısı:

Etiket ile okuyucu girişlerine aynı frekansta bir işareti alacak şekilde bir rezonans devresi eklenir ve böylelikle başka frekanslardan gelen istenmeyen işaretler bastırılmış olur. Etiket aktif ise okuyucudan gelen bu işaret sadece etiketin uyandırılmasını sağlarken etiketin yarı aktif veya pasif olması durumunda ise üretilecek cevabın geri-saçılım yöntemiyle gönderilmesinde de işe yarar.

2) Veri Kodlama:

Okuyucu ile etiket arasındaki iletişim gerçekleştirilirken verinin de bir kodlama yapılarak gönderilmesi ise verinin iletim kanalına tam olarak uyum sağlamasını sağlayacaktır. Bu şekilde verinin enterferans ve başka etiketlerin işaretleriyle çarpışma gibi olgulardan sıyrılması da sağlanacaktır [1].

Veri kodlama yapılırken gözetilmesi gereken kriterler, kodlanan işaretin etikete taşıyabildiği güç miktarı, sahip

olduğu band genişliği ve diğer etiketlerin yol açtığı çarpışma olayına olan bağışıklığı olarak özetlenebilir [3].

Bu kriterler yakından incelendiğinde ilki için etikete taşınan gücün maksimum olması istendiği söylenebilir. İkinci kriter için ise kodlanmış işaretin az bir band genişliği kullanması istenmektedir ki bu sayede pek çok farklı işaret RFID uygulamasına ayrılmış sınırlı frekans bandında kendine yer bulabilsin. Son kriterde ise çarpışmaya olan bağışıklığın yüksek olması istenmektedir ki çok etiketin bulunduğu ortamlarda rahat çalışılabilsin. Aslında 2. ve 3. kriterlerin çok sayıda etiketin bulunduğu ortamlar için geçerli olduğu söylenebilir.

3) Modülasyon:

İletim ortamı olan hava yoluyla verimli veri transferi sağlamanın ikinci önemli yöntemi de gönderilen veriyi modüle ederek göndermektir. Radyo frekansında haberleşmede gönderilecek veri, modüle edilen bir taşıyıcı dalga üstünde taşınır. Üç tür sayısal modülasyon sınıfı vardır. Bunlar, genlik kaydırmalı anahtarlama (ASK), frekans kaydırmalı anahtarlama (FSK), ve faz kaydırmalı anahtarlama (PSK). Her üç türün de güç tüketimi, güvenilirlik ve band genişliği kriterlerini sağlama karakteristiği farklıdır.

Okuyucudan etikete giden işaret, etiketin pasif olması durumunda etiketten okuyucuya geri dönen işaretten çok daha güçlü olacağından bu işareti bastırması ihtimali vardır. Bu ihtimali önlemek amacıyla etiketten okuyucuya geri döndürülecek işaretin genelde gelen taşıyıcı dalganın frekansının bir oranı olan farklı bir taşıyıcı dalga frekansında döndürülmesi sağlanır. Bunu sağlamak amacıyla etikette bir frekans bölücü devresi kullanılır. Geri dönen dalganın taşıyıcısına alt-taşıyıcı denir.

1) Çarpışma:

RFID sistemlerinin tasarımında karşılaşılan önemli bir problem de okuyucunun menziline olmasına rağmen etiketin okunamamasıdır. Bu tip bir problemle genelde çok sayıda etiketin bulunduğu ortamlarda karşılaşılır. Bu sorunun kaynağı, genelde etiketlerin aynı anda gönderdikleri verilerin birbiri ile karışması veya veri kaybına yol açmasıdır. Bu tip bir durumda etiketin sağlıklı bir şekilde okunabilmesinden bahsedilemez. Başka türde etkenler de “çarpışma” denilen olgunun ortaya çıkmasına yol açabilir. Üç tür çarpışma olayı betimlenebilir:

- Tek okuyucu ve çok sayıda etiketin bulunduğu ortamda oluşan çarpışma
- Tek etiket ve çok sayıda okuyucunun bulunduğu ortamda oluşan çarpışma
- İki veya daha fazla sayıda okuyucunun aynı frekans aralığını kullanmaları neticesinde ortaya çıkan çarpışma olayı

Gelişen uygulamalar ile birlikte RFID sistemlerinde çok sayıda etiketin aynı ortamı paylaştığı uygulamalar yaygınlaşmaktadır. Bunlara örnek olarak, kütüphanecilik, havaalanı bagaj sistemi veya marketlerde ürünlerin kodlanması gibi uygulamalar verilebilir [2]. İşte bu tip uygulamalarda okuyucular, bir ortamda çok sayıda etiketin varlığını algılayabilecek şekilde tasarlanmalıdırlar. Eğer bu algılama yapılamazsa okuyucu aynı anda birden çok sayıda etiketin verisini almaya çalışacaktır ki bu durumun da çarpışmaya yol açacağı açıktır.

Bu çarpışmanın önüne geçilebilmesi için etiket ile okuyucu arasındaki iletişim için belli bazı kuralların belirlenmesi gerekmektedir. Bu kuralların tümüne *çarpışma önleme protokolü* denir [2]. Pasif etiketlerin sahip olduğu hesaplama yeteneği genelde düşük olduğundan ve birbirleriyle iletişim de kuramadıkları için pasif etiketleri içeren uygulamalarda çarpışmayı önleme meselesi ile okuyucu doğrudan sorumlu olacaktır. Genelde okuyucunun bu sorunu çözme yöntemi olarak belirlenen süreçte önce ortamda menzile giren tüm etiketlerin belirlenmesi, daha sonra da bu etiketlerin tek tek tanımlanması gerekmektedir. Tek bir etiketi diğerlerinden tecrit ederek adresleme ve bu yolla tanımlama tekniğine *tekilleme* denir. Tekilleme tekniği uygulayarak ortamda bulunan tüm etiketleri tanımlayan okuyucu daha sonraki aşamada istediği etikete bir tek onun adresini ya da tanımlama numarasını kullanarak ulaşabilir ve istediği veriyi çarpışma riski olmadan ondan alabilir. Okuyucu ile etiket arasındaki haberleşmede kullanılan çarpışma önleme protokolleri kullanılan frekansa ve uygulamaya göre standard hale getirilmeye çalışılmaktadır.

2) Frekansla ilgili düzenlemeler:

Yerel hükümet düzenlemeleri, her ülkede RFID sistemler için kullanılacak elektromanyetik spektrum parçasını belirlemektedir. Pek çok RFID sistemi ISM (Industrial-Scientific-Medical) bandında çalışmaktadır [3]. ISM bandı kullanımı, düşük güç harcayan ve kısa menzile sahip RF uygulamaları için lisans gerektirmeyen bir özelliğe sahiptir. Bu bandlar ITU tarafından belirlenmiştir.

Dünya çapında RFID sistemleri için belirlenen en önemli taşıyıcı frekansları 0-135 kHz, 13.56 MHz, 27.125 MHz, 40.68 MHz, 433.92 MHz, 869.0 MHz, 915.0 MHz, 2.45 GHz, 5.8 GHz ve 24.125 GHz olarak belirtilmiştir [1]. Bu frekansların kullanılabilirliği her ülkenin kendi yasal düzenlemeleri tarafından belirlenmiştir [2].

III. RFID SİSTEMLERİNDE GÜVENLİK KAVRAMI VE GÜVENLİĞİN SAĞLANMASI

A. RFID Sistemlerinde Güvenlik Kriterleri

Günümüzde pek çok alanda birçok uygulamada kullanılan RFID sistemleri güvenlik sorunuyla karşı karşıyadır. Bu sorunun kökeninde etiket ile okuyucu arasındaki veri transferinin gözlenebilir olması yatmaktadır. Etiket ile okuyucu arasında gönderilen veri araya giren bir gözlemci tarafından gözlenebilir. Bu gözlemci eğer ilgili teçhizata sahipse arada durmanın yanı sıra iletilen veriyi kopyalayabilir veya değiştirebilir. Bu tür saldırılar önemli verilerin aktarıldığı RFID sistemleri için kabul edilemez bir durumdur. Bu durumun oluşmasını engellemek için güvenliği sağlanamamış bir ortam olarak kabul edilen etiket ile okuyucu arasındaki hava ortamında verinin gizli bir şekilde gitmesi sağlanmalıdır. Bir RFID sisteminde güvenliğin ne kadar önemli olduğu kullanıldığı uygulamaya bağlıdır ve önce ilgili uygulamada güvenliğe ne derece ihtiyaç duyulduğu belirlenerek bu konuda ona göre tutum takınılmalıdır.

Eğer ilgili uygulamada güvenlik sağlanmasına ihtiyaç var ise kullanılacak RFID sisteminin de özellikleri düşünülerek uygun bir kriptografi algoritması belirlenmeye çalışılır. Bu algoritma

belirlenirken değerlendirilen temel ölçütler algoritmanın gerçekleştirilebildiği bellek alanı ile sisteme harcattığı güç miktarıdır. Tabi bu ölçütler değerlendirilirken bir de algoritmanın sisteme sağladığı güvenlik de gözlemlenmesi gereken bir diğer etmendir. Sonuç olarak, kullanılacak algoritma belirlenirken ihtiyaç duyulan bellek alanı, harcanılan güç ve bunun karşılığında sağlanan güvenlik bir denge oluşturacak şekilde en iyi çözümü sunan algoritma seçilmelidir.

Bunlarda akla ilk geleni aktif bir etiketin şifrelenmiş bir kimlik bilgisini içinde barındırması ve sık sık şifreleme amacıyla kullandığı anahtarı değiştirmesidir. Ancak anahtarın çok sık değiştirilmesi pil ömrünü oldukça hızlı tükettiğinden en fazla saatte bir anahtarın değiştirilmesi yöntemi önerilmektedir [5].

Geleneksel şifreleme yöntemleri arasında önerilen ikinci bir şifreleme yöntemi ise iki taraflı bir soru-cevap formatında bir şifreleme algoritması kullanmaktır. Buna örnek olarak gelişmiş şifreleme standardı (AES) algoritması verilebilir. AES, simetrik anahtar kullanan çok güçlü fakat fazla güç harcayan bir şifreleme algoritmasıdır.

Çok kullanılan kriptografi yöntemleri arasında RFID sistemleri üzerinde kullanılması önerilen bir diğer yöntem de açık anahtar şifreleme yöntemidir. Bir sonraki kısımda bu yöntem incelenmektedir.

B. RFID Sistemlerinde Kullanılması Olası Şifreleme Algoritmalarının İncelenmesi:

Açık anahtarlı krypto sistemlerinde iletişimin taraflarından sadece biri, elinde protokolde kullanılacak olan şifreleme ve şifre çözme anahtarlarını bulundururken, şifreleme anahtarını diğer tarafa herkesin görebileceği şekilde güvenli olmayan yoldan gönderir [6]. Diğer taraf da bu anahtarı alır, asıl istenen veriyi şifrelemede kullanır ve şifrelenmiş halde verisini güvenli olmayan yoldan karşı tarafa gönderir. Şifrelenmiş veriyi alan taraf ise kendi şifre çözme anahtarını kullanarak veriyi çözer. Şifreleme anahtarı güvenli olmayan bir yoldan gönderildiğinden şifre çözme anahtarının şifreleme anahtarı ile doğrudan bir bağı bulunmaması ya da şifreleme anahtarına bakılarak hesaplanmasının pratik olarak imkansız olması istenmektedir. Bu çalışmada açık anahtarlı krypto sistemi olarak eliptik eğri krypto sistemi kullanılacaktır.

C. Eliptik Eğri Kriptosistemi

Eliptik eğri kriptosistemi (EEK) [11][12] bir açık anahtar kriptosistemi olup RSA [13] açık anahtar kriptosistemine alternatif olarak 1985 yılında öne sürülmüştür. EEK'nin güvenilirliği ayrık logaritma problemine (ALP) dayanmaktadır. NESSIE (New European Schemes for Signature, Integrity and Encryption) tarafından yayımlanan rapora [14] göre EEK daha kısa anahtar ile RSA kriptosistemi ile aynı güvenlik seviyesi sağlayabilmektedir. Ayrıca aynı anahtar uzunluğu için EEK ile, RSA kriptosisteminden daha hızlı şifreleme yapılabilir [14].

K gibi bir alan üzerinde tanımlı bir Eliptik Eğri, aşağıda verilen Weierstrass denkleminin çözüm kümesi ve sonsuz O noktalarının birleşiminden oluşmaktadır [15].

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

Bu çözüm kümesi nokta toplama işlemi ile bir Abelian Grup oluşturmaktadır. Oluşturulan grubun birim elemanı y eksenini üzerinde olduğu varsayılan sonsuzdaki O noktasıdır.

Çözüm kümesi bir grup oluşturduğuna göre, eliptik eğri üzerinde nokta toplama ve nokta çarpma işlemleri gerçekleştirilebilmektedir. P_1 ve P_2 , E eliptik eğrisi üzerinde tanımlı iki nokta olmak üzere bu noktaların toplamı aşağıda verilen yöntemle bulunur;

P_1 ve P_2 noktaları bir doğruyla birleştirilir. Bu iki noktayı birleştiren doğru eliptik eğriyi Q gibi bir üçüncü noktada daha keser. Bu Q noktasının x eksenine göre simetrisinin alınmasıyla $P_1 + P_2$ değeri bulunur. Özel durumlar ele alınacak olursa, $P_1 = P_2$ gibi bir seçimde noktaları kesen doğru P_1 noktasından geçen eğriye teğet geçen doğrudur.

1) $GF(2^m)$ Alanı Üzerindeki Eliptik Eğriler

$GF(2^m)$ alanında tanımlı ya da başka bir deyişle alan karakteristiği $char(K) = 2$ olan eliptik eğrilerdir. $char(K) = 2$ olan eliptik eğriler için 1 eşitliği ile verilen Weierstrass denklemi sadeleştirilebilir [10]. Bu dönüşüm eğriye aşağıdaki gibi yansır;

$$E' : y^2 + xy = x^3 + a_2x^2 + a_6 \quad (2)$$

$GF(2^m)$ için $P = (x_1, y_1)$, $Q = (x_2, y_2) \in E$ eliptik eğrisi olmak üzere, $P + Q = (x_3, y_3) = P_3$ ve ilgili ara değerler aşağıdaki gibidir;

$$-P = (x_1, y_1 + x_1) \quad (3)$$

$$\lambda = \begin{cases} \frac{y_1 + y_2}{x_1 + x_2}, P \neq Q \\ x_1 + \frac{x_1}{y_1}, P = Q \end{cases} \quad (4)$$

$$x_3 = \begin{cases} \lambda^2 + \lambda + x_1 + x_2 + a_2, P \neq Q \\ \lambda^2 + \lambda + a_2, P = Q \end{cases} \quad (5)$$

$$y_3 = \begin{cases} \lambda(x_1 + x_3) + x_3 + y_1, P \neq Q \\ \lambda(x_1 + x_3) + x_3 + y_1, P = Q \end{cases} \quad (6)$$

Çarpmaya göre ters alma işlemini donanım olarak gerçekleştirme yüksek alan gerektirir. Değişkenler üzerinde dönüşümler yaparak projektif koordinat sistemine geçilirse, bu koordinat sisteminde çarpmaya göre ters alma sayısı azaltılır. Projektif koordinat sistemi bu çalışmada kullanılacaktır.

2) Eliptik Eğri Üzerinde Skaler Nokta Çarpma İşlemi

Eliptik eğri üzerindeki temel işlem bir noktanın k skaler sayısı ile çarpımıdır. Q ve P tanımlanan eğri üzerinde noktalar, k bir tamsayı olmak üzere nokta çarpma işlemi aşağıdaki gibidir;

$$Q = k.P \quad (7)$$

Skaler çarpma işlemi P noktasının kendisiyle $k-1$ defa toplanması anlamına geldiği için aşağıdaki gibi bir gösterim kullanılabilir;

$$Q = \underbrace{P + P + \dots + P}_{k-1 \text{ a defa toplanma}} \quad (4.49)$$

$Q = k.P$ çarpması için ikile-ve-topla algoritması kullanarak işlem gerçekleştirilebilir [6]. Bu teknikte k değerinin ikili tabanda gösterimi kullanılarak aşağıdaki gibi bir algoritma uygulanır.

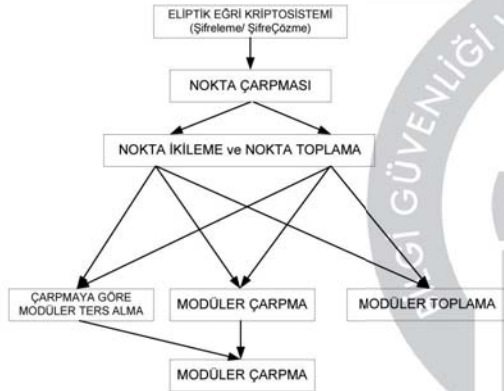
Algoritma 1 : İkile-ve-Topla Algoritması

GİRİŞ: $k = (1k_{n-2} \dots k_1 k_0)_2$ ve $P = (x, y)$

ÇIKIŞ: $Q = kP = (x', y')$

1. $Q \leftarrow P$
2. **for** i **from** $n-2$ **downto** 0 **do**
3. $Q \leftarrow 2Q$
4. **if** $k_i = 1$ **then**
5. $Q \leftarrow Q + P$

Projektif koordinatların kullanıldığı bir nokta çarpma işleminde; nokta çiftleme ve nokta toplama işlemleri mevcuttur. Bu iki işlemin gerçekleştirilmesi için de modüler çarpmaya göre ters alma, modüler çarpma ve modüler toplama işlemlerine ihtiyaç vardır. İşlemlerin hiyerarşisi aşağıdaki şekilde belirtilmiştir.



Şekil 2. Nokta Çarpma İşlemi ve Bileşenleri

D. Bir RFID Sistemi İçin EEK'nin Gerçeklenmesi

Bir RFID sisteminde kurulacak olan ECC algoritmalı şifreleme sistemi doğal olarak karşılıklı işlemler yapan bir okuyucu ile aktif bir etiketten oluşacaktır. Aktif etiketin içinde şifreleme hesaplamaları yapabilmek için bir adet mikroişlemci ve yeteri kadar bellek alanı gerekmektedir.

Bu çalışmada mikroişlemci birimi olarak Silicon Laboratories firmasının C8051F060 uygulama geliştirme kiti kullanılmıştır [7]. Bu kitle bir adet seri port bulunmaktadır ve eliptik eğri üzerinde hesaplamalar yapıldıktan sonra karşı tarafa gönderilmesi istenen veri seri port üzerinden gönderilecektir. Seri porta da HAC-UM 96 RF modem bağlandığında üretilen veri hava yoluyla gönderilmeye hazır hale gelecektir [8]. Karşı taraf için de benzer yapıda bir blok kurulduğunda güvenli yoldan bir RFID sistemi kurulmuş olacaktır.

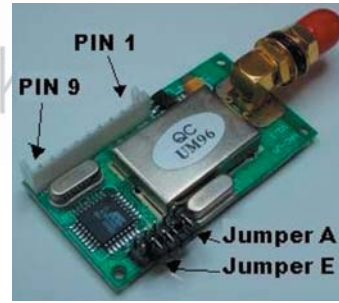
1) C8051F060 Mikrokontrolör Kiti ve HAC-UM96 RF Modem:

Güvenlik protokolünün gerçekleştirilmesi için etiketin de okuyucu gibi kompleks işlemleri yapabilmesi istenmektedir. Bu sebepten dolayı iletişimin iki tarafı da hesaplama kapasitesi bakımından birbirine eş kabul edilmekte ve simetrik olacak şekilde hem etiketin içinde hem de okuyucunun içinde aynı mikrokontrolör birimi kullanılmıştır.

Mikrokontrolörün dış dünya ile bağlantısı RS-232 protokolünü kullanan UART üzerinden bir RF modeme bağlanarak gerçekleştirilecektir. Bu modemın bazı özellikleri şu şekilde belirtilmiştir:

- İletim sırasında aktarılan güç oldukça düşüktür ve 10 mW kadardır.
- 433 MHz civarında ayarlanabilen 8 kanal kullanan taşıyıcı frekansı kullanmaktadır.
- Gauss frekans kaydırmalı anahtarlama (GFSK) kullanan sistem havada meydana gelebilecek olan girişime (enterferans) ve iletilen bitlerde meydana gelebilecek hatalara karşı dayanıklıdır ve bit hata oranı oldukça düşük olmaktadır.
- 300 ile 500 metre arasında değişen güvenilir iletim menziline sahiptir.
- Modem, bir UART cihazıdır ve ona gönderilen veri uygun çerçeve içinde gönderilmelidir. Bu cihaz için uygun çerçeve saniyede 9600 bit olmaktadır.
- 2 tane seri portu ve 3 tane arayüzü bulunmaktadır. Kullandığı arayüzler, TTL düzeyinde UART, RS-232 ve RS-485'dir.
- Düşük güç tüketimine ve uyku modu özelliğine sahiptir. Veri gönderirken maksimum 40 mA akım kullanırken veri alırken maksimum 30 mA akım kullanır ve uyku moduna girdiğinde maksimum 20 μ A akım çekmektedir [8].

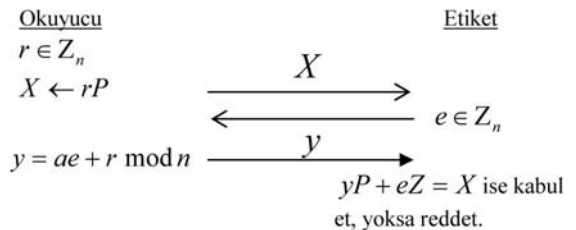
RF modemın resmi ise Şekil 3'de gösterilmektedir.

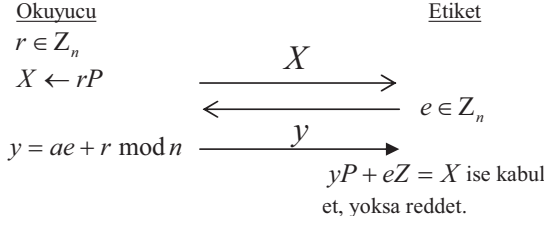


Şekil 3. HAC-UM96 RF modemın resmi [8]

2) Kimlik Doğrulama Protokolü

Kimlik doğrulama protokolü sistemin iki tarafı arasında veri transferi başlamadan önce iki tarafın da birbirini sınaması ve tanımlaması aşamasını barındırır. Bu sistemde kullanılan protokol Şekil 4' de verilmiştir [9].





Şekil 4. Schnorr'un kimlik doğrulama protokolü [9]

Bu tanımlama protokolü gereği ilk aşamada kullanılan parametreler tanıtılmalıdır.

r : okuyucunun kullandığı gizli şifreleme anahtarı

P : eliptik eğri üzerinde tanımlanmış x ve y koordinatları olan bir nokta

e : etiketin kullandığı açık parametre

a : okuyucunun kullandığı gizli parametre

Z : $Z = -aP$ işlemi sonucu ortaya çıkar. Bu işlem okuyucunun içinde yapılır ve işlemin sonucu olan Z parametresi etikete gönderilir.

Burada gösterilen $X = rP$ işlemi eliptik eğri skaler çarpma işlemidir.

Burada bahsedilen parametrelerin hepsi de 163 bit uzunluğundadır, yani 163 bitlik EEK uygulanmaktadır.

IV. SONUÇLAR

Bu çalışmada ilk önce çeşitli RFID sistemleri incelenmiştir. Bu incelemeler sonucunda güvenli uygulamalar için aktif etiketlerin uygun olduğu görülmüştür. ISM bandında 433 MHz frekansını kullanan bir RFID sisteminin güvenli olarak gerçekleştirilmesi yapılmıştır. Kimlik doğrulama için açık anahtarlı kriptoloji sistemi olan eliptik eğri kriptoloji sistemi kullanılmıştır. EEK 163 bit kullanılarak gerçekleştirilmiştir.

Kimlik doğrulama için Schnorr tarafından önerilen kimlik doğrulama protokolü kullanılmıştır [9]. Bu protokol 8-bitlik bir mikroişlemci üzerinde gerçekleştirilmiştir. Okuyucu ve etiket arasındaki haberleşme mikroişlemci setine seri porttan bağlanmış RF modemler kullanılarak gerçekleştirilmiştir.

V. KAYNAKLAR

- [1] K. Finkenzeller, RFID Handbook, Carl Hanser Verlag, Münih, 2003.
- [2] H. Lehpamer, RFID Design Principles, Artech House, Norwood, 2008.
- [3] S. A. Weis, Security and Privacy in Radio-Frequency Identification Devices, *Master Thesis*, MIT, Massachusetts, 2003.
- [4] D. E. Brown, RFID Implementation, McGraw-Hill, New York, 2007.
- [5] A. Parmar, D. Byambajav, B. Englert, Evaluating and improving the security of RFID tags in shipping containers, Final Report on METRANS Project, California State University Long Beach, 2007.
- [6] A. Menezes, P. van Oorschot, ve S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
- [7] Silicon Laboratories C8051F060/1/2/3/4/5/6/7 datasheet <http://www.keil.com/dd/docs/datashts/silabs/c8051f06x.pdf>.
- [8] HACCUM UM96 Datasheet, User Manual http://www.sparkfun.com/datasheets/RF/UM96_Tutorial_Manual.pdf.
- [9] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls ve I. Verbauwhede, An Elliptic Curve Processor Suitable For RFID-Tags, Katholieke Universiteit Leuven, ESAT/COSIC, Belçika ve Philips Araştırma Laboratuvarları, Eindhoven, Hollanda, 2006.
- [10] S. B. Örs Yalçın, Hardware Design of Elliptic Curve Cryptosystems and Side-Channel Attacks, *PhD Thesis*, Katholieke Universiteit Leuven, Belçika, 2005.
- [11] N. Koblitz, Elliptic Curve Cryptosystem. *Mathematics of Computation*, Vol. 48: 203-209, 1987.
- [12] V. Miller, Uses of Elliptic Curves in Cryptography. In H. C. Williams, Editor, *Advances in Cryptology: CRYPTO'85, volume 218 of Lectures Notes in Computer Science*, Springer-Verlag, 417-426, 1985.

[13] R. L. Rivest, A. Shamir ve L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2):120-126, February 1978.

[14] NESSIE Consortium, NESSIE Security Report, *Technical report NESSIE*. <http://www.cosic.esat.kuleuven.ac.be/nessie/deliverables/D20-v2.pdf>, 2003.

[15] L. C. Washington, Elliptic curves: number theory and cryptography, Boca Raton : Chapman & Hall/CRC, 2003.

Proposing a Wireless PKI Model Optimized for M-Commerce Applications

Fariborz Mousavi MADANI, Iran BIMAR

Abstract—The rapid advances in wireless mobile communication technology and the growth of e-commerce applications have naturally led to the development of e-commercial services on wireless medium through mobile phones. As more mobile devices are developed, security issues of crucial importance to the wired environment are resurfacing and creating a similar degree of impact. PKI which assures security issues in wired networks has difficulties to be implemented in wireless medium due to the limited performance of mobile phone such as less memory and less powerful CPU. Therefore a wireless PKI customized to mobile phone is needed. In this paper we present a wireless PKI for mobile phone based on the work presented in Ref [1].

Keywords— Mobile phone, M-Commerce, Wireless Public Key Infrastructure, Digital certificate, SCVP.

I. INTRODUCTION

MOBILE wireless telephones, or cell phones, are those who have shortwave analog or digital transmission capabilities that allow users to establish wireless connections to nearby transmitters. Today's cell phone is rapidly evolving to integrate with PDAs, thus providing users with increased wireless email and Internet access. Mobile phones with information-processing and data networking capabilities make a new field of study named Mobile Commerce. Mobile commerce is an electronic commerce contains some services and applications, brought to mobile users via mobile devices such as palmtops, PDAs. In order to deliver these mobile services and applications over the Internet in a secure, scalable and manageable way, new architectures and protocols customized to wireless internet are essential. Basic Security services defined in the literature [1]-[10] are confidentiality and integrity of data, authentication, and non-repudiation. Architectures and protocols customized to wireless Internet must fulfill these services as those in the wired Internet. Nowadays many security protocols on Internet and most security applications for e-commerce are based on public key cryptography [1]. Public key infrastructure (PKI) is an integrated secure platform based on asymmetric encryption, with a collection of mechanisms for creating, distributing and using public key certificates to transmit user's public key and user's identity in a secure and reliable way. Its combination with wireless network technology leads to the wireless PKI (WPKI).

WPKI optimizes the traditional PKI and applies it to the wireless environment. Mobile phones have many limitations of screen size, input utility, processing power and memory. Especially, the processing power of many mobile terminals is quite limited. This must be taken into account when cryptographic algorithms are chosen. Therefore, the number of cryptographic algorithms must be minimized and small-sized algorithms must be chosen to reduce RAM requirements as low as possible [1], [2]. Wireless data network presents more constrained communication environment such as less bandwidth and has different protocol compared to wired internet protocol. In this paper, we propose a Wireless Public Key Infrastructure (WPKI) model for mobile commerce. For this purpose we will make some enhancements in WPKI model presented in [1]. Section 2 introduces public key infrastructure, its problems and limitations in mobile phone. In Section 3 we describe the reference WPKI model, its limitations and propose an enhanced model to acquit limitations. The performance of the proposed WPKI is analyzed in Section 4. Section 5 concludes this paper.

II. PKI AND ITS LIMITATIONS

Public key infrastructure (PKI) is an integrated secure platform based on asymmetric encryption, with a collection of mechanisms for creating, distributing and using public key certificates to transmit user's public key and user's identity in a secure and reliable way. In the PKI's entities show in Figure 1, Certificate and CRL forms the core of PKI, hence verifying the correctness of certificate is a fundamental building block for public key applications. While digital certificates provide a secure mechanism to identify and authenticate an entity via the verification of a digital signature, there must also be mechanisms in place to validate that certificate and the associated private key. This issue is commonly known as certificate validation and is based on the concept of certificate revocation. Certificates may be revoked for various reasons, including, but not limited to, change of name, change of association between subject and CA and compromise or suspicion of compromise of the corresponding private key. There must be mechanisms in place for a requesting entity to retrieve status information of a certificate that may have been revoked. One method, as defined by [RFC3280] defines the concept of certificate revocation lists (CRLs) that are used to convey information about certificates revoked by a Certification Authority (CA). Although CRL's are in use in many environments, they have some properties that make their

School of Engineering, Alzahra University, Tehran, Iran.
mosavif@alzahra.ac.ir, iran_bimar@yahoo.com

use in mobile environments unattractive [6]. In particular, the use of CRL's requires additional processing by the client that may be difficult to implement in a constrained mobile device. Also, CRL's are often quite large in size and thus raise network latency and bandwidth issues [6].

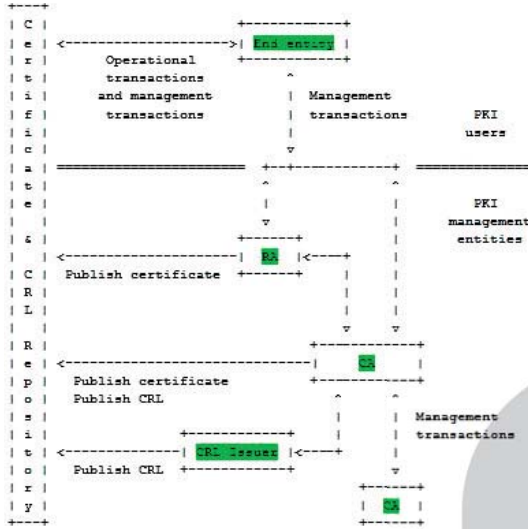


Fig. 1. PKI entities

The explosive growth of the Internet has fuelled the creation of new and exciting information services. Mass-market, handheld wireless devices present a more constrained computing environment compared to desktop computers. Because of fundamental limitations of power and form-factor, mass-market handheld devices tend to have [7]:

- Less powerful CPUs
- Less memory (ROM and RAM)
- Restricted power consumption
- Smaller displays
- Different input devices (e.g., a phone keypad)

Similarly, wireless data networks present a more constrained communication environment compared to wired networks. Because of fundamental limitations of power, available spectrum, and mobility, wireless data networks tend to have [7]:

- Less bandwidth
- More latency
- Less connection stability
- Less predictable availability

In order to apply wireless PKI to mobile phone through wireless internet with the same level of security as that of wired internet, the following requirements must be satisfied [1]:

- Select optimal digital signature algorithm to be calculated in mobile phone
- Minimize data size to be stored in mobile phone and to be transmitted through wireless bandwidth

- Optimize CMP protocol to be processed in mobile phone and through wireless bandwidth
- Optimize certificate validation scheme

III. WPKI ARCHITECTURE

In this model, Yong Lee and her co-workers apply X.509 certificate as certificate of mobile phone, because verification of mobile certificate is not difficult in the server with adequate performance. Assumptions of this model are:

- Communication is between mobile phone and server as content provider, and excludes communication between mobile phones
- This model has one CA
- End entity such as a mobile phone or server has only one public key pair and one certificate for one purpose

In this model, as Figure 2 shows, CA issues a certificate, publishes its directory, and sends only URL of the certificate to the mobile phone. When a mobile phone communicates with server, the mobile phone sends URL of the certificate to server, not the certificate itself.

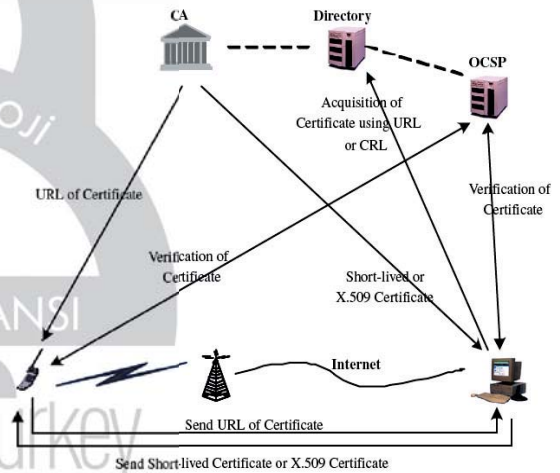


Fig. 2. WPKI model

The server can easily access the directory and acquire the certificate. Authors introduce Online Certificate Status Protocol (OCSP), and the mobile phone delegates OCSP to validate certificates rather than validation in the mobile phone by itself.

For digital signature algorithm, mobile phone cannot measure the generation time of RSA 1024-bit public key pair because it takes so long time. Thus, the alternative digital signature algorithm with same security level was required and they chose ECC-based Elliptic Curve Digital Signature Algorithm (ECDSA) that is recommended by [8] and [9]. For ECDSA 163-bit key size, equivalent to RSA 1024-bit key size; it takes shorter time to generate public key pair in mobile phone than RSA algorithm [1].

For Certificate and CRL profiles they describe Wireless X.509 certificate profile issuing for mobile phone and server, and short-lived certificate profile issuing for server to reduce

verification load of mobile phone. X.509 certificate consists of basic field and extension field. To reduce size of certificate they omitted some extension fields. Their profile defines that names should not be reused for different entities and CAs conforming to this profile should not generate certificates with unique identifiers. Authority key identifier and subject key identifier are used to identify the public key where an issuer and/or subject have multiple signing keys. The private key usage period extension allows the certificate issuer to specify a different validity period for the private key than validity period of the certificate. They also assume that the private key usage period is same as the validity period of the certificate and do not use this extension. For the issuer alternative names extension, because they assume one CA, this extension was omitted. The extended key usage indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension. Since applying OSCP for certificate validation in this model, they use domain information and authority information access extension for specifying how to access of OSCP server. How a mobile phone securely requests a certificate to CA and CA issues it to the mobile phone in this model? They consider that the followings are requirements of certificate request protocol as mentioned in [10]:

- Certificate request message is constructed at mobile phone. This value should include a public key, end-entity's reference number like as ID and password. They assume that other requested certificate fields, and additional control information related to the registration process are made in out-of-band
- A POP (Proof of Possession) of the private key corresponding to the public key for which a certificate is being requested value is included in certificate request message
- Method that the certificate request message is securely communicated to a CA

To satisfy these requirements, they designed wireless certificate management protocol and developed this protocol on mobile phone. Since a password could be transferred to a CA by hash value, confidentiality of the password could be guaranteed. They use the public key as one time information for prevention of replay attack.

For short-lived certificate, the mobile phone validates the certificate through verifying only signature and valid period in the certificate. The server acquires a certificate from directory using URL of the certificate received from the mobile phone, and sends mobile phone its certificate with CA's certificate and ARL (Authority Revocation List) together.

The assumptions made in this model require us to have just one CA. So if the number of CAs exceeds one, certification path cannot be supported. Moreover, an entity is forced to have just one certificate. So limitations of this model are summarized as:

- No more than one CA
- No more than on certificate for mobile user

Having one CA decreases flexibility of the model. Because lots of organizations have their own rules which rises consistency issues. Also, it is difficult to convince all users to take their certificates from one CA. This model is more suitable for domestic markets due to limitations of one CA and one certificate per user.

A. The Proposed WPKI Architecture

In this section we briefly describe Server-Based Certificate Validation Protocol (SCVP) as an alternate for Certificate Validation Scheme in this model. As Figure 3 shows, we substituted OSCP with SCVP.

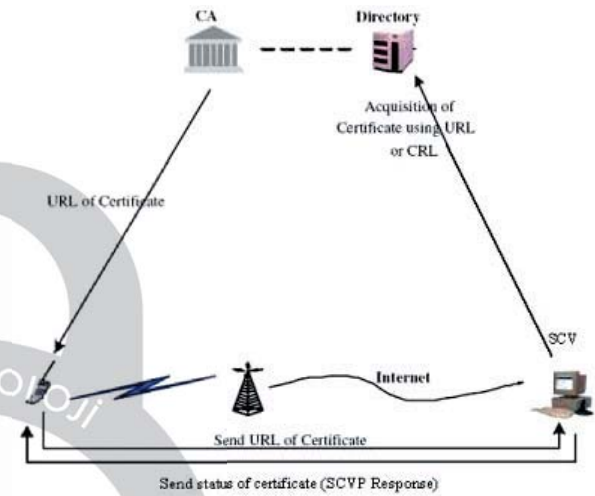


Fig. 3. SCVP Based WPKI

The Server-Based Certificate Validation Protocol (SCVP) allows a client to delegate certification path construction and certification path validation to a server. The path construction or validation (e.g., making sure that none of the certificates in the path are revoked) is performed according to a validation policy, which contains one or more trust anchors [9]. It allows simplification of client implementations and use of a set of predefined validation policies. With this protocol we can exclude the assumption of having one CA from Model.

B. SCVP

As we mentioned before mobile phone is burdened with the overhead of constructing and validating the certification paths. SCVP reduces this overhead for two classes of certificate-using applications [9]. The first class of applications wants just two things: confirmation that the public key belongs to the identity named in the certificate and confirmation that the public key can be used for the intended purpose. Such clients can completely delegate certification path construction and validation to the SCVP server. This is often referred to as delegated path validation (DPV).

The second class of applications can perform certification path validation, but they lack a reliable or efficient method of constructing a valid certification path. Such clients delegate certification path construction to the SCVP server, but not validation of the returned certification path. This is often referred to as delegated path discovery (DPD) [9]. In

constrained execution environments, such as telephones and PDAs, memory and processing limitations may preclude local implementation of complete, PKIX compliant certification path validation [9]. The Delegated Path Validation (DPV) protocol allows a server to validate one or more public key certificates on behalf of a client according to a validation policy. If the DPV request does not specify a validation policy, the server response must indicate the validation policy that was used. Policy definitions can be quite long and complex. Hence mobile phone can simply reference a validation policy or accept the DPV server's default validation policy. The certificate to be validated must either be directly provided in the request or unambiguously referenced [9]. Based on our WPKI Model, mobile phone prepares URL of certificate in DPV request. The DPV server must have the certificate to be validated. The DPV server must include either the certificate or an unambiguous reference to the certificate (in case of a CA key compromise) in the DPV response [9] and [10].

For the client to be confident that the certificate validation was handled by the expected DPV server, the DPV response must be authenticated, unless an error is reported (such as a badly formatted request or unknown validation policy). There are two mechanisms for validation of SCVP responses [9]:

- Based on the client's knowledge of a specific SCVP server key (simple key validation)
- Based on validation of the certificate corresponding to the private Key used to protect the SCVP response. (SCVP Server Certificate Validation)

The simple key validation method is where the SCVP client has a local policy of one or more SCVP server keys that directly identify the set of valid SCVP servers. Mechanisms for storage of server keys or identifiers are a local matter. For example, a client could store cryptographic hashes of public keys used to verify Signed Data responses. Alternatively, a client could store shared symmetric keys used to verify MACs in Authenticated Data responses. Because of limitation of mobile phone mentioned in the last section, SCVP Server Certificate Validation is not advisable, hence we don't describe it.

IV. PERFORMANCE ANALYSIS

This section analyzes the performance of the proposed model in comparison to the antecedent Model. At the 163-bit ECC/1024-bit RSA security level, an elliptic curve exponentiation for general curves over arbitrary prime fields is roughly 5 to 15 times as fast as an RSA private key operation, depending on the platform and optimizations [8]. Since the short-lived certificate has excluded from the proposed model, 181 bytes is removed from the model. In certificate validation scheme, SCVP is the best choice for certificate validation to the mobile phone, the mobile phone does not need to acquire CAs certificate and ARL from directory or send short lived certificate to OSCP. This reduces the number of transactions between mobile phone and the wired system through wireless bandwidth. In the proposed WPKI model, the mobile phone has only two stages for certificate validation through SCVP request and response.

Certificate validation cost of the proposed scheme is not increased, compared to the validation cost of the wired PKI. The validation cost of the wireless PKI is same as the cost of the wired PKI in the worst case as follows. In wireless PKI, certificate validation procedure is the same as the wired PKI. To save the cost due to expensive wireless bandwidth, we need to optimize the certificate validation procedure in wireless link. Instead of the procedure that user terminal directly requests and download CA certificate and ARL from directory, after server validate the certificate which mobile phone requested, the server sends the status of certificate to user terminal in the short size scheme. Therefore not only the CA certificate and ARL of the directory are not transferred to the user terminal but also user terminal doesn't do anything more to validate certificate. Thus the cost of direct download of CRL from directory and certificate download from server in user terminal is reduced. Compared to the antecedent model, because SCVP request/response procedure is substituted to OSCP procedure and server, the number of the total transactions is decreased to two and of course the big size of CRL is not transferred through wireless link, so the wireless bandwidth is saved. Also unlike the antecedent model, having more than one CA is conceivable and certificate path validation is available. Also based on [1] comparing wireless CMP to RFC2511 and RFC2510 as the certificate management protocol for wired PKI, the module size of the WCMP is smaller than the wired CMP, nevertheless having the same functionality [1].

V. CONCLUSION

In this paper, we proposed wireless PKI technology that provides similar security level as wired PKI supporting mobile phone. The proposed wireless PKI model aimed at secure M-commerce based on mobile phone through wireless communication. On the mobile phone with low performance, we selected ECDSA algorithm to reduce the computational complexity of public key algorithm. To reduce the complexity of certificate validation, we suggest the Server-Based Certificate Validation Protocol (SCVP) which allows a mobile terminal to delegate certification path construction and certification path validation to a server.

REFERENCES

- [1] Y. Lee, J. Lee, J. Song, "Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce", Computer Communications, Elsevier, 30 (2007), pp. 893-903.
- [2] M. Hassinen, K. Hyppönen, E. Trichina, "Utilizing national public-key infrastructure in mobile payment systems", Electronic Commerce Research and Applications, Elsevier, 2007, pp. 214-231.
- [3] R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile: IETF RFC3280", IETF Network Working Group, April 2002.
- [4] OMA, Online Certificate Status Protocol Mobile Profile Candidate Version V1.0, 27 Jan 2004.
- [5] OMA, Wireless Application Protocol Architecture Specification, WAP-210-WAPArch-20010712.
- [6] OMA, Wireless Application Protocol Public Key Infrastructure Definition, WPKI WAP-217-WPKI Version 24-Apr-2001.
- [7] OMA, Wireless Transport Layer Security, WAP-261-WTLS, April 2001.
- [8] K. Lauter, "The Advantage of Elliptic Curve Cryptography for Wireless Security", IEEE Wireless Communications, February 2004 -1536-284/04.
- [9] T. Freeman, R. Housley, A. Malpani, D. Cooper, W. Polk, "Server-Based Certificate Validation Protocol (SCVP)", NIST RFC5055, December 2007.
- [10] D. Pinkas, R. Housley, "Delegated Path Validation and Delegated Path Discovery Protocol Requirements", RSA Laboratories, RFC3379, September 2002.

Çoklu Etmen Sistemlerinde Rol Tabanlı Erişim Denetimi için Bir Yaklaşım Önerisi

Fatih TEKBACAK, Tuğkan TUĞLULAR, Oğuz DİKENELLİ

Özet—Bu çalışmada, şu anda yaygın olarak kullanılan sözdizimsel rol tabanlı erişim denetimi (RBAC) yaklaşımları ile beraber çalışabilecek ontoloji güdümlü bir rol hiyerarşisi ve katmanlı bir erişim denetimi mimarisini çoklu etmen sistemlerinin rol tabanlı etmenlerinde uygulayabilmek amaçlanmaktadır. Bu doğrultuda XACML (eXtensible Access Control Markup Language) modeline dayalı bir şekilde OWL anlamsal veb dili ve SWRL kural dili kullanarak ontoloji güdümlü erişim denetim modelinin geliştirilmesi düşünülmektedir.

Abstract—In this study, our goal is to develop an ontology based role hierarchy that could collaboratively process with syntactic role based access control (RBAC) approaches and apply a multi-tier access control architecture on role based agents of multi agent environments. In this way, the focus is on the development of an access control model based on XACML (eXtensible Access Control Markup Language) by using OWL semantic web language and SWRL rule language.

Anahtar Kelimeler—Ontoloji, OWL, politika, RBAC, XACML

I. GİRİŞ

SON dönemlerde gelişen yüksek performanslı bilgisayarlarla hesaplama ve ağ teknolojileri, geniş ölçekli dağıtık uygulamaların fazlaşmasına sebebiyet vermiştir. Bu uygulamaların özellikle evrensel olarak kullanılan internet üzerinde veriye ve diğer uygulamalara erişimi önemli bir gereksinim olarak karşımıza çıkmaktadır. Veb servisleri ve yazılım etmenleri gibi bu amaca hizmet eden ve bir ağ üzerinde bilginin paylaşılmasını sağlamak için standart protokolleri kullanan teknolojilerde de erişim denetimine ihtiyaç duyulmaktadır.

Erişim denetimi sıklıkla bir sistemdeki kaynaklara erişim kısıtı koymak şeklinde betimlenerek bu kaynakların sadece ayrıcalığa sahip olan elemanlar tarafından kullanılabilirdiği öngörülmektedir. Rol tabanlı erişim denetimi (RBAC) yaklaşımında ise sistemdeki elemanların erişim hakları, görevlerine ve gerçekleştirdikleri eylemlere göre düzenlenir [1].

RBAC modelleri; organizasyonel yapıları, modelleme yetenekleri ve yönetsel yükleri azaltma potansiyelleri ile yoğun bir şekilde çalışılan araştırma konularındandır. Rollerin

kalıtım hiyerarşisi sayesinde elemanların birbirleri ile olan ilişkileri rol seviyesinde düzenlenir. Bu yaklaşımla birlikte erişim kısıtları rollere verilerek bu rollere sahip elemanların yönetimi daha kolay bir şekilde gerçekleşir. RBAC modeli yaygın olarak kabul edilmekle birlikte varolan bir sisteme uygulanması bazı problemlerle karşılaşılmasına neden olabilir. Örneğin, varolan sistemlerin bir kısmı rol bazında organize edilmemiş olabilir. Fakat dağıtık ortamların çalışmasında kullanılan rol bazlı yaklaşımlar, özellikle yazılım etmenlerinin rol tabanlı ve hedef güdümlü mimarileri için uygun bir çözüm olanağı sunmaktadır [2].

Anlamsal Veb bağlamında ontolojiler, kavramların ve aralarındaki ilişkilerin biçimsel tanımlamalarını sağlar ve anlamsal seviyede heterojen ortamların birlikte çalışabilirliğinin üstesinden gelmek amacı ile kullanılır. Bu yaklaşım, şu ana kadar deklaratif veya sözdizimsel olarak gerçekleştirilmeye çalışılan erişim denetimi politika tanımlamalarının ilgili kavramlarının veya bu kavramlar arasındaki ilişkilerin, geliştirilebilecek ontolojiler yardımı ile standart bir gösterime sahip olmasını sağlayabilir. Böylece RBAC modeli anlamsal bir dil olan OWL ve kural dili olan SWRL yardımı ile geliştirilebilir [3].

II. GEÇMİŞ ÇALIŞMALAR

Özellikle veb servisleri üzerinde kullanılmak için tasarlanan XML tabanlı güvenlik dilleri, kapsamlı ve bütünlük güvenlik çözümleri sunmayı hedeflemektedir. Bununla beraber erişim kontrolü alanında politikalar oluşturmak ve erişim kontrol kuralları belirlemek amacı ile bir dil ve bu yapıyı uygulamaya koymak için bir mimari üzerinde çalışmalar yapılmıştır. Bu çalışmalardan genel tanımlamaları bulunan XACML(Extensible Access Control Markup Language) [4] ve X-RBAC(XML Role Based Access Control) [5] ile veb servisleri üzerinde yapılan çalışmalarda kullanılabilen WS-Policy [6] kavramları akademide ve endüstride kabul görmüş yaklaşımlar olarak karşımıza çıkmaktadır.

XACML, erişim denetimi politikalarını ifade, değiş tokuş ve standartlaştırma amacı ile son dönemde OASIS tarafından önerilen bir yaklaşımdır. XACML, kendileri XML dili ile gösterilen nesnelerin yetkilendirme politikalarının da XML'de tanımlanması amacı ile tasarlanmıştır ve çoğu politika gösterim mekanizmalarının işlevselliklerini de tanımlayabilmektedir. Ayrıca farklı kuralları ve farklı politikaları değişik durumlar altında birleştirebilme ve RBAC ile kaynak koruma politikalarını konfigüre edebilme yetisine sahiptir.

Manuscript received November 28, 2008.

Fatih Tekbacak is with the Department of Computer Engineering, Izmir Institute of Technology, Izmir, 35430 Turkey. e-mail: (fatih.tekbacak@iyte.edu.tr).

Asst. Prof. Dr. Tuğkan Tuğlular is with the Department of Computer Engineering, Izmir Institute of Technology, Izmir, 35430 Turkey. e-mail: (tugkantuglular@iyte.edu.tr).

Prof. Dr. Oğuz Dikenelli is with the Department of Computer Engineering, Ege University, Izmir, Turkey. e-mail: (oguz.dikenelli@ege.edu.tr).

X-RBAC ise RBAC modelinin genişletilmiş haline dayandırılmıştır. X-RBAC, farklı alanlarda bulunan ortamların arabuluculuk politikalarını belirtmek için bir çatı sunar ve RBAC modelini zamansal kısıtlar, rol nitelikleri, içeriksel haller ve durum değişimlerinin ön koşulları ile genişletmeye çalışır.

XACML ve X-RBAC, XML tabanlı yaklaşımlardır ve birçok dağıtık uygulamada kullanılmaktadırlar. Bununla beraber, XML politika tanımlamaları makine yorumlaması seviyesinde yeterli olamamaktadır. XML DTD ve şemaları verinin sözdizimsel belirtilmelerinde yeteri kadar esneklik sağlar. Fakat verinin yorumlanması üzerindeki anlaşılarda yeterli başarıyı gösterememektedirler, çünkü her uygulama alanı kendi terimlerinin anlamları üzerinde anlaşmaya varmak zorundadır. Güvenlik politikalarının makine tarafından yorumlanması, belirlenen bir politikanın yanlış kullanımı veya hatalı bir şekilde yayılımını engellemek açısından önem taşımaktadır.

Anlamsal web araştırmaları, güvenlik gereksinimlerinin nasıl tanımlanacağı üzerinde de odaklanmaktadır. KAOs [7], web servisleri, dağıtım hesaplama ve çoklu etmen sistem platformları için politikalar hakkında gösterim ve çıkarsama üzerine kurulu OWL tabanlı bir yaklaşımdır. KAOs; insan, etmen ve diğer işlevsel aktörlerin organizasyonlarını içeren alanlar hakkında gösterim ve çıkarsama yapmak amacı ile ontolojilerden yararlanır. Rei [8], politikaların anlamsal bir gösteriminin üzerine kurulu ödev mantığı tabanlı bir politika dilidir. Ponder [9], dağıtık sistemlerin ve ağların yönetimi için geliştirilmiş nesne tabanlı bir politika dilidir. Ponder dilinin geliştiricileri KAOs ve Rei'de kullanılan politika yönetim kavramlarının birçoğunun önderliğini yapmıştır. Fakat bu çalışmaların hiçbirisi RBAC politika belirtilmelerini içermediği için bu yöndeki ihtiyacı karşılamak gerekmektedir.

Son dönemde dağıtık bir ortamda gerçekleştirilebilecek uygulamaların güvenlik politikalarını doğru bir şekilde anlayabilmek ve yorumlayabilmek amacı ile, RBAC politikalarının gösterimi için OWL dili kullanılarak ontolojiler geliştirilmeye ve SWRL dili kullanılarak kurallar arasında sonuç çıkarılabilir ilişkiler kurulmaya çalışılmaktadır [3]. OWL, betimleme mantığının RDF dilindeki gösterimlerinin üzerine kurulu bilgi gösterim dilleri ailesindedir. Buna dayalı olarak politikalar tanımlarken OWL dilinin kullanımı birçok avantaj içermektedir. İlk olarak birçok politika dili; hedefleri, nesneleri, eylemleri ve zaman, mekan gibi diğer kısıtları içeren sınıfları tanımlamalıdır. Bir politika geliştirilirken onun mevcudiyeti bu sınıfların açık bir şekilde belirlenmesi ile oluşturulabilmektedir (tam zamanlı işçi veya umuma açık yazıcı kavramları gibi). Bu durum, özellikle politikaların kendi alanlarında şemaları ve veri modellerine sahip farklı organizasyonlar tarafından paylaşıldığında ciddi bir önem taşımaktadır. OWL'ın ikinci bir avantajı da analiz ve çalıştırma safhalarında kullanılmak amacı ile diğer mantıksal biçimlere dönüştürülebilmesidir. Bu yaklaşımla da rol tabanlı erişim denetiminin hangi kısımlarının betimleme mantığı ile, hangi kısımlarının ontolojik çıkarsama gereksinimleri ile özdeşleşebileceğine dair çalışmalar yapılmaktadır [10], [11].

Veb servisleri üzerinde kullanılan WS-Policy genel modeli

ile XML tabanlı politika gösterimleri ve bu politikaların doğru çalıştırılmasının gözlenebilmesi amacı ile sistem mimarileri üzerinde durulmuştur [12]. Ardagna ve arkadaşlarının yaptığı [12] çalışmada kullanılan politikaların yönetimi, değerlendirilmesi ve karar verilmesi aşamalarından oluşan üç katmanlı servis mimarisinin yazılım etmenlerinde de benzeri bir şekilde uygulanabileceği görülmüştür.

III. SİSTEM MİMARİSİ

Erişim denetimi politikalarını çoklu etmen mimarilerinde uygulayabilmek amacı ile karşılanmasına ihtiyaç duyulan; birimsellik, politika dilinden bağımsızlık, genişletilebilirlik, yeniden kullanılabilirlik, yüksek performans, donanım ve yazılımdan bağımsızlık gibi gereksinimler bulunmaktadır.

Şekil 1'de gösterilen mimari veb servisleri üzerinde gerçekleştirilen benzer bir yaklaşımın [12] çoklu etmen sistemlerine entegrasyonunu ele almaktadır. Sistem, kullanıcı etmeni, politika karar etmeni(PKE), politika değerlendirme etmeni(PDE), politika yönetim arayüzü ve politika veri havuzu isimli bileşenlerden oluşmaktadır.

A. Kullanıcı Etmeni

Rol tabanlı erişim hakkına sahip olabilmek amacı ile PKE'ye talepte bulunur. Bu talep sonucunda sahip olabileceği haklar veya eğer bir hakka sahip olamayacaksa bir istisna tanımlı kullanıcı etmenine geri döner.

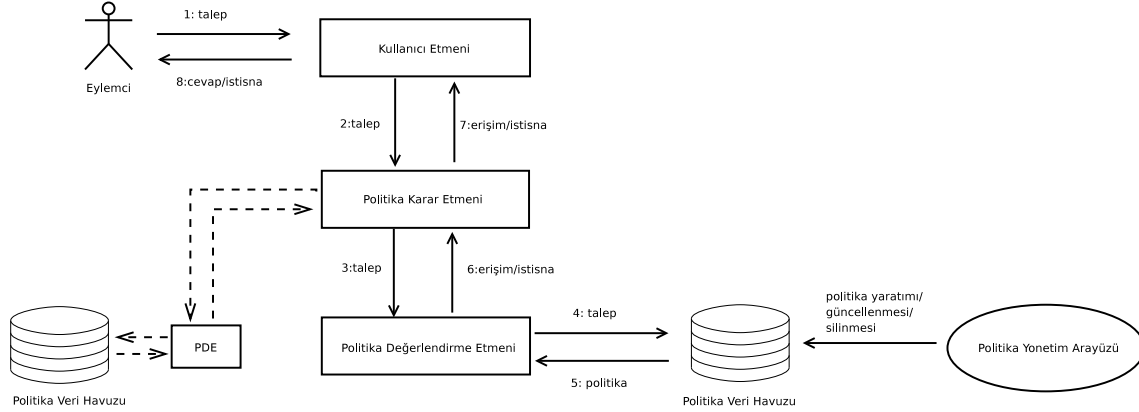
B. Politika Karar Etmeni

Kullanıcı etmeninden gelen talepleri PDE'ye aktarır ve geri dönen taleplerden erişim hakkı verilmişse erişim hakkını, verilmemişse sahip olduğu istisna işleme ontolojisi yardımı ile erişim kontrolüne neden sahip olmadığına dair bilgileri kullanıcı etmenine döndürür. Örneğin, kullanıcı sertifikasında PDE'nin kontrolü sırasında uygun olmayan bir parametre ile karşılaşıldığında erişim hakkının bu yüzden verilemeyeceği kullanıcı etmenine bildirilir. Ayrıca PKE'nin farklı PDE'lerin olduğu bir platformda talepleri birden çok PDE'ye yollama ve gelen verileri tümleştirip kullanıcı etmenine gönderme gibi arabuluculuk özelliğine de sahip olması düşünülmektedir.

C. Politika Değerlendirme Etmeni

PKE'den gelen talep doğrultusunda kullanıcı etmeninin sertifika bilgilerini kontrol ettikten sonra, Politika Veri Havuzu'na giderek o rolün diğer bir etmen üzerinde sahip olduğu yetkileri, gerektiğinde çıkarsama yaparak, döndürür. Politika veri havuzunda bulunan roller ve yetkilere göre PDE'de değerlendirme yapılmalıdır.

Farklı etmen platformlarında bulunan PDE'ler veya bu görevi üstlenen veb servislerine PKE'den gelen talep aynı anda iletilir. Bu taleplerin sonucunda farklı ortamlardan dönen bilgiler XACML politika entegrasyon algoritmaları [13], [14] yardımı ile PKE'de değerlendirilip yetkilere uygun kararlar verilir. Böylece çoklu etmen sistemlerinin otonom çalışan hedef güdümlü etmenleri, erişim denetimi hedefini gerçekleştiren etmenlerden aldıkları geri bildirim doğrultusunda çalışmalarına devam ederler.



Şekil 1. Çoklu etmen sistemleri için erişim denetimi mimarisi

D. Politika Veri Havuzu

Rolleri, rollerin sahip olduğu hedefleri ve rollerin sahip olduğu erişim politikalarını içeren bir bilgi tabanıdır. Sistem yöneticisi tarafından Politika Yönetim Arayüzü yardımı ile sürekli olarak yaratma/okuma/güncelleme/silme operasyonları ile sistemin güncel tutulmasına katkıda bulunur.

E. Politika Yönetim Arayüzü

Politikaların girilebilmesi için yöneticiye bir arayüz sunulacaktır. Bu aşamada varolan arayüzlerden de yararlanılması düşünülmektedir [15], [16]. Bu arayüzün önemli avantajlarından bir tanesi geçersiz politikalar girmenin engellenmesi veya bir role ait birbiri ile çelişen ekleme/güncelleme operasyonlarının yapılabilmesidir. Bu arayüzün içermesi düşünülen geçerlik sınaması işlevi sayesinde [17] politikaların iyi biçimlendirilmiş olarak Politika Veri Havuzu'nda tutulabilmesi sağlanacaktır.

Veb servisleri üzerinde uygulanan yaklaşımda [12], politikaların XML dosyaları içerisinde bulunması ve politika ambarı adı altında bir ilişkisel veritabanında tutulması öngörülüp bu veriler Servis, Metod ve Politika Konumu özelliklerine ait bir çokuzlu olarak tanımlanmakta iken çoklu etmen sistemlerinde bu yapının Rol, Hedef ve Yetki şeklinde tutulması planlanmaktadır.

IV. ERİŞİM DENETİMİ POLİTİKALARININ ANALİZİ

XACML, vebde bulunan kaynaklar üzerindeki politikaları belirtmek amacı ile kullanılan ifade yeteneği yüksek, OASIS standardı çerçevesinde tanımlanan XML tabanlı bir dildir. XACML gibi ifade yeteneği yüksek politika dilleri ile beraber çözülmesi gereken yeni durumlarla da karşılaşmaktadır. Örneğin, kullanıcılar, güvenlik politikalarının içinde bulundukları sistemdeki etkisini ve sonuçlarını anlamakta güçlük çekmektedir. Bununla beraber, erişim denetimindeki en önemli durum, tanımlanan politikalarındaki yetkilendirmelerin yetki dışı varlıklara izin vermesi ve bu durumun elle kontrol edilmeye çalışılmasıdır. Böylece eksik

tanımlanmış güvenlik politikaları, saldırganlara istemeyerek de olsa erişim yetkisi verilmesine neden olabilmektedir.

Bahsedilen problemlerin üstesinden gelebilmek amacı ile, XACML biçimlendirmesinin doğrultusunda, birinci derece mantığın karar verilebilir alt kümelerinden oluşan bir dil ailesinin mensubu olan betimleme mantığı (DL) ve veb ontoloji dili (OWL) kullanılarak çalışmalar yapılmaktadır [18]. Politika analizinin, betimleme mantığının çıkarsama yetenekleri ile örtüşmesi, daha önceden betimleme mantığı kavramları temel alınarak gerçekleştirilmiş çıkarsama motorlarının kullanılabilmesine olanak sağlamaktadır. Tanımlanılacak çatıyı betimleme mantığı ve sonuç olarak veb ontoloji dili ile oluşturmaya çalışmanın bazı yararları vardır [18]:

- OWL dilinin doğası gereği isimlendirme amacı ile URI tanımlamaları kullanması ve ontolojiler arasında linkler gerçekleştirmeye izin vermesi, veb kaynakları üzerinde bir erişim denetim dili için uygun olabileceğini göstermektedir.
- OWL ile politikada kullanılan nesneler için ontoloji tabanlı tanımlamalar ile erişim denetim yaklaşımları geliştirilebilir. Betimleme mantığına dayalı çıkarsama motorları kullanılarak politikanın bulunduğu alanın tanımlamaları ile politikanın kendisi entegre edilebilir. Makine tarafından işlenebilir standart bir dil ile politikaların kendi alanlarında tanımladıkları kavramlar, veb üzerinde paylaşılabılır ve tekrar kullanılabilir.

Kolovski ve arkadaşlarının yaptığı çalışmalar [18] doğrultusunda, kendi çalışmamızda da açık kaynak kodlu bir betimleme mantığı çıkarsama motoru olan Pellet [19] kullanılması düşünülmektedir.

A. XACML'e Genel Bir Bakış

XACML politikalarının kökünde *Policy* ve *PolicySet* kavramları bulunmaktadır. *PolicySet*, diğer *Policy* ve *PolicySet* tanımlamalarını tutan bir barındırıcıdır. Bunun yanında uzaktaki sistemlerde bulunan politikalara olan referansları da tutabilmektedir. Bir *Policy*, yalnızca bir erişim denetimi

politikasını gösterebilmekte ve *Rule* olarak tanımlanan kurallar kümesi ile ifade edilebilmektedir. Her XACML politika belgesi sadece ve sadece bir *Policy* veya *PolicySet* kök elemanını içermektedir. Bununla birlikte bir *Policy* veya *PolicySet*, birden fazla politika ve herbiri farklı erişim denetimi kararlarını etkileyebilecek kurallardan meydana gelebilmektedir.

Öznitelikler, bir XACML politikasının en temel birimidir. Erişim talebinin yapılmasında yardımcı olan *Subject*, *Resource*, *Action* veya *Environment* tanımlamalarının tipik özelliklerini gösterir. Örneğin, bir kullanıcının rolü, erişmek istediği dosya, şu anki zaman gibi kavramların hepsi öznitelik değerleridir. XACML'de gösterilen erişim talepleri, öznitelik-değer çiftlerinin bir listesini ifade etmektedir.

Rule olarak tanımlanan kurallar, XACML'in karar verme aşamasındaki en temel elemanıdır. Aslında bir *Rule*, erişim isteğini girdi olarak alan ve erişimle alakalı izin verip vermemeye karar veren bir fonksiyondur. Eğer bir kural, bir erişim talebine uygulanabilecek ise, *Target* elemanı kullanılır. Bir *Target*, verilen bir talebe uygulayabilmek amacı ile bir kurala uyan *Subject*, *Resource* ve *Action* tanımlamaları için kullanılan en basit durum setidir.

B. Politika İfadeleri

[11] ve [18] çalışmalarında kullanılan erişim politikalarındaki *Subject*, *Action* ve *Resource* kavramlarının betimleme mantığı tanımları ve rollerine eşleştirilmesi yaklaşımı, çalışmamıza da yol göstermektedir. Düşünülen yaklaşıma göre, varolan bir alanı modellemede kullanılan ontoloji ve alt sınıf ilişkilerinden yararlanarak bu ontolojideki kavramlar ile politika varlıkları birbirine bağlanabilmektedir.

Alan ontolojileri kullanarak yaygın politika tabirlerinin betimleme mantığında nasıl ifade edilebileceği bazı durumlar temel alınarak gösterilebilir [11], [18]:

- Rol hiyerarşileri alt sınıf aksiyomları ile kolayca ele alınabilir. Bir alt sınıf, mirasını aldığı üst sınıfın erişim ayrıcalıklarına sahiptir.
- Öznitelikler üzerindeki hiyerarşiler, betimleme mantığı kullanılarak ele alınabilir.
- Görev ayrımı kısıtları, ayrışık aksiyomları yardımı ile yakalanabilir.
- Nicelik kısıtları, verilen herhangi bir öznitelik üzerinde ifade edilebilir.

C. XACML'de Rol Tabanlı Erişim Denetimi

XACML'deki rol tabanlı erişim denetiminin politikaları ifade edebilmek için sahip olduğu profil, temelde beş tane veri elemanından meydana gelir [20]:

Kullanıcılar: XACML'in *Subject* tanımı kullanılarak gerçekleştirilir.

Roller: XACML'in *Subject* özniteliklerinden bir veya birkaçını kullanarak ifade edilirler. Rollerin seti, uygulama ve politika alanına özgüdür.

Nesneler: XACML'in *Resource* tanımı kullanılarak ifade edilirler.

Operasyonlar: XACML'in *Action* tanımı kullanılarak ifade edilirler.

Yetkilendirmeler: XACML'in rol *PolicySet* ve yetki *PolicySet* örnekleri ile ifade edilirler.

V. ETMEN TABANLI MİMARİLERDE ROL KAVRAMI

Roller, etmenlerin yaygın olarak sahip olduğu davranışları tanımlayabilmek için yararlı bir soyutlama gösterimi olarak etmen sistemlerinde kullanılabilir. Rollerin çoklu etmen sistemlerinde iki farklı bakış açısından tanımlanabildiği görülmektedir [21]:

Kavramsal Bakış Açısı: Rol, bir etmenin bazı etkileşimler içinde yer aldığı ve belirli bir yönde evrimleştiği kısıtların bütünüdür. Özellikle çoklu etmen sistemlerinde, bir etmen yükümlü olduğu rollerin özelliklerine göre davranır.

Gerçekleştirim Bakış Açısı: Rol, onun yükümlü olduğu etmenin belirli özellikleri ve davranışlarının sarmalanmasıdır.

Roller, bir etmenin sistemde sahip olduğu hakları ve görevleri tanımlar. Bu tanımlar etmen sistemlerinin bazı karakteristik özelliklerinin altını çizmeye ihtiyaç duymamıza neden olmaktadır [21], [22]:

- Bir etmen aynı anda birden fazla role sahip olabilir.
- Etmenler dinamik olarak rollerini değiştirebilir.
- Etmenler (roller değil) eylemleri gerçekleştirirler.
- Roller birbirinden izole edilmiş degillerdir, diğer rollerle bağlantı halindedirler.
- Rol yardımı ile bir etmenin diğer etmenlerle nasıl etkileşim kurduğu bilinebilir.
- Roller, tekrar kullanıma yardımcı olur.

VI. ÇOKLU ETMEN SİSTEMLERİNDE ROL TABANLI ERİŞİM DENETİMİ YAKLAŞIMI

Bölüm IV-C'de anlatılan veri elemanları özel bir alandan bağımsız bir şekilde tanımlanmaktadır. Kolovski ve arkadaşlarının çalışmasında [18] ifade edilen betimleme mantığı yaklaşımı rol tabanlı erişim denetimi profiline uygulanabilir ve başka ortamlara adapte edilebilir. Çalışmamızın katkısı ise, bu profilde tanımlanan kavramların açıklanan yaklaşımın uygulanabileceği bir alan olarak çoklu etmen platformlarına entegrasyonudur.

XACML ifadelerinin temel tanımlamaları yanında yazılım etmenlerinde bulunan Hedef kavramının da anlatılan yaklaşıma eklenmesi düşünülmektedir. Böylece farklı rollere sahip olan etmenlerin, hedefler üzerinde yetkilerini kullanabilmesi, farklı rollerin sahip olduğu ortak hedefleri paylaşabilmesi, rollerin delegasyonu gibi yaklaşımların oluşturulabilmesi öngörülmektedir.

```
<owl:Class rdf:ID="Goal"/>  
<owl:Class rdf:ID="CommonGoal"/>
```

Bu eklemeler ortamın alan ontolojisinde tanımlanacaktır. XACML-DL olarak adlandırılan XACML'e betimleme mantığının eklenerek geliştirildiği yapı ve ortamın sahip olduğu yazılım etmenlerine özgü alan ontolojisi Pellet [19] isimli bir çıkarsama motoru üzerinde çalıştırılacak; böylece erişim talebinde bulunan etmenin isteği Şekil 1'de tanımlanan mimarideki etmenlerden geçecektir. Sonuç olarak istekte

bulunan etmene rol tabanlı erişim detayları hakkında bilgi dönüşü sağlanacaktır.

Bir rolün diğer bir rolle ortak hedeflerini, farklı rollerin veya hedeflerin delegasyonu ilişkilerini belirleyecek atama ifadelerinin aşağıdaki gibi tanımlanması düşünülmektedir.

```
<owl:ObjectProperty rdf:ID="hasGoal">
  <rdfs:range rdf:resource="#Goal"/>
  <rdfs:domain rdf:resource="#Role"/>
</owl:ObjectProperty>
```

```
<owl:ObjectProperty rdf:ID="hasCommonGoal">
  <rdfs:subPropertyOf
    rdf:resource="#hasGoal">
  <rdfs:range rdf:resource="#Role"/>
  <rdfs:domain rdf:resource="#Role"/>
</owl:ObjectProperty>
```

```
<owl:ObjectProperty rdf:ID="hasRDelegate">
  <rdfs:range rdf:resource="#Role"/>
  <rdfs:domain rdf:resource="#Role"/>
</owl:ObjectProperty>
```

```
<owl:ObjectProperty rdf:ID="hasGDelegate">
  <rdfs:range rdf:resource="#Goal"/>
  <rdfs:domain rdf:resource="#Role"/>
</owl:ObjectProperty>
```

Üzerinde durulması gereken önemli noktalardan bir tanesi de bir etmenin tek bir role bağlı olmamasıdır. Etmenler, yaşam süreçleri boyunca görevlerini gerçekleştirebilmek amacı ile değişik rollere sahip olabilirler veya onları bırakabilirler. Rol ataması, etmen tasarım aşamasında statik olarak tanımlanabileceği gibi eğer etmen onun görevi için en uygun rolü seçebilme yetisine sahip ise dinamik de olabilir. Etmenlerin, tasarım aşamasında veya çalışma aşamasında sahip olduğu rollerin ve ilgili izinlerin birbirleri ile çelişmesi gibi durumları engellemek için statik görev ayrımı ve dinamik görev ayrımı kavramları bulunmaktadır. Bu kavramlar Şekil 1'de gösterilen etmenlerde var olan XACML yapılarında XACML-DL ile alan ontolojilerinde var olan OWL tanımlamalarında ise SWRL kural dili yardımı ile gerçekleştirilecektir. Böylece kullanıcı, rol ve görev arasındaki çelişkileri ortadan kaldırmaya yardımcı olacak kuralları tanımlayıp çalıştırabilecektir. Kurallar tanımlanmadan önce roller arasındaki çelişki ilişkisinin tanımlanması gerekmektedir [23].

Her etkileşim boyunca etmenler birden çok role sahip olabilirler. Çalışma süresi boyunca var olan rollere aktif rol denir. Odell ve arkadaşlarının yaptığı çalışmaya göre [24] etmenlerin sahip olduğu roller, dönemlik aktiviteye göre aktifleştirilebilir, askıya alınabilir veya iki rolün dinamik görev ayrımı kısıtlarına göre değiştirilebilir. Örneğin, aynı anda personel ve yönetici rollerini üstlenen bir etmen, hedef ve ihtiyaçlar doğrultusunda yönetici rolünü aktive ederek personele talepte bulunabilir veya yönetici rolünü askıya alıp personel rolünü aktifleştirerek üst kademesinde bulunan müdürüne raporlar hazırlama hedefine sahip olabilir.

Etmen tabanlı yazılım geliştirmede, rolleri kullanarak etkileşimi modellemenin farklı avantajları vardır [25]. İlki, etmen tabanlı uygulamaları geliştirirken, algoritmik kavramlar

ile etkileşim kavramları arasındaki ayrılıkları belirlemektir. İkinci olarak çözümlerin ve deneyimlerin tekrar kullanımına olanak sağlanır. Aslında roller bir bağlam ile ilişkilidir ve tasarımcılar önceden tanımlanmış rolleri, uygulamalarının sahip olduğu bağlama göre kullanabilir. Böylece roller, bir çeşit tasarım desenine dönüşür [26].

VII. SONUÇLAR

Bu çalışmadaki amaç, yaygın olarak kullanılan sözdizimsel rol tabanlı erişim denetimi yaklaşımlarının entegre şekilde çalışabildiği ontoloji güdümlü bir rol hiyerarşisi ve katmanlı bir erişim denetimi mimarisini çoklu etmen sistemlerinin rol tabanlı etmenlerinde uygulayabilmektir. Bu mimarideki rollere sahip etmenlerin kimlik doğrulamasının ise TÜBİTAK Kamu Sertifikasyon Merkezi aracılığı ile elde edilen akıllı kartların içerdiği sertifikalar yardımı ile gerçekleştirilmesi düşünülmektedir.

Rol tabanlı erişim denetimi mimarisi için, XACML modeline dayalı ontoloji güdümlü erişim denetim modelinin geliştirilmesi, örnek rol senaryoları üzerinden politika veri havuzuna bir arayüz yardımı ile politikalar eklenmesi amaçlanmaktadır.

Bu çalışma sürecinde, sistemin ihtiyaçlarını karşılamak amacı ile etmenlerin sorumluluklarını çözümleyebilecek farklı rol belirtim senaryoları üzerinden roller tanımlanacak, etmenler tarafından sahip olunan bu rollerin Şekil 1'de gösterilen sistem mimarisinde belirtilen katmanlardan geçebilmesi için gerekli olan görevler, iletişim yetenekleri ve etmenler arası bağımlılıklar SEAGENT [27] çoklu etmen sisteminin rol modeli temel alınarak gerçekleştirilmeye çalışılacaktır.

KAYNAKLAR

- [1] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, C. E. Youman, *Role-Based Access Control Models*. IEEE Computer 29(2): 38-47, 1996.
- [2] F. Chen, S. Li, H. Yang, *Enforcing Role-Based Access Control Systems with an Agent-Based Service Oriented Approach*, Proceedings of the 2007 IEEE International Conference on Networking, Sensing and Control, April 2007.
- [3] D. Wu, X. Chen, J. Lin, M. Zhu, *Ontology-Based RBAC Specification for Interoperation in Distributed Environment*, ASWC 2006: 179-190, 2006.
- [4] T. Moses, ed., *OASIS eXtensible Access Control Markup Language (XACML) Version 2.0*, 24 July 2003.
- [5] J. B. D. Joshi, *Access-control language for multidomain environments*. Internet Computing, IEEE, Vol 8, Is 6. IEEE Inc., Piscataway, pp. 40-50, 2004.
- [6] D. Box, *Web Services Policy Framework (WS-Policy) version 1.1*, May 2003.
- [7] A. Uszok, J. M. Bradshaw, M. Johnson, R. Jeffers, A. Tate, A. Dalton, S. Aitken, *KAOs Policy Management for Semantic Web Services*, IEEE Intelligent Systems, v.19 n.4, p.32-41, July 2004.
- [8] L. Kagal, T. Finin, A. Johshi, *A Policy Language for Pervasive Computing Environment*. In proceedings of IEEE 4th International Workshop on Policies for Distributed Systems and Networks (POLICY 2003), Lake Como, Italy, 2003.
- [9] N. Damianou, N. Dulay, E. Lupu, M. Sloman: *The Ponder Policy Specification Language*. In proceedings of Workshop on Policies for Distributed Systems and Networks (POLICY 2001). Springer-Verlag, Bristol, UK, 2001.
- [10] T. W. Finin, A. Joshi, L. Kagal, J. Niu, R. S. Sandhu, W. H. Winsborough, B. M. Thuraisingham, *ROWLBAC: Representing role based access control in OWL*, in Proc. SACMAT, pp.73-82, 2008.
- [11] M. Smith, A. Schain, K. Clark, A. Griffey, V. Kolovski: *Mother, May I? OWL-based Policy Management at NASA*. Proceedings of the OWLED 2007 Workshop on OWL: Experiences and Directions, Innsbruck, Austria, June 6-7, 2007.

- [12] C. A. Ardagna, E. Damiani, S. D. C. Di Vimercati, P. Samarati, *A Web Service Architecture for Enforcing Access Control Policies*, Proceedings of the First International Workshop on Views on Designing Complex Architectures, Electronic Notes in Theoretical Computer Science, Volume 142, Pages 47-62, January 2006.
- [13] P. Mazzoleni, E. Bertino, B. Crispo, S. Sivasubramanian, *XACML policy integration algorithms: not to be confused with XACML policy combination algorithms!*, Proceedings of the eleventh ACM symposium on Access control models and technologies, Pages: 219 - 227, 2006.
- [14] P. Mazzoleni, B. Crispo, S. Sivasubramanian, E. Bertino, *XACML Policy Integration Algorithms*, ACM Transactions on Information and System Security (TISSEC), Volume 11, Issue 1, February 2008.
- [15] Xacml Studio, <http://xacml-studio.sourceforge.net/>.
- [16] Policy Studio, <http://www.nextlabs.com/html/?q=policy-studio>.
- [17] Margrave, <http://www.cs.brown.edu/research/plt/software/margrave/>.
- [18] V. Kolovski, J. Hendler, B. Parsia, *Analyzing Web Access Control Policies*, Security, Privacy, Reliability and Ethics Track, Access Control and Trust on the Web Session(WWW 2007), May 2007.
- [19] E. Sirin, B. Parsia, B. C. Grau, A. Kalyanpur, Y. Katz, *Pellet: A practical OWL-DL reasoner*, J. Web Sem. 5(2): 51-53, 2007.
- [20] A. Anderson, *Core and hierarchical role based access control (RBAC) profile of XACML v2.0*, OASIS Standard, 1 February 2005.
- [21] Q. Yan, L. J. Shan, X. J. Mao, Z. C. Qi, *RoMAS: A Role-Based Modeling Method for Multi-Agent System*, Proceedings of International Conference on Active Media Technology, 2003.
- [22] M. Puviani, G. Cabri, L. Leonardi, *Agent Roles: From Methodologies to Infrastructures*, International Symposium on Collaborative Technologies and Systems(CTS 2008), May 2008.
- [23] W. Di, L. Jian, D. Yabo, Z. Miaoliang, *Using Semantic Web Technologies to Specify Constraints of RBAC*, Proceedings of the Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'05), 2005.
- [24] J. Odell, H. V. D. Parunak, S. Brueckner, J. Sauter, *Changing Roles: Dynamic Role Assignment*, Journal of Object Technology, volume 2, pages 77-86, 2003.
- [25] G. Cabri, L. Ferrari, L. Leonardi, *Supporting the Development of Multi-Agent Interactions via Roles*, AOSE 2005: 154-166, 2005.
- [26] Y. Aridor, D. Lange, *Agent Design Pattern: Elements of Agent Application Design*, International Conference on Autonomous Agents, ACM Press, 1998.
- [27] O. Dikenelli, *SEAGENT MAS platform development environment*, AA-MAS (Demos) 2008: 1671-1672, 2008.

A Strong Two-Way Authentication Method for Low Capacity Solutions

Gökhan DALKILIÇ, H. Şen ÇAKIR, M. Hilal ÖZCANHAN

Abstract— One of the widely known challenge - response authentication methods is the two-way authentication. First two-way authentication methods were limited by those days' capacity of processing power and had limited security. The later protocols and standards on the other hand were too broad and resource demanding because they aimed at addressing all of the security demands of the "future"- as seen in those times. With the availability of new techniques and new tools at low costs, a finer granularity on the security of low capacity, low cost environments has become possible with good cost/performance ratios. Of course these solutions need careful design and functional definition, before being used in small designs. Our alternative two-way authentication is a step towards giving more meaning to the parameters suitable for low cost solutions, instead of using public-keys or certificates and still have a key exchange protocol as secure as others.

Keywords — authentication, mutual-authentication, low-cost devices, security.

I. INTRODUCTION

To pay respect to Diffie Hellman let us remind ourselves that they were the fathers of two-way authentication. Even though the first Diffie Hellman authentication[1] was susceptible to a man-in-the-middle attack, some considerable time passed until this vulnerability was tackled and remedied for.

Up to present day, cryptographers are still working on two-way authentication to make it stronger against all known attacks. To this end today's popular public-key and public certificate tools are utilized. But these tools are known to cost in terms of ownership, processing, storing and protection. Relying on abundant resources in applications is nothing but seeking a forceful solution to counter-measure the vulnerabilities of two-way authentication. To give an example, designers are pushing the use of public certificates for authentication in small scale devices and even in wireless solutions. To exaggerate the abuse of resources, the certificates are required in every step until the whole transaction finishes.

Every network and hardware expert knows that passing certificates attached to each and every step of the transaction is a costly act in terms of network traffic and processing power. To cut the costs of the network load, some institutions using

certification technologies opt to use their own local certificate authorities. This puts the whole operation in jeopardy, since hacking intermediary certificate authorities and public-keys are among today's new hobbies. In addition, the cost of premises and user protection of such certificate servers do not match the efforts spent in the design of the authentication tool. Designing a more appropriate authentication method and spending less on servers would be a much better solution.

One vulnerability of public certificate authentication is that people rarely question the validity of the certificate of their transaction partners. The awareness of questioning the validity of the public certificate of an applicant is reduced to a just "click ok" action by many users. Such care free applications cannot be accepted as secure.

We attempt to address these issues by providing a low cost alternative to the public-keys and certificates in two-way authentication, robust enough to make two-way authentication more cost effective in advanced systems and more affordable in low cost, low capacity solutions.

II. PRESENT SOLUTIONS AND CONFORMITY TO STANDARDS

The flaws of Diffie Hellman key exchange; conversation in clear text and the full reliance on a stranger's identity have been tackled by many. Oakley key exchange[2] is one of the most famous of them all. However, it is commonly accepted that it is computationally very intensive and requires a lot of resources. Of course, there are other work adding extra security to the original Diffie Hellman key exchange, but there is a need for some standards to provide a common ground for the basic criteria that everybody should accomplish to claim that their two-way authentication method is secure. The standard in this area is the X.509 standard[3] which is discussed below.

A. The X.509 Standard

Standardization authorities trying to put some standards to one-way, two-way and three way authentication protocols have come up with a standard for two-way authentication, too. This is the X.509 Strong Two-Way Authentication standard and must be studied here, to prove that our proposed alternative is in conformity with the standards and does not open up new flaws by over simplifying some parameters or steps.

The X 509 Strong Two-Way Authentication standard – shown in Fig. 1 - asks the initiator A to use a time stamp, a nonce , the ID of the responder, sign all of these in a new entry and pass the proposed session key K_{ab} encrypted with the public key of the responder B. Similarly the responder has to send its own timestamp, nonce and ID. B also has to sign the nonce and its ID

Manuscript received November 10, 2008. Date of paper submission November 10, 2008.

Gökhan Dalkılıç is with the Computer Engineering Department, Dokuz Eylül University, İzmir, 35160 TR (e-mail: dalkilic@cs.deu.edu.tr).

H. Şen Çakır is with the Computer Engineering Department, Dokuz Eylül University, İzmir, 35160 TR (e-mail: sen@cs.deu.edu.tr).

M. Hilal Özcanhan is with the Computer Engineering Department, Dokuz Eylül University, İzmir, 35160 TR (e-mail: hozcanhan@cs.deu.edu.tr).

and send it to A, together with its own secret encrypted with A's public key. The standard is well balanced in terms of doing the same computations and exchanging similar parameters, by the partners. However, there are a few points worth pointing out here. The first point is although the ID of the responder is present, the ID of the initiator is missing in the challenge.

That piece of information is needed for two reasons: To be sure that the first message indeed arrived from the initiator and

A $\rightarrow$ B : { $t_A, r_A, ID_B, \text{sgnData}, E[PU_B, K_{ab}]$ }
 B $\rightarrow$ A : { $t_B, r_B, ID_A, \text{sgnData}, E[PU_A, K_{ba}]$ }
 Notation :
 t_A, t_B : timestamp of A and B, optionally expiration time also incl.
 r_A, r_B : nonce, pseudo-random number of A and B.
 ID_A, ID_B : Identity of A and B.
 sgnData : signature of A or B over parameters (t_X, r_X, ID_X)
 PU_A, PU_B : Public-key of A and B.
 K_{ab}, K_{ba} : Secret parameter of A sent to B and B to A.

Fig. 1. The X.509 Strong Two-Way Authentication standard. © Copyrighted, Cryptography and Network Security [4], by William Stallings.

to protect the responder from DoS attacks[4]. The signature of values and the encryption-decryption processes involve intensive computations and assumes that both parties have the necessary capacity to do the calculations fast. Another point is the assumption that each side has the public-key of the other beforehand[4]. It is obvious that even if the two sides are total strangers to each other, there is a mediator -the certificate authority- that authenticates the two sides to each other. But the question arises "Do we really need certificates, signatures or public-keys in low cost-low capacity solutions to make an exchange secure?". We don't because the low cost solutions cannot make the computations of certificates easily.

B. Can certificates, public- keys and signatures be replaced by other secure parameters and algorithms in low cost solutions?

We may rephrase the question as "Can low capacity solutions with shared secrets exchange secure session keys too, without the need for certificates?" The answer is "Yes, they can." With the advances in integrated devices and the drop in their prices, new technologies make it possible to have the secure secrets needed for two-way authentication. When used properly, these technological devices can match the security of the expensive certificates and public-keys, as we will show shortly.

A note of caution before indulging in details though: In the X.509 standard, the parameters are used to calculate the session key and provide additional security. However, the parameters can be used to calculate the *key* to encrypt the *session key* before exchanging it, if that "interim" key is secure than the authentication is as secure as the others.

III. THE PARAMETERS OF THE PROPOSED TWO-WAY AUTHENTICATION

First of all, the parameters of the proposed two-way key exchange will be outlined. Our proposed two-way authentication is shown in Fig. 2. Here also five parameters are passed, in the challenge. Let us remember that the motive is to add more meaning to the parameters. The timestamp, the nonce and the ID

of the responder are preserved. However, the ID of the initiator will also be added for denying DoS attacks and for informing B about whose secret tables (which secrete to share) to use. Then, three of these four parameters will be hashed together with a secret shared by both parties and will be sent for B to compare the clear text with the hashed version. The computation of the

1. A $\rightarrow$ B { $t_A, r_A, ID_A, ID_B, h(r_A, ID_A, ID_B, \text{secret}_{AX})$ }
2. B $\rightarrow$ A { $t_B, r_B, ID_B, ID_A, h(r_B, r_A, \text{secret}_{AX}), E(K_\Phi, K_s)$ }

Notation :

t_A, t_B : timestamp of A and B, optionally expiration time also incl.
 r_A, r_B : nonce, pseudo-random number of A and B.
 ID_A, ID_B : Identity of A and B.
 secret_{AX} : shared secret , comes from Table A
 PU_A, PU_B : Public-key of A and B.
 K_Φ, K_s : Calculated encryption key and secret parameter of B sent to A.

Fig. 2. The alternative Two-Way Authentication proposed.

secret secret_{AX} used in the challenge will be explained below.

In the response there are six parameters as opposed to the five of X.509. Again the timestamp, the nonce and the ID of the challenger are preserved. However, the ID of the responder will be added for preventing DoS attacks and for informing A about whose secret tables to use. Again the clear text parameters, excluding timestamp, will be hashed together with the same secret secret_{AX} and will be sent to A to compare the clear text with the hashed result. Then there is an additional parameter where the session key is passed in encrypted form. Let us now study the details of the exchanged parameters, because compared to X.509 standards some parameters have additional roles, some parameters are missing and there are unexplained shared secrets.

A. The ID Parameters: ID_A and ID_B

The ID parameters have always been the weak point of challenge-response authentications. Our suggestion, this value is strengthened for both by the inclusion of a unique serial number (S/N_X), by concatenating the IP address (IP_X) with S/N_X (1).

$$ID_A \equiv IP_A \parallel S/N_A ; \quad ID_B \equiv IP_B \parallel S/N_B \quad (1)$$

Obviously, there will be an additional security in identities because they have become unique and dynamic. Thus, when a party changes its address, it can be traced and a peculiar IP address for a device may mean a masquerade attack and thus ring some alarms.

The Serial Numbers S/N_A and S/N_B are coming from a secure memory location[5,6]. Another property is to help the exchange partners match the serial number of its reciprocal to the secret tables A and B of the same reciprocal, which will be used during the key exchange. In other words, every device has a unique pre-lasered Table A and a re-writeable Table B. Fig. 3 shows the features of a commercial product[5] where the product has a unique, factory-lasered 64-bit serial number used as an input to a hashing engine. More information on that technology and tables is given in section V. Let us for now accept that we can have a unique and dynamic ID for our partners A and B. In Fig. 3 only a one-way authentication commercial product is depicted for simplicity but the same device can be used for two-way authentication; since B has what A contains, on a piece of paper

supplied by the manufacturer. The principle is still the same: A device with a unique serial number hinting at unique static and dynamic secrets, that it shares with B.

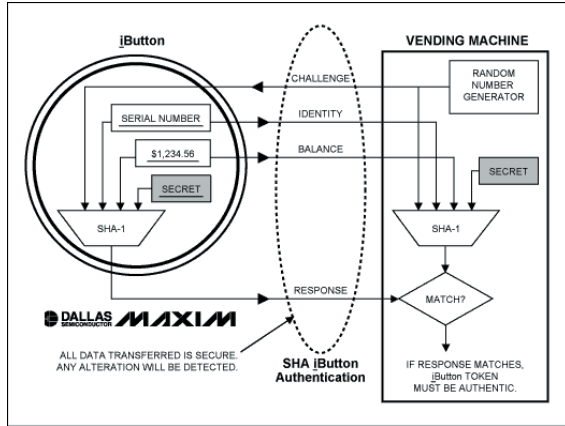


Fig. 3. A typical commercial application of a serial number in an authentication process. © Copyright Courtesy of Dallas Maxim Semiconductor [5].

B. The Timestamps and Nonces t_A , t_B and r_A , r_B

These parameters are the same as those used in the X.509 standard. There are no alternative or additional properties of timestamps. The use of the nonces is the same but there is an additional role for each of the nonce values. These additional roles and the regular usage will be explained in the section where the mechanism of the key exchange is outlined.

C. Instead of Signatures, The Secret(s) of A

Parameters utilized in the X.509 standard are agreed upon beforehand, that is parties share some information before they start the exchange. They know that the last parameter passed is encrypted with a public-key. The most important issue is the strength of the public-key encryption. We claim that if the encryption key K_Φ used in our design is as secure as the public-key of the X.509 standard, then our alternative authentication is also as secure. Furthermore, in X.509 there is only one private key, in ours there are many secrets leading to many keys.

In Fig. 4 there is another commercial product[7,8] where an internal 8 byte secret is input together with other parameters into a hashing engine, namely a SHA-1 engine[5,7,9,10,11]. This example shows that it is possible to have a secret inherent in a low cost system, which can be used together with the other secrets as an input to a hashing function. The hash function is sometimes accepted as a raw version of a signature. The important issue here is to make sure that the secrets stored in the device can be trusted. This is tackled later in section V. Secret protection requires that the internal secret never leaves the system. The best security is to keep the secret inside the processor while using it to hash the inputs. For our purposes we assume that today's manufacturers guarantee to provide us with many secrets of satisfactory lengths inside a low capacity device; i.e. eight different 64 bit secrets. Therefore, we can imagine having a table of eight different unique static secrets. Let this be the Table A of Fig. 5.

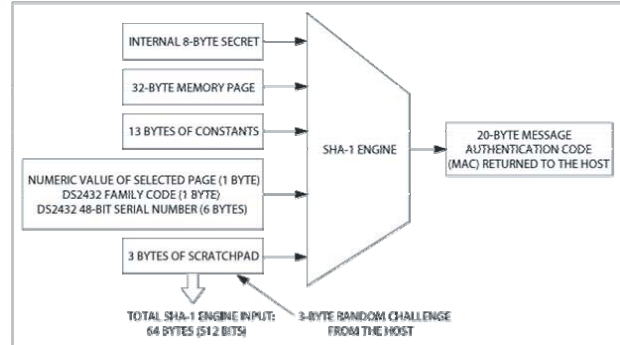


Fig. 4. A typical commercial application of a secret number as an input to a hashing engine, in an authentication process. © Copyright Courtesy of Dallas Maxim Semiconductor [7].

Table B will be unrevealed shortly.

pointerA#	Table A	pointerB#	Table B
1	secret _{A0}	1	secret _{B0}
2	secret _{A1}	2	secret _{B1}
3	secret _{A2}	3	secret _{B2}
4	secret _{A3}	4	secret _{B3}
5	secret _{A4}	5	secret _{B4}
6	secret _{A5}	6	secret _{B5}
7	secret _{A6}	7	secret _{B6}
8	secret _{A7}	8	secret _{B7}

Fig. 5. The static and dynamic secret tables of A.

Of course, the manufacturer supplies the unique Table A during delivery; thus only the responder should have a prior copy of the secrets. In our alternative we will not just use Table A's secrets but other inputs as well to make a hash, e.g. an entry from Table B. That mechanism and Table B is explained below, in detail.

The hash of the two parties' IDs together with the first secret entry of Table A looks very similar to the signed data of the X.509 standard. But our alternative is cheaper in every respect.

D. Instead of Public Keys: Table A & Table B of party A.

Looking back at our proposed key exchange shown in Fig. 2 the key K_Φ that is used to encrypt the session key is in the heart of our design. While in other key exchanges the session key is co-generated, in our design the session key is generated by the responder B. The key that encrypts the session key; K_Φ , is co-generated instead. Let us see the inputs to K_Φ . In the previous section, we had introduced a shared secret from a table while calculating the hash of the challenge parameters. So we already have Table A of Fig. 5 with eight secrets, written once and only read internally. At the very beginning of the key exchange, when the two parties have just initialized, A starts using the first entry in Table A; that is secret_{A0} to calculate the hash in the challenge. Moreover, A points to a secret from Table B using its nonce r_A in the challenge. B uses the secret secret_{Bx} pointed by A as one of the inputs to calculate K_Φ . How B calculates the value of x in secret_{Bx}

is left to the explanation of the exchange mechanism in section IV.

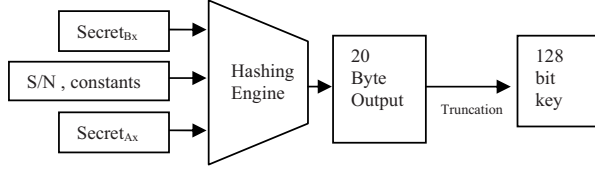


Fig. 6. Calculation of key K_ϕ .

Some commercial eeproms and secure microcontrollers also supply a memory page that can be filled by the user. Thus, the user can create more secrets in another protected table, over just one wire (called 1-wire [9,10]). This technology is explained briefly in section IV. In our case, let us assume that Table B of Fig. 5 is the table we created. B uses this shared secret, e.g. secret_{B6} , some constants, secret_{A0} as input to the same SHA-1 function and truncates the 20 byte outcome to desired key length of 128 bits, as shown in Fig.6. Since a SHA-1 engine is already used to hash the challenge parameters, why not use the same hashing engine SHA-1 for calculating K_ϕ . Obtaining K_ϕ by using manufacturer made static and user defined secrets, remove any doubts on the static secrets. Since K_ϕ is calculated by using the eight by eight secret tables many would think that the value of K_ϕ is limited to a possibility of 64. That is not true. The outcome of the SHA-1 engine is 20 bytes and K_ϕ is obtained by truncating this value, which makes K_ϕ more random. By making the truncation method complicated a huge number of K_ϕ values can be obtained. One simple way may be, looking at the last digit of the nonce r_A . E.g. if it is 0: take the right-most 128 bits of the SHA-1 outcome; if it is 1: take the leftmost 128 and if it is 2: take the mid 128bits. Even this simple trick yields a 3x128 possible values of K_ϕ .

Also observe that K_ϕ is never passed on the communication line, a property of the session key K_s in the other key exchanges. Therefore there is no loss of property in our suggested alternative. The explanation of how the entries from Tables A and B are chosen when the old one expires is left to section IV below, when the mechanism is elaborated on.

E. The session key

The key K_s that is the heart of other designs is a relaxed issue in our case. It is simply generated keeping in mind all the recommendations given by cryptographers. Its length, uniqueness and other properties are left to the choice of the solution owner. But since there is a SHA-1 engine in our example[5,7]; maybe a SHA-2 in a more expensive solution, this same hash function can be used to calculate K_s . Any preferred entries from tables A and B, together with the serial number, a random number (seed) and any other entries in the rest of the secure memory can be the input to the hash engine. The 20 byte output can be truncated in any preferred way to obtain a 128 bit key K_s . The vital point is that this new session key K_s is encrypted using K_ϕ before being sent to A. Commercial devices with an embedded AES encryption engine and a SHA-1 hashing engine are common today. Therefore, K_s can be encrypted using K_ϕ with an AES engine and sent to A in the response.

IV. THE EXCHANGE MECHANISM

Our proposed two-way authentication alternative (Fig. 2) does not look much different than the X.509 standard which means we have not deviated far from the standard. However, some parameters have additional meaning and uses.

A. The Challenge

Let us start by studying the challenge. The first parameter, the time stamp t_A is the same as that in the X.509 standard.

$$A \rightarrow B \{t_A, r_A, ID_A, ID_B, h(r_A, ID_A, ID_B, \text{secret}_{Ax})\}$$

Fig. 7. The challenge of the proposed key exchange.

It consists of an optional generation and expiration time. Thus a delayed delivery of the first message can be detected and a retransmit request can be made by B.

The second parameter, the unique random number- nonce r_A - however has three roles instead of two. The commonly known role is to help detect replay attacks. B must compare nonce r_A with the previous nonces and reject any challenges with the same nonce. Thus nonces are not discarded but stored for later comparisons. The second role of nonce r_A is a challenge to party B to show both, that it has received this fresh nonce r_A untampered and will send a response proving it has the shared secret, secret_{Ax} . This will be explained in the response section. Additionally, as a third role *nonce r_A is a pointer to the secret_{Bx}*, one of the parameters used to calculate K_ϕ . Since the nonce is a large random number, the pointer to secret_{Bx} is calculated as follows (2), for an eight entry table:

$$x = (\text{lastdigit of nonce } r_A) \bmod 8 ; \text{ therefore } 0 \leq x \leq 7 \quad (2)$$

Assuming that the last digit of nonce r_A is 3, in the challenge, party A is telling party B to use the secret at location 3 of Table B in Fig. 6- which happens to be secret_{B2} . B uses this value to calculate K_ϕ and uses K_ϕ it to encrypt K_s as explained in the previous section.

The initiator A, also sends its identity ID_A - authenticated with its serial number, as an additional parameter compared to the X.509 standard. This parameter is absent in X.509 because A signs some parameters with its private key. B can only open it by using A's public key; hence thinking it must have definitely come from A. But this requires B to know the public key of A and make a computation to strip the signed information out of the signature and compare with that sent in clear text. We believe that this can clog low capacity devices, in case of a DoS attack. Our suggestion is to send the initiators identity ID_A in clear text, for B to be able to drop the call quickly, in case of an unexpected challenger.

The authentication of A's identity and the integrity check of the clear data are done in the next parameter. Identities are hashed together with the nonce r_A and secret_{A0} . And this is very similar to the signing process, in the X.509 standard. The hash has the secret_{A0} as an input, which is never passed to B. Including A's nonce in the hash makes sure that if r_A was tampered on the way it will be detected by B, because the result of the hash will not match the clear text values that A has sent.

Finally, ID_B is necessary for B to check quickly if itself is the

intended address. If not, it simply drops the call.

The last point to mention is the missing parameter of X.509, in our alternative. In standard X.509, party A both starts off an exchange and at the same time forces a session key K_s in one go. It was mentioned before too that using public-keys as a means for exchanging secrets overwhelms low cost, low capacity solutions. But more critical than that; accepting a secret and the identity of a caller in the same step can be a flaw. Because again a malicious attacker can clog B. The final session key should be settled only in the second step, when parties really prove one to the other. After that parties can decide to share other secrets or more keys thereafter.

B. The Response

The responder namely B, upon receiving the call from A, looks at the timestamp t_A . If the message is old, it drops the call immediately and hopes that if it were a real call the sender syncs its time and makes a new call; after a random amount of time. Similarly, a check is run for the nonce r_A . If it is the same as the last message's nonce, again the call is dropped.

Next B checks the identity of the caller. B must have an idea about the IP address and the serial number of A. Assume that B has a table of serial numbers. B now identifies which secret tables A and B are to be used. If A is an expected caller B goes on to the next check which is the destination address. If B understands that the challenge is for itself, it goes to the final step of checking; otherwise again the call is dropped.

In the final step of checking, if it is the first contact with A after an initialization (more on this in section VI) B knows that A is using secret_{A0} and calculates the hash which has four inputs. If the result of this hash is a match to the clear text data then A is indeed the party making the challenge and the challenge is new. Furthermore it is guaranteed that the contents of the challenge have not been tampered with, on the way.

$B \rightarrow A \{t_B, r_B, ID_B, ID_A, h(r_B, r_A, \text{secret}_{A0}), E(K_\Phi, K_s)\}$

Fig. 8. The response of the proposed key exchange.

After making these checks B responds by sending its own timestamp for party A (Fig. 8) to decide if the response is old or not. Expiration time was sent by A and can be verified by resending it. Time synchronization will not be taken up here, but it is expected that if too many calls are dropped, the parties are expected to do a time sync.

The next parameter $\text{nonce } r_B$ however also has three roles in our alternative. The first one is a check for A to see if the response is a replay or not. The second role is its presence in the hash for the parameters to be passed, to authenticate their integrity. Here B calculates the hash of its nonce r_B , A's nonce r_A and the secret secret_{A0} . B sends this hash value to A to prove that indeed it has received the fresh nonce of A, finished all checking and has the secret secret_{A0} apriori, as expected. This authenticates that the responder is indeed B and gives A the chance to test if nonce r_B has been tampered with.

Thirdly, $\text{nonce } r_B$ is a pointer to the next secret_{Ax} for A, to use in the next key exchange challenge. Since nonce r_B is a large random number, the pointer is calculated as follows (3):

$$x = (\text{lastdigit of nonce } r_B) \bmod 8 ; \text{ therefore } 0 \leq x \leq 7 \quad (3)$$

Assuming the last digit of nonce r_B is 6, in the response, B is telling party A that when the time expires and A has to make a new challenge, the secret at location 6 of Table A in Fig. 6 has to be used— which happens to be secret_{A5} . Thus, nonce r_B is a forecast to A about the next secret to be used in the next challenge.

The parameters ID_B and ID_A were explained in detail before. The only difference is their order, in the response. This is only a matter of syntax.

Finally, B computes K_Φ as described in section III using the secret secret_{Bx} dictated by A's nonce r_A (as explained in the above section) and generates a session key K_s . B then encrypts K_s using a pre-decided algorithm, i.e. AES, and sends K_s to A, in an encrypted form.

A has both secrets secret_{Ax} and secret_{Bx} . secret_{Ax} dictated by B in B's nonce r_B , and secret_{Bx} dictated by A itself. Thus calculates K_Φ , as well. After calculating K_Φ , A decrypts the encrypted message and recovers the session key K_s . That ends the two-way authentication process and the exchange of a secret session key. Observe that no numbers about K_Φ is sent to each other, but is obtained by either party, from their tables and through some calculation.

V. TECHNOLOGY OF OUR SECURE SECRETS

In this section the reliability of random number generators, static and dynamic secrets, hashing and encrypting engines supplied by manufacturers will be discussed. Although it is not the scope of this paper to detail on these technologies an effort will be made to persuade the reader that our reliance on these technological capabilities is sound.

The first concern is how secure the secrets recorded on the devices are, at the time of manufacturing. Manufacturers claim that they can prove their products contain encrypted information that only the issuing authority could have created[5,7], plus once written these secrets cannot be read from outside the device but only used as an input to the internal hashing engines. To fend off side-channel attacks, advanced tamper detection, special NV SRAM memories and electromagnetic radiation control technologies are used [7].

Another issue is the 1-wire property of commercial devices [5,7,9,10]. To reach the encrypted code space of a product only one wire is used and the whole of the circuitry need not be powered on. Manufacturers submit proof that tampering detection, encrypted memory and MAC authentication before read and write operations are well up to the security standards[7].

The third concern is whether the secrets are unique and only supplied to the buyer. This can be compared to the trust toward certificate authorities. Major manufacturers of security technologies build their industry on the trust they supply to their markets, therefore they are the secret authorities of their field.

Another issue is the quality of the hashing/encryption engines inside the devices[5,7,8,9]. Manufacturers claim that they guarantee both the uniqueness of the random numbers generated—an essential aspect of authentication, and the conformity of hashing function and encryption algorithm of their products to

standards [5,8,9]. In short, all inputs and engines involved in an authentication process can be on embedded on a secure device.

The technologies using public-keys and certificates have costs incurring from annual fees, processing power and fast connection to third parties. Our alternative, on the other hand has no such costs.

VI. HOW SECURE IS OUR ALTERNATIVE

The proposed alternative has to be strong against known attacks. In terms of a key exchange authentication our alternative doesn't have a security flaw. It is as strong as the hardware is. Therefore, the only vulnerability may lie in hardware side channel attacks[6]. To address this type of attack, some information about the efforts of the manufactures were given in section V, but that is not all. More information about the definition of side channel attacks and suggested remedies are given in the references[6], the evaluation of these side channel attacks will not be discussed any further here because they are the topic of a different argument.

The originality and thus the security of our alternative lies not in the generation of the session key to be exchanged, but in the composition of a key that will be used to encrypt the session key. No matter how strong our key might be the strength of our alternative depends on the encryption algorithm used to encrypt the session key. Once that algorithm is compromised or gets old, a new algorithm has to be employed in the key exchange process[8]. That is to say; we recommend to use AES instead of DES or 3DES for the encryption algorithm but it is quite possible that some day AES will be declared weak. So our authentication is as strong as AES and no more. The same argument is true for the SHA-1 hashing engine used. New products are coming out with SHA-512 engines, but for the time being they are not low cost.

As for DoS attacks, if the attacker intercepts the identity of A in the challenge and resends the challenge to B, he will not be able to clog B. Because, B uses the nonce or the IP address of A to drop the challenge. However, if the attacker spoofs the IP of A, as well as tampering with the timestamp and the nonce B discovers the attack after examining the hash value in the challenge. Just one hash calculation is not expected to clog B.

VII. FUTURE WORK

There are a few things that need to be done in the future. First of all instead of eight member secret tables, 64 or more secrets should become available[8]. Furthermore, the secrets can be 128 bit instead of 64 bits. But these are related with the chip manufacturers. Our future work may be related to making better use of the timestamp parameters, i.e. making them intelligent like we did for the nonces. It is possible to add more security by studying the timestamps as natural numbers as well.

One more future work is about the initialization of the two parties. It may appear as a problem if one of the parties initializes during or before the key exchange starts. How will one know that the other has initialized. This needs a full consideration because it can turn into a security flaw. But with some work a special timestamp or a new special parameter hinting toward an

initialization can be utilized. Even the first key exchange after any initialization state can be discarded and the key at the end of the second key exchange process can be accepted as the valid key.

VIII. CONCLUSION

The offered method is for two-way authentication in limited capacity devices, in order to replace public-keys or certificates. As two parties know each other a key K_Φ can be shared. To increase the security of the key, the key has a lifetime. Each party has the same two distinct set of secrets. One is unique and inherent in the hardware and the other set is co-defined by both parties. Generated session key is encrypted by using K_Φ which is the output of the SHA-1 function.

The inputs of the SHA-1 which finally yields to K_Φ are the serial numbers, the nonces, addresses and the secrets from both sides. K_Φ is never transferred between the two sides and it makes the algorithm as secure as public-key cryptosystems.

REFERENCES

- [1] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trans. on Information Theory, Vol. IT-22, November 1976, pp. 644-654.
- [2] H. Orman, "The OAKLEY Key Determination Protocol", RFC2412, November 1998.
- [3] C. Adams, S. Farrell, "Internet X.509 Public Key Infrastructure: Certificate Management Protocols", RFC 2510, March 1999.
- [4] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone "Handbook of Applied Cryptography", CRC Press, 1996, Ch.12 pp511-512.
- [5] Dallas Semiconductor of Maxim Integrated Products Inc., Application Note 1770, "Securing Electronic Transactions Using SHA-1 Secure Hash Algorithm
- [6] Dallas Semiconductor of Maxim Integrated Products Inc., Application Note 3824, "Security in Embedded Systems".
- [7] Dallas Semiconductor of Maxim Integrated Products Inc., Application Note 3675, "Protecting the R&D Investment—Two-Way Authentication and Secure Soft-Feature Settings".
- [8] Dallas Semiconductor of Maxim Integrated Products Inc., Application Note Application Note 152, "SHA iButton Secrets and Challenges".
- [9] Dallas Semiconductor of Maxim Integrated Products Inc., Application Note Application Note 190, "Challenge and Response with 1-Wire SHA devices".
- [10] Texas Instruments, SLUS696A—June 2006—Revised February 2007, "SHA-1/HMAC Based Security and Authentication IC with SDQ Interface".
- [11] Texas Instruments, SLUA389A—July 2006—Revised October 2006, "How to Implement SHA-1/HMAC Authentication for bq26100".

Provable Electronic Marketplace Bidding Auction Protocol with Bid Privacy

Wenbo SHI, Injoo JANG, Hyeong Seon YOO

Abstract—In this paper, we proposed a provable electronic marketplace bidding auction protocol. The proposed protocol tries to reduce DOS attack and avoids replay data attack by providing ticket token and deal sequence number to the supplier. It utilizes efficient LPN-based authentication method to accomplish lightweight authentication. And it publishes an interpolating polynomial for sharing the data of determination process and avoids collusion between a customer and a certain supplier. Also it relaxes trust assumptions for three-party. According to comparison and analysis with other protocols, our proposed protocol shows good security and less computation cost.

Keywords —Anonymity, Electronic auction

I. INTRODUCTION

IN 2002, Collins et al. presented a multi-agent marketplace, MAGNET (Multi-Agent Negotiation Test-bed) for electronic business-to-business market [1]. As business value and criticality of electronic transactions increase, it becomes ever more important to examine the security risks present and take steps to avoid them. So Jaiswal et al. proposed security protocol to improve MAGNET in 2004, which consider security problem into real-world networks [2]. But the improved protocol still has some weaknesses: vulnerable to the replay data attack, DOS (denial-of-service) attack, anonymity disclosure weakness, collusion between a customer and a certain supplier.

The proposed protocol adopts conference key concept [3] and ticket token in supplier group. Also market generates deal sequence number (*dsn*) and random number (*r*) for suppliers who have download requests for quotes (*RFQ*). It utilizes efficient LPN-based authentication method to accomplish lightweight authentication [4,5]. When auction is closed, market constructs a simple interpolating polynomial for sharing the data of determination process in supplier group who have taken part in this auction. Sharing the data of determination process can avoid collusion between a customer and a certain supplier. Furthermore, we relax the assumption about collusion between customer agent and supplier agents and trust

assumptions for three-party in Jaiswal's scheme.

Sealed-bid security is inherent weakness, because it isn't easy to avoid auctioneer opening bids especially in two party's protocol. In Chang's protocol, there isn't a deliberate mechanism which can avoid opening bid before bidding phase is closed. It provides an auctioneer opportunity to collude with a certain bidder and leak updated information about bids to the bidder, so the anonymity of bidders depends on auctioneers [6]. In Liaw's protocol, the third party also can leak the information to a bidder whom he intends to collude with, so the anonymity of bidders depends on the third party [7]. In the proposed protocol, nobody else but the bidder himself can open bids before bidding phase is closed. It guarantees identity non-disclosure independently.

II. PROPOSED SCHEME

The proposed protocol has following phases: planning, bidding, auction close and winner determination (Fig. 1).

For convenience, we assume there are n_1 customers (C), n_2 suppliers (S) and one market (M) in our auction scheme. A certification authority (CA) is needed in key pre-distribution long-term key process. CA chooses and publishes large prime number p_1, p_2 such that p_1-1 and p_2-1 have large prime factors. Let q_1, q_2 are prime divisor of p_1-1 and p_2-1 separately, g_1 and g_2 are generator with order q_1, q_2 in $GF(p_1)$ and $GF(p_2)$ separately. Let S_i be the identity of a supplier, C_i be the identity of a customer.

CA assigns secret key $x_{i1} \in \mathbb{Z}^*_{q_1}$ and computes public key $y_{i1} = g_1^{x_{i1}} \bmod p_1$ for each C and M, where $1 < i_1 \leq n_1+1$ [3]. CA assigns secret key $x_{i2} \in \mathbb{Z}^*_{q_2}$ and computes public key $y_{i2} = g_2^{x_{i2}} \bmod p_2$ for each S and M, where $1 < i_2 \leq n_2+1$. CA assigns two symmetric key $x_{i3} \in_{\mathbb{R}} \{0,1\}^k, y_{i3} \in_{\mathbb{R}} \{0,1\}^k$, for each S and M, where $1 < i_3 \leq n_2+1$. Then, CA gives those secret keys to M, each C and S in a secure way.

A. Planning

C_i sends $M_i = S_{K_c}(RFQ)$ a RFQ message which is signed by C_i 's secret key S_{K_c} to M for publishing. After receiving RFQ message, M verifies and publishes *RFQ*. M constructs ticket token polynomial by steps below:

- 1). Randomly chooses integer r and ticket token $T \in \mathbb{Z}^*_{q_2}$ and gets timestamp t from the system and computes $A = g^r \bmod p$, $B = r \cdot T + H(t || A) \cdot x_{m2} \bmod q_2$, where $H()$ is a one-way hash function.

Wenbo Shi is with the School of Computer science and Engineering, Inha University, Incheon, Korea.

Injoo Jang is with the School of Computer science and Engineering, Inha University, Incheon, Korea.

Hyong Seon Yoo is with the School of Computer science and Engineering, Inha University, Incheon, Korea.

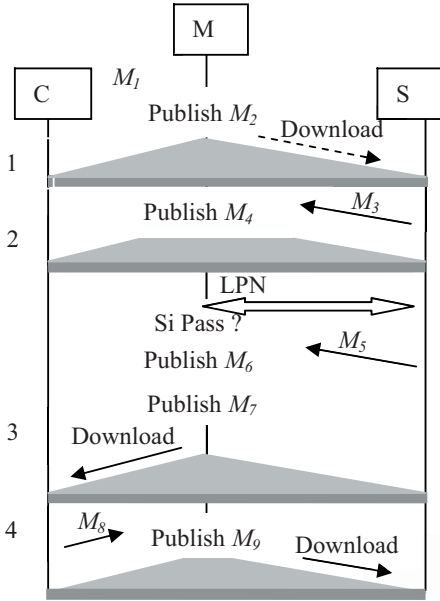


Fig. 1. The proposed protocol

- 2). Computes secret key shared with each S as: $k_{mi2} = y_{i2}^r \bmod p_2$, where $1 \leq i_2 \leq n_2$
- 3). Constructs ticket token polynomial $f(x)$ for publishing:

$$f(x) = \prod_{i_2=1}^{n_2} (x - k_{mi2}) + T \bmod p_2$$

$$= x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0 \bmod p_2 \quad (1)$$

Where $c_{n-1}, c_{n-2}, \dots, c_1, c_0 \in \mathbb{Z}^*q_2$

- 4). Publishes $M_2 = A, B, t, c_{n-1}, c_{n-2}, \dots, c_1, c_0$.

B. Bidding

If S_i is interested in this auction, S_i will do such steps:

- 1). Gets $A, B, t, c_{n-1}, c_{n-2}, \dots, c_1, c_0$ from M's publish board.
- 2). Checks whether t is a valid data or not.
- 3). Computes the secret key shared with M as:

$$k_{i2m} = A^{x_{i2}} \bmod p_2 \quad (2)$$

- 4). Gets T by computing $f(k_{mi2})$
- $$f(k_{i2m}) = (k_{i2m})^n + c_{n-1}(k_{i2m})^{n-1} + \dots + c_1(k_{i2m}) + c_0 \bmod p_2$$
- $$= T \bmod p_2 \quad (3)$$

5. Verify T by computing $H(t||A)$ and check the equation:

$$g^B \equiv A^T * y_{m2}^{H(t||A)} \bmod p_2 \quad (4)$$

After getting T , S_i use T to download RFQ . When S_i downloads the RFQ , M generates dsn and r to S_i . After getting dsn and r from M, S_i generates a bid-message comprising of RFQ number ($RFQ\#$), dsn and r , symmetric auction-session key (k_a), bid data (bid), where k_a is generated by S_i himself. Then S_i signs, hashes and encrypts message and sends M_3 to market. Where $M_3 = [RFQ\#, dsn, H(r, dsn), E_{k_a}(S_{k_s}(bid)), H(r, E_{k_a}(S_{k_s}(bid)))]$, $S_{k_s}(bid)$ is a bid data block signed by S_i 's secret key S_{k_s} , $E_{k_a}(S_{k_s}(bid))$ is a data block encrypted by k_a . After receiving messages came from S, M publishes all $M_4 = (RFQ\#, (dsn, M_3, H(M_3)))$ on publish board.

C. Auction close

When the auction is closed, M authenticates each S's agent by steps below:

1. S_i chooses a blinding vector a_i randomly $a_i \in_R \{0,1\}^k$, and sends $\{dsn, S_i, a_i, T_1\}$ to M, where T_1 denotes a valid timestamp.
2. After receiving $\{dsn, S_i, a_i, b_i\}$, M checks T_1 and chooses challenge b_i randomly $b_i \in_R \{0,1\}^k$, publishes $(dsn, S_i, a_i, b_i, T_2)$, where T_2 denotes a valid timestamp.
3. S_i gets b_i from publish board, then computes response $z_i = a_i x \oplus b_i y \oplus v$, and sends $\{dsn, S_i, z_i, T_3\}$, where v denotes a noise bit, T_3 denotes a valid timestamp.
4. After receiving $\{dsn, S_i, z_i, T_3\}$, M checks T_3 and publishes (dsn, S_i, z_i) and accepts the round if $a_i x \oplus b_i y = z_i$.

After that, M announces whether S_i 's agent passes the authentication or not. If passed, S_i 's agent send $M_5 = S_{S_{k_s}}(dsn, r, x_{i3} \oplus y_{i3} \oplus k_a)$. After receiving it, M publishes $M_6 = dsn, r, x_{i3} \oplus y_{i3} \oplus k_a$. S can check and verify whether their messages were actually received and displayed by M. M publish $M_7 = RFQ\#, E_{P_{k_c}}((dsn_1, r_1, k_{a1}), \dots, (dsn_i, r_i, k_{ai}), \dots, (dsn_n, r_n, k_{an}))$, where $E_{P_{k_c}}()$ is encrypted by C's public key y_{i1} . According to the message published by M, C_i will download corresponding M_3 from the publish/subscribe system, and decrypt the data block and get all valid bid information. Having authenticated S group twice, M can make sure that each participant is legitimate S.

D. Winner determination

C_i sends message about winner information $M_8 = S_{S_{k_c}}(RFQ\#, r_{winner})$ to M. After M receiving C_i's message, M checks whether the winner contained in legitimate S list $(dsn_1, r_1, k_{a1}), \dots, (dsn_i, r_i, k_{ai}), \dots, (dsn_n, r_n, k_{an})$. If the winner is contained, M publishes the winner information on board for notifying S. If there is a controversy about winner, M will choose a large prime number p and a primitive element g for $GF(p)$, where $GF(p)$ is the set of integers $\{0, 1, \dots, p-1\}$ with arithmetic operations defined modulo p . And M generates a symmetric session key K , $K \in \mathbb{Z}^*q$. Then M uses the signature datum of S who have taken part in current auction to construct a derivation function $F(x)$ and conceals K in it. After that, M publish the coefficient $c'_{n-1}, c'_{n-2}, \dots, c'_1, c'_0$ of the $F(x)$, where $S_{S_{k_{si}}}(k_{ai}, r_i)$ are S's signature data ($i=1, 2, \dots, n$). M encrypts bid data of determination process and publish $M_9 = RFQ\#, E_k(\text{bid determination process})$.

$$F(x) = \prod_{i=1}^n (x - h_i) + K \bmod p$$

$$= x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0 \bmod p \quad (5)$$

$$\text{Where } h_i = g^{S_{S_{k_{si}}}(k_{ai}, r_i) \bmod p-1} \quad (6)$$

$$c'_{n-1}, c'_{n-2}, \dots, c'_1, c'_0 \in \mathbb{Z}^*q$$

III. SECURITY ANALYSIS

Theorem 1. Assume no man can modify publish message except M. After M publish $A = g^r \bmod p$, $B = r * T + H(t||A) * x_{m2} \bmod q_2$, t , coefficients $c_{n-1}, c_{n-2}, \dots, c_1, c_0 \in \mathbb{Z}^*q_2$ of ticket token function (1), no man can get ticket token T besides S group.

Proof. Because M has computed each S's secret key k_{mi2} as the solution of the ticket token polynomial function $f(x)$, where $k_{mi2} = y_{i2}^r \bmod p_2$, $1 \leq i_2 \leq n_2$. Furthermore, only legal S can compute $k_{mi2} = y_{i2}^r \bmod p_2$, where $k_{mi2} = k_{i2m}$. So legal S can have the valid k_{mi2} that satisfies $f(k_{mi2}) = T \bmod p_2$ for getting T .

Situation 1. If one attacker wants to obtain r from $A = g^r \bmod p$, he will face the difficulty of solving the intractable discrete logarithm problem.

Situation 2. If one attacker wants to obtain T from $B = r * T + H(t|A) * x_{m2} \bmod q_2$, because there are two unknown parameters r and x_{m2} , still he must solve the intractable discrete logarithm problem.

Situation 3. If one attacker wants to compute T from the function $f(x)$, he should know the valid k_{mi2} that satisfies $f(k_{mi2}) = T \bmod p_2$. It means that the attacker must solve the intractable discrete logarithm problem.

Theorem 2. Assume M received S's message M_3 safely. M can make sure that M_3 comes from legal S group. After M publish M_4 on board, S can make sure that M receive RFQ very well.

Proof. S open RFQ# and dsn information for temporary identity in M_3 . We make sure that the key k_a larger than 160 bits and therefore is able to withstand the exhaustive key search attack on data block $E_{ka}(S_{Sks}(bid))$ [8]. Because M cannot decrypt the data block $E_{ka}(S_{Sks}(bid))$, and M has recorded r as r' in planning phase, market can just verify whether information dsn and data block $E_{ka}(S_{Sks}(bid))$ are valid by computing $hash(r, dsn) \stackrel{?}{=} hash(r', dsn)$ and $hash(r, E_{ka}(S_{Sks}(bid))) \stackrel{?}{=} hash(r', E_{ka}(S_{Sks}(bid)))$. Because an attack cannot get valid r to forge $hash(r, dsn)$ and $hash(r, E_{ka}(S_{Sks}(bid)))$. After verifying the data block, M can make sure whether M_3 come from legal S or not. After M published $M_4 = (RFQ\#, (dsn, M_3, hash(M_3)))$ on board, S can verify whether M receive their message M_3 correctly by computing $hash(M_3) \stackrel{?}{=} hash(M_3')$.

Theorem 3. Assume M finished the communication with S by LPN authentication method. Mutual authentication has achieved between M and each S.

Proof. The hardness of the computational LPN problem has been shown to be NP-complete [4]. Our LPN-based authentication method adopted HB^+ computing prototype. Even though Gilbert proposed that HB^+ is not secure against a man-in-the-middle attack [5], because our auction scheme inherits the idea of publish system, we can make sure that the process of authentication is secure and sets up mutual authentication.

The condition when HB^+ protocol attack happen is that the attacker can manipulate challenges sent by M to a S during the authentication message exchanges. In our LPN-based authentication process, M utilizes publish system to show messages which S have sent. So S can check and verify whether their messages were actually received and displayed by market. We assume that there is an attacker in the middle, and he can

manipulate message sent by S to M. But the attacker cannot modify any information, because S can check the message on board each round. Due to the publish system, the attacker cannot manipulate the challenges published by M. According to what is mentioned above, the attacker doesn't have any opportunity to disturb the authentication process.

Theorem 4. Assume M publish message correctly, where message are coefficients $c'_{n-1}, c'_{n-2}, \dots, c'_1, c'_0 \in Z^*_q$ of function $F(x)$ and E_k (bid determination process), then M can make sure that S who have taken part in this auction can check fair deal.

Proof. Because M computes each S's signature data $S_{Sksi}(k_{ai}, r_i)$ as the solution h_i (see equation (6)) of the polynomial function $F(x)$, where $S_{Sksi}(k_{ai}, r_i)$ is S's signature data ($i=1, 2, \dots, n$). So only legal S who have taken part in this auction session have the valid h_i that satisfies $f(h_i) = K \bmod p$ for computing K from the function. After getting K , each legal S can decrypt data block E_k (bid determination process) and check the fair deal.

Situation 1. If an attacker want to compute K from the coefficients of function(5), he should know the valid h_i that satisfies $f(h_i) = K \bmod p$. It means that the attacker must solve the intractable discrete logarithm problem. Therefore, the attacker certainly cannot reconstruct the $F(x)$ to get the session key K from there n points $(1, F_i(1)), (2, F_i(2)), \dots, (n, F_i(n))$ only.

IV. SECURITY ANALYSIS

In this section, we discuss Chang's protocol (a), Liaw's protocol (b) and proposed protocol (c) [6, 7]. The comparisons of computation operations of the initial phase and bidding phase among those protocols are shown in TABLE I. Assume length of the prime number p is 1024 bits in Diffie-Hellman and public key encryption, symmetric key length is 128 bits (for AES), hash function digest is 160 bits (for SHA-1), public key certification is 1024 bits, signature length is 320 bits (for DSA). Because operation of RSA's computation can be summarized as a modular exponentiation operation, and the computation cost of a modular exponentiation computation is about $O(|n|)$ times that of a modular multiplication computation where $|n|$ denotes bit length of n . So compared with a modular multiplication computation in Z_n^* , the computation time consumed by hashing operations, symmetric encryptions or decryptions can be neglected. And symmetric cryptosystem is 1000 times faster than asymmetric cryptosystem and hash function is 10 times faster than symmetric cryptosystem [9].

V. CONCLUSIONS

As mentioned above, the current paper proposed an electronic marketplace bidding auction protocol whose security is based on the well-known Discrete Logarithm assumption. It satisfies security requirements of an electronic auction, such as anonymity, non-repudiation, verifiability etc. And the proposed scheme relaxes trust assumptions for three-party in Jaiswal's scheme. According to discussion and analysis with Chang et

al.'s protocol and Liaw et al.'s protocol, our proposed protocol shows better security in anonymity, fairness and reliance on the third party. Therefore, the advantages of our proposed bidding auction protocol are difficulty collusion.

TABLE I.
NUMBER OF OPERATIONS FOR PHASES

Phase	a	b	c
Initiation phase	4 HF	5 HF	2HF
	2 SKE	0	0
	2 SKD	0	0
	2 PKE	3 PKE	1 PKE
	2 PKD	3 PKD	1 PKD
	4 ME	0	6ME
	2 R	5 R	3 R
Bidding phase	0	0	4 HF
	2 SKE	0	1 SKE
	2 SKD	0	0
	1 PKE	5 PKE	1 PKE
	1 PKD	5 PKD	0
	0	0	1MM

PKE: Public Key Encryption; PKD: Public Key Decryption;
SKE: Symmetric Key Encryption; SKD: Symmetric key decryption;
HF: Hash Function; ME: Modular Exponentiation;
R: generate a random number; MM: Modular multiplication

REFERENCES

- [1] J. Collins, W. Ketter and M. Gini, "A multi-agent negotiation testbed for contracting tasks with temporal and precedence constraints," International Journal of Electronic Commerce, vol.7, no.1, pp.35-57, 2002
- [2] A.Jaiswal, Y. kim and M. Gini, "design and implementation of a secure multi-agent marketplace," Electronic Commerce Research and Applications, vol.3, no.4, pp.355-368,2004
- [3] E.K. Ryu, J.-Y. Im and K.Y. Yoo, "Security of Tseng - Jan's conference key distribution system," Applied Mathematics and Computation, 167(2), 833-839,2005
- [4] O.Regev, "On Lattices, Learning with errors, Random Linear Codes. and Cryptography," 37th ACM symposium on theory of computing, 84-93,2005
- [5] H. Gilbert, M. Robshaw, H. Silbert, "An active attack against HB+ - a provable secure lightweight authentication protocol,"Cryptology ePrint Archive, Report 2005/237, 2005
- [6] Chang, Y.F. and Chang ,C.C, "Enhanced anonymous auction protocols with freewheeling bids", 20th International Conference on Advanced Information Networking and Applications, AINA (1), 353-358 ,2006
- [7] Horng-Twu Liaw, Wen-Shenq Juang and Chi-Kai Lin, "An electronic online bidding auction protocol with both security and efficiency," Applied Mathematics and Computation, 174(2), 1487-1497, 2006
- [8] National Institute of Standards and Technology (NIST), Digital signature standard. Federal Information Processing Standards Publication, FIPS PUB 186, p. 20, 1994
- [9] Chun-I Fan, Yung-Cheng Chan and Zhi-Kai Zhang, "Robust remote authentication scheme with smart cards," Computers & Security , 24(8) , 619-628, 2005

Variant Constructions for TMTO based on Random Mapping Statistics

Nurdan SARAN, Ali DOĞANAKSOY

Abstract—The time memory trade-off (TMTO) is a generic method, introduced by Hellman, for quickly inverting a one-way function. In this paper we present some properties of random mappings in terms of TMTO attacks. We also propose new variants of the technique. Firstly, we present a technique to construct Perfect Hellman tables by using random mapping properties. Finally, we give a variant distinguished method (DP) method which has a high success rate for random permutations.

Keywords —Cryptanalysis, Time Memory Trade Off Method, Random Mappings Statistics.

I. INTRODUCTION

One-way functions exist in almost all areas of cryptography. Securities of encryption schemes, authentication mechanisms, and various other cryptographic protocols depend on the hardness of inverting one-way functions which they are based on. By inversion of a one-way function, we mean a process which finds a pre-image of a given point, if there exists any. Exhaustive search is an obvious method to find a pre-image of a given point which is trying all possible inputs and checking whether they yield the given value. If it is the case that the search operation is expected to be done for different points in the future -a more likely case to happen in real life-, the time required by exhaustive search may turn out to be excessive. Constructing a lookup table containing pre-images of all points may be another solution. In this situation, it requires extreme amounts of memory for the functions acting on large sets. Balancing the gap between the solution time and the required memory, in other words trading memory for time, is important. Hellman[1] proposes a probabilistic method which suggests a tradeoff between time and memory by storing some pre-computed data in the memory. Time Memory Trade Off (TMTO) has a lower time complexity (in online phase) than exhaustive search and a lower memory complexity than lookup table. If the attacker has a large memory, the computation time will be less.

There are mainly two improvements on TMTOs. Following Hellman's work on DES, Rivest introduces the concept of distinguished points(DP) which reduces the number of table lookups. In his dissertation [2], Borst gives expressions on success probability and complexity for distinguished points. [3] Standaert et al claim that they corrected the probability of success for distinguished points to correspond with practical implementations. Efficient mask functions are proposed and

experimentally confirmed and used to build a FPGA design to perform realistic tradeoffs against the block cipher DES. The second improvement is called as Rainbow Tables. Oechslin [4] proposes Rainbow Tables in which a successive reduction function is used for each column in the chain, rather than constructing r tables with different reduction functions. There are t reduction functions; one for each column. In [5], Barkan et al. give the upper bound for coverage and lower bound for worst case time complexity when the structures of f is not used and describe some variants of rainbow tables. In [6] Hong and Sarkar apply TMTO on various block cipher modes of operations and they show how to apply multiple data TMTO to both CBC and CFB modes of operations. In addition, they show that hash function's preimage resistance is not equal to its digest length. Hong et al. [7] propose a variant of the DP technique, named variable DP (VDP), and show how to combine distinguished points with rainbow approach.

Babbage [8] and Golic [9] independently apply TMTOs on stream cipher. Application of TMTO on stream ciphers is different than the application of TMTO on block ciphers. When a stream cipher is taken into account, there are two types of attack, in terms of the one-way function the attacker tries to invert. The aim of the attacker might be inverting the function from secret key(k bit) to output prefix(k bit) [6] or inverting the function from internal state(s bit) to output prefix(s bit)[8]-[10]. If an attacker can find any of the actual states then he can find the rest of the keystream. Thus, he does not have to find the initial state (or the key). Moreover, he may find the initial state by using reverse engineering methods in many cases. Biryukov and Shamir [10] generalize TMTOs to multiple data and call Time/Memory/Data Trade Offs(TMDT) for stream ciphers. When D bits of keystream is given (there is no difference between known plaintext and chosen plaintext attack when a stream cipher is taken into account), $D - \log(N) + 1$ overlapping prefixes can be obtained. In the online stage, when D bits are given, it is aimed to find the pre-image of any one of these prefixes. Total memory is reduced from mt to mt/D . Since Hellman's table for block ciphers is constructed for a particular plaintext block, the multiple prefix is useless. On the other hand, precomputed table can be used on multiple prefixes for stream ciphers. [11]-[12] introduce time/memory/key trade-off(TMK) attack on block ciphers, Hellman's algorithm is generalized for the case of multiple data. Distinguished points on stream ciphers are studied by [10]-[13]. Distinguished points method is applied on stream ciphers, and it is called BSW sampling. Biryukov, Shamir and Wagner [13] improve Golic's attack in which the key is computed in about one second during the first two

N. Saran is with the Department of Computer Engineering, Cankaya University, Ankara, e-mail: buz@cankaya.edu.tr

A.Doğanaksoy is with the Department of Mathematics, METU, email: aldoks@metu.edu.tr.

minutes of the conversation on a single PC. Dunkelman and Keller [14] show the treatment of IV in TMTOs and claim that setting the IV length to be equal to the key length, k , does not ensure a k -bit security against TMTTO attacks. For each chosen IV, the attacker prepares a Hellman table (or Rainbow table) to invert the function from key to the output prefix. Therefore, the resistance to TMTTO attacks is considered to be an important criteria when designing a stream cipher.

Random mappings are functions from a finite set of n elements onto m elements. They are widely used in combinatorial problems. Various characteristics of random mappings have been studied in [15], [16], [17], [18]. Random mapping statistics have a great importance place when constructing TMTTOs table. Our main question in this study is "Is it possible to have a high success rate of TMTTO by using the properties of random mappings?"

In the following section, we briefly summarize Hellman's construction, and the two main improvements of the attack. Then we calculate the expected values of two of the random mapping properties, and summarize the results in the literature. Finally, we give new constructions for TMTTOs based on random mapping statistics.

II. PRELIMINARIES

A. Hellman's Construction

Hellman introduced a TMTTO attack and applied on the block cipher, DES. A TMTTO application is composed of two phases; an offline (precomputation) phase and online phase.

Offline Phase: Starting at random m points, chains of length t are generated by iteratively evaluating $f = E \circ R$, E represents for encryption function and R represents for reduction function. $m \times (t+1)$ matrix is formed which is called Hellman table. By this way, k tables are computed in which each table has different R so if two entries in two tables are the same, usage of different functions will result in different elements in the next chain item. To save memory we store only the first and last element of a chain. By knowing the starting point, the successive elements can be recalculated in the chain. This process is expected to be equivalent to the exhaustive search.

Online Phase: For a preimage of a given point c_0 , it is tried to find out if the key that is used to generate c_0 is among the one used in the generated table. To do so, starting by checking if c_0 is equal to any points of the last column (any endpoints), it is tested to find the preimage by computing the previous entry. If c_0 is not equal to any points of the last column, $f(c_0)$ is calculated and checked for a match in the $(t-1)^{st}$ column. f is applied repeatedly until c_0 is in the second column of the matrix. It should be noted that finding a match doesn't imply that the desired key is found, it may be a false alarm.

B. Rainbow Tables

Oechslin suggested to use Rainbow tables of size $mt \times t$ in which different reduction functions are applied for each iteration, instead of having t different tables. Generating a table without merges is another trade because it will increase the precomputation time. Perfect tables are tables in which

there is no merges. Firstly more chains are generated since merging chains will have the identical endpoints, they can be easily discarded (in both rainbow and DP tables). In [19] Avoine . stated that to construct a perfect Hellman table is not efficient since all chains have to be looked up. We give in Section IV-A a new construction technique that constructs Perfect Hellman Tables .

C. DP Tables

Rivest suggested to use distinguished points as endpoints for the chains to reduce the number of memory accesses. In distinguished points, the chain is terminated whenever a distinguished property is obtained, instead of generating fixed length chains. Only endpoints which encountered a distinguished point in less than t iterations will be stored otherwise they will be discarded. Chains are generated until a distinguished point is reached and the triple $(SP, EP, lengthofchain)$ is stored. Otherwise until t_{max} iterations if a distinguished point is not reached , that chain is discarded. Moreover if the chain length is less than some t , say t_{min} that chain is also discarded. If same distinguished point occurs in different chains, the triple with maximum chain length is stored (since merging chains will have the same endpoint). It is clear that the chain lengths are variable. This improvement reduces the memory access in the online phase, since the ciphertext is compared to the end points only if it is a distinguished point.

III. RANDOM MAPPING STATISTICS

Let $\mathcal{X}$ denote the finite domain of size n and $\mathcal{F}_n$ denote the collection of all functions (f) from domain $\mathcal{X}$ into range $\mathcal{X}$. We will consider only random mappings model where every function from $\mathcal{F}_n$ is equally likely to be chosen. So the sample space consists of n^n random mappings in other words the probability that a particular function(f) from $\mathcal{F}_n$ is chosen will be $\frac{1}{n^n}$.

Starting from a point $x_0 \in \mathcal{X}$ and iteratively applying f , the following sequence is obtained;

$$\{x_0, f(x_0), f^2(x_0), \dots\}. \quad (1)$$

The k -th iteration of f on $\mathcal{X}$, where $0 \leq k \leq n$ will be $f^k(x_0) = f(f^{k-1}(x_0))$ where $f^0(x_0) = x_0$. For some $k \geq 0$ if $f^k(x_0) = y$ then we will call y to be a k th image of x_0 in f . For some $k \leq 0$ if $f^k(x_0) = y$ then we will call y to be a k th inverse of x_0 in f . For $k < 0$, $f^k(x_0)$ may not exist, which we will call *terminal nodes*, (in other words, a node may have no inverse image) or may not be uniquely determined (more than one inverse which will cause a *false alarm* from a view point of TMTTO). Each random mapping, f can be represented by a functional graph.

A. Graph Representation of Functions

A functional graph of a function $f : \mathcal{X} \rightarrow \mathcal{X}$ is a directed graph whose nodes are the elements of $\mathcal{X}$ and whose edges are the ordered pairs $(x, f(x))$, for all $x \in \mathcal{X}$.

In Figure 1 , the typical behavior of an iteration operation is given. Since the set $\mathcal{X}$ is finite, after some iterations, we

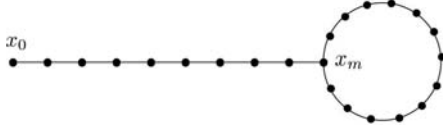


Fig. 1: Functional Graph

will encounter a point that has occurred before. Let $f^m(x_0)$, $0 \leq m \leq n-1$ be the point that the iteration enters a loop. Then $f^m(x_0) = f^k(f^m(x_0))$, k is the smallest positive integer which we call the *cycle length*. The path between x_0 and $f^m(x_0)$ is called the *tail length*. The sum of the tail length and cycle length is defined as the ρ -length.

The statistical behaviors of random mappings (See [17], [20], [16], [18], [21], [15]) are summarized as in the followings:

Theorem 1: The probability distributions for random functional graph of size n are:

(i) Number of Components

$$Pr(\#components = k) = \frac{n!}{k!n^n} \sum_{\mu=k}^n S_{\mu}^k \sum_{k_1, \dots, k_n} \frac{1}{k_1! \dots k_n!} \left(\frac{1}{1!}\right)^{k_1} \dots \left(\frac{1}{n!}\right)^{k_n} \quad (2)$$

where S_{μ}^k are Stirling's Numbers of the First Kind and sum over all choices of $k_1, \dots, k_n$ with $k_i > 0$ ($i = 1, \dots, \mu$) and $\sum_{i=1}^n k_i = \mu$, $\sum_{i=1}^n i k_i = n$

(ii) ρ -length

$$Pr(\rho - length = k) = \frac{(n-1)!}{(n-k)!} \frac{k}{n^k} \quad (3)$$

(iii) Cycle-length

$$Pr(cycle - length = k) = \sum_{j=k}^n \frac{(n-1)!}{(n-j)!n^j} \quad (4)$$

Although the expected values of random mappings are widely studied in literature, we calculate the expected values for ρ length and cycle length and resulting tail length with a different approach.

1) ρ -length:

$$\begin{aligned} E(\rho - length = k) &= \sum_{k=0}^n \frac{(n-1)!}{(n-k)!} \frac{k^2}{n^k} \text{ by writing } k \rightarrow n-k \\ &= \frac{(n-1)!}{n^n} \sum_{k=0}^n \frac{(n-k)^2}{k!} n^k \\ &= \frac{(n-1)!}{n^n} \left[n^2 \sum_{k=0}^n \frac{n^k}{k!} - 2n \sum_{k=0}^n \frac{n^k k}{k!} + \sum_{k=0}^n \frac{k^2 n^k}{k!} \right] \end{aligned}$$

$$\text{Let } Y_1 = \sum_{k=0}^{n+1} \frac{n^k}{k!}, Y_2 = \sum_{k=0}^{n+1} \frac{n^k k}{k!}, Y_3 = \sum_{k=0}^{n+1} \frac{n^k k^2}{k!}$$

and define

$$F(x) = \frac{e^{nx}}{2} \text{ thus } F(x) = \sum_{k=0}^{\infty} \frac{n^k x^k}{k!} \text{ then } Y_1 \approx F(1)$$

$$F'(x) = \frac{ne^{nx}}{2} \text{ thus } F'(x) = \sum_{k=0}^{\infty} \frac{kn^k x^{k-1}}{k!} \text{ then } Y_2 \approx F'(1)$$

$$F''(x) = \frac{n^2 e^{nx}}{2} \text{ thus } F''(x) = \sum_{k=0}^{\infty} \frac{k^2 n^k x^{k-2}}{k!} - \frac{kn^k}{k!} \text{ then } Y_3 \approx F''(1) + F'(1)$$

$$\begin{aligned} E(k) &= \frac{n!}{n^n} [(n^2) e^n - 2n(ne^n) + n^2 e^n + ne^n] \\ &\cong \frac{n!}{n^n} \frac{e^n}{2} = \sqrt{\frac{\pi n}{2}} \end{aligned}$$

2) cycle-length :

$$\begin{aligned} E(cycle - length = k) &= \sum_{k=0}^n \sum_{j=k}^n \frac{(n-1)!}{(n-j)!n^j} k \\ &= \sum_{j=1}^n \frac{(n-1)!}{(n-j)!n^j} + 2 \sum_{j=2}^n \frac{(n-1)!}{(n-j)!n^j} + \dots + \frac{(n-1)!}{n^n} \\ &= \frac{1}{2} \sum_{j=0}^n \frac{(n-1)!(j+1)j}{(n-j)!n^j} \\ &= \frac{(n-1)!}{2} \sum_{j=0}^n \frac{(j+1)j}{(n-j)!n^j} \text{ by writing } j \rightarrow n-j \\ &= \frac{(n-1)!}{2n^n} \sum_{j=0}^n \frac{(n-j)(n-j+1)}{j!n^{-j}} \\ &= \frac{(n-1)!}{2n^n} \left[(n^2 + n) \sum_{j=0}^n \frac{n^j}{j!} - (2n+1) \sum_{j=0}^n \frac{n^j j}{j!} + \sum_{j=0}^n \frac{j^2 n^j}{j!} \right] \\ &= \frac{(n)! e^n}{2n^n} = \sqrt{\frac{\pi n}{8}} \end{aligned}$$

Since $E(\rho - length) = E(cycle - length) + E(tail - length)$, then $E(cycle - length = k) = \sqrt{\frac{\pi n}{8}}$

Theorem 2: The expected values for a random mapping are [20]-[17]

- (i) Number of components = $\frac{\ln(n)}{2}$
- (i) Number of terminal nodes = $e^{-1}n \approx 0,3679n$
- (ii) Number of image nodes = $(1 - e^{-1})n \approx 0,6321n$
- (iii) Average cycle length = $\sqrt{\frac{\pi n}{8}} \approx 0,6267\sqrt{n}$
- (iv) Average tail length = $\sqrt{\frac{\pi n}{8}} \approx 0,6267\sqrt{n}$
- (v) Average ρ length = $\sqrt{\frac{\pi n}{2}} \approx 1,2533\sqrt{n}$
- (vi) Average component size = $\frac{2n}{3}$

- (vii) Maximum cycle length = $0.78248\sqrt{n}$
- (viii) Maximum tail length = $1.73746\sqrt{n}$

B. Random Permutations

Permutations have the unary functional graphs that the sum of in-degrees must be the same as the sum of the out-degrees. Each node must have exactly one inverse. There are no terminal nodes and tail nodes. This also shows that every node is cyclic.

Let $\alpha(n)$ be the number of cycles in a permutation. Then we have

$$Pr(\alpha(n) = j) = \frac{S_n^j}{n!}$$

where $S_n^j, 1 \leq j \leq n$ is a Stirling number of first kind [18].

Let L_n be the expected length of the longest cycle in a random permutation then

$$\lim_{n \rightarrow \infty} (L_n/n) = 0.62432965$$

Theorem 3: The expected values for a random permutation are

- (i) Number of components = $\sum_{i=1}^n \frac{1}{i}$
- (ii) Number of terminal nodes = 0
- (iii) Number of image nodes = n
- (iv) Average cycle length = $\frac{n+1}{2}$
- (v) Average tail length = 0
- (vi) Average ρ length = $\frac{n+1}{2}$
- (vii) Maximum cycle length = $0.62432965n$

It should be noted that the average cycle length as seen from a random node, u , is as in the above theorem.

However the average cycle length of a mapping is

$$\text{Average cycle length} = \frac{n}{\#components} = \frac{n}{\ln n}.$$

Since $\#components \approx \ln n$

IV. VARIANT CONSTRUCTIONS

A. Perfect Hellman

Assuming the encryption function is modeled as a random mapping the set into itself, if we consider the graph representation of a random mapping, we choose our start points as terminal nodes (we mean the points which have no preimage). It is clear that to find the terminal nodes, it is necessary to increase precomputation from N to $2N$. Since there are $N' = N * e^{-1}$ terminal nodes, starting from N' by iteratively applying f we construct a Hellman table. In [19], starting from m_0 random points, maximum number of perfect chains of length t is given as

$$m(t, m_0) = \frac{m_0}{1 + \frac{tm_0}{2N}}$$

and maximum number of chains of length t by starting with m_0 equal to N is given as

$$m_{max} = \frac{2N}{t+2}$$

Starting from N' points, maximum number of chains of length t of Perfect Hellman table will be $m_{max} \approx \frac{2N}{t+6}$.

This shows us that the complexity of Perfect Hellman table will approximately be equal to the complexity of Perfect Rainbow table.

B. Variant Distinguished Point Table

Our main aim is to construct a table from distinguished point to distinguished point. Let D be the number of distinguished points. We construct a table of size, D . To do this, we first list distinguished points as starting points. Then, we iteratively apply f until a distinguished point is reached. By constructing a table in this manner, we have $\approx 99\%$ success rate for a random permutation. Average cycle length for a random permutation is $\approx \frac{n}{\ln n}$. The memory complexity of the attack is equal to the number of distinguished points.

For a random mapping, we can construct the same table. If there is no distinguished point in the chain, then the chain will enter in an infinite loop. In order to prevent this undesired situation, we iterate until a predefined time, t , then the chain is discarded. (The reader should note that t will be smaller than the average cycle length of a random mapping).

V. CONCLUSION

Resistance against TMTO attacks is an important criteria for designing a cipher. In this paper, we summarize the random mapping statistics in terms of TMTO attacks. We also give the expected values of cycle length, ρ length and tail length of a random mapping. Then some properties of random permutations are given. We present some variant constructions of TMTOs depending on the random mapping statistics. Perfect Hellman tables are constructed by choosing the starting points from the terminal nodes of a random mapping. A table from distinguished point to distinguished point is constructed without restrictions of time, t for random permutations. Variant distinguished point method can also be applied on random mappings.

REFERENCES

- [1] M. E. Hellman, "A cryptanalytic time-memory trade-off," *IEEE Transactions on Information Theory*, vol. 26, no. 4, pp. 401–406, 1980.
- [2] J. Borst, "Block ciphers: Design, analysis and side-channel analysis," Ph.D. dissertation, Katholieke Universiteit Leuven, 2001.
- [3] F.-X. Standaert, G. Rouvroy, J.-J. Quisquater, and J.-D. Legat, "A time-memory tradeoff using distinguished points: New analysis & fpga results," in *CHES*, ser. Lecture Notes in Computer Science, B. S. K. Jr., Çetin Kaya Koç, and C. Paar, Eds., vol. 2523. Springer, 2002, pp. 593–609.
- [4] P. Oechslin, "Making a faster cryptanalytic time-memory trade-off," in *CRYPTO*, ser. Lecture Notes in Computer Science, D. Boneh, Ed., vol. 2729. Springer, 2003, pp. 617–630.
- [5] E. Barkan, E. Biham, and A. Shamir, "Rigorous bounds on cryptanalytic time/memory tradeoffs," in *CRYPTO*, ser. Lecture Notes in Computer Science, C. Dwork, Ed., vol. 4117. Springer, 2006, pp. 1–21.

- [6] J. Hong and P. Sarkar, "New applications of time memory data trade-offs," in *ASIACRYPT*, ser. Lecture Notes in Computer Science, B. K. Roy, Ed., vol. 3788. Springer, 2005, pp. 353–372.
- [7] J. Hong, K. C. Jeong, E. Y. Kwon, I.-S. Lee, and D. Ma, "Variants of the distinguished point method for cryptanalytic time memory trade-offs," in *ISPEC*, ser. Lecture Notes in Computer Science, L. Chen, Y. Mu, and W. Susilo, Eds., vol. 4991. Springer, 2008, pp. 131–145.
- [8] S. Babbage, "Improved "exhaustive search" attacks on stream ciphers," in *ECOS 95 (European Convention on Security and Detection)*, no. 408 in IEE Conference Publication, May 1995.
- [9] J. D. Golic, "Cryptanalysis of alleged a5 stream cipher," in *EUROCRYPT*, 1997, pp. 239–255.
- [10] A. Biryukov and A. Shamir, "Cryptanalytic time/memory/data tradeoffs for stream ciphers," in *ASIACRYPT*, ser. Lecture Notes in Computer Science, T. Okamoto, Ed., vol. 1976. Springer, 2000, pp. 1–13.
- [11] A. Biryukov, S. Mukhopadhyay, and P. Sarkar, "Improved time-memory trade-offs with multiple data," in *Selected Areas in Cryptography*, ser. Lecture Notes in Computer Science, B. Preneel and S. E. Tavares, Eds., vol. 3897. Springer, 2005, pp. 110–127.
- [12] S. Mukhopadhyay and P. Sarkar, "Application of Ifsrs in time/memory trade-off cryptanalysis," in *WISA*, ser. Lecture Notes in Computer Science, J. Song, T. Kwon, and M. Yung, Eds., vol. 3786. Springer, 2005, pp. 25–37.
- [13] A. Biryukov, A. Shamir, and D. Wagner, "Real time cryptanalysis of a5/1 on a pc," in *FSE*, ser. Lecture Notes in Computer Science, B. Schneier, Ed., vol. 1978. Springer, 2000, pp. 1–18.
- [14] O. Dunkelman and N. Keller, "Treatment of the initial value in time-memory-data tradeoff attacks on stream ciphers," *Inf. Process. Lett.*, vol. 107, no. 5, pp. 133–137, 2008.
- [15] J. Arney and E. A. Bender, "Random mappings with constraints on coalescence and number of origins," *Pacific J. Math.*, vol. 103, no. 2, pp. 269–294, 1982.
- [16] D. E. Knuth, *Art of Computer Programming, Volume 2: Seminumerical Algorithms (3rd Edition)*. Addison-Wesley Professional, November 1997. [Online]. Available: <http://www.amazon.ca/exec/obidos/redirect?tag=citeulike09-20&path=ASIN/0201896842>
- [17] B. Harris, "Probability distributions related to random mappings," *The Annals of Mathematical Statistics*, vol. 31, no. 4, pp. 1045–1062, 1960.
- [18] V. F. Kolchin, *Random Mappings*. Springer, -Verlag, 1986.
- [19] G. Avoine, P. Junod, and P. Oechslin, "Time-memory trade-offs: False alarm detection using checkpoints," in *INDOCRYPT*, ser. Lecture Notes in Computer Science, S. Maitra, C. E. V. Madhavan, and R. Venkatesan, Eds., vol. 3797. Springer, 2005, pp. 183–196.
- [20] P. Flajolet and A. M. Odlyzko, "Random mapping statistics," in *EUROCRYPT*, 1989, pp. 329–354.
- [21] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. Boca Raton, Florida: CRC Press, 1996, uRL: <http://cacr.math.uwaterloo.ca/hac>.

Extended Results for Independence and Sensitivity of NIST Randomness Tests

Ali DOĞANAKSOY, Barış EGE, Köksal MUŞ

Abstract—Statistical tests are of crucial importance in determining the quality of pseudo random number generators. But these tests, when used together in a test suite, should be independent to have reliable results. In this study, we evaluate the dependency of the tests in the NIST test suite by experimental results. We also analyze the sensitivity of these tests to some basic transformations.

Keywords —NIST, Randomness Tests, Independence.

I. INTRODUCTION

Pseudo random number generators (PRNGs) are used in various subjects from cryptography to simulations. In cryptography, PRNGs are needed to provide security in authentication protocols, digital signature protocols, generation of encryption keys, etc. As a result of this, the quality of a PRNG is of crucial importance when used in cryptography. Therefore the quality of a PRNG should be carefully determined.

Since a theoretical approach to show the quality of a PRNG is not feasible, statistical testing of sample sequences are used for this purpose. There are various test suites [1], [2], [3], [4], [5] in literature which are collections of statistical randomness tests to evaluate various properties of a PRNG. However, as Soto stated in [6], the tests in a statistical test suite should be independent to achieve reliable results. In [7], the correlation among *approximate entropy*, *overlapping serial* and *universal* test is shown using defective sources. Recently in [8], it is shown that *frequency*, *overlapping template*, *longest run of ones*, *random walk height* and *maximum order complexity* tests are correlated for sequences of length $n = 20$ and $n = 30$, through observing all possible sequences. Also in [8], the concept of *sensitivity of tests to simple transformations* is introduced.

In this paper, since it is not feasible to observe all possible sequences for long sequences, we apply a new approach and extend the ideas in [8] to longer sequences to evaluate the independence and sensitivity of some chosen tests from the NIST Test Suite through experimental results.

In Section II, we provide basic descriptions of the tests we used in the study and statistical ideas used in NIST Test Suite. In Sections III and IV, experimental results on the independence and sensitivity of the tests are presented respectively. In the last section, we give some concluding remarks and point out some possible future work directions.

We would like to thank Meltem Sönmez Turan and members of the SADIST Workgroup (Onur Koçak, Dilek Arslan and Cihangir Tezcan) for their comments and support on our paper.

II. NIST TEST SUITE

NIST Test Suite consists of a total of 16 tests which evaluate the randomness of a given sequence or a random number generator. These tests focus on a variety of non-randomness properties in a sequence. The descriptions (from [1]) of the tests used for the study in this paper are given below.

- **Frequency (Monobits) Test:** The focus of the test is the proportion of zeros and ones for the entire sequence. The purpose of this test is to determine whether that number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence. The test assesses the closeness of the fraction of ones to $\frac{1}{2}$, that is, the number of ones and zeros in a sequence should be about the same.
- **Test for Frequency Within a Block:** The focus of the test is the proportion of zeros and ones within m -bit blocks. The purpose of this test is to determine whether the frequency of ones in an m -bit block is approximately $\frac{m}{2}$.
- **Runs Test:** The focus of this test is the total number of zero and one runs in the entire sequence, where a run is an uninterrupted sequence of identical bits. A run of length k means that a run consists of exactly k identical bits and is bounded before and after with a bit of the opposite value. The purpose of the runs test is to determine whether the number of runs of ones and zeros of various lengths is as expected for a random sequence. In particular, this test determines whether the oscillation between such substrings is too fast or too slow.
- **Test for the Longest Run of Ones in a Block:** The focus of the test is the longest run of ones within m -bit blocks. The purpose of this test is to determine whether the length of the longest run of ones within the tested sequence is consistent with the length of the longest run of ones that would be expected in a random sequence. Note that an irregularity in the expected length of the longest run of ones implies that there is also an irregularity in the expected length of the longest run of zeros. Long runs of zeros were not evaluated separately due to a concern about statistical independence among the tests.
- **Random Binary Matrix Rank Test:** The focus of the test is the rank of disjoint sub-matrices of the entire sequence. The purpose of this test is to check for linear dependence among fixed length substrings of the original

sequence.

- **Overlapping (Periodic) Template Matching Test:** The focus of this test is the number of pre-defined target substrings. The purpose of this test is to reject sequences that show deviations from the expected number of runs of ones of a given length. For this test, an m -bit window is used to search for a specific m -bit pattern. If the pattern is not found, the window slides one bit position. For this test, when the pattern is found, the window again slides one bit, and the search is resumed.
- **Linear Complexity Test:** The focus of this test is the length of a generating feedback register. The purpose of this test is to determine whether or not the sequence is complex enough to be considered random. Random sequences are characterized by a longer feedback register. A short feedback register implies non-randomness.
- **Serial Test:** The focus of this test is the frequency of each and every overlapping m -bit patterns across the entire sequence. The purpose of this test is to determine whether the number of occurrences of the 2^m m -bit overlapping patterns is approximately the same as would be expected for a random sequence. The pattern can overlap.
- **Approximate Entropy Test:** The focus of this test is the frequency of each and every overlapping m -bit pattern. The purpose of the test is to compare the frequency of overlapping blocks of two consecutive/adjacent lengths (m and $m + 1$) against the expected result for a random sequence.
- **Cumulative Sum (Cusum) Test:** The focus of this test is the maximal excursion (from zero) of the random walk defined by the cumulative sum of adjusted $(-1, +1)$ digits in the sequence. The purpose of the test is to determine whether the cumulative sum of the partial sequences occurring in the tested sequence is too large or too small relative to the expected behavior of that cumulative sum for random sequences. This cumulative sum may be considered as a random walk. For a random sequence, the random walk should be near zero. For non-random sequences, the excursions of this random walk away from zero will be too large.

A number of tests in the test suite have the *standard normal* and the *chi-square* (χ^2) as reference distributions. If the calculated test statistic falls in extreme regions of the reference distribution, the sequence under test is considered to be non-random. The standard normal distribution (i.e., the bell-shaped curve) is used to compare the value of the test statistic obtained from the random number generator with the expected value of the statistic under the assumption of randomness. The test statistic for the standard normal distribution is of the form $z = \frac{(x-\mu)}{\sigma}$, where x is the sample test statistic value, and μ and σ^2 are the expected value and the variance of the test statistic. The χ^2 distribution (i.e., a left skewed curve) is used to compare the goodness-of-fit of the observed frequencies of a sample measure to the corresponding expected frequencies of the hypothesized distribution. The test statistic is of the form $\chi^2 = \sum \left(\frac{(o_i - e_i)^2}{e_i} \right)$, where o_i and e_i are

the observed and expected frequencies of occurrence of the measure, respectively.

III. INDEPENDENCE OF TESTS

Two tests T_1 and T_2 are called independent if the corresponding p -values of these tests are independent [8]. (i.e., the p -values obtained from T_1 by applying the test to the sequences that fail T_2 , should be uniformly distributed.)

Also whenever the test statistic is lower than a fixed value $\alpha = 0.01$, we will call the tested sequence a failing sequence; and we will call the set of all failing sequences of a test, the rejection region of that test.

In this section, we analyze the dependency of the NIST tests, given in the previous section, by first looking at the rejection regions of the tests and then the p -value distributions of the individual tests in this rejection regions.

Note that cusum test described in Section II outputs two p -values, one from the sequence itself and one from the inverse of the same sequence. Similarly serial test also outputs two p -values regarding one for the transition from $(m - 1)$ -bit templates to m -bit templates and one for the transition from $(m - 2)$ -bit templates to $(m - 1)$ and m -bit templates.

We have analyzed the tests through $m = 10^5$ sequences of length $n = 5000$ in our study. But this n value restricted our study to the tests given in Section II since *random excursions*, *random excursion variant* and *universal* tests do not produce a p -value for this input size. Moreover, we also excluded *discrete fourier transform (spectral)* and *non-overlapping template matching* tests since the former did not produce a large enough rejection region for our inputs and the latter for ease of computation. The $(i, j)^{th}$ entry of the Table II represents the proportion of the sequences that fail T_i and T_j to the sequences that fail T_j . The expected value of this proportion is 0.01 so we marked the values greater than 0.1 to show significant deviations from this value. The parameters we used for the tests are given in Table I.

TABLE I
PARAMETERS USED FOR THE TESTS.

Test Name	Block Length
Block Frequency	128
Overlapping Template Matching	9
Approximate Entropy	8
Serial	9
Linear Complexity	500

According to Table II, *frequency*, *cusum1* and *cusum2* tests are closely related. Also *approximate entropy*, *serial1* and *serial2* tests also look related from this table, however the relation values between approximate entropy and serial tests seem to be deficient since the symmetric entries of the table are expected to have similar values [8]. But the relation between *serial1* and *serial2* is clear from the table as well as in theory.

In addition to this, we have made another observation that even though the most of the tests look uncorrelated in Table II, the distribution of the p -values in the rejection regions of each other are usually non-uniform. So we computed the values in

TABLE II
RELATION OF THE TESTS FOR $n = 5000$ AND $m = 10^5$.

Frequency	Block Frequency	Cumulative Sum1	Cumulative Sum2	Runs	LongestRun	Rank	Overlapping Template	Approximate Entropy	Serial1	Serial2	Linear Complexity
Frequency	0.0389	0.7407	0.7332	0.0161	0.1568	0.0064	0.0159	0.0168	0.0218	0.0112	0.0098
Block Frequency	-	-	-	-	-	-	-	-	-	-	-
Cumulative Sum1	0.0388	0.7406	0.7331	0.0160	0.1567	0.0063	0.0158	0.0167	0.0217	0.0111	0.0097
Cumulative Sum2	0.7446	0.7405	0.7330	0.0159	0.1566	0.0062	0.0157	0.0166	0.0216	0.0110	0.0096
Runs	0.782	0.7399	0.7324	0.0158	0.1565	0.0061	0.0156	0.0165	0.0215	0.0109	0.0095
LongestRun	0.0184	0.0183	0.0182	0.0181	0.0180	0.0179	0.0178	0.0177	0.0176	0.0175	0.0174
Rank	0.0183	0.0182	0.0181	0.0180	0.0179	0.0178	0.0177	0.0176	0.0175	0.0174	0.0173
Overlapping Template	0.0182	0.0181	0.0180	0.0179	0.0178	0.0177	0.0176	0.0175	0.0174	0.0173	0.0172
Approximate Entropy	0.0181	0.0180	0.0179	0.0178	0.0177	0.0176	0.0175	0.0174	0.0173	0.0172	0.0171
Serial1	0.0180	0.0179	0.0178	0.0177	0.0176	0.0175	0.0174	0.0173	0.0172	0.0171	0.0170
Serial2	0.0179	0.0178	0.0177	0.0176	0.0175	0.0174	0.0173	0.0172	0.0171	0.0170	0.0169
Linear Complexity	0.0178	0.0177	0.0176	0.0175	0.0174	0.0173	0.0172	0.0171	0.0170	0.0169	0.0168

Table III by evaluating the distributions of p -values through χ^2 distribution. The $(i, j)^{th}$ entry in Table III represents the χ^2 value of the distribution of p -values of T_i in the rejection region of T_j . In this table, the values less than 0.0001 are represented as 0 and values less than 0.01 are marked to show non-uniform distribution of p -values. The tables which these results were derived are also given in Appendix A.

IV. SENSITIVITY OF TESTS

Correlation coefficient is used to measure correlation between two random variables. There are number of different coefficients for different situations. In this section of our study, Pearson product-moment correlation coefficient [9] is implemented to find the correlation between the p -values of sequences and transformed sequences under basic transformations such as:

- **Inversion:** Taking the sequence in reverse order.
- **Complement:** Complementing every bit of the sequence.
- **1-Shifting:** 1 bit left shifting.
- **8-Shifting:** 8 bit left shifting.

The Pearson product-moment correlation coefficient r_{xy} is

$$r_{xy} = \frac{cov(X, Y)}{\sigma(x)\sigma(y)} = \frac{\sum x_i y_i - \sum x_i \sum y_i}{\sqrt{n \sum x_i^2 - (\sum x_i)^2} \sqrt{n \sum y_i^2 - (\sum y_i)^2}}$$

TABLE III
DISTRIBUTIONS OF p -VALUES IN THE REJECTION REGIONS OF EACH OTHER.

Frequency	Block Frequency	Cumulative Sum1	Cumulative Sum2	Runs	LongestRun	Rank	Overlapping Template	Approximate Entropy	Serial1	Serial2	Linear Complexity
Frequency	0.0389	0.7407	0.7332	0.0161	0.1568	0.0064	0.0159	0.0168	0.0218	0.0112	0.0098
Block Frequency	-	-	-	-	-	-	-	-	-	-	-
Cumulative Sum1	0.0388	0.7406	0.7331	0.0160	0.1567	0.0063	0.0158	0.0167	0.0217	0.0111	0.0097
Cumulative Sum2	0.7446	0.7405	0.7330	0.0159	0.1566	0.0062	0.0157	0.0166	0.0216	0.0110	0.0096
Runs	0.782	0.7399	0.7324	0.0158	0.1565	0.0061	0.0156	0.0165	0.0215	0.0109	0.0095
LongestRun	0.0184	0.0183	0.0182	0.0181	0.0180	0.0179	0.0178	0.0177	0.0176	0.0175	0.0174
Rank	0.0183	0.0182	0.0181	0.0180	0.0179	0.0178	0.0177	0.0176	0.0175	0.0174	0.0173
Overlapping Template	0.0182	0.0181	0.0180	0.0179	0.0178	0.0177	0.0176	0.0175	0.0174	0.0173	0.0172
Approximate Entropy	0.0181	0.0180	0.0179	0.0178	0.0177	0.0176	0.0175	0.0174	0.0173	0.0172	0.0171
Serial1	0.0180	0.0179	0.0178	0.0177	0.0176	0.0175	0.0174	0.0173	0.0172	0.0171	0.0170
Serial2	0.0179	0.0178	0.0177	0.0176	0.0175	0.0174	0.0173	0.0172	0.0171	0.0170	0.0169
Linear Complexity	0.0178	0.0177	0.0176	0.0175	0.0174	0.0173	0.0172	0.0171	0.0170	0.0169	0.0168

where x_i 's and y_i 's are the i^{th} block of sequences which we are investigating the correlation and n is the number of used p -values in a sequence.

Pearson product-moment correlation coefficient can be computed only if both of the standard deviations are finite and both of them are nonzero. And it is a result of Cauchy-Schwarz inequality that the absolute value of correlation coefficient cannot be larger than 1.

The coefficients reveal the degree of linear dependence between the p -values. The closer the absolute value of the coefficient is 1, the correlation between the corresponding tests become stronger. Independency of the corresponding tests implies that the correlation coefficient is 0. But converse is not true in general. Actually, having correlation coefficient 0 only means that there is no linear relation between the p -values [10].

The correlation coefficients of p -values through basic transformations are given in Table IV.

TABLE IV
CORRELATION COEFFICIENTS UNDER BASIC TRANSFORMATIONS.

	Inverse	Complement	1-Shift	8-Shift
Frequency	1	1	1	1
Block Frequency	0,869472	1	0,98266	0,869472
Cumulative Sums 1	0,723222	1	0,999438	0,995701
Cumulative Sums 2	0,723222	1	0,999437	0,995707
Runs	1	1	0,999121	0,999112
Longest Run	1	0,059991	0,473792	1
Rank	-0,003203	0,086677	0,086092	-0,00155
Overlapping Template	0,370533	-0,004004	0,993046	0,96608
Approximate Entropy	1	1	1	1
Serial 1	1	1	1	1
Serial 2	1	1	1	1
Linear Complexity	0,639843	0,404223	0,481013	0,00491

The entries of the Table IV show the correlation between the corresponding test results of a sequence and its transformed form. We have highlighted the values greater than 0.80 to point out correlated p -values. In this respect, the frequency, block frequency, runs, approximate entropy, serial 1 and serial 2 tests are strong against these transformations as they produce correlated p -values. But although cumulative sums tests are strong against complement, 1-shift and 8-shift transformations, it can be seen from the table that the correlation coefficient does not give a strong result for the inverse transformation. In addition, longest run of ones test is strong against inverse and 8-shift transformations, but we can only say that a linear relation of the p -values with 1-shifted ones are unlikely as in complemented ones. Similarly, overlapping template matching test is strong against shifting transformations but again it is unlikely to have a linear relation for inverse and complement transformed results. Finally, for the rank and linear complexity tests a linear relation between the raw p -values and transformed ones are unlikely to have.

V. CONCLUSION

Statistical testing is an important aspect on determining the quality of a PRNG. To achieve this purpose, several test suites are proposed. But as well as having many tests to examine different randomness properties of sequences, having these tests independent is also of crucial importance in designing a test suite. In this work, we experimentally show that, looking at the failing sequences from NIST tests, we may conclude that most tests in this suite are independent. But as we have observed through the distribution of the p -values taken from the rejection regions of the tests, there is a relation, in this sense, among most tests. We also examined the sensitivity of NIST tests to some basic transformations. It is of interest to extend these ideas further to commonly used randomness tests which are not included in the NIST test suite as future work.

REFERENCES

- [1] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo. A statistical test suite for random and pseudorandom number generators for cryptographic applications. 2001. <http://www.nist.gov>.
- [2] D. E. Knuth. *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming*. Addison-Wesley, 1981.

- [3] W. Caelli, E. Dawson, L. Nielsen, and H. Gustafson. CRYPT-X statistical package manual, measuring the strength of stream and block ciphers, 1992.
- [4] G. Marsaglia. The Marsaglia random number CDROM including the DIEHARD battery of tests of randomness. 1996.
- [5] Pierre L'Ecuyer and Richard Simard. Testu01: A c library for empirical testing of random number generators. *ACM Trans. Math. Softw.*, 33(4):22, 2007.
- [6] J. Soto. Randomness testing of the AES candidate algorithms, 1999.
- [7] P. Hellekalek and S. Wegenkittl. Empirical evidence concerning aes. *ACM Trans. Model. Comput. Simul.*, 13(4):322–333, 2003.
- [8] Meltem Sönmez Turan, Ali Doganaksoy, and Serdar Boztas. On independence and sensitivity of statistical randomness tests. In Solomon W. Golomb, Matthew G. Parker, Alexander Pott, and Arne Winterhof, editors, *SETA*, volume 5203 of *Lecture Notes in Computer Science*, pages 18–29. Springer, 2008.
- [9] Joseph L. Rodgers and Alan W. Nicewander. Thirteen ways to look at the correlation coefficient. *The American Statistician*, 42(1):59–66, 1988.
- [10] David S. Moore. *The Basic Practice of Statistics with Cdrom*. W. H. Freeman & Co., New York, NY, USA, 1999.

APPENDIX A p -VALUE DISTRIBUTION TABLES

Below are the tables used to derive the values in Table III.

TABLE V
DISTRIBUTIONS OF p -VALUES IN THE REJECTION REGION OF THE FREQUENCY TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
BlockFrequency	271	192	151	117	71	67	49	33	21	5
CumulativeSums2	977	0	0	0	0	0	0	0	0	0
CumulativeSums1	977	0	0	0	0	0	0	0	0	0
Runs	97	112	92	98	98	90	86	93	130	81
LongestRun	593	177	89	57	21	16	13	7	4	0
Rank	94	48	95	0	189	154	245	152	0	0
OverlappingTemplate	87	92	83	121	76	175	139	73	131	0
ApproximateEntropy	262	168	118	108	91	63	56	43	42	26
Serial1	164	131	124	122	88	102	75	61	64	46
Serial2	109	98	95	99	102	96	97	89	91	101
LinearComplexity	124	64	50	63	86	88	107	100	93	202

TABLE VI
DISTRIBUTIONS OF p -VALUES IN THE REJECTION REGION OF THE BLOCK FREQUENCY TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	180	124	109	91	82	64	69	63	61	57
BlockFrequency	231	133	116	90	85	88	53	55	32	17
CumulativeSums2	224	122	133	90	68	78	66	62	36	21
Runs	103	108	86	80	96	85	92	83	90	77
LongestRun	144	110	95	91	79	75	78	82	58	88
Rank	93	51	91	0	179	148	197	141	0	0
OverlappingTemplate	105	71	70	137	73	154	120	49	121	0
ApproximateEntropy	191	103	118	106	83	70	68	67	47	47
Serial1	119	103	85	90	88	91	89	85	84	66
Serial2	114	84	76	102	75	94	77	98	92	88
LinearComplexity	138	46	52	57	63	101	85	80	103	175

TABLE VII
DISTRIBUTIONS OF p -VALUES IN THE REJECTION REGION OF THE CUMULATIVE SUMS 1 TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	979	2	1	0	0	0	0	0	0	0
BlockFrequency	297	190	155	122	66	62	49	26	11	4
CumulativeSums2	973	8	1	0	0	0	0	0	0	0
Runs	111	115	97	98	109	82	79	85	124	82
LongestRun	557	168	103	61	26	27	22	10	6	2
Rank	102	55	101	0	178	151	235	160	0	0
OverlappingTemplate	95	95	81	117	76	178	149	64	127	0
ApproximateEntropy	273	160	109	101	93	69	58	53	36	30
Serial1	178	124	122	106	90	94	85	68	68	47
Serial2	106	105	91	100	99	107	90	95	94	95
LinearComplexity	115	68	49	62	88	93	104	104	99	200

TABLE VIII
DISTRIBUTIONS OF p -VALUES IN THE REJECTION REGION OF THE
CUMULATIVE SUMS 2 TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	1031	8	3	0	0	0	0	0	0	0
BlockFrequency	315	209	163	117	76	68	44	31	16	3
CumulativeSums1	1017	21	4	0	0	0	0	0	0	0
Runs	109	104	97	109	112	89	103	96	134	89
LongestRun	582	184	95	71	37	29	16	18	6	4
Rank	111	57	96	0	203	163	250	162	0	0
OverlappingTemplate	89	97	85	138	80	186	142	76	149	0
ApproximateEntropy	266	171	122	117	104	70	66	58	40	28
Serial1	172	134	124	123	100	99	92	82	68	47
Serial2	116	109	106	104	116	93	102	94	94	108
LinearComplexity	136	72	56	67	90	95	109	99	106	212

TABLE IX
DISTRIBUTIONS OF p -VALUES IN THE REJECTION REGION OF THE RUNS
TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	102	91	108	90	114	95	107	103	87	88
BlockFrequency	114	86	97	97	81	102	95	112	99	102
CumulativeSums1	105	81	103	95	106	114	92	100	84	105
CumulativeSums2	101	96	98	86	104	106	92	97	96	109
LongestRun	254	140	88	105	99	79	73	51	47	49
Rank	121	41	108	0	178	167	215	155	0	0
OverlappingTemplate	92	83	94	138	73	169	139	65	132	0
ApproximateEntropy	258	167	114	101	84	81	47	59	40	34
Serial1	164	133	122	102	87	108	71	99	60	59
Serial2	115	92	79	90	98	114	81	101	93	122
LinearComplexity	146	67	44	67	75	109	88	110	116	163

TABLE X
DISTRIBUTIONS OF p -VALUES IN THE REJECTION REGION OF THE
LONGEST RUN OF ONES TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	404	129	75	63	47	49	52	68	33	43
BlockFrequency	124	108	115	106	98	105	77	91	77	62
CumulativeSums1	384	110	58	61	55	42	38	58	48	48
CumulativeSums2	391	114	77	61	53	64	40	64	58	41
Runs	199	128	99	103	66	76	64	73	80	75
Rank	93	66	99	0	195	142	214	154	0	0
OverlappingTemplate	85	69	63	145	80	181	143	65	132	0
ApproximateEntropy	248	163	113	99	85	64	59	63	37	52
Serial1	158	126	103	107	94	92	80	76	74	53
Serial2	86	116	100	106	92	81	89	90	102	101
LinearComplexity	124	75	42	47	60	89	101	94	127	206

TABLE XI
DISTRIBUTIONS OF p -VALUES IN THE REJECTION REGION OF THE MATRIX
RANK TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	164	150	150	172	164	156	150	146	144	162
BlockFrequency	155	158	158	163	160	146	156	155	155	152
CumulativeSums1	163	149	140	146	152	187	125	153	163	180
CumulativeSums2	156	158	134	185	138	169	137	161	141	179
Runs	152	158	146	141	134	169	161	155	157	165
LongestRun	160	167	169	145	135	164	133	174	146	165
OverlappingTemplate	106	133	100	221	116	277	229	117	259	0
ApproximateEntropy	292	186	169	164	148	147	133	122	113	84
Serial1	158	166	145	140	149	170	150	158	160	162
Serial2	138	164	158	169	156	153	149	160	147	164
LinearComplexity	221	125	80	85	118	172	149	151	173	284

TABLE XII
DISTRIBUTIONS OF p -VALUES IN THE REJECTION REGION OF THE
OVERLAPPING TEMPLATE TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	135	113	109	111	110	100	136	117	106	98
BlockFrequency	135	137	133	126	92	114	99	104	109	86
CumulativeSums1	136	115	112	105	88	126	109	129	94	121
CumulativeSums2	135	102	119	116	107	122	94	129	103	108
Runs	106	110	100	133	114	121	112	111	113	107
LongestRun	114	125	114	101	123	85	111	115	99	128
Rank	126	62	126	0	232	162	239	188	0	0
ApproximateEntropy	208	137	142	110	112	106	96	95	74	55
Serial1	113	117	116	118	111	107	101	138	107	107
Serial2	119	109	103	99	112	130	118	102	112	131
LinearComplexity	158	82	58	71	90	123	119	98	104	232

TABLE XIII
DISTRIBUTIONS OF p -VALUES IN THE REJECTION REGION OF THE
APPROXIMATE ENTROPY TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	326	288	276	244	259	218	219	249	198	227
BlockFrequency	250	244	246	261	213	246	275	245	261	263
CumulativeSums1	302	283	255	256	258	250	211	258	221	210
CumulativeSums2	329	267	267	262	226	284	216	213	216	224
Runs	331	290	274	238	258	223	225	229	225	211
LongestRun	370	291	263	251	244	230	226	212	214	203
Rank	258	142	277	0	466	432	569	360	0	0
OverlappingTemplate	211	215	187	324	191	442	374	154	406	0
Serial1	2497	7	0	0	0	0	0	0	0	0
Serial2	1595	446	194	103	79	37	25	16	8	1
LinearComplexity	355	182	126	158	166	257	236	277	276	471

TABLE XIV
DISTRIBUTIONS OF p -VALUES IN THE REJECTION REGION OF THE SERIAL
1 TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	138	125	109	104	103	79	77	102	76	95
BlockFrequency	100	114	92	98	83	90	111	109	101	110
CumulativeSums1	136	115	86	115	96	93	84	108	88	87
CumulativeSums2	145	117	100	106	89	103	84	98	88	78
Runs	132	131	111	89	108	97	89	80	90	81
LongestRun	170	117	100	98	75	91	86	89	100	82
Rank	87	47	115	0	208	170	226	155	0	0
OverlappingTemplate	98	90	60	120	81	184	149	64	162	0
ApproximateEntropy	1008	0	0	0	0	0	0	0	0	0
Serial2	781	133	46	20	14	8	3	2	1	0
LinearComplexity	156	75	48	53	61	99	109	108	108	191

TABLE XV
DISTRIBUTIONS OF p -VALUES IN THE REJECTION REGION OF THE SERIAL
2 TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	106	113	85	100	92	92	100	108	77	113
BlockFrequency	96	91	94	95	93	97	119	100	97	104
CumulativeSums1	89	119	103	87	105	101	81	102	99	102
CumulativeSums2	116	101	86	96	85	110	97	112	99	84
Runs	106	110	107	90	93	99	96	89	93	103
LongestRun	97	111	91	106	90	105	96	96	98	96
Rank	119	53	104	0	178	188	191	153	0	0
OverlappingTemplate	91	72	59	147	71	191	129	71	155	0
ApproximateEntropy	913	54	15	2	2	0	0	0	0	0
Serial1	843	96	31	11	3	2	0	0	0	0
LinearComplexity	126	77	51	54	63	107	101	103	109	195

TABLE XVI
DISTRIBUTIONS OF p -VALUES IN THE REJECTION REGION OF THE LINEAR
COMPLEXITY TEST.

	[0, 0.1]	(0.1, 0.2]	(0.2, 0.3]	(0.3, 0.4]	(0.4, 0.5]	(0.5, 0.6]	(0.6, 0.7]	(0.7, 0.8]	(0.8, 0.9]	(0.9, 1]
Frequency	330	375	358	385	345	329	347	387	321	364
BlockFrequency	330	305	400	378	364	373	347	351	333	360
CumulativeSums1	333	337	343	363	345	389	352	367	326	386
CumulativeSums2	355	332	387	339	339	360	357	373	320	379
Runs	349	361	365	385	377	308	341	364	344	347
LongestRun	379	369	335	377	345	344	334	352	365	341
Rank	378	180	382	0	637	616	785	563	0	0
OverlappingTemplate	268	310	245	458	270	626	551	247	566	0
ApproximateEntropy	576	472	427	365	329	324	303	269	246	230
Serial1	338	350	347	370	332	312	386	354	356	396
Serial2	357	342	340	351	323	357	387	342	350	392

Alternative Approach to Maurer's Universal Statistical Test

Ali DOĞANAKSOY, Cihangir TEZCAN

Abstract—Statistical tests for randomness play an important role in cryptography since many cryptographic applications require random or pseudorandom numbers. In this study, we introduce an alternative approach to Maurer's Universal Test. This approach allows us to test short binary sequences as small as 66 bits and to choose slightly larger block sizes. Moreover, it does not have an initialization part and requires less time to test a binary sequence.

Keywords —Randomness, Statistical Test, Maurer's Universal Test

I. INTRODUCTION

RANDOM numbers have many uses in cryptography such as keystreams of one-time pads, secret keys of symmetric cipher systems, public key parameters, session keys, nonces, initialization vectors and salts. Hence statistical randomness tests are of great importance for cryptographers for testing the security of cryptographic applications.

There are various statistical test suites in the literature such as NIST [2] which is used as an evaluation tool in the AES selection process, Knuth [8], DIEHARD [5], TestU01 [7], and Crypt-X [6], all of which consisting of a number of statistical tests. In this study, we introduce a new approach to Maurer's Universal Test [1] which is one of the 16 tests used in NIST statistical test suite.

Maurer's Universal Test has an initialization part and most of the blocks in this segment has no effect in the test statistic. Moreover, in NIST statistical test suite, block sizes between 6 and 16 are recommended, where the lower bound makes the test inapplicable for binary sequences shorter than 387,840 bits. However, our approach does not contain an initialization part, it can be used to test short sequences as small as 66 bits and block size can be chosen larger for long sequences. Moreover the new approach requires slightly less time to test a binary sequence.

The outline of the paper is as follows. In section II, we briefly summarize Maurer's Universal Test and introduce our approach in section III. In section IV, we present the advantages of this approach and in the last section, we conclude our paper.

II. MAURER'S UNIVERSAL TEST

Maurer's Universal Statistical Test which is introduced by Ueli M. Maurer in 1992 in [1] measures per-bit entropy of

Ali Doğanaksoy is with the Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Ankara, 06531 TURKEY e-mail: (aldoks@metu.edu.tr).

Cihangir Tezcan is with the Institute of Applied Mathematics, Middle East Technical University, Ankara, 06531 TURKEY e-mail: (forgottenlance@gmail.com).

a stream which is considered as the correct quality measure for a secret key source in a cryptographic application. The test is designed to detect any one of the very general class of statistical defects that can be modeled by an ergodic source with finite memory M where M is less than or equivalent to the block size L .

Let $\{a_n\} = a_1, a_2, \dots, a_N$ be a binary sequence of length N . To apply the test, we partition this sequence into adjacent non-overlapping blocks of length L and compute the integer values of these blocks and obtain a new sequence $\{t_n\} = t_1, t_2, \dots, t_k$ where $k = \lfloor \frac{N}{L} \rfloor$ and $t_i \in \{0, 1, 2, \dots, 2^L - 1\}$. The remaining bits at the end of the sequence are discarded.

The first Q blocks of $\{t_n\}$ is called the initialization part and the remaining K blocks are called the test part where $K + Q = \lfloor n/L \rfloor$. For every block in the test part, we calculate the distance of that block to its previous occurrence. That is, the distance r for the block t_i means t_i and t_{i-r} are the same and the integers between them are different than t_i . These calculations can be done efficiently by scanning the sequence $\{t_n\}$ once and storing the places of the last occurrences of blocks in an array of size 2^L . If we denote these distances by c_i , the test statistic f_n is

$$f_n = \frac{1}{K} \sum_{i=1}^K \log_2 c_i. \quad (1)$$

The reference distribution for the test statistic is the half-normal distribution. The p-value is obtained as follows:

$$c = 0.7 - \frac{0.8}{L} + \left(4 + \frac{32}{L}\right) \frac{K^{-3/L}}{15} \quad (2)$$

$$\sigma = c \sqrt{\frac{\text{variance}(L)}{K}} \quad (3)$$

$$p - \text{value} = \text{erfc} \left(\left| \frac{f_n - \text{expectedvalue}(L)}{\sqrt{2}\sigma} \right| \right). \quad (4)$$

If the obtained p-value is less than the probability of type I error, which is a small value between 0.01 and 0.001, we assume that the sequence is obtained from a non-random resource.

An efficient and clear implementation of the complementary error function erfc can be found in [3]. The values of variances and expected values are given in Table IV at Appendix A.

III. THE NEW APPROACH

Let $\{a_n\} = a_1, a_2, \dots, a_N$ be a binary sequence of length N . By partitioning this sequence into adjacent non-overlapping blocks of length L and computing the integer values of these blocks, we obtain a new sequence $\{t_n\} = t_1, t_2, \dots, t_k$ where $k = \lfloor \frac{N}{L} \rfloor$ and $t_i \in \{0, 1, 2, \dots, 2^L - 1\}$. The remaining bits at the end of the sequence are discarded. Moreover, from $\{t_n\}$ we obtain yet another sequence $\{c_n\}$ where c_i is the distance between the integer t_i and its next occurrence. If the integer t_i is its final occurrence in the sequence $\{t_n\}$, we assign the value 0 to c_i . Thus the sequence $\{c_n\}$ also has length k . Note that in this approach we do not use an initialization part. Hence when calculating the distances, considering the previous occurrence of a block, instead of its next occurrence does not change the test statistic.

If c_i is r for some i , this means that t_i and t_{i+r} are the same integers and the integers between them are different than t_i . The probability of such a situation is

$$\text{prob}(c_i = r) = \frac{(2^L - 1)^{r-1}}{(2^L)^r}. \quad (5)$$

Thus the probability for $c_i = 0$ is obtained in the following way:

$$\text{prob}(c_i = 0) = 1 - \sum_{i=1}^k \frac{(2^L - 1)^{i-1}}{(2^L)^i}. \quad (6)$$

Note that since t_k is the last element of the sequence $\{t_n\}$, c_k must be 0. Similarly c_{k-1} is either 0 or 1. Thus a distance r in the sequence c_i can be observed only in $k - r$ different places. Hence the expected number of appearance of the value r in the sequence $\{c_n\}$ is

$$E(r) = (k - r) \frac{(2^L - 1)^{r-1}}{(2^L)^r}. \quad (7)$$

Let d_i denote the number of appearance of the value i in the sequence $\{c_n\}$. We apply the test by calculating d_i 's and performing χ^2 of goodness of fit test to d_i and $E(i)$ values.

The number of appearance of 0 in the $\{c_n\}$ sequence is equivalent to the number of distinct integers in the $\{t_n\}$ sequence. To apply the test, we require that every integer in the set $\{0, 1, \dots, 2^L - 1\}$ should appear in $\{t_n\}$ at least once. Thus we will consider the cases when the probability of every possible integer values not appearing in $\{t_n\}$ is less than 10^{-4} . Hence to perform the test, the largest block size L that can be chosen for a $\{t_n\}$ sequence with length k is the largest L value satisfying the following equation:

$$1 - \left(\frac{2^L - 1}{2^L}\right)^k - \left(\frac{2^L - 2}{2^L}\right)^k - \dots - \left(\frac{1}{2^L}\right)^k > 0.9999 \quad (8)$$

The largest L values satisfying the above inequality are the suggested block sizes and are given in Table I.

We apply χ^2 of goodness of fit test to obtain p-values. The degree of freedom d is $k - 1$ and χ^2 value is

$$\chi^2 = \sum_{i=1}^k \frac{(d_i - E(i))^2}{E(i)} \quad (9)$$

TABLE I
LARGEST POSSIBLE BLOCK SIZES

Sequence Length	Block Size
$66 \leq n \leq 206$	2
$207 \leq n \leq 571$	3
$572 \leq n \leq 1,454$	4
$1,455 \leq n \leq 3,509$	5
$3,510 \leq n \leq 8,224$	6
$8,225 \leq n \leq 18,839$	7
$18,840 \leq n \leq 42,407$	8
$42,408 \leq n \leq 94,269$	9
$94,270 \leq n \leq 207,448$	10
$207,449 \leq n \leq 452,663$	11
$452,664 \leq n \leq 980,823$	12
$980,824 \leq n \leq 2,112,599$	13
$2,112,600 \leq n \leq 4,257,059$	14
$4,257,060 \leq n \leq 9,657,775$	15
$9,657,776 \leq n \leq 20,522,858$	16
$20,522,859 \leq n \leq 43,460,243$	17
$43,460,244 \leq n \leq 91,749,460$	18
$91,749,461 \leq n \leq 193,156,859$	19
$193,156,860 \leq n \leq 405,629,468$	20
$405,629,469 \leq n \leq 849,890,425$	21
$849,890,426 \leq n \leq 1,777,043,709$	22

and we use the complement of incomplete gamma function *gammap* (see [3] for an efficient and clear implementation) to obtain the p-value where

$$p\text{-value} = \text{gammap}\left(\frac{d}{2}, \frac{\chi^2}{2}\right) \quad (10)$$

If the obtained p-value is less than the probability of type I error, which is a small value between 0.01 and 0.001, we assume that the sequence is obtained from a non-random resource.

Since we assumed that every possible integer values is observed in the sequence $\{t_n\}$, before testing a binary sequence, we check that if the corresponding $\{t_n\}$ sequence is as we desired. If it is not, the test will not be applied to that binary sequence.

IV. COMPARISON

In Maurer's Universal Test, the initialization segment contains $10 \cdot 2^L$ bits and most of the blocks of this part have no effect in the test result. This is due to the fact that only the place of the last occurrence of an integer in the initialization part is considered in the test segment. However, there is no initialization part in the presented method which allows us to test the whole sequence without wasting any parts of the sequence.

Another important difference between the two methods is the length of the sequences that can be tested. In Maurer's Universal Test, sequences which are shorter than 387,840 bits cannot be tested. However, our approach can be applied to test sequences as short as 66 bits.

It is important to notice that Maurer's Universal Test requires a long sequence with initialization part of $10 \cdot 2^L$ blocks and test part of $1000 \cdot 2^L$ blocks which makes the test not suitable for block size length larger than 16. In our new method, the block size can be taken larger than 16 for long sequences but notice that the distances are stored in an array of size 2^L in both methods. Hence the test becomes infeasible for large L .

Yet another difference is the speed of the both algorithms. Since there are no logarithms involved in our method, it requires less time to test a binary sequence. We measured the speed of the tests by testing 1000 binary sequences of length 800000 bits on a PC with an Athlon 64 3700+ processor at 2.2 GHz, 3 GB of RAM and running Windows XP. These sequences are taken from [5] and we used the same block size for both of the tests. Results are given in the Table II.

TABLE II
THE TIME COMPARISON OF THE TWO TESTS BASED ON 1,000 RANDOM SEQUENCES OF LENGTH 800,000 BITS

Maurer's Universal Test	102 seconds
New method	87 seconds

The linear relationship between the two tests can be seen from Pearson product-moment correlation coefficient [4], which is a value between -1 and 1 . Correlation between the variables gets stronger when the coefficient comes closer to -1 or 1 . However, the correlation coefficient 0 does not mean that the variables are uncorrelated since it measures only the linear relationship. By using the p-values we obtained from the speed comparison of the tests, we calculated Pearson's coefficient as 0.3 .

V. CONCLUSION

In this study, we proposed an alternative method for applying Maurer's Universal Statistical Test. The comparison of this approach and Maurer's Universal Test is made in Section IV. Although the idea behind the both methods are the same, the differences in the test structure (especially the initialization part of Maurer's Universal Test) result in different p-values for a binary sequence.

Our approach does not use an initialization part and it can be used to test short binary sequences. It allows us to work with larger block sizes and it requires less time to test a binary sequence. The linear relationship between the two tests can be seen from Pearson product-moment correlation coefficient which is calculated in section IV.

APPENDIX A

MAURER'S UNIVERSAL TEST PARAMETERS

The number of blocks used in the initialization part of Maurer's Universal Test and the block sizes are given in Table III. The expected values and variances are given in Table IV.

ACKNOWLEDGMENT

The authors would like to thank Meltem Sönmez Turan for her helpful comments.

TABLE III
PARAMETERS IN NIST STATISTICAL TEST SUITE

n	L	$Q = 10 \cdot 2^L$
$\geq 387,840$	6	640
$\geq 904,960$	7	1,280
$\geq 2,068,480$	8	2,560
$\geq 4,654,080$	9	5,120
$\geq 10,342,400$	10	10,240
$\geq 22,753,280$	11	20,480
$\geq 49,643,520$	12	40,960
$\geq 107,560,960$	13	81,920
$\geq 231,669,760$	14	163,840
$\geq 496,435,200$	15	327,680
$\geq 1,059,061,760$	16	655,360

TABLE IV
EXPECTED VALUES AND VARIANCES

L	expectedvalue	variance
6	5.2177052	2.954
7	6.1962507	3.125
8	7.1836656	3.238
9	8.1764248	3.311
10	9.1723243	3.356
11	10.170032	3.384
12	11.168765	3.401
13	12.168070	3.410
14	13.167693	3.416
15	14.167488	3.419
16	15.167379	3.421

REFERENCES

- [1] U. M. Maurer, *A Universal Statistical Test for Random Bit Generators*, Journal of Cryptology. Vol. 5, No. 2, 1992, pp. 89-105.
- [2] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, 1992.
- [3] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, *Numerical Recipes in C: The Art of Scientific Computing*, 2nd Edition, ISBN 0521431085, Cambridge University Press, 1992.
- [4] J. L. Rodgers and W. A. Nicewander, *Thirteen Ways to Look at the Correlation Coefficient*, The American Statistician, Vol. 42, No. 1 (Feb., 1988), pp. 59-66.
- [5] G. Marsaglia, *DIEHARD Statistical Tests*, <http://stat.fsu.edu/pub/diehard/>.
- [6] Information Security Institute, *Crypt-X*, 1998, <http://www.isi.qut.edu.au/resources/cryptx/>.
- [7] P. L'Ecuyer and R. Simard, *TestU01: A C Library for Empirical Testing of Random Number Generators*, ACM Transactions on Mathematical Software, 33, 4, Article 22, August 2007.
- [8] D.E. Knuth, *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming*, Addison-Wesley, 1981.

Threshold Cryptography Based on Blakley Secret Sharing

İlker Nadi BOZKURT, Kamer KAYA, Ali Aydın SELÇUK, Ahmet M. GÜLOĞLU

Abstract—Function sharing deals with the problem of distribution of the computation of a function (such as decryption or signature) among several parties. The necessary values for the computation are distributed to the participating parties using a secret sharing scheme (SSS). Several function sharing schemes have been proposed in the literature, with most of them using Shamir secret sharing as the underlying SSS. In this paper, we investigate how threshold cryptography can be conducted with Blakley secret sharing scheme and present a novel function sharing scheme for the RSA cryptosystem. The challenge is that constructing the secret in Blakley's SSS requires the solution of a linear system which normally involves computing inverses, while computing inverses modulo $\phi(N)$ cannot be tolerated in a threshold RSA system in any way.

Keywords —threshold cryptography, RSA, function sharing, Blakley secret sharing.

I. INTRODUCTION

The secure storage of the private keys of a cryptosystem is an important problem. The possession of a highly sensitive key by an individual may not be desirable as the key can easily be lost or as the individual may not be fully trusted. Giving copies of the key to more than one individual increases the risk of compromise. A solution to this problem is to give shares of the key to several individuals, forcing them to cooperate to find the secret key. This not only reduces the risk of losing the key but also makes compromising the key more difficult. In threshold cryptography, secret sharing deals with this problem, namely, sharing a highly sensitive secret among a group of n users so that only when a sufficient number t of them come together can the secret be reconstructed. Well-known secret sharing schemes (SSS) in the literature include Shamir [12] based on polynomial interpolation, Blakley [2] based on hyperplane geometry,

and Asmuth-Bloom [1] based on the Chinese Remainder Theorem.

A shortcoming of secret sharing schemes is the need to reveal the secret shares during the reconstruction phase. The system would be more secure if the subject function can be computed without revealing the secret shares or reconstructing the secret. This is known as the function sharing problem. A function sharing scheme requires distributing the function's computation according to the underlying SSS such that each part of the computation can be carried out by a different user and then the partial results can be combined to yield the function's value without disclosing the individual secrets. Several protocols for function sharing have been proposed in the literature [3], [4], [5], [6], [13], [8], [11]. Nearly all the existing solutions for function sharing uses Shamir secret sharing as the underlying SSS.

In this paper we present a novel threshold RSA signature scheme based on Blakley's secret sharing as we explain below.

A. Secret Sharing Schemes

The problem of secret sharing and the first solutions were introduced in 1979 independently by Shamir [12] and Blakley [2]. A (t, n) -secret sharing scheme is used to distribute a secret d among n people such that any coalition of size t or more can construct d but smaller coalitions cannot.

Shamir secret sharing is based on polynomial interpolation over a finite field. It uses the fact that we can find a polynomial of degree $t - 1$ given t data points. To generate a polynomial $f(x) = \sum_{i=0}^{t-1} a_i x^i$, a_0 is set to the secret value and the coefficients a_1 to a_{t-1} are assigned random values in the field. The value $f(i)$ is given to user i . When t out of n users come together, they can construct the polynomial using Lagrange interpolation and can find the secret.

Blakley secret sharing scheme has a different approach based on hyperplane geometry: To implement a (t, n) threshold scheme, each of the n users is given a hyperplane equation in a t dimensional space over a finite field

İlker Nadi Bozkurt, Kamer Kaya and Ali Aydın Selçuk are with the Department of Computer Engineering, Bilkent University, Ankara, 06800, Turkey e-mail: {bozkurti,kamer,selcuk}@cs.bilkent.edu.tr.

Ahmet M. Güloğlu is with Department of Mathematics, Bilkent University, Ankara, 06800, Turkey e-mail: gu-loglua@fen.bilkent.edu.tr.

such that each hyperplane passes through a certain point. The intersection point of the hyperplanes is the secret. When t users come together, they can solve the system of equations to find the secret.

B. Function Sharing Schemes

Function sharing is the concept of distribution of the computation of a function such that when a sufficient number of users come together they can compute the value of the function without revealing their secret shares but less than the threshold number of users cannot. This problem is related to secret sharing as the secret values needed for partial computations are distributed using secret sharing.

Several solutions for sharing the RSA, ElGamal, and Paillier private key operations have been proposed in the literature [3], [4], [5], [6], [7], [10], [11], [13], [9]. Almost all of these schemes have been based on the Shamir SSS.

The additive nature of the Lagrange's interpolation formula used in the combining phase of Shamir's scheme makes it an attractive choice for function sharing, but it also provides several challenges. One of the most significant challenges is the computation of inverses in $\mathbb{Z}_{\phi(N)}$ for the division operations in Lagrange's formula where $\phi(N)$ should not be known by the users. There are two main difficulties in this respect:

- 1) An inverse x^{-1} will not exist modulo $\phi(N)$ if $\gcd(x, N) \neq 1$.
- 2) Even when x^{-1} exists it should not be computable by a user, since that would enable computing $\phi(N)$.

Early solutions to this problem, albeit not very efficient, were given in [3], [11]. Afterwards an ingenious solution was given by Shoup [13] where he removed the need of taking inverses in Lagrange interpolation.

Shoup's practical RSA scheme has inspired similar works on different cryptosystems. Fouque et al. [7] proposed a similar threshold solution for the Paillier cryptosystem and used it in e-voting and lottery protocols. Later, Lysyanskaya and Peikert [10] improved this work and obtained a threshold Paillier encryption scheme secure under the adaptive security model. The current paper is also inspired by Shoup's work.

C. Our Contribution

In this work, we show how to do threshold RSA signatures using Blakley SSS. Blakley's scheme, which is based on solving linear systems, naturally requires computing inverses for reconstructing the secret. We show, in a spirit similar to Shoup's work, how to utilize

Blakley's SSS for threshold cryptography while avoiding computation of inverses modulo $\phi(N)$ completely.

II. BLAKLEY'S SECRET SHARING SCHEME

Blakley's SSS uses hyperplane geometry to solve the secret sharing problem. The secret is a point in a t -dimensional space and n shares are affine hyperplanes that pass through this point. An affine hyperplane in a t -dimensional space with coordinates in a field $\mathcal{F}$ can be described by a linear equation of the following form:

$$a_1x_1 + a_2x_2 + \dots + a_tx_t = b.$$

The intersection point is obtained by finding the intersection of any t of these hyperplanes. The secret can be any of the coordinates of the intersection point or any function of the coordinates. We take the secret to be the first coordinate of the point of intersection.

A. Dealing Phase

Let m be a prime and let $\mathcal{F} = \mathbb{Z}_m$ be the field we are working on. The dealer generates a secret point x in $\mathcal{F}^t$, where the first coordinate $x[1]$ is set to the secret value (the RSA private key d in our case) and sets the values of the other coordinates randomly from the field $\mathcal{F}$. The i th user will get a hyperplane equation over $\mathcal{F}$,

$$a_{i1}x_1 + a_{i2}x_2 + \dots + a_{it}x_t = y_i. \quad (1)$$

For a (t, n) threshold scheme there will be n such hyperplane equations, and hence we will have an $n \times t$ linear system,

$$Ax = y. \quad (2)$$

The dealer then sends the secret value of y_i along with $a_{i1}, \dots, a_{it}$ to user i . The coefficients a_{ij} are not sensitive and can be made public if needed.

B. Share Combining Phase

Share combining step is simply finding the solution of a linear system of equations. Suppose that a coalition $\mathcal{S} = \{i_1, \dots, i_t\}$ of users come together. They form a matrix $A_{\mathcal{S}}$ using their hyperplane equations and solve

$$A_{\mathcal{S}}x = y_{\mathcal{S}}, \quad (3)$$

where $y_{\mathcal{S}}$ is the vector of the secret shares of the users. The secret is found as the first coordinate of the solution.

III. SHARING RSA SIGNATURE COMPUTATION

In this section, we describe our threshold RSA signature scheme with Blakley secret sharing.

A. Setup

In the RSA setup phase, choose two large primes p and q , and compute the RSA modulus as $N = pq$. The public key e is chosen as a prime number relatively prime to $\phi(N)$, the details of which will be explained in Section V. After choosing e , the private key d is computed such that $ed \equiv 1 \pmod{\phi(N)}$. Then the dealer shares the private key d among n users using Blakley SSS in $\mathbb{Z}_{\phi(N)}$.

B. Signing

Let $H(\cdot)$ be a hash function mapping input messages to $\mathbb{Z}_N^*$ and let $w = H(M) \in \mathbb{Z}_N^*$ be the hashed message to be signed. Assume a coalition $\mathcal{S}$ of size t wants to obtain the signature $s = w^d \pmod{N}$.

1) *Generating the Partial Signatures:* Let $\mathcal{S} = \{i_1, \dots, i_t\}$ be the coalition of t users, forming the linear system

$$A_{\mathcal{S}}x = y_{\mathcal{S}}.$$

Let c_{ij} be the ij -th cofactor of matrix $A_{\mathcal{S}}$ and let $C_{\mathcal{S}}$ be the adjugate matrix,

$$C_{\mathcal{S}} = \begin{pmatrix} c_{11} & c_{21} & \dots & c_{t1} \\ c_{12} & c_{22} & \dots & c_{t2} \\ \vdots & \vdots & \ddots & \vdots \\ c_{1t} & c_{2t} & \dots & c_{tt} \end{pmatrix}.$$

If we denote the determinant of $A_{\mathcal{S}}$ by $\Delta_{\mathcal{S}}$, we have

$$A_{\mathcal{S}}C_{\mathcal{S}} = C_{\mathcal{S}}A_{\mathcal{S}} = \Delta_{\mathcal{S}}I_t, \quad (4)$$

where I_t denotes the $t \times t$ identity matrix.

For our scheme, each user $i \in \mathcal{S}$ computes his partial signature as

$$s_i = w^{c_{i1}y_i} \pmod{N}. \quad (5)$$

2) *Combining the Partial Signatures:* To combine the partial signatures, we simply compute

$$s_p = s_{i_1}s_{i_2}\dots s_{i_t} \pmod{N}. \quad (6)$$

Note that, from equation (4), we have

$$s_p = w^{\Delta_{\mathcal{S}}d} \pmod{N}. \quad (7)$$

Given that e is a prime number relatively prime to $\Delta_{\mathcal{S}}$, it is easy to compute the signature $s = w^d \pmod{N}$ from s_p . Take

$$s = s_p^a w^b \pmod{N}, \quad (8)$$

where a and b are integers such that

$$\Delta_{\mathcal{S}}a + eb = 1, \quad (9)$$

which can be obtained by the extended Euclidean algorithm on $\Delta_{\mathcal{S}}$ and e .

IV. SOLUTION OF THE LINEAR SYSTEM

In Blakley's SSS, the private key is found by solution of the linear system $A_{\mathcal{S}}x = y_{\mathcal{S}}$. However, this system may not have a unique solution over $\mathbb{Z}_{\phi(N)}$. If $\gcd(\Delta_{\mathcal{S}}, \phi(N)) > 1$, the matrix $A_{\mathcal{S}}$ will not have an inverse modulo $\phi(N)$, and the linear system will have many different solutions. Interestingly, our threshold signature scheme computes the correct signature in this case as well.

When $\gcd(\Delta_{\mathcal{S}}, \phi(N)) > 1$ and the linear system yields many different solutions for d , note that the value $\Delta_{\mathcal{S}}d$ is a fixed number for all these possible solutions, and is equal to

$$\Delta_{\mathcal{S}}d = \sum_i c_{i1}y_i.$$

Hence, the incomplete signature

$$\begin{aligned} s_p &= w^{\sum_i c_{i1}y_i} \pmod{N} \\ &= w^{\Delta_{\mathcal{S}}d} \pmod{N} \end{aligned}$$

is the same for every solution of the system $A_{\mathcal{S}}x = y_{\mathcal{S}}$.

Then the signature s is obtained from s_p as

$$s = s_p^a w^b \pmod{N},$$

where a and b are the integer solutions of $\Delta_{\mathcal{S}}a + eb = 1$. Hence, the signature s is $w^d \pmod{N}$ for the right d value, computed according to the public key e .

V. CHOOSING e

The choice of e is critical in the setup phase because the solution depends on e and $\Delta_{\mathcal{S}}$ being relatively prime. To achieve this, we can either choose a special matrix whose determinant we know to be relatively prime to e , or choose e as a sufficiently large prime according to t and n so that the probability that $\Delta_{\mathcal{S}}$ is divisible by e will be negligible for any coalition $\mathcal{S}$.

A. Choosing e Probabilistically

The probability of a random integer's being divisible by a prime e is $1/e$. So, if we have a (t, n) threshold scheme, the probability that the determinant of none of the $\binom{n}{t}$ $A_{\mathcal{S}}$ matrices will be divisible by e is $(1 - \frac{1}{e})^{\binom{n}{t}}$. If we take $e \gg \binom{n}{t}$, we have

$$\left(1 - \frac{1}{e}\right)^{\binom{n}{t}} \approx 1. \quad (10)$$

B. Using a Vandermonde Matrix

A simple choice for the matrix A that enables us to guarantee that e will be relatively prime to the determinant of the coefficient matrix is to choose the rows of the matrix A as the rows of a Vandermonde matrix. Then, A_S will have the following form for any coalition S :

$$A_S = \begin{pmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{t-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{t-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_t & a_t^2 & \dots & a_t^{t-1} \end{pmatrix}$$

The determinant of the Vandermonde matrix is nonzero, provided that no two rows are identical, and it is found by the following formula :

$$|A_S| = \prod_{i,j=1, i < j}^t (a_i - a_j) \quad (11)$$

Without loss of generality take $(a_1, a_2, \dots, a_n) = (1, 2, \dots, n)$. Obviously $\prod_{i,j=1, i < j}^t (a_i - a_j)$ divides $\prod_{i,j=1, i < j}^n (a_i - a_j)$. We also have

$$\prod_{i,j=1, i < j}^n (a_i - a_j) = 1^{\alpha_1} 2^{\alpha_2} \dots (n-1)^{\alpha_{n-1}} \quad (12)$$

for some $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$. Hence by choosing e as a prime greater than n we can guarantee that the determinant of any A_S will be relatively prime to e .

VI. CONCLUSION

We presented an RSA threshold signature scheme based on Blakley secret sharing. To the best of our knowledge, this is the first threshold RSA signature scheme that uses Blakley SSS as the underlying secret sharing scheme. The scheme is as efficient as Shoup's practical threshold RSA signature and can be easily implemented. Moreover, this approach can be extended to other public key cryptosystems where the private key is used in the exponent.

REFERENCES

- [1] C. Asmuth and J. Bloom. A modular approach to key safeguarding. *IEEE Trans. Information Theory*, 29(2):208–210, 1983.
- [2] G. Blakley. Safeguarding cryptographic keys. In *Proc. of AFIPS National Computer Conference*, 1979.
- [3] Y. Desmedt. Some recent research aspects of threshold cryptography. In *Proc. of ISW '97, 1st International Information Security Workshop*, volume 1196 of LNCS, pages 158–173. Springer-Verlag, 1997.
- [4] Y. Desmedt and Y. Frankel. Threshold cryptosystems. In *Proc. of CRYPTO'89*, volume 435 of LNCS, pages 307–315. Springer-Verlag, 1990.
- [5] Y. Desmedt and Y. Frankel. Shared generation of authenticators and signatures. In *Proc. of CRYPTO'91*, volume 576 of LNCS, pages 457–469. Springer-Verlag, 1992.
- [6] Y. Desmedt and Y. Frankel. Homomorphic zero-knowledge threshold schemes over any finite abelian group. *SIAM Journal on Discrete Mathematics*, 7(4):667–679, 1994.
- [7] P. A. Fouque, G. Poupard, and J. Stern. Sharing decryption in the context of voting or lotteries. In *Proc. of FC 2000, 4th International Conference on Financial Cryptography*, volume 1962 of LNCS, pages 90–104. Springer-Verlag, 2001.
- [8] H. F. Huang and C. C. Chang. A novel efficient (t,n) threshold proxy signature scheme. *Information Sciences*, 176(10):1338–1349, 2006.
- [9] K. Kaya and A. A. Selçuk. Threshold cryptography based on Asmuth-Bloom secret sharing. *Information Sciences*, 177(19):4148–4160, 2007.
- [10] A. Lysyanskaya and C. Peikert. Adaptive security in the threshold setting: From cryptosystems to signature schemes. In *Proc. of ASIACRYPT 2001*, volume 2248 of LNCS, pages 331–350. Springer-Verlag, 2001.
- [11] A. De Santis, Y. Desmedt, Y. Frankel, and M. Yung. How to share a function securely? In *Proc. of STOC94*, pages 522–533, 1994.
- [12] A. Shamir. How to share a secret? *Comm. ACM*, 22(11):612–613, 1979.
- [13] V. Shoup. Practical threshold signatures. In *Proc. of EUROCRYPT 2000*, volume 1807 of LNCS, pages 207–220. Springer-Verlag, 2000.

Genetik Algoritma Kullanarak Görüntü Kaynaştırma Tabanlı Görünür Damgalama

Veysel ASLANTAŞ, Rifat KURBAN

Özet— Gelişen teknolojiyle beraber sayısal bilginin güvenliği oldukça önem kazanmıştır. Görüntü damgalama, sahiplik ve telif haklarının korunması gibi pek çok alanda kullanılan bir tekniktir. Bu çalışmada, Genetik algoritma kullanarak dalgacık domeninde görüntü kaynaştırma tabanlı bir görünür damgalama yöntemi önerilmiştir. Farklı barındırıcı resim ve damga üzerinde gerçekleştirilen simülasyonlarda önerilen yöntemin hem sayısal hem de görsel olarak iyi sonuçlar verdiği görülmüştür.

Anahtar kelimeler— Görünür damgalama, Görüntü kaynaştırma, Ayrık dalgacık dönüşümü, Genetik algoritma

Abstract— Due to the developments in technology, security of the digital data is becoming more important. Image watermarking techniques can be used for ownership claim and copyright protection. In this paper, an image fusion based visible watermarking method using Genetic algorithm in wavelet domain is proposed. In the simulations which were realized on different host and watermark images, the numerical and visual results of the proposed method are satisfactory.

Keywords— Visible watermarking, Image fusion, Discrete wavelet transform, Genetic algorithm

I. GİRİŞ

İnternet ve iletişim teknolojilerindeki ilerlemelerle beraber sayısal bilginin güvenliği de oldukça önem kazanmıştır. Bu amaçla görüntü, ses ve video gibi çoklu ortam verileri için sahiplik, telif hakları ve bilgi korsanlığı gibi alanlarda kullanılabilecek pek çok sayısal damgalama yöntemi geliştirilmiştir. Damgalama yöntemleri görünür ve görünmez yaklaşımlar olarak sınıflandırılabilir. Görünür yöntemler sahipliğin logolar vasıtasıyla açıkça iddia edilebilmesini sağlarken, görünmez yöntemler bu hakların saklı bir şekilde korunmasını sağlarlar [1-4].

Görüntü kaynaştırma, farklı algılayıcılardan veya geometrik parametreleri değiştirilmiş bir algılayıcıdan elde edilen görüntülerin birleştirilmesine denir. Medikal görüntüleme, uzaktan algılama ve sınırlı görüş derinliğinin artırılması gibi uygulamalarda kullanılmaktadır. Pek çok görüntünün veya görüntü özelliğinin birleştirilerek tek bir görüntü elde edilmesi işlemi olarak da tanımlanmaktadır. Elde edilen sonuç resim,

kaynak resimlerden elde edilmiş genişletilmiş bilgileri ihtiva etmektedir [5,6].

Sayısal damgalamanın önemli uygulamalarından birisi de özellikle web ortamında bilgilerin kötüye kullanımını engelleme amaçlı olarak bir dokümanın kaynağının tanımlanması için görünür sahiplik bilgisinin ifade edilmesidir [7]. Genelde görünür damga bir metin veya logo biçimindeki ikincil bir resimdir. Görünür damgalama, barındırıcı resim ile damga resminin bir alanda birleştirilmesi yani kaynaştırılması işlemi olarak da düşünülebilir. Diğer bir ifadeyle, görüntü kaynaştırma alanındaki yaklaşımlar, görünür damgalama alanına genişletilerek uyarlanabilir. Görünür damgalamada olması gereken özellikler şu şekilde sıralanabilir:

- damgalanmış resim barındırıcı resimden olabildiğince bilgi ihtiva ederken damganın karakteristiği de açıkça görülebilmelidir,
- görünür damgalama yöntemi, gözlemcide yanıltıcı bozulmalar ve tutarsızlıklar meydana getirmemelidir,
- damga gürültüye ve çeşitli ataklara karşı dayanıklı olmalı ve damganın yok edilebilmesi olabildiğince zor olmalıdır [8].

Görünür damgalama alanındaki ilk çalışmalar IBM sayısal kütüphane organizasyonu tarafından Vatikan kütüphanesindeki sayısallaştırılmış belgelerin işaretlenmesi amacıyla yapılmıştır [9]. Damganın dayanıklılığı ölçeklenerek orijinal resimlerin parlaklık bileşenlerine gömme işlemi gerçekleştirilmiştir. Blok tabanlı ayrık kosinüs dönüşümü (AKD) domeninde doku, kenar ve parlaklık bilgisine dayalı çeşitli çalışmalar gerçekleştirilmiştir [10]. Diğer taraftan ayrık dalgacık dönüşümü (ADD) ile yapılan çalışmalarda dalgacık katsayıları sınıflandırılarak belli oranlarda birleştirilmiştir [7,8].

Bu çalışmada, ADD ile dalgacık dönüşümü yapılan barındırıcı resim ile damga lineer bir kaynaştırma kuralı ile birleştirilerek damgalanmış resim elde edilmektedir. Bu işlem sırasında her alt bant için gerekli olan birleştirme ağırlıkları Genetik Algoritma (GA) kullanılarak optimal olarak belirlenmektedir. Katsayıların kalitesinin belirlenebilmesi için korelasyon tabanlı bir metrik önerilmiştir. Böylece barındırıcı resim ve damganın içeriğinden bağımsız optimal bir yöntem elde edilmiştir.

Çalışmanın devamı şu şekilde organize edilmiştir: 2. bölümde geliştirilen yöntem, 3. bölümde ise gerçekleştirilen simülasyon çalışmaları ve sonuçları verilmiştir. Son bölümde

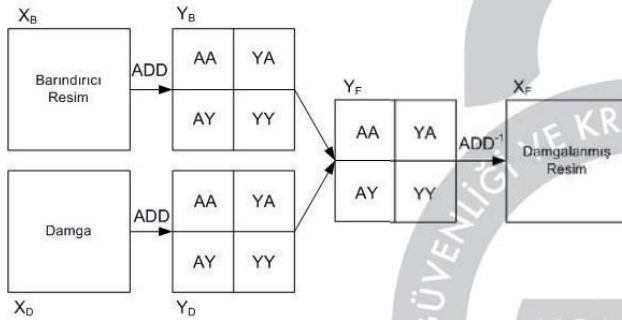
V. Aslantaş (e-posta: aslantas@erciyes.edu.tr, tel: +903524374901 32602) ve R. Kurban, Erciyes Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği bölümünde görev yapmaktadırlar.

elde edilen sonuçlar değerlendirilmiştir.

II. GÖRÜNÜR DAMGALAMA

A. Dalgacık Domeninde Görüntü Birleştirme Tabanlı Görünür Damgalama

Dalgacık dönüşümü verinin çoklu çözünürlüklü bir gösterimidir ve görüntünün daha düşük çözünürlüklü versiyonlarını ihtiva etmektedir. Ayrık dalgacık dönüşümü (ADD) işlemi işaretin bir grup alçak-geçiren ve yüksek-geçiren filtreden geçirilmesiyle elde edilir. Yüksek-geçiren filtre ana dalgacık fonksiyonunu ve alçak-geçiren filtre ise ölçekleme fonksiyonunu ifade eder. 2 boyutlu bir verinin dekompozisyon işleminde filtreler önce yatay daha sonra dikey olarak uygulanır. Böylece, bir yaklaşım görüntüsü (AA), üç tane de detay görüntüsü (AY, YA, YY) elde edilir. Bu iteratif işlemler boyunca her bir iterasyonda işaretin belli bir frekans bölgesindeki kısmı işaretin kalan kısmıdır (AA alt bandı) ve istenirse sürekli olarak daha sonraki seviyelerde dekompoze edilebilir.



Şekil 1. Görünür damgalama yönteminin genel çatısı.

Şekil 1'de görünür damgalama yönteminin genel çatısı görülmektedir. Dalgacık domeninde görünür damgalama yapılırken, ilk adımda barındırıcı resim (X_B) ile damga'nın (X_D) ADD'leri hesaplanmaktadır. Elde edilen katsayılar bir kaynaştırma kuralına göre birleştirilir ve ters ADD hesaplanarak damgalanmış resim (X_F) elde edilir. Görüntü kaynaştırmada olduğu gibi, çoklu-çözünürlüklü görünür damgalama yaklaşımlarının temel dayanağı insan görme sisteminin yerel karşıtlık değişimlerine olan duyarlılığı gerçeğidir [7,8]. Görüntü kaynaştırma ve görünür damgalama arasındaki fark birleştirme işlemi sırasında ortaya çıkar. Görüntü kaynaştırmada kaynak resimler aynı sahneye ait farklı algılayıcılardan veya parametreleri değişmiş bir algılayıcıdan elde edilen görüntülerdir. Görünür damgalamada ise kaynak resimler barındırıcı resim ve damgadır. Görünür damgalamada, barındırıcı resim damgadan daha önemlidir. Dolayısıyla damgalanmış resimde barındırıcı resim damgaya oranla daha baskın olmalıdır.

Lineer ağırlıklı birleştirme yönteminde her bant için ağırlık katsayıları (w) belirlenmektedir. Bu değerler 0 ile 1 aralığındadır. Bu işlem, Denklem (1)'de verildiği gibi gerçekleştirilir:

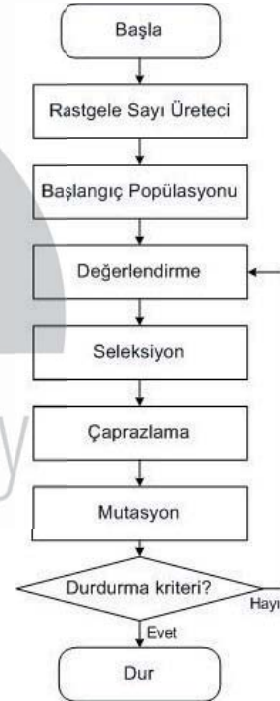
$$\begin{aligned} Y_F^{AA} &= w^{AA} \cdot Y_B^{AA} + (1 - w^{AA}) \cdot Y_D^{AA} \\ Y_F^{AY} &= w^{AY} \cdot Y_B^{AY} + (1 - w^{AY}) \cdot Y_D^{AY} \\ Y_F^{YA} &= w^{YA} \cdot Y_B^{YA} + (1 - w^{YA}) \cdot Y_D^{YA} \\ Y_F^{YY} &= w^{YY} \cdot Y_B^{YY} + (1 - w^{YY}) \cdot Y_D^{YY} \end{aligned} \quad (1)$$

Ağırlık katsayıları (w) 0.5'den büyük olduğu durumlarda damgalanmış resimde barındırıcı resim daha baskınken, 0.5'den küçük değerlerde damga daha baskın olmaktadır. Bu yöntemde w katsayılarının uygun bir şekilde belirlenmesi gerekmektedir.

Optimizasyon için, basit yapısı ve uygulama kolaylığı ile ön plana çıkan ve literatürde çok fazla uygulama alanına sahip Genetik algoritma tercih edilmiştir.

B. Genetik Algoritma

Temel bir Genetik Algoritma (GA) [11] beş bileşenden meydana gelmektedir: rastgele sayı üretici, uygunluk değerlendirme birimi ve seleksiyon, çaprazlama ve mutasyon için genetik operatörler. Şekil 2'de temel GA'nın bileşenleri görülmektedir.



Şekil 2. Temel GA'nın bileşenleri.

Başlangıç popülasyonu, algoritmanın başlamasından önce rastgele sayı üretici tarafından üretilen sayı vektörleri kümesidir. Her bir vektör optimizasyon problemi tarafından adreslenen bir muhtemel çözümü ifade eder. Değerlendirme birimi her bir birey için bir uygunluk değeri hesaplar. Uygunluk değeri çözümün kalitesini ölçen bir değerdir. Genetik operatörlerin amacı daha kaliteli çözümleri bulmaktır. Seleksiyon operatörü doğal seleksiyon fonksiyonu icra eder.

Bireyleri temsil eden vektörler diğer vektörler ile birlikte değerlendirilerek uygunluk değerine bağlı bir olasılık ile gelecek nesiller için seçilirler. Çaprazlama operatörü rastgele olarak birey çiftleri seçer. En basit çaprazlama operatörü ebeveyn bireyin rastgele bir noktasından kesilerek diğer ebeveyn bireyin kuyruğu ile yer değiştirilmesiyle gerçekleştirilir. Çaprazlama operatörünün işlem miktarı çaprazlama oranı tarafından belirlenir. Mutasyon operatörü rastgele bireyi temsil eden vektördeki sayıları değiştirir. Mutasyon miktarını mutasyon oranı parametresi belirler. Algoritmanın bir çevrimi değerlendirme, seleksiyon, çaprazlama ve mutasyon operatörlerinin uygulanmasıyla tamamlanır. Algoritmanın her bir döngüsünde yeni bir çözüm nesli oluşturulur [12].

C. Genetik Algoritma Kullanarak Görünür Damgalama

Dalgacık uzayında görüntü kaynaştırma tabanlı görünür damgalamada w katsayılarının uygun bir şekilde belirlenebilmesi için bu katsayıları temsil eden vektörleri ihtiva eden bir başlangıç popülasyonu oluşturulmaktadır. GA kullanılarak bu katsayılar optimize edilmektedir. Ancak burada en büyük problem, elde edilecek katsayıların kalitesinin nasıl ölçüleceğidir. Genetik operatörlerin çalışabilmesi için popülasyondaki her bir olası çözümün kalite değerinin bilinmesi gerekir. Popülasyondaki her bir birey Denklem (2)'deki vektör şeklinde ifade edilmektedir.

$$w_i = [w^{AA} w^{AY} w^{YA} w^{YY}] \quad (2)$$

Çözümlerin kalitesini hesaplamada temel mantık elde edilen damgalanmış resmin barındırıcı resme olan benzerliğini maksimize ederken, damgalanmış resimden çıkartılan damganın orijinal damgayla olan benzerliğini de maksimize etmektir. Bu amacı gerçekleştirebilmek için Denklem (3)'de önerilen kalite ifadesinden yararlanılmıştır.

$$k = K(X_F, X_B) + K(X_{CD}, X_D) \quad (3)$$

K verilen iki veri arasındaki korelasyon katsayısını, X_{CD} ise damgalanmış resimden çıkartılan damgayı ifade etmektedir. Korelasyon katsayıları Denklem (4) kullanılarak hesaplanmıştır:

$$K(A, B) = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \bar{A})^2 \right) \left(\sum_m \sum_n (B_{mn} - \bar{B})^2 \right)}} \quad (4)$$

$\bar{A}$ ve $\bar{B}$, sırasıyla A ve B 'nin ortalamalarını ifade etmektedir.

Damgalanmış resimden, damgayı elde edebilmek için takip eden denklem kullanılmıştır:

$$X_{CD} = \frac{X_F - w^{AA} \cdot X_B}{(1 - w^{AA})} \quad (5)$$

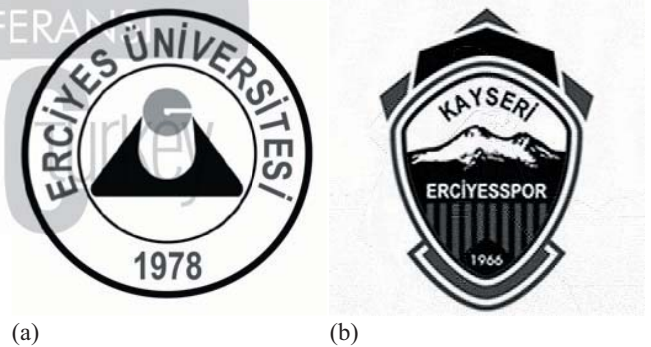
Denklem (4) ile elde edilen korelasyon katsayısı $[-1,1]$ aralığında bir değerdir. 1 olması durumunda maksimum benzerlik ifade edilir. Dolayısıyla, Denklem (3)'de verilen ifade değer olarak büyüdükçe elde edilen çözümün kalitesi de artacaktır.

III. SİMÜLASYON SONUÇLARI

Simülasyon çalışmaları iki farklı 256x256 boyutlarında 8-bit gri seviye barındırıcı resim ve damga üzerinde gerçekleştirilmiştir. Barındırıcı resimler ve damgalar sırasıyla Şekil 3 ve 4'de görülmektedir. İlk simülasyonda barındırıcı resim olarak Şekil 3(a), damga olarak ise Şekil 4(a)



Şekil 3. Barındırıcı resimler: (a) Lena, (b) Kameraman.



Şekil 4. Damgalar: (a) Erciyes Üniversitesi logosu, (b) Erciyespor logosu.

kullanılmıştır. Diğerinde ise barındırıcı resim olarak Şekil 3(b), damga olarak Şekil 4(b) kullanılmıştır.

Giriş resimlerinin ayrık dalgacık dönüşümünün hesaplanmasında Daubechies 1 filtre ailesi kullanılarak 1 seviye dekompozisyon yapılmıştır.

Uygulamada w ağırlık katsayılarının optimize edilmesi için kullanılan GA'ya ait kontrol parametreleri Tablo 1'de verilmiştir.

TABLO 1. GA KONTROL PARAMETRELERİ.

Veri tipi	Reel sayı vektörü
Popülasyon boyutu	32

Jenerasyon sayısı	100
Mutasyon oranı	0.1
Çaprazlama oranı	0.8

Elde edilen kaynaştırma katsayıları ise Tablo 2’de verilmiştir. Tablodaki sonuçlar incelendiğinde, GA’nın amaç fonksiyonunu optimize etmek için farklı alt bantlar için farklı katsayılar hesapladığı görülmüştür. Diğer taraftan katsayıların barındırıcı resim ve damganın içeriğine göre değiştiği de görülmektedir.

TABLO 2. SİMÜLASYON SONUCUNDA GA İLE ELDE EDİLEN KAYNAŞTIRMA KATSAYILARI.

	w^{AA}	w^{AY}	w^{YA}	w^{YY}
Şekil 3(a) – 4(a)	0.9170	0.9512	0.9077	0.9450
Şekil 3(b) – 4(b)	0.9247	0.8900	0.9184	0.8541

Gerçekleştirilen simülasyonlar sonucunda elde edilen korelasyon katsayıları Tablo 3’de verilmiştir. Tablodan da görüleceği üzere optimizasyon algoritması hem barındırıcı resim ile damgalanmış resmin benzerliğini ($K(X_F, X_B)$) artırmakta hem de çıkartılmış damga ile orijinal damganın benzerliğini ($K(X_{CD}, X_D)$) artırmaya çalışmaktadır. Diğer taraftan, önerilen yöntem iki benzerlik oranını dengelemeye de çalışmaktadır. Çünkü barındırıcı resim ile damgalanmış resim benzerliğini maksimum yapması durumunda, damgalanmış resim ile barındırıcı resim aynı olur. Bu durumda damga hiç gömülmez ve diğer benzerlik ölçütü çok küçük çıkar. Dikkat edilirse elde edilen sonuçlarda çıkartılan damga ile orijinal damganın benzerliği neredeyse maksimumdur. Algoritma önce bu kısmı maksimize edip daha sonra olabildiğince barındırıcı resim ile damgalanmış resmin benzerliğini maksimize etmektedir. Görüleceği üzere burada elde edilen ile vazgeçilen arasında bir dengeleme söz konusudur. GA bu işlemi başarıyla gerçekleştirmektedir.

TABLO 3. SİMÜLASYON SONUCUNDA GA İLE ELDE EDİLEN KORELASYON KATSAYILARI.

Şekil 3(a) – 4(a)	$K(X_F, X_B)$	0.9872
	$K(X_{CD}, X_D)$	0.9958
Şekil 3(b) – 4(b)	$K(X_F, X_B)$	0.9919
	$K(X_{CD}, X_D)$	0.9963

GA ile elde edilen damgalanmış resimler Şekil 5’de verilmiştir. Resimlerden görüleceği üzere GA ile elde edilen damgalanmış resimde damganın görünürlüğü kaybedilmeden barındırıcı resmin baskınlığı korunmuştur. Örneğin Şekil 5(b)’de logonun kameramanın koyu renk elbisesi üzerine gelen kısımlarında bile algoritmanın belirlediği katsayılar sayesinde damga bozulmadan gömülmüş ve görsel olarak ayırt etmek mümkün hale gelmiştir. Şekil 6’da damgalanmış resimlerden çıkartılan damgalar görülmektedir. Şekillerden de görüleceği üzere elde edilen damgalar orijinal damgalara görsel olarak oldukça benzemektedir.



(a) (b)
Şekil 5. Damgalanmış resimler



(a) (b)
Şekil 6. Çıkartılan damgalar

IV. SONUÇ

Bu çalışmada dalgacık domeninde lineer görüntü kaynaştırma yöntemi görünür damgalama problemine başarıyla uygulanmıştır. Kaynaştırma katsayılarının optimum olarak elde edilmesinde GA kullanılmıştır. Önerilen yöntem oldukça pratik ve kullanışlıdır. Elde edilen damgalanmış resimler hem barındırıcı resme oldukça yüksek oranda benzemektedir hem de üzerindeki damga çıkartılabilecek nitelikte ve barındırıcı resimden daha az baskın olarak görülmektedir. GA ile elde edilen katsayıların kullanımında hem sayısal hem de görsel olarak iyi sonuçlar elde edilmiştir.

İleriki çalışmalarda yöntemin literatürdeki görünür damgalama yöntemleri ile ayrıntılı bir karşılaştırması gerçekleştirilebilir. Diğer taraftan kullanılan ayrık dalgacık dönüşümünün dekompozisyon seviyesinin ve kullanılan dalgacık filtre ailesinin sonuç üzerine etkileri inceleyebilir ve görünür damgalamada kullanılabilecek farklı performans metrikleri geliştirilebilir.

KAYNAKLAR

- [1] S.P. Mohanty, P. Guturu, E. Kougianos, N. Pati, "A novel invisible color image watermarking scheme using image adaptive watermark creation and robust insertion-extraction", Proc. of the 8. IEEE International Symposium on Multimedia, 2006.
- [2] L. Ruizhen, T. Tieniu, "Survey of watermarking for digital images," Journal of China Institute of Communications, vol. 21, pp39-48, 2000.
- [3] W. Huang, J. Gou, "An Image Fusion-Based Multi-Watermarking Algorithm", Proceedings of the 2006 IEEE International Conference on Networking, Sensing and Control, 266- 269, 2006.

- [4] D. Zhang; S. Qu; B. Kang; "A New Digital Image Hiding Approach Using Multi-Image Fusion", International Workshop on Knowledge Discovery and Data Mining, 553-557, 2008.
- [5] V. Aslantas, A. Bulatov, R. Kurban, "Multi-focus image fusion using a fuzzy criterion function", 6th International Symposium on Intelligent And Manufacturing Systems (IMS 2008), 14-17 October 2008.
- [6] S. Nikolov, et al., "Wavelets for image fusion," in Wavelets in Singal and Image Analysis, A.A. Petrosian and EG. Meyer (eds.), 2001 Kluwer Academic Publishers, pp. 213-241.
- [7] Y. Hu, J. Huang, S. Kwong, Y.K. Chan, "Image Fusion Based Visible Watermarking Using Dual-Tree Complex Wavelet Transform", LNCS 2939, Digital Watermarking, 86-100, 2004.
- [8] Y. Hu, S. Kwong, "An image fusion based visible watermarking algorithm", Proceedings of the 2003 International Symposium on Circuits and Systems, 794-797, 2003.
- [9] G.W. Braudaway, K.A. Margerlein, F.C. Mintzer, "Protecting publicavailable images with a visible image watermark", Proc. SPIE Conf. on Optical Security and Counterfeit Deterrence Techniques. vol. SPIE 2659, pp. 126-132, 1996.
- [10] M.S. Kankanhalli, Rajmohan, K.R. Ramakrishnan, "Adaptive visible watermarking of images", IEEE Int. Conf. on Multimedia Computing and Systems. vol.1, pp. 568-573, 1999.
- [11] J.H. Holland, "Adaptation in natural and artificial system: an introductory analysis with applications to biology, control and artificial intelligence" Cambridge, MA: MIT Press; 1992.
- [12] V. Aslantas, "A singular-value decomposition-based image watermarking using genetic algorithm", AEU - International Journal of Electronics and Communications, Volume 62, Issue 5, 386-394, 2008.



SEA Şifreleme Algoritması Kullanarak Güvenli Kablosuz Algılayıcı Ağ Haberleşmesinin Gerçekleştirilmesi

Cüneyt BAYILMIŞ, Murat ÇAKIROĞLU

Özet— Kablosuz Algılayıcı Ağ (KAA)'ların sınırlı kaynaklara sahip olması ve herkese açık olan kablosuz iletişim ortamı üzerinden haberleşmesi etkin güvenlik çözümlerinin geliştirilmesini zorlaştırmaktadır. Güvenilir iletişimin en önemli gereksinimi olan şifreleme/şifre çözme prosedürlerinin genellikle çok karmaşık ve işlem yükünün oldukça fazla olması popüler şifreleme algoritmalarının KAA'larda kullanılabilirliğini güçlendirmektedir. Bu sebeple KAA'larda kullanılan şifreleme algoritmalarından mümkün olan en az işlem yükü ile en uygun güvenlik seviyesini sağlaması beklenmektedir. Bu çalışmada, blok tabanlı yeni bir şifreleme algoritması olan Ölçeklenebilir Şifreleme Algoritması (Scalable Encryption Algorithm, SEA) kullanılarak KAA'larda güvenli iletişimin gerçekleştirilmesi amaçlanmaktadır. MICAz düğümleri üzerinde gerçekleştirilen SEA algoritmasının başarımlı bellek gereksinimi, çalışma zamanı, güvenlik ve esneklik kriterleri açısından ele alınmakta ve elde edilen sonuçlar Skipjack algoritması ile karşılaştırılmaktadır.

Anahtar Kelimeler—Kablosuz Algılayıcı Ağlar, Güvenlik, SEA

I. GİRİŞ

Kablosuz Algılayıcı Ağ (KAA)'lar, bakım gerektirmeden uzun yıllar çalışabilmeleri ve çok çeşitli alanlarda kullanılabilmeleri sebebiyle hem endüstriyel uygulamalarda hem de akademik çalışmalarda çok popüler bir alan haline gelmiştir. KAA'ları meydana getiren düğümler, genellikle iki adet standart pil ile beslenen, veri saklama/işlem kapasitesi sınırlı olan ve kısa mesafeli kablosuz ortam üzerinden haberleşen tümdevrelerdir [1]. Kaynakları sınırlı olan bu düğümlerin, çoğu uygulama için dış ortamda bulunması ve kablosuz olarak haberleşmesi KAA'ların çeşitli saldırılara maruz kalma riskini arttırmaktadır. Bu sebeple güvenliğin en önemli tasarım ölçütü olduğu askeri ve tıbbi uygulamalar başta olmak üzere birçok uygulama alanında kablosuz algılayıcı ağların veri gizliliği, bütünlüğü, tazeliliği ve kimlik doğrulaması gibi hayati güvenlik gereksinimlerini karşılaması gerekmektedir [2-5].

KAA'ların kısıtlı donanımsal kaynaklara sahip olması, bilgisayar ağlarında kullanılan geleneksel güvenlik

çözümlerinin KAA'larda doğrudan kullanılmasını güçlendirmektedir. ECC, RSA, AES, T-DES, RC5 gibi popüler şifreleme algoritmalarının gerektirdiği işlem yükünün oldukça fazla olması, bu algoritmaların saklama ve işlem yapma kabiliyeti sınırlı olan kablosuz algılayıcı düğümleri üzerinde gerçekleştirilmesini zorlaştırmaktadır. Ayrıca kullanılan şifreleme algoritmasının düğümlerin işlem yükünün ve iletilen paket boyutlarının artmasına yol açması beraberinde enerji tüketimlerinin de önemli ölçüde artmasına ve düğümlerin yaşam sürelerinin azalmasına neden olmaktadır. Bu sebeple KAA'larda kullanılan şifreleme algoritmalarından mümkün olan en az işlem yüküyle istenilen güvenlik gereksinimlerini karşılaması beklenmektedir. Sınırlı komut setine ve işlem yapma kabiliyetine sahip işlemciler için geliştirilmiş, basit şifreleme rutinleri içeren fakat doğrusal/farksal kriptanaliz tekniklerine karşı dayanıklı olan SEA (Scalable Encryption Algorithm-Ölçeklenebilir Şifreleme Algoritması) şifreleme algoritması [6-7], bu özellikleri sebebiyle KAA'ların güvenlik gereksinimlerini karşılayabilecek niteliktedir.

Bu çalışmada, KAA'ların düşük maliyetli olarak güvenli haberleşme ihtiyaçlarını karşılayabilmek amacıyla SEA şifreleme algoritmasının kablosuz algılayıcı düğümleri üzerinde gerçekleştirilmesi yapılmış ve gerçekleştirilmeden elde edilen performans değerleri sunulmuştur.

Bu makalenin literatüre temel katkıları şunlardır;

- KAA'larda SEA şifreleme algoritması kullanılarak güvenli iletişimin düşük maliyetle gerçekleştirilmesi,
- SEA şifreleme algoritmasının gerçekleştirilmesinin idealleştirilmiş benzetim ortamları yerine MICAz kablosuz algılayıcı ağ platformu üzerinde yapılması.

Makalenin geri kalan kısımları şu şekilde düzenlenmiştir: Bölüm 2'de KAA güvenliği hakkında bilgi verilmektedir. 3. Bölümde SEA şifreleme algoritmasının özellikleri açıklanmakta, Bölüm 4'de SEA algoritmasının gerçekleştirilmesinde kullanılan deney düzeneği ve araçlar tanıtılmaktadır. Bölüm 5'de ise gerçekleştirilmeden elde edilen sonuçlar sunulmakta ve son bölümde makale sonuçlandırılmaktadır.

Cüneyt Bayılmış ve Murat ÇAKIROĞLU, Sakarya Üniversitesi, Teknik Eğitim Fakültesi, Bilgisayar Sistemleri Öğretmenliği, Esentepe Kampüsü, Sakarya, Tel:2642956456, Fax:2642956421
e-mail: {cbayilmis, murate}@sakarya.edu.tr

II. KABLOSUZ ALGILAYICI AĞLARDA GÜVENLİK

Askeri ve tıbbi uygulamalar, doğal felaketlerin tespiti, bina güvenlik sistemleri v.b. birçok alanda kullanılmakta olan KAA'ların çeşitli türdeki saldırılara karşı güvenilir bir şekilde çalışabilmesi son derece hayati önem arz etmektedir. Ancak, düşük maliyetin sağlanabilmesi için donanımsal kaynakları sınırlı olan düğümlerin tercih edilmesi, geleneksel güvenlik tekniklerinin KAA'larda kullanılmasını zorlaştırmaktadır. Bununla birlikte, algılayıcı düğümlerinin çoğu uygulama için dış ortamda bulunması ve paylaşımlı olan kablosuz ortam üzerinden haberleşmesi saldırganların işini kolaylaştırmakta ve KAA'ların güvenlik açısından diğer ağlara nazaran daha fazla risk taşımasına sebep olmaktadır. KAA'larda güvenlik 3 temel perspektifte incelenebilir [2]:

- KAA'ların güvenliğini kısıtlayan unsurlar,
- KAA güvenlik gereksinimleri,
- KAA güvenliğini tehdit eden saldırılar ve savunma yöntemleri.

A. KAA Güvenliğini Kısıtlayan Unsurlar

KAA'lar, geleneksel ağlara oranla daha fazla sınırlamaya sahip özel bir ağ hüviyetindedir. Sınırlı donanımsal kaynaklar, güvenli olmayan iletişim kanalı, düğümlerin uzun süreler boyunca gözetimsiz çalışması gibi sebepler, geleneksel güvenlik tekniklerinin doğrudan KAA'larda kullanılmasını zorlaştırmaktadır. Güvenli bir ağ tasarımı gerçekleştirebilmek için bu sınırlamaları dikkate almak gerekmektedir.

B. KAA Güvenlik Gereksinimleri

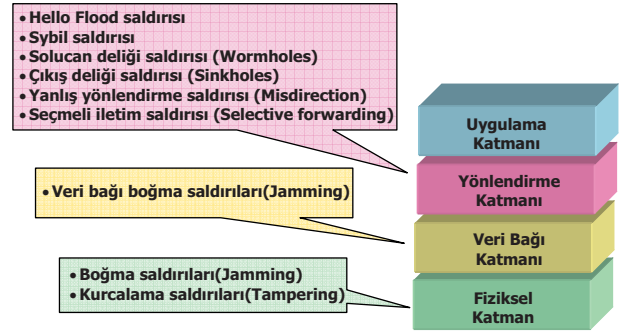
KAA'lar, geleneksel bilgisayar ağlarının ihtiyaç duyduğu güvenlik gereksinimlerine ek olarak sadece kendine has olan güvenlik gereksinimlerine de sahiptir. Bu özel gereksinimlerin birçoğu KAA'ların dış ortamda olmalarından kaynaklanmaktadır.

KAA güvenli iletişim gereksinimleri özetle şunlardır:

- Veri gizliliği (Data Confidentiality)
- Veri bütünlüğü (Data Integrity)
- Veri tazeliliği (Data Freshness)
- Kimlik doğrulama (Authentication)
- Kendi kendini örgütlenme (Self Organization)
- Zaman eşleşmesi (Time Synchronization),
- Güvenli konum belirleme (Secure Localization)

C. Saldırı ve Savunma Önlemleri

KAA'lar yapısı gereği birçok türdeki saldırılara karşı açıktır. Özellikle farklı katmanlardaki fonksiyonların işleyişini bozmayı hedefleyen Hizmet Engelleme (Denial of Service-DoS) Saldırıları KAA güvenliği için önemli bir tehdit unsurdur. Şekil 1'de KAA katmanlarını etkileyen DoS Saldırıları görülmektedir. DoS saldırıları dışında trafik analiz, düğüm kopyalama (node replication), gizliliğin ortadan kaldırılması (attacks against privacy) gibi birçok saldırı türü KAA için önemli tehditlerdendir [4-5].



Şekil 1. KAA katmanlarını etkileyen DoS saldırı türleri

Yukarıda bahsedilen saldırıların birçoğunun vermiş olduğu zararlar veri gizliliği, bütünlüğü ve tazeliliğinin sağlanmasının yanında iletişimin kimlik denetimi ile gerçekleştirilmesi sayesinde en aza indirilebilir. Bu sebeple güvenli iletişimde, düğümlerin bir şifreleme yöntemiyle paketleri şifrelemesi, bütünlüğünü kontrol etmesi ve kimlik denetimini gerçekleştirmesi gerekmektedir. Literatürde sunulan güvenlik çözümlerinden SPIN [8] ve INSENS [9] protokolleri RC5, TinySec güvenlik paketi [10] Skipjack ve 802.15.4 standardı AES şifreleme algoritmalarını kullanmaktadır. Bu çalışmada yeni bir şifreleme algoritması olan SEA'nın algılayıcı düğümleri üzerinde gerçekleştirilmesi üzerinde durulmaktadır. Bu sebeple bir sonraki bölümde SEA algoritması ayrıntılı olarak incelenmektedir.

III. ÖLÇEKLENEBİLİR ŞİFRELEME ALGORİTMASI (SCALABLE ENCRYPTION ALGORITHM, SEA)

SEA, bellek büyüklüğü ve işlem gücü gibi sınırlı kaynaklara sahip gömülü sistemlere yönelik geliştirilmiş, bir şifreleme algoritmasıdır [6-7]. Simetrik blok şifreleme yaklaşımına dayanan SEA'nın tasarım kriterleri küçük bellek alanı, küçük kod büyüklüğü ve sınırlı komut setidir. Bu sebeple sadece, ÖZEL VEYA, bit/kelime rotasyonları, mod 2^b toplama ve s-box gibi bit operasyonlarını kullanır.

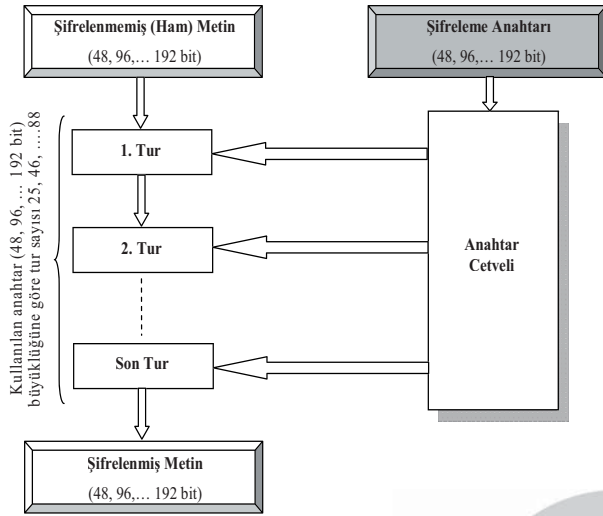
Oldukça esnek bir yapıya sahip olan SEA, $SEA_{n,b}$ şeklinde ifade edilmektedir ve farklı metin, anahtar/kelime uzunlukları üzerinde çalışabilmektedir. Ayrıca, değişken tur sayılarıyla Feistel yapısına dayanan SEA, aşağıdaki parametreler ile tanımlanmaktadır:

- n : ham metin ve anahtar büyüklüğü
- b : kelime büyüklüğü
- $n_b = \frac{n}{2b}$: Feistel dallanması başına kelime sayısı
- n_r : Şifreleme tur sayısı

SEA algoritmasının gerçekleştirilmesinde n ve b parametreleri hedef işlemcinin özelliğine uygun olarak seçilebilir. Ancak anahtar ve ham metin büyüklüğü 48, 96, ..., 192 bit gibi 6'nın katları olması gerekmektedir. Bir diğer önemli nokta ise uygun bir güvenlik düzeyinin sağlanabilmesi için kelime uzunluğunun $b \geq 8$ ve tur sayısının en az

$n_r = \frac{3n}{4} + 2 \cdot (n_b + \lceil b/2 \rceil)$ olması gerekmektedir. Şekil-2'de

SEA algoritmasının yapısı görülmektedir.



Şekil 2. Ölçeklenebilir şifreleme algoritması (SEA)

IV. SEA ALGORİTMASININ GERÇEKLEMESİ

SEA algoritmasının gerçekleştirilmesi, Crossbow firmasının popüler bir ticari ürünü olan MICAz kablosuz algılayıcı düğümleri üzerinde TinyOS [11] işletim sistemi kullanılarak gerçekleştirilmiştir. MICAz, 128 KB kod, 4KB veri hafıza içeren ve 16 MHz hızında çalışan ATMEGA128L mikrodenetleyiciye sahiptir. Kablosuz iletişimi Chipcon CC2420 alıcı/verici tüm devresini kullanarak 250 Kbit/s hızında gerçekleştirebilmektedir.

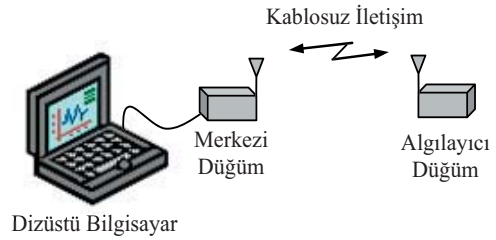
SEA algoritmasının en önemli özelliklerinden biri farklı işlemci büyüklüklerinde ve farklı anahtar/ham metin büyüklüklerinde çalıştırılabilmesidir. Bu çalışmada anahtar /ham metin büyüklüğü 96 bit ve kelime uzunluğu 8 bit olarak seçilmiştir. (SEA_{96,8}).

İlk olarak C dilinde yazmış olduğumuz ve daha sonra nesC diline uyarladığımız SEA algoritmasının gerçekleştirilmesinde ve başarımının ölçülmesinde kullanılan araçlar şunlardır:

- Algılayıcı düğümlerinin TinyOS işletim sistemi üzerinde gerçekleştirilen SEA algoritmasını kullanarak güvenli iletişim gerçekleştirebildiğini analiz etmek için kablosuz algılayıcı ağ düzeneği (Şekil-3).
- SEA algoritmasının algılayıcı düğümlerin belleğinde kapladığı alan, düğümlerin şifreleme/şifre çözme işlemlerinde harcadığı süre ve SEA'nın sağlayabildiği bant genişliği ölçütlerinin elde edilmesi için AVR Studio 4 [13] ve AVR GCC [14] yazılımları kullanılmıştır.

Şekil 3'de SEA algoritmasının gerçekleştirildiği bir dizüstü bilgisayar, bir merkezi düğüm ve bir kablosuz algılayıcı düğümden oluşan KAA deney düzeneği görülmektedir. Algılayıcı düğüm merkezi düğüm ile 200 paket/s hızında şifrelenmiş veri iletişimi gerçekleştirmektedir. Merkezi düğüm ise almış olduğu şifreli veriyi çözerek USB bağlantısı üzerinden

bilgisayara aktarmaktadır. Bilgisayarda merkezi düğümden gelen bilgiyi göstermektedir. Bu düzenek ile düğümlerin SEA algoritmasını kullanarak şifreleme, şifre çözme ve kimlik doğrulama işlemlerini gerçek uygulamalarda başarılı bir şekilde gerçekleştirebildiği kontrol edilmektedir.



Şekil 3. Kablosuz algılayıcı ağ deney düzeneği

V. GERÇEKLEME SONUCU VE DEĞERLENDİRME

Şifreleme algoritmalarının başarımının ölçülmesinde, çalışma zamanı (şifreleme/şifre çözme işlemlerinde harcanan süre), bellek gereksinimi, bant genişliği, güvenlik (kırılma süresinin uzunluğu), esneklik, standartlaştırılabilme, hedeflenen sisteme uygunluk kriterleri göz önüne alınmaktadır [12]. Bu çalışmada SEA şifreleme algoritmasının başarım değerlendirilmesi aşağıdaki kriterlere göre yapılmaktadır.

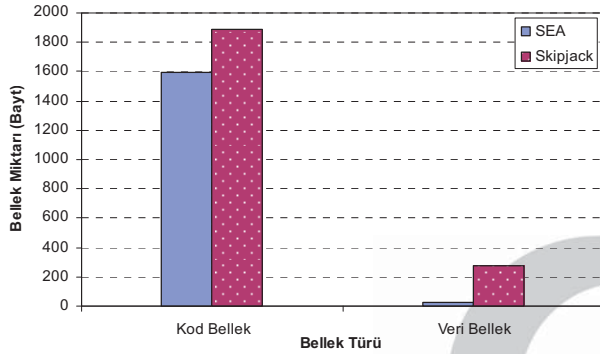
- Bellek gereksinimi,
- Çalışma zamanı ve bant genişliği
- Güvenlik ve esneklik

Şifreleme algoritmalarının hedeflenen cihaz ve ortamlara olan yüksek bağımlılığından dolayı değerlendirilmesi ve birbirleriyle karşılaştırılması oldukça zordur. Buna rağmen fikir vermesi açısından SEA şifreleme algoritması, TinySec güvenlik paketi içerisinde kullanılan Skipjack şifreleme algoritması ile karşılaştırılmaktadır. Her iki algoritmanın C dilinde yazmış olduğumuz versiyonları AVR Studio 4 ve AVR GCC araçları yardımıyla derlenerek benzetilmiş ve ihtiyaç duydukları bellek miktarları, şifreleme/şifre çözme süreleri ve bant genişlikleri elde edilmiştir.

A. Bellek Gereksinimi

Şekil 4'de SEA ve Skipjack algoritmalarının şifreleme ve şifre çözme işlemleri için ihtiyaç duyduğu bellek miktarları

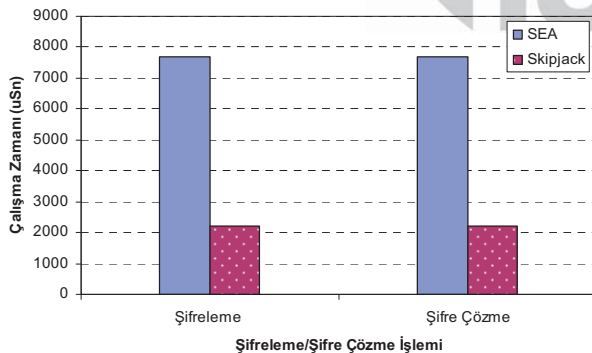
görülmektedir. SEA, kod belleğinde 1598 bayt yer kaplarken veri belleğinde sadece 25 bayt'lık bir alan tutmaktadır. Skipjack algoritması kod bellekte 1884 bayt, veri bellekte ise 274 bayt alan kaplamaktadır. Her iki algoritmanın ihtiyaç duyduğu kod bellek miktarları birbirine yakınken SEA, Skipjack algoritmasına oranla yaklaşık olarak 11 kat daha az veri bellek alanı kullanmaktadır. SEA'nın oldukça düşük veri belleğine ihtiyaç duyması, temelini basit bit operasyonlarına dayanmasından kaynaklanmaktadır.



Şekil 4. SEA ve Skipjack algoritmalarının bellek gereksinimleri

B. Çalışma Zamanı ve Bant genişliği

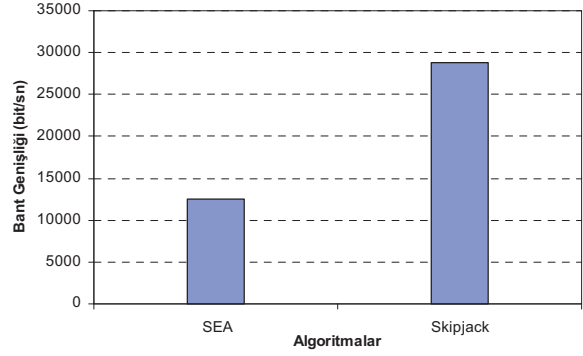
Şekil 5'de SEA ve Skipjack algoritmalarının çalışma zamanları görülmektedir. SEA algoritmasının şifreleme/şifre çözme süresi (7708 μ s), Skipjack algoritmasının şifreleme/şifre çözme süresinden (2220 μ s) yaklaşık olarak 3,5 kat daha fazladır. Bu SEA ve Skipjack şifreleme algoritmalarının kullanmış oldukları anahtar/ham metin büyüklüğü, algoritmalarına ait kural tabloları ve tur sayılarının farklılıklarından kaynaklanmaktadır. Örneğin SEA bu çalışma için 96 bit anahtar ve ham metin kullanırken, Skipjack 80 bit anahtar ve 64 bit ham metin kullanmaktadır. Bir başka fark olarak da SEA'nın bu çalışma için 93 tur Skipjack'ın ise 32 tur ile şifreleme rutinlerini gerçekleştirmesidir.



Şekil 5. SEA ve Skipjack algoritmalarının şifreleme/şifre çözme işlemleri için harcadıkları zaman

Şekil 6'da SEA ve Skipjack algoritmalarının sağlayabildikleri bant genişlikleri görülmektedir. Her iki algoritma şifreleme ve şifre çözme işlemlerinde aynı bant

genişliklerini sağlamaktadır. Şekilden görüldüğü gibi SEA algoritması, Skipjack algoritmasından yaklaşık 2,3 kat daha az bant genişliği sağlamaktadır (SEA: 12454 bit/s, Skipjack:28828 bit/s).



Şekil 6. SEA ve Skipjack algoritmalarının kullandıkları bant genişlikleri (şifreleme ve şifre çözme işlemleri için aynı bant genişliğini kullanmaktadır)

C. Güvenlik ve Esneklik

Skipjack, çalışma zamanı ve bant genişliği açısından SEA'ya oranla daha verimli olmasına rağmen sağlayabildiği güvenlik seviyesi açısından daha gerilerdedir. Skipjack algoritmasının 31 turlu indirgenmiş versiyonu ve 32 turlu tam versiyonlarının kırılabilceği literatürde gösterilmektedir [15,16]. Bunun yanında SEA algoritması için herhangi bir kriptanaliz çalışması henüz bulunmamaktadır. Ayrıca SEA'nın parametreye bağlı olarak yapılandırılabilmesi istenilen güvenlik seviyesinin ayarlanabilmesine imkân tanımaktadır.

VI. SONUÇ

Bu çalışmada MICAz düğümlerden oluşan temel bir kablosuz algılayıcı ağ üzerinde SEA şifreleme algoritması kullanarak güvenli iletişim gerçekleştirilmiş ve SEA şifreleme algoritmasının KAA'lar için uygunluğu bellek kullanımı, çalışma zamanı, bant genişliği, güvenlik ve esneklik kriterleri açısından değerlendirilmiştir. SEA'nın başarımının kıyaslanmasında KAA uygulamalarında popüler olarak tercih edilen Skipjack algoritması kullanılmıştır. Her iki algoritmanın başarım değerlendirilmesi aynı koşullarda gerçekleştirilmiştir.

DeneySEL sonuçlar incelendiğinde SEA algoritmasının Skipjack algoritmasından daha az bellek gereksinimine ihtiyaç duyduğu görülmektedir. Ancak SEA'nın şifreleme ve şifre çözme süresi Skipjack algoritmasına oranla daha fazla ve sağlayabildiği bant genişliği daha düşüktür. Bunun temel sebebi SEA'nın daha fazla tur ile şifreleme işlemlerini gerçekleştirmesidir. Bununla beraber Skipjack'ın kriptanalizinin yapılması ve SEA'ya karşı henüz bir saldırının gerçekleştirilmemesi güvenlik açısından SEA'yı daha avantajlı kılmaktadır. Ayrıca SEA'nın farklı kelime uzunluklarına sahip işlemciler (8 bit, 32 bit vb.) uygun olarak yapılandırılabilmesi, anahtar ve ham metin büyüklüklerinin

değiştirilebilmesi farklı türdeki kablosuz algılayıcı ağ platformlarında kolaylıkla kullanılabilmesini mümkün kılmaktadır.

TEŞEKKÜR

Yazarlar Doç.Dr. İsmail ERTÜRK Bey'e MICAz kablosuz algılayıcı düğümleri sağladığı için teşekkür etmektedirler

KAYNAKLAR

- [1] I. F. Akyildiz , W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless Sensor Networks: Survey", *Computer Networks*, vol. 38, 2002, pp. 393–422.
- [2] A. Perrig, J. Stankovic., D. Wagner, "Security in Wireless Sensor Networks", *Communication of the ACM*, vol. 47, 2004pp. 53–57.
- [3] N. Bandırmalı, C. Bayılmış, I. Ertürk, "Kablosuz Algılayıcı Ağlarda Güvenlik", *Ulusal Teknik Eğitim, Mühendislik ve Eğitim Bilimleri Genç Araştırmacılar Sempozyumu, UMES'07*, 2007, pp. 37–40.
- [4] M. Çakıroğlu, A.T. Özcerit, "Denial of Service Attack Resistant MAC Protocol Design for Wireless Sensor Networks", *J. Fac. Eng. Arch. Gazi Univ.*, vol. 22, no 4, 2007, pp. 697-707.
- [5] M. Çakıroğlu, A.T. Özcerit, Ö. Çetin, H. Ekiz., "MAC Layer DoS Attacks in Wireless Sensor Networks: A Survey", *Proc. of the ICWN'06*, 2006.
- [6] F. -X. Standaert, G. Piret, N. Gershenfeld, J.-J. Quisquater., "SEA: A Scalable Encryption Algorithm for Small Embedded Applications", *CARDIS 2006, Lecture Notes in Computer Science*, vol. 3928, April 2006, pp. 222-236.
- [7] F. Macé, F.-X. Standaert, J.-J. Quisquater, "FPGA Implementation(s) of a Scalable Encryption Algorithm", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 16, no.2, Nov. 2007, pp. 212 – 216.
- [8] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. Culler, "SPINS:Security Protocols for Sensor Networks", *Wireless Networks*, vol. 8, 2002, 521-534.
- [9] J. Deng, R. Han, S. Mishra, "INSENS: Intrusion-tolerant routing in wireless Sensor NetworkS". *Technical Report CU CS-939-02, Department of Computer Science, University of Colorado*, November 2002.
- [10] C. Karlof, N. Sastry and D. Wagner , "TinySec: Link Layer Security for Tiny Devices" , [Online], Available: www.cs.berkeley.edu/~nks/tinysec/
- [11] TinyOS Kullanımı [Online] http://docs.tinyos.net/index.php/Using_TinyOS
- [12] M. Tektaş, F. Baba, E.M. Çalışkan, "Şifreleme Algoritmalarının Sınıflandırılması ve Bir Kredi Kartı Uygulaması", *Third International Advanced Technologies Symposium*, Ankara, 2003.
- [13] Atmel Corporation. Avr studio 4.12, build 498. Available from: http://www.atmel.com/dyn/products/tools_card.asp?tool_id=2725.
- [14] AVR-GCC, Ücretsiz AVR C ve Assembler Derleyicisi, <http://gcc.gnu.org/>
- [15] E. Biham, A. Biryukov, A. Shamir, "Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials", *Proc. of Eurocrypt' 99*, 1999, pp. 12-23
- [16] R. Chung-Wei Phan, "Cryptanalysis of full Skipjack block cipher", *Electronics Letters*, Vol. 38, No. 2, January 2002.

Encryption with First Order Splines

Alla LEVINA, Yuri DEMJANOVICH

Abstract—The aim of this paper is to construct new cryptography algorithm. Proposed algorithm bases on wavelet decompositions for the spaces of first order splines. The algorithm is simple in practice and analysis; processes of enciphering and deciphering have explicit mathematical structures.

Keywords —First order splines, mesh, formulas of decomposition and reconstruction from wavelet theory.

I. INTRODUCTION

Well-known piecewise linear continuous functions (first order splines) had been used in mathematics since Euler. Spline theory had been developed in the middle of the XXth century. The term *spline* were introduced in mathematics by Isaac Schoenberg (1946). Splines were the tool of theoretical investigations till 1960. Since 1960 splines had become also the tool for computer simulations of different situations in science, engineering and techniques.

Proposed paper discusses an application of splines to construction of cryptography algorithms. Using of splines and their wavelet decompositions lead to rather wide variety of the keys defined by mesh, order of ejection of nodes and number of rounds. The offered algorithms can be also applied to the key transfer. At present research on using wavelet decomposition of splines of second, third and upper order continues, algorithm based on wavelet decomposition of splines of second degree is presented in work [1, 2].

The paper is organized as follows, in section II basic concepts of algorithm are presented, sections III and IV presents processes of enciphering and deciphering, and section V demonstrates the work of the discussed algorithm in the case of the block size equal to 256 bits.

II. BASIC CONCEPTS

Presented algorithm is relative to class of block ciphers, process of enciphering and deciphering consists of K identical rounds.

We discuss mesh X as the ordered set of real numbers x_j , such that $x_j < x_{j+1}$: $X = \{x_j\}_{j \in \mathbb{Z}}$.

Let $K = (X, \gamma, K)$ be a key; here X is a mesh, γ is an order of ejection of nodes from the mesh and K is number of round.

Let us suppose that the mesh is periodic with the period N so $x_j = x_{j+N} \forall j \in \mathbb{Z}$.

The order of nodes that will be removed from the mesh X is $\gamma = \{\gamma_n\}_{n \in [1, \dots, K]}$, where K is the number of round of enciphering; on each round only one node is removed from the mesh and γ_n is the number of casually chosen node x_j .

St. Petersburg State University, Math and Mechanics department, Russia.
Email: alla_levina239@yahoo.com

Let us suppose that a sequence $C = \{c_i\}_{i \in \mathbb{Z}}$, $|c_i| = M$ is a plaintext; here $|c_i|$ —quantity of elements which are ciphered, C is the ordered set.

On each round one node with the number γ_j is taken out from the mesh, where j is number of the round. Process of enciphering based on formulas of decomposition from wavelet theory; as a result we get sequence $\{c_i^{-j}\}_{i \in \mathbb{Z}}$, and after K rounds we obtain the ciphertext. On deciphering the plaintext restores with the help of formulas of reconstruction from wavelet theory.

III. PROCESS OF ENCIPHERING

Let us describe in more details process of enciphering. In the process of encryption K rounds are made. On first round we get plaintext $\{c_i\}_{i=0, \dots, M}$, and also we know key K .

For the convenience of record of formulas we shall consider nonnegative integers i, j .

The first round:

- 1) Let eject node x_{γ_1} from primary mesh X .
- 2) Received mesh defines as X^{-1} , its nodes will be equal:

$$x_j^{-1} = x_j \quad \text{if } j < \gamma_1 \quad (1)$$

$$x_j^{-1} = x_{j+1} \quad \text{if } j > \gamma_1 \Rightarrow \quad (2)$$

$X^{-1} = \{x_j^{-1}\}$. The node x_{γ_1} will be defined as ξ .

- 3) Let us write down and count formulas of decomposition for splines of first degree:

$$c_i^{-1} = c_i \quad \text{if } 0 \leq i < \gamma_1 \quad (3)$$

$$c_i^{-1} = c_{i+1} \quad \text{if } \gamma_1 \leq i \leq M-1 \quad (4)$$

$$b^{-1} = c_{\gamma_1} - (x_{\gamma_1+1}^{-1} - x_{\gamma_1}^{-1})(x_{\gamma_1+1}^{-1} - \xi)^{-1}c_{\gamma_1-1} - (x_{\gamma_1}^{-1} - \xi)(x_{\gamma_1+1}^{-1} - \xi)^{-1}c_{\gamma_1+1} \quad (5)$$

- 4) At the end we make a shift of sequence c_i^{-1} as follows:

$$c_0^{-1} \rightarrow c_1^{-1} \rightarrow c_2^{-1} \dots \rightarrow c_{M-1}^{-1} \rightarrow c_0^{-1}$$

Formulas (3)-(6) are written down using the notation of a new mesh X^{-1} . On first round sequences $\{c_i^{-1}\}_{i=0, \dots, M-1}$ and b^{-1} have been got.

All rounds except K -th round go by analogy with the first, we take out from the mesh X^{-i} node x with number γ_i and count formulas of decomposition for splines of the first degree.

K -th round:

- 1) By analogy with previous rounds we have:

$$c_i^{-K} = c_i^{-K+1} \quad \text{if } 0 \leq i < \gamma_K \quad (6)$$

$$c_i^{-K} = c_{i+1}^{-K+1} \quad \text{if } \gamma_K \leq i \leq M-K \quad (7)$$

$$b^{-K} = c_{\gamma_K}^{-K+1} - (x_{\gamma_K+1}^{-K} - x_{\gamma_K}^{-K})(x_{\gamma_K+1}^{-K} - \xi)^{-1} c_{\gamma_K-1}^{-K} - (x_{\gamma_K}^{-K} - \xi)(x_{\gamma_K+1}^{-K} - \xi)^{-1} c_{\gamma_K+1}^{-K} \quad (8)$$

On K -th round shift is not made. Sequence $\{c_i^{-K}\}_{i=0, \dots, M-K}$ and b^{-K} have been received.

As a result after K rounds we have got two sequences

$$\{b^{-n}\}_{n=1,2, \dots, K}, \quad \{c_i^{-K}\}_{i=0,1,2, \dots, M-K}.$$

Sequence $\{c_i^{-K}, b^{-n}\}_{n=1,2, \dots, K; i=0,1,2, \dots, M-K}$ is the ciphertext.

IV. PROCESS OF DECIPHERING

Process of decryption goes by analogy with process of encryption, the same key K and formulas of reconstruction are used.

We know number of rounds K so the sequence $\{c_i^{-K}, b^{-n}\}_{n=1,2, \dots, K; i=0,1,2, \dots, M-K}$ can be divided in two sequences:

$$\{b^{-n}\}_{n=1,2, \dots, K}, \quad \{c_i^{-K}\}_{i=0,1,2, \dots, M-K}.$$

We know the primary mesh X and the order of nodes removal γ so we can receive meshes $X^{-1}, \dots, X^{-K+1}, X^{-K}$, as it has been described in process of enciphering.

On each round we are taking out from the mesh X^{-i+1} only one node x with the number γ_i , where i is the number of round, and we are receiving mesh X^{-i} . For deciphering we need the reverse order, i.e. on first round we need the mesh X^{-K} , on second X^{-K+1} and on K -th X^{-1} .

The first round:

- 1) We take the mesh X^{-K} , $\xi = x_{\gamma_K}^{-K}$
- 2) We write down and count formulas of reconstruction for the splines of first degree:

$$c_i^{-K+1} = c_i^{-K} \quad \text{if } 0 \leq i < \gamma_K \quad (9)$$

$$c_i^{-K+1} = c_{i-1}^{-K} \quad \text{if } \gamma_K + 1 \leq i \leq M - K + 1 \quad (10)$$

$$c_{\gamma_K}^{-K+1} = (x_{\gamma_K+1}^{-K} - x_{\gamma_K}^{-K})(x_{\gamma_K+1}^{-K} - \xi)^{-1} c_{\gamma_K-1}^{-K} + (x_{\gamma_K}^{-K} - \xi)(x_{\gamma_K+1}^{-K} - \xi)^{-1} c_{\gamma_K+1}^{-K} + b^{-K} \quad (11)$$

- 3) We make a shift c_i^{-K+1} as follows:

$$c_0^{-K+1} \leftarrow c_1^{-K+1} \leftarrow c_2^{-K+1} \dots \leftarrow c_{M-K+1}^{-K+1} \leftarrow c_0^{-K+1}$$

We have got the sequence $\{c_i^{-K+1}\}_{i=0, \dots, M-K+1}$.

K -th round:

- 1) We take the mesh X^{-1} , $\xi = x_{\gamma_1}$

2)

$$c_i = c_i^{-1} \quad 0 \leq i < \gamma_1 \quad (12)$$

$$c_i = c_{i-1}^{-1} \quad \gamma_1 + 1 \leq i \leq M \quad (13)$$

$$c_{\gamma_1} = (x_{\gamma_1+1}^{-1} - x_{\gamma_1}^{-1})(x_{\gamma_1+1}^{-1} - \xi)^{-1} c_{\gamma_1-1}^{-1} + (x_{\gamma_1}^{-1} - \xi)(x_{\gamma_1+1}^{-1} - \xi)^{-1} c_{\gamma_1+1}^{-1} + b^{-1} \quad (14)$$

Shift is not made on K -th round.

Thus, after K rounds the initial text $\{c_i\}_{i=0, \dots, M}$ has been restored.

V. DEMONSTRATION OF THE WORK OF ALGORITHM

Presented algorithm is a parametrized algorithm in that it can operate on block sizes of 128, 192, 256 or 512 bits. Now will be presented the work of the algorithm with the block size of 256 bits.

If block size equal to 32 bytes then 30 rounds are specified and we will have 33 nodes in the mesh.

A plaintext is a sequence $\{c_0, c_1, \dots, c_{31}\}$, and key is $K = \{X, \gamma, K\}$, where $K = 30$, $X = \{x_0, x_1, \dots, x_{32}\}$, $\gamma = \{\gamma_n\}_{n=0, \dots, 32}$.

Elements of plaintext held in the matrix C .

Number of columns — N , $N = M/4$, and 4 rows. For block equal 32 bytes C will be 4x8 matrix.

$$C = \begin{pmatrix} c_0 & c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 \\ c_8 & c_9 & c_{10} & c_{11} & c_{12} & c_{13} & c_{14} & c_{15} \\ c_{16} & c_{17} & c_{18} & c_{19} & c_{20} & c_{21} & c_{22} & c_{23} \\ c_{24} & c_{25} & c_{26} & c_{27} & c_{28} & c_{29} & c_{30} & c_{31} \end{pmatrix}.$$

$$\text{Nodes of primary mesh held in matrix } X: X = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \dots \\ x_{32} \end{pmatrix}.$$

$c_0, c_1, \dots, c_{31}, x_0, \dots, x_{32}$ - bytes.

- Process of the encrypting.

Process of encrypting consists of four operation:

- Getting of mesh, which will be using on this round.
- Getting of new elements.
- Shift of the elements.
- Creating of matrix B .

On each round number of elements in matrix C will be decrease on one element, for staying matrix C four-by-eight matrix, we will add 0 on each round, as it will be presented below.

Also on each round we will get element b^{-i} , and we will put it in the matrix B , matrix B is also four-by-eight matrix.

In the beginning

$$B = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Elements $\{b^{-n}\}_{n=1, \dots, K}$ we will put in the matrix B from the position $\{M - K \div N, M - K \bmod N\}$, numeration of rows and columns in B starts from $\{0,0\}$.

On first round we get matrix C , mesh X , and number of node γ_1 .

Process of enciphering on i -th round:

1) We get mesh X^{-i} :

$$X^{-i} = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & 0 & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_0^{-i+1} \\ x_1^{-i+1} \\ \dots \\ x_{\gamma_i}^{-i+1} \\ \dots \\ x_{L-i}^{-i+1} \end{pmatrix} =$$

$$= \begin{pmatrix} x_0^{-i} \\ x_1^{-i} \\ \dots \\ x_{L-i-1}^{-i} \end{pmatrix}.$$

2) We get matrix C^{-i} : $C^{-i} =$

$$= \begin{pmatrix} c_0^{-i+1} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & c_{\gamma_i-1}^{-i+1} & c_{\gamma_i+1}^{-i+1} & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & c_{M-i+1}^{-i+1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

3) Shift of the elements:

$$\begin{pmatrix} c_0^{-i+1} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & c_{\gamma_i-1}^{-i+1} & c_{\gamma_i+1}^{-i+1} & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & c_{M-i+1}^{-i+1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\rightarrow$$

$$\begin{pmatrix} c_{M-i+1}^{-i+1} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & c_{\gamma_i-1}^{-i+1} & c_{\gamma_i+1}^{-i+1} & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & c_0^{-i+1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Let us write matrix C^{-i} in new designations:

$$C^{-i} = \begin{pmatrix} c_0^{-i} & c_1^{-i} & c_2^{-i} & c_3^{-i} & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & c_{M-i}^{-i} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

4) We count and put down in the matrix B element b^{-i} :

$$b^{-i} = \left(1, -\frac{(x_{\gamma_i+1}^{-i} - x_{\gamma_i}^{-i})}{(x_{\gamma_i+1}^{-i} - \xi)}, -\frac{(x_{\gamma_i}^{-i} - \xi)}{(x_{\gamma_i+1}^{-i} - \xi)} \right) \cdot \begin{pmatrix} c_{\gamma_i}^{-i+1} \\ c_{\gamma_i+1}^{-i+1} \\ c_{\gamma_i+1}^{-i+1} \end{pmatrix},$$

$$\xi = x_{\gamma_i}^{-i+1}$$

$$B = \begin{pmatrix} 0 & 0 & b^{-1} & b^{-2} & b^{-3} & \dots & \dots & \dots \\ b^{-7} & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & b^{-i} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

K -th round:

1) We get mesh X^{-K} :

$$X^{-K} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_0^{-K+1} \\ x_1^{-K+1} \\ x_2^{-K+1} \\ x_3^{-K+1} \end{pmatrix} =$$

$$= \begin{pmatrix} x_0^{-K} \\ x_1^{-K} \\ x_2^{-K} \end{pmatrix}.$$

2) We calculate C^{-K} :

$$C^{-K} = \begin{pmatrix} c_0^{-K} & c_2^{-K+1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

In new designations:

$$C^{-K} = \begin{pmatrix} c_0^{-K} & c_1^{-K} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

3) Shift is not made.

4) We calculate and put in the matrix B element b^{-K}

$$b^{-K} = \left(1, -\frac{(x_{\gamma_K+1}^{-K} - x_{\gamma_K}^{-K})}{(x_{\gamma_K+1}^{-K} - \xi)}, -\frac{(x_{\gamma_K}^{-K} - \xi)}{(x_{\gamma_K+1}^{-K} - \xi)} \right) \cdot \begin{pmatrix} c_{\gamma_K}^{-K+1} \\ c_{\gamma_K+1}^{-K+1} \\ c_{\gamma_K+1}^{-K+1} \end{pmatrix}$$

$$\xi = x_{\gamma_K}^{-K+1}$$

$$B = \begin{pmatrix} 0 & 0 & b^{-1} & b^{-2} & b^{-3} & \dots & \dots & \dots \\ b^{-7} & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & b^{-K} \end{pmatrix}.$$

Ciphertext is $C = C^{-K} + B$:

• Process of the decrypting.

We have the matrix C and the key $K \Rightarrow$ so we know the number of rounds $K \Rightarrow$ we know block length $M = K + 2$.

If we know the block length we can get from the matrix C matrix C^{-K} and B :

$$B = \begin{pmatrix} 0 & 0 & b^{-1} & b^{-2} & b^{-3} & b^{-4} & b^{-5} & b^{-6} \\ b^{-7} & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & b^{-K} \end{pmatrix},$$

$$C^{-K} = \begin{pmatrix} c_0^{-K} & c_1^{-K} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

We know the primary mesh X , so we can count $X^{-1}, \dots, X^{-i}, \dots, X^{-K}$, and put it in the matrix X^{all} ,

matrix X^{all} is $L - 1$ -by- K , in this case 32-by-30

$$X^{all} = \begin{pmatrix} x_0^{-1} & \dots & x_0^{-i} & \dots & x_0^{-K} \\ x_1^{-1} & \dots & x_1^{-i} & \dots & x_1^{-K} \\ x_2^{-1} & \dots & x_2^{-i} & \dots & x_2^{-K} \\ \dots & \dots & \dots & x_3^{-i} & 0 \\ \dots & \dots & \dots & \dots & 0 \\ x_{31}^{-1} & \dots & \dots & \dots & 0 \end{pmatrix}.$$

Process of deciphering consists of two operations:

- Counting of elements.
- Shift of the elements.

Process of deciphering on i -th round:

- 1) We take $L-i$ elements of i -th column of the matrix $X^{all} \Rightarrow$

$$X^{-i} = \begin{pmatrix} x_0^{-i} \\ x_1^{-i} \\ x_2^{-i} \\ \dots \\ x_{L-i}^{-i} \end{pmatrix}.$$

Count:

$$c_{\gamma_i}^{-i+1} = \left(\frac{(x_{\gamma_i+1}^{-i} - x_{\gamma_i}^{-i})}{(x_{\gamma_i+1}^{-i} - \xi)}, \frac{(x_{\gamma_i}^{-i} - \xi)}{(x_{\gamma_i+1}^{-i} - \xi)}, b^{-i} \right) \cdot \begin{pmatrix} c_{\gamma_i-1}^{-i} \\ c_{\gamma_i}^{-i} \\ 1 \end{pmatrix}$$

$$\xi = x_{\gamma_i}^{-i+1}$$

Let us write $C^{-i+1} : C^{-i+1} =$

$$\begin{pmatrix} c_0^{-i} & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & c_{\gamma_i-1}^{-i} & c_{\gamma_i}^{-i+1} & c_{\gamma_i}^{-i} & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & c_{M-i}^{-i} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

- 2) Let make a shift of C^{-i+1} :

$$\begin{pmatrix} c_0^{-i} & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & c_{\gamma_i-1}^{-i} & c_{\gamma_i}^{-i+1} & c_{\gamma_i}^{-i} & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & c_{M-i}^{-i} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow$$

$$\begin{pmatrix} c_1^{-i} & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ c_{\gamma_i-1}^{-i} & c_{\gamma_i}^{-i+1} & c_{\gamma_i}^{-i} & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & c_{M-i}^{-i} & c_0^{-i} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Let us write it in new designations:

$$C^{-i+1} = \begin{pmatrix} c_0^{-i+1} & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ c_8^{-i+1} & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & c_{M-i+1}^{-i+1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

k -th round:

- 1) From the matrix X^{all} we are taking 1-th row $\Rightarrow$

$$X^{-1} = \begin{pmatrix} x_0^{-1} \\ x_1^{-1} \\ x_2^{-1} \\ \dots \\ x_{31}^{-1} \end{pmatrix}.$$

Count:

$$c_{\gamma_1} = \left(\frac{(x_{\gamma_1+1}^{-1} - x_{\gamma_1}^{-1})}{(x_{\gamma_1+1}^{-1} - \xi)}, \frac{(x_{\gamma_1}^{-1} - \xi)}{(x_{\gamma_1+1}^{-1} - \xi)}, b^{-1} \right) \cdot \begin{pmatrix} c_{\gamma_1-1}^{-1} \\ c_{\gamma_1}^{-1} \\ 1 \end{pmatrix}$$

where $\xi = x_{\gamma_1}$

Let us write matrix C :

$$C = \begin{pmatrix} c_0^{-1} & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & c_{\gamma_1-1}^{-1} & c_{\gamma_1}^{-1} & c_{\gamma_1}^{-1} & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & c_{30}^{-1} \end{pmatrix},$$

Let us write elements of matrix C in new designations:

$$C = \begin{pmatrix} c_0 & c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 \\ c_8 & c_9 & c_{10} & c_{11} & c_{12} & c_{13} & c_{14} & c_{15} \\ c_{16} & c_{17} & c_{18} & c_{19} & c_{20} & c_{21} & c_{22} & c_{23} \\ c_{24} & c_{25} & c_{26} & c_{27} & c_{28} & c_{29} & c_{30} & c_{31} \end{pmatrix}.$$

- 2) Shift is not made on last round.

The plaintext has been restored.

VI. CONCLUSION

The offered algorithm is well protected against attacks, process of enciphering and deciphering flows quickly. Also one of the advantages of the given algorithm is that it can be used both as block and as a stream algorithm. In the future it is planned to analyze the application of this cryptalgorithm in different areas.

ACKNOWLEDGMENT

This work was supported (partly) with RFFI grants 07-01-00269 and 07-01-00451.

REFERENCES

- [1] Demjanovich Y. K., Levina A. B. *On wavelet decomposition of linear spaces over arbitrary field and some applications* Mathematical modeling 2008 T. 20 (on russian)
- [2] Demjanovich Y. K., Levina A. B. *Wavelet decomposition and decoding* St. Petersburg, Methods of calculations 22. Spb: St. Petersburg University, 2008. p. 56-64 (on russian)
- [3] Demjanovich Y. K., *Minimal splines and splashes* Vestnic of StPetersburg University . Number 1. 2008, 2 p. 8-22 (on russian)
- [4] Demjanovich Y. K., Makarov A. A. *Kalibrovchnye parities for nonpolynomial splines* St.Petersburg, problems of mathematical analyze 34, 2006 p. 29-54 (on russian)
- [5] Demjanovich Y. K., *Splashes and minimal splines* St. Petersburg, 2003. p. 200. (on russian)

Survey on Transformation Based Algorithms in Digital Image Watermarking

Ersin ELBAŞI

Abstract—Digital watermarking has received increasing attention in recent years. Distribution of movies, music, and images is now faster and easier via computer technology, especially on the Internet. Hence, the content owners (e.g., movie studios and recording companies) are concerned about illegal copying of their content. Watermarking is a pattern of bits (logo or noise) inserted into a digital image, video, text or audio which identifies the copyright information [11]. This survey paper defines watermarking technique in digital images and explains main frequency based algorithms.

Keywords—Watermarking, Transformation, DCT, DFT, DWT, Embedding, Detection

I. INTRODUCTION

Watermarking and cryptography are two standard multimedia security methods. However, cryptography is not an effective method because it does not provide permanent protection for the multimedia content after delivery. The contents of the documents are protected from stealing and manipulation during the delivery, but after decryption there is no protection for the documents [11].

The most important properties of a watermarking system are robustness, invisibility, data capacity, and security. An embedded watermark should not introduce a significant degree of distortion in the cover multimedia element. Robustness is the resistance of the watermark against normal A/V processes or intentional attacks. Data capacity refers to the amount of data that can be embedded without affecting perceptual transparency.

The security of a watermark can be defined to be the ability to thwart hostile attacks such as unauthorized removal, unauthorized embedding, and unauthorized detection. There are basically two approaches to embed

a watermark: spatial domain and transform domain (e.g., DCT, DFT, or DWT). In the spatial domain, the watermark is embedded by modifying the pixel values in the original image. Transform domain watermarking is similar to spatial domain watermarking; in this case, the coefficients are modified. Both methods have advantages and disadvantages: One disadvantage of spatial domain watermarking is that the cropping attack might remove the watermark [11].

There are several criteria to classify watermarking techniques. Table 1.1 shows some fundamental categories [2].

Criteria	Types
Based on Type	Image, Video, Audio, Text
Human Perception	Visible, Invisible
Working Domain	Spatial Domain, Frequency Domain
Watermark Type	Pseudo Random Number (PRN) sequence, Visual Watermark
Information Type	Non-Blind, Semi-Blind, Blind

Table 1: Categories of watermarking techniques

Video watermarking is still an open research area because of a number of challenging problems: embedding large amount of data, redundancy between frames, and robustness against temporal attacks (e.g., frame averaging, frame dropping, and frame swapping) [3].

There are several application areas that range from copy protection to broadcast communication [12]. Film and music makers, TV stations, and courts are very much interested in using digital watermarking and cryptography as two complementary technologies. Table 2 shows the main application fields of multimedia watermarking.

Manuscript received October 30, 2008.

Ersin Elbaşı is with The Scientific and Technological Research Council of Turkey, Ankara (corresponding author to provide phone 312 468 5300-1124, e-mail: ersin.elbasi@tubitak.gov.tr)

Applications	Purpose
Copy Control	Prevent unauthorized copying
Broadcast Monitoring	Identify the video item being broadcasting
Fingerprinting	Trace back a malicious user
Authentication	Insure that the original content not changed
Copyright protection	Prove ownership

Table 2: Watermarking Application Areas

II. WATERMARKING METHODS

There are three major watermarking schemes in multimedia. The first is spatial domain watermarking, which basically embeds a visible logo or a PRN sequence directly to selected pixels in the host image. The second is transform domain watermarking such as DCT, DWT or DFT. The third is only for audio or video files, that is compressed domain watermarking. A video watermarking scheme usually should satisfy some requirements such as transparency, robustness, (blind) oblivious detection, free-from deadlock problem, public key detection, and so on. However, all the current watermarking methods only satisfy part of the requirements. For example, some methods are really robust (oblivious) but they are non-oblivious (not robust enough).

Cox et al. [5] proposed secure spread spectrum watermarking algorithm. This algorithm uses the Discrete Cosine Transformation in gray scale image. Proposed algorithm is as follows:

Embedding:

1. Compute the $N \times N$ DCT of an $N \times N$ gray scale cover image I .
2. Embed a sequence of real values $X = \{x_1, x_2, \dots, x_n\}$ according to $N(0,1)$, into the n largest magnitude DCT coefficients, excluding the DC component.
3. $V_i' = V_i(1 + \alpha X_i)$, $i=1, 2, \dots, n$
4. Compute the inverse DCT to obtain the watermarked cover image I' .

Detection:

1. Compute the DCT of the watermarked (and possibly attacked) cover image I^* .
2. Extract the watermark X^* : $X_i^* = (V_i^* - V_i) / \alpha V_i$ $i=1, \dots, n$.
3. Evaluate the similarity of X^* and X using.

$$Sim(X, X^*) = \frac{X \cdot X^*}{(X^* \cdot X^*)^{1/2}}$$

4. If $Sim(X, X^*) > T$, a given threshold, the watermark exist.

Piva et al. [6] presented DCT based watermark recovering without resorting to the uncorrupted original image. This

algorithm provides extra robustness against intentional and distortions. Proposed algorithm is as follows:

Embedding:

1. Compute $N \times N$ DCT of the image I .
2. Reorder the DCT coefficients into zig-zag scan.
3. Generate the vector T by selecting the first $L+M$ coefficients: $T = \{t_1, t_2, \dots, t_L, \dots, t_{L+M}\}$.
4. Skip the lowest L coefficients and embed the watermark $X = \{x_1, x_2, \dots, x_M\}$ in the last M numbers, to obtain $T' = \{t_1, t_2, \dots, t_L, t'_{L+1}, \dots, t'_{L+M}\}$.
5. $t'_{L+i} = t_{L+i} + \alpha_i |t_{L+i}| \cdot X_i$

Detection:

1. Apply the $N \times N$ DCT to the corrupted image I^* .
2. Generate the vector T^* by selecting the coefficients from $(L+1)$ th to the $(L+M)$ th: $T^* = \{t^*_{L+1}, t^*_{L+2}, \dots, t^*_{L+M}\}$
3. Compute the correlation Z between the DCT coefficients marked with a codemark X and a possibly different mark Y :

$$z = \frac{Y \cdot T^*}{M} = \frac{1}{M} \sum_{i=1}^M y_i t^*_{L+i}$$

4. Compose it to the threshold

$$S_z = \frac{\alpha}{3M} \sum_{i=1}^M |t^*_i|$$

Experimental results demonstrated that the watermark algorithm is robust to several signal processing techniques and geometric distortions.

Dugad et al. [7] proposed wavelet based scheme for watermarking images. Algorithms is as follows:

Embedding:

1. Compute the $N \times N$ DWT of an $N \times N$ gray scale image I .
2. Exclude the low pass DWT coefficients.
3. Embed the watermark into the DWT coefficients $> T_1$: $T = \{t_i\}$, $t'_i = t_i + \alpha |t_i| x_i$, where i runs over all DWT coefficients $> T_1$.
4. Replace $T = \{t_i\}$ with $T' = \{t'_i\}$ in the DWT domain.
5. Compute the inverse DWT to obtain the watermarked image I' .

Detection:

1. Compute the DWT of the watermarked and possibly attacked image I^* .
2. Exclude the low pass DWT coefficients.
3. Select all the DWT coefficients higher than T_2 .

$$4. \text{ Compute the sum } z = \frac{1}{M} \sum_{i=1}^M y_i t^*_i, \text{ where } i \text{ runs over all}$$

DWT coefficients $> T_2$, y_i represents either the real watermark or a fake watermark, t^*_i represents the watermarked and possibly attacked DCT coefficients.

$$5. \text{ Choose a predefined threshold } T_z = \frac{\alpha}{2M} \sum_{i=1}^M |t^*_i|.$$

6.If z exceeds T_z , the conclusion is the watermark is present.

Caldelli et al. [13] proposed geometric invariant in DFT frequency domain. Algorithm works as follows:

Embedding:

- 1.Take the luminance layer of an YUV image.
- 2.Compute the Discrete Fourier Transform (DFT).
- 3.Select the magnitudes of some DFT coefficients according to a secret key.
- 4.Modify the magnitudes in such a way to create a local peak.
- 5.Compute the average and the standard deviation over a window centered on the point to be changed.
- 6.The magnitude of the center coefficient will have a value equal to the local average plus n -times ($n = 4,5$) the standard deviation.
- 7.The peaks are arranged in quadruplets, with pixels belonging to the same quadruplet being collinear.
- 8.Moreover these spikes are posed in such a way that quadruplets are concatenated to form a chain.
- 9.Concatenation is achieved by letting the final peak in each quadruplet to be the initial peak of the subsequent quadruplet of the chain.
- 10.The peaks form a constellation that represents the watermark and the template.
- 11.A very general geometric invariant (the *Cross-Ratio of four collinear points-CR*) is adopted to be resistant against complex geometrical attacks.

Detection:

- 1.Take the luminance layer of the watermarked YUV image.
- 2.Compute the Discrete Fourier Transform (DFT).
- 3.Identify all the local maxima through an exhaustive search.
- 4.If the central coefficient, within a window whose size is equal or smaller than that adopted in the embedding step, is the maximum in the window, this is assumed to be a peak.
- 5.The spikes located in very low and in very high frequencies are not considered.
- 6.The watermark is embedded in middle frequency range.
- 7.For an image of size 256x256 about 400 points are generally recovered.
- 8.This is quite a large number and the watermark is always well-hidden.
- 9.If an attacker wants to destroy the watermark, he should modify or delete all these coefficients, resulting in a big loss of image quality.
- 10.The next step is to check all the existing quadruplets of four collinear points, to compute their Cross Ratios and compare them with those characterizing the watermark.
- 11.If the secret key is known, it is possible to determine which are the correct values of Cross Ratios and which is the exact concatenation order among those selected.

Kusyk et al. [9] proposed a semi-blind logo watermarking for color images in the DFT domain. The proposed algorithm is as follows:

Embedding:

- 1.Compute the DFT of the $N \times N$ cover image.
- 2.Move the origin to the center.
- 3.Obtain the magnitudes of DFT coefficients.
- 4.Divide the $N \times N$ matrix of magnitudes into four $(N/2) \times (N/2)$ matrices M_{ul} , M_{ur} , M_{ll} , M_{lr} . ul : upper left, ur : upper right, ll : lower left, lr : lower right.
- 5.Define three frequency bands: low, middle, and high.
- 6.Embed a visual binary watermark in these three bands by determining the embedding locations.
- 7.In each band:
 - a.Choose a magnitude a in matrix M_{ul} , and the corresponding magnitude b in matrix M_{ur} .
 - b.Compute the mean $m = (a+b)/2$, and choose the value of the parameter p .
 - c.Embedding bit 1: If $a < m - (p/2 * m)$ then do not modify a and b else $a = m - (p/2 * m)$ and $b = m + (p/2 * m)$
 - d.Embedding bit 0: If $a > m + (p/2 * m)$ then do not modify a and b else $a = m + (p/2 * m)$ and $b = m - (p/2 * m)$
- 8.Copy the modified magnitudes in matrix M_{ul} to matrix M_{lr} .
- 9.Copy the modified magnitudes in matrix M_{ur} to matrix M_{ll} .
- 10.Obtain the DFT coefficients of the entire image using the modified magnitudes.
- 11.Compute the inverse DFT.

Detection:

- 1.Compute the DFT of the $N \times N$ watermarked (and possibly attacked) image.
- 2.Move the origin to the center.
- 3.Obtain the magnitudes of DFT coefficients.
- 4.Divide the $N \times N$ matrix of magnitudes into four $(N/2) \times (N/2)$ matrices M_{ul} , M_{ur} , M_{ll} , M_{lr} .
- 5.Use the three frequency bands and the embedding locations defined in the embedding process: low, middle, and high.
- 6.In each band, if $a > b$ then bit = 0 else bit = 1.

Ganic et al. [10] proposed DWT-SVD based watermarking algorithm. Embedding and extraction algorithms are as follows:

Embedding:

- 1.Using DWT, decompose the cover image into four subbands: LL, LH, HL, and HH.
- 2.Apply SVD to each subband image: $A^k = U_a^k \Sigma_a^k V_a^{kT}$
- 3.Apply SVD to the visual watermark: $W = U_w \Sigma_w V_w^T$
- 4.Modify the singular values in each subband: $\lambda_i^{*k} = \lambda_i^k + \alpha_k \lambda_{wi}$, $i=1, \dots, n$

5. Construct the watermarked image: $A^{*k} = U_a^k \sum_a^{*k} V_a^{kT}$

Extraction:

1. Decompose the watermarked cover image into four subbands: LL, HL, LH, and HH.

2. Apply SVD to each subband image:

$$A^{*k} = U_a^k \sum_a^{*k} V_a^{kT}$$

3. Extract the singular values from each subband:

$$\lambda_{wi}^k = (\lambda_i^{*k} - \lambda_i^k) / \alpha_k, i = 1, \dots, n$$

4. Construct the four visual watermarks using the singular

$$\text{vectors: } W^k = U_w \sum_w^k V_w^{kT}$$

Chae et al. [14] proposed robust embedding in wavelet coefficients. Algorithm is as follows:

1. Decompose by one level the host and signature images using the DHWT. This results in four bands, which are usually referred to as the LL, LH, HL and HH bands.

2. Each signature image coefficient is expanded into 2x2 block as follow:

3. Each coefficient value is linearly scaled to a 24 bit representation.

4. Let A, B, C represent, respectively, the most significant byte, the middle byte, and the least significant byte in a 24 bit representation. Three 24-bit numbers, A', B', C', are generated with their most significant bytes set to A, B and C, respectively, and with their two least significant bytes set to zero.

5. The host image coefficients are also linearly scaled within each band to a 24 bit representation. The minimum and maximum values in each band will be used in the inverse transformation below.

6. The scaled host image coefficients are now added to the expanded signature transform to form a new fused transform. Let $h(m,n)$ be the (m,n) th wavelet coefficient of the host image, and let $s(m,n)$ be the (m,n) th signature coefficient after forming the expanded blocks as described in the above. Note that after expansion each of the bands in the signature wavelet transform is of the same dimension as the host image bands. The fused (m,n) th coefficient is computed as:

$$w(m,n) = \alpha \cdot h(m,n) + s(m,n)$$

7. Where the scale factor determines the relative percentage of the host and signature image components in the new image.

8. The fused transform coefficients in each band are scaled back to the levels of the host image transform coefficients using the minimum and maximum coefficient values in step 3.

9. An inverse transform is now computed to give the watermarked image.

10. In detection following similarity formula used:

$$S = \frac{\sum_{m,n} s^*(m,n) \cdot s(m,n)}{\sum_{m,n} (s^*(m,n))^2}$$

III. ATTACKS ON WATERMARKED IMAGE

A watermark should be robust against attacks. We can classify attacks in several ways. Direct or indirect attacks:

1. Direct attacks attempt to remove, obscure, or render the watermarks undetectable in the content.

2. Indirect attacks leave the watermark undamaged, but seek to undermine the validity of the scheme that uses the watermark as its basis.

Another attack classification scheme is based on the attack type: Geometric attacks and statistical attacks:

1. Common signal processing: The watermark should be detected after signal processing attacks such as digital-to-analog, analog-to-digital conversion, resampling, gaussian noise, histogram equalization, etc.

2. Common geometric distortions: Rotation, resizing, cropping and scaling are the most common attacks in this class.

IV. EVALUATION IN WATERMARKING

Measurement of image and video quality is a challenging problem in many applications from lossy compression to printing attacks. The quality measures can be classified into two groups: subjective and objective. There are a number of objective measures. We mention some of these measures [107].

The Mean Square Error (MSE): MSE is an old, proven measure of control and quality the MSE is defined as follows:

$$MSE = \frac{\sum (f(i,j) - F(i,j))^2}{N^2},$$

where $f(i,j)$ is the original image that contains $N \times N$ pixels, and $F(i,j)$ is the watermarked image.

The Peak-signal-to Noise Ratio (PSNR): The PSNR is most commonly used as a measure of quality of reconstruction in image watermarking. It is a ratio between the maximum value of a signal and the magnitude of background noise. It is most easily defined via the mean squared error.

$$PSNR = 20 \times \log_{10} \left(\frac{255}{RMSE} \right),$$

where RMSE is the square root of MSE.

Measure of Singular Value Decomposition (M-SVD): M-SVD is a new measure which expresses the quality of

watermarked images. It is based on the Singular Value Decomposition (SVD). M-SVD is a bivariate measure that computes the distance between the singular values of the original image and watermarked image blocks.

$$D_i = SQRT \left[\sum_{i=1}^n (s_i - s'_i)^2 \right],$$

where s_i are the singular values of the original block, s'_i are the singular values of the distorted block, and n is the block size. If the image size is k , we have $(k/n) \times (k/n)$ blocks.

The numerical measure is derived from the graphical measure. It computes the global error expressed as a single numerical value depending on the distortion type:

$$M - SVD = \frac{\sum_{i=1}^{(k/n) \times (k/n)} (|D_i - D_{mid}|)}{(k/n) \times (k/n)},$$

where D_{mid} represents the mid point of the sorted D_i 's, k is the image size, and n is the block size.

Similarity Ratio (SR): Defined by $SR = S/(S+D)$, where S denotes the number of matching pixel values in compared images, and D denotes the number of different pixel values in compared images. The Similarity Ratio is used in evaluation of non-blind watermark extraction.

V. CONCLUSION

Digital watermarking has received increasing attention in recent years. Distribution of movies, music, and images is now faster and easier via computer technology, especially on the Internet. Hence, the content owners (e.g., movie studios and recording companies) are concerned about illegal copying of their content. Watermarking and cryptography are two standard multimedia security methods. However, cryptography is not an effective method because it does not provide permanent protection for the multimedia content after delivery to consumers. The most important properties of a watermarking system:

- Robustness
- Invisibility
- Data capacity
- Security

There are several issues in video watermarking that makes processing difficult. Such as:

- Large amount of frames
- Similarity between frames
- Temporal attacks (frame dropping, frame averaging, frame swapping etc.)

REFERENCES

- [1] E. Elbasi, A. M. Eskicioglu, "A DWT-Based Robust Semi-Blind Image Watermarking Algorithm Using Two Bands", IS&T/SPIE's 18th Annual Symposium on Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII Conference, San Jose, CA, January 15-19, 2006.
- [2] P. Tao and A. M. Eskicioglu, "A Robust Multiple Watermarking Scheme in the DWT Domain," Optics East 2004 Symposium, Internet Multimedia Management Systems V Conference, Philadelphia, PA, October 25-28, 2004, pp. 133-144.
- [3] P. Chan, M. R. Lyu and R. T. Chin, "Copyright Protection on the Web: A Hybrid Digital Video Watermarking Scheme," Proceedings 13th International World Wide Web Conference, New York, May 17-22, 2004, pp.354-355.
- [4] C. Hsu, J. Wu, "DCT-Based Watermarking for Video", IEEE Transaction on Consumer Electronics, Vol. 44, No. 1, February 1998, pp. 206-216
- [5] I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, 6(12), December 1997, pp.1673-1687.
- [6] A. Piva, M. Barni, F. Bartolini, V. Cappellini, "DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image," Proceedings of International Conference on Image Processing, Washington, DC, October 26 - 29, 1997, pp. 26-29.
- [7] R. Dugad, K. Ratakonda and N. Ahuja, "A New Wavelet-Based Scheme for Watermarking Images," Proceedings of 1998 International Conference on Image Processing (ICIP 1998), Vol. 2, Chicago, IL, October 4-7, 1998, pp. 419-423.
- [8] W. Zhu, Z. Xiong and Y.-Q. Zhang, "Multiresolution Watermarking for Images and Video," IEEE Transactions on Circuits and Systems for Video Technology, 9(4), June 1999, pp. 545-550.
- [9] J. Kusyk and A. M. Eskicioglu, "A Semi-blind Logo Watermarking Scheme for Color Images by Comparison and Modification by Comparison and Modification of DFT Coefficients Optics East 2005, Multimedia Systems and Applications VIII Conference, Boston, MA, October 23-26, 2005.
- [10] E. Ganic, A.M. Eskicioglu, "Robust DWT-SVD domain image watermarking: embedding data in all frequencies", International Multimedia Conference, Proceedings of the 2004 workshop on Multimedia and security table of contents, Magdeburg, Germany.
- [11] Ersin Elbasi, "Multimedia Security: Digital Image and Video Watermarking", Doctorate Thesis, 2007, The City University of New York.
- [12] G. Doerr, J. Dugelay, "A Guide Tour of Video Watermarking", Signal Processing: Image Communication 18 (2003), pp. 263-282.
- [13] R. Caldelli, M. Barni, F. Bartolini, A. Piva: Geometric-Invariant Robust Watermarking through Constellation Matching in the Frequency Domain. ICIP 2000.
- [14] J. J. Chae, B. S. Manjunath, "A Robust Embedded Data from Wavelet Coefficients", SPIE International Conference on Storage and Retrieval for Image and Video Databases VI, 1998.

Secure Homogeneous Matrix Algebra via Oblivious Polynomial Evaluation

Mert ÖZARAR, Atilla ÖZGİT

Abstract—With the increasing demand to the Internet technologies, the number of opportunities for cooperative computation gets larger, where the answer depends on the private inputs of separate entities. The communicating parties often may not want to disclose their secret data to the other principal while taking the advantage of collaboration, hence concentrating on the results rather than private and perhaps useless data values. Developing algorithms to conduct such computations while preserving the privacy of the inputs for a target case is referred to as Secure Multi-party Computation. In this work, secure multi-party dot product algorithm is designed to be used as a building block for matrix algebraic problems like calculating determinants, traces and eigenvalues on a shared matrix. The cooperation of principals is in homogeneous manner and the cryptographic tool to perform such a computation is oblivious polynomial evaluation. Under given security assumptions like passive adversaries, the privacy validities of the algorithms are justified using polynomial time reduction and statistical indistinguishability.

Keywords —Privacy Preservation, Secure Multi-party Computation, Matrix Algebra, Oblivious Polynomial Evaluation

I. INTRODUCTION

WITH the increasing demand to the Internet technologies, the number of tremendous opportunities for cooperative computation gets larger, where the answer depends on the private inputs of separate entities. These computations could occur between trusted partners, between partially trusted partners, or even between competitors. The problem is trivial if the context allows the conduct of these computations by a trusted entity that would know the inputs from all the participants; however if the context disallows this then the techniques of secure multi-party computation (SMC) become very relevant and can provide useful solutions.

Multi-party computation (MPC) is an extremely general subject, and a protocol enabling general secure multi-party computation is a very strong tool that can theoretically solve almost any cryptographic protocol problem. In MPC, one considers a number of parties $P_1, \dots, P_n$ who initially each possess some inputs $x_1, \dots, x_n$ and we then want to securely

compute some function f on these inputs where $f(x_1, \dots, x_n) = (y_1, \dots, y_n)$ such that P_i learns y_i but no other information. This should hold, even if players exhibit some amount of adversarial behavior [13,14].

For example, two or more competing large financial firms might jointly invest in a project that must satisfy all organizations' goals while preserving their private and valuable financial data. For performing such computations, if none of the parties can be trusted enough to know all the inputs, privacy will become a primary concern. Hence the techniques for secure multi-party computation are quite relevant and practical to overcome the privacy gaps.

In this paper, we investigate how various matrix algebra problems could be solved in a cooperative environment, where parties need to solve a computational problem based on their joint data, but neither wants to disclose its private data to the other party. Some of the target problems in this framework are as follows:

Problem I (Dot Product): Alice has a vector $(x_1, \dots, x_n)$, and Bob has also another vector $(y_1, \dots, y_n)$. They want to determine the dot product $z = x_1 \cdot y_1 + \dots + x_n \cdot y_n$, without revealing each others vector.

For the remaining problems, we have the following assumption:

Assumption 1 (N-Party Homogenous Cooperation): There exist N parties each having a matrix M_i . The size of M_i is $m_i \times k$ and the total sum of m_i 's is equal to k . Let K be a square matrix with dimension $k \times k$. Construct K as the horizontal concatenation of M_i 's as follows:

$$K_{k \times k} = \begin{pmatrix} [M_1] \\ [0] \end{pmatrix} + \dots + \begin{pmatrix} [0] \\ [M_i] \end{pmatrix} + \dots + \begin{pmatrix} [0] \\ [M_N] \end{pmatrix}$$

Problem II (Determinant): All joint parties want to compute the determinant of the common matrix K . Notice that K is square and the determinant is well-defined.

Problem III (Trace): All joint parties want to compute the trace of the common matrix K to the corresponding diagonal elements found in the previous problem.

Problem IV (Eigenvalue): All joint parties want to compute the eigenvalue of the common matrix K without disclosing their private inputs to the other party. Since characteristic polynomial for calculating the eigenvalues is a special kind of determinant computation, the algorithm for problem II can be suitably applicable. In section 4, the corresponding algorithms

Manuscript received October 7, 2008.

M. Ö. is with the Department of Computer Engineering, METU, Ankara, 06531 TURKEY (e-mail: ozarar@ceng.metu.edu.tr).

A. Ö. is also with the Department of Computer Engineering, METU, Ankara, 06531 TURKEY (e-mail: ozgit@ceng.metu.edu.tr).

are presented using oblivious polynomial evaluation (OPE) as the cryptographic mechanism.

In general, the semi-honest model seems to be the right fit for our setting, where there is no realistic way to verify that the parties are submitting their true graphs as private inputs. It is proven that our constructions are secure in the *semi-honest* model. Assuming that a party correctly follows the protocol, there is no efficient adversary that can extract more information from the transcript of the protocol execution than is revealed by that party's private input and the result of the OPE algorithm. We will compose our protocols in a modular manner and will argue about their privacy using well-known sequential composition theorems in the semi-honest adversary model [2]. Designing communication and round efficient secure protocols for linear algebraic problems in the malicious model still remains an open problem.

The organization of the paper is as follows: Section 2 discusses the related work on SMC. The privacy definitions and formulation, different models of cooperative computation, cryptographic tools and what kinds of assumptions are used for algorithm design are briefly explained. Section 4 gives the OPE technique together with multi-party dot product protocol. Then in section 5 which is the heart of the paper gives the solution to privacy preserving homomorphic matrix algebraic problems like determinant, trace and eigenvalue for multi-party case. Finally section 6 concludes this paper and proposes several future research directions.

II. RELATED WORK

The secure multi-party computation problem starts with the work of [18] and [19], then extended by [9] and by many others. The first representations are through a combinatorial circuit, and then the parties run a short protocol for every gate in the circuit. While this approach is appealing in its generality and simplicity, the generated protocols depend on the size of the circuit. This size depends on the size of the input domain, and on the complexity of expressing such a computation. Moreover, it involves large constant factors in their complexity. Therefore, as Goldreich points out in [10], using the solution derived by these general results for special cases of multi-party computation can be impractical; special solutions should be developed for special cases for efficiency reasons. This is our motivation of seeking special solutions to matrix algebra problems, solutions that are more efficient than the general theoretical solutions.

There are two actors in oblivious transfer protocol namely, the sender and the receiver. The sender's input is a pair (x_0, x_1) and the receiver's input is a bit $\sigma \in \{0, 1\}$. At the end of the protocol the receiver learns x_σ (and nothing else) and the sender learns nothing. Oblivious transfer is often the most computationally intensive operation of secure protocols, and is repeated many times. Each invocation of oblivious transfer typically requires a constant number of invocations of trapdoor permutations (i.e. public-key operations, or exponentiations). It is possible to reduce the amortized overhead of oblivious

transfer to one exponentiations per a logarithmic number of oblivious transfers, even for the case of malicious adversaries [17]. Oblivious polynomial evaluation is a technique based on oblivious transfer and explained in the next section.

The SMC applications distributed in broad range areas can be enumerated as follows: Atallah et. al. [1] proposes preliminary work for solving computational geometry problems including scalar product, permutation, vector dominance, equality testing, point inclusion and intersection. In the consecutive papers of Du et. al. [4,5,6], the authors define a set of new privacy preserving cooperative scientific computation problems: privacy preserving cooperative linear system of equations problem and privacy preserving cooperative linear least-square problem. They have developed protocols to solve these problems. Du et. al. [3] also studies the problem of how to conduct the statistical analysis in a compact environment where neither of parties wants to disclose their private data. The secure two-party statistical analysis problem could be solvable in a way more efficient than the general circuit evaluation approach.

OPE is applied to SMC problems especially under privacy preserving data mining concept which is introduced in the work of Pinkas et. al. [12]. A privacy preserving ID3 decision tree algorithm is explained intensively. In another previous work [15], secure multi-party overall mean problem is analyzed and solved by OPE, as well. Jha et. al. [11] also primarily gets concentrated on weighted average problem for the applications on clustering using OPE. Neural network applications are studied using OPE methods as well like Yan-Cheng et. al. [20]. Within the context of privacy-preserving data mining, Goethals et. al. [8] presents a private scalar product protocol based on standard cryptographic techniques and proved that it is secure.

III. PRIVACY FORMULATION, MODELS OF COOPERATION, CRYPTOGRAPHIC TOOLS

In this section, the privacy formulation for the given problems is defined. The models for sharing a common matrix are illustrated. Moreover, the oblivious polynomial evaluation which is used as a cryptographic tool to construct the privacy requirements is briefly explained together with the remarks on assumptions for the kind of adversaries.

A. Privacy Formulation

In this subsection, we provide a formulation of privacy for the desired protocols. The formulation uses a semi-honest adversary model. Remark that in the matrix algebraic privacy problems, both parties only know their input and output. Definition of privacy is based on the intuition that parties should learn nothing more from the messages used in privacy-preserving protocol, i.e., the messages received by a party during an execution of a privacy-preserving protocol can be "effectively computed" by only knowing its input and output. This idea is formalized below:

Definition 1: Let x and y be inputs of the two parties and $\langle f_1(x, y), f_2(x, y) \rangle$ be the desired functionalities, i.e., the first party wants to compute $f_1(x, y)$, and the second wants to compute $f_2(x, y)$. Let P be a two-party protocol to compute f . The view of the first party after having participated in protocol P (denoted by $VIEW_1(x, y)$) is $(x, r, m_1, \dots, m_t)$, where r are the random bits generated by party 1 and $m_1, \dots, m_t$ is the sequence of messages received by party 1, while participating in protocol P . $VIEW_2(x, y)$, for the second party can be defined in a similar manner.

We say that P privately computes f if there are probabilistic polynomial-time algorithms (PPTA), denoted by S_1 and S_2 such that

$$\{S_1(x, f_1(x, y))\}_{x,y} \equiv_s \{VIEW_1(x, y)\}_{x,y}$$

$$\{S_2(x, f_2(x, y))\}_{x,y} \equiv_s \{VIEW_2(x, y)\}_{x,y}$$

In the equation given above, $\equiv_s$ denotes statistically indistinguishable. Two probability ensembles $X = \{X_w\}_{w \in S}$ and $Y = \{Y_w\}_{w \in S}$ indexed by S are statistically indistinguishable if for some negligible function $\mu: \mathbb{N} \rightarrow [0, 1]$ and all $w \in S$,

$$\sum_{\alpha} |Prob(X_w = \alpha) - Prob(Y_w = \alpha)| < \mu(|w|)$$

A function $\mu: \mathbb{N} \rightarrow [0, 1]$ is called negligible if for every positive polynomial q , and all sufficiently large n 's, $\mu(n) < q(n)^{-1}$. There is a weaker notion of indistinguishability called computationally indistinguishable. We will use statistical indistinguishability throughout the paper especially in subsection 4.1, but all the results hold even if the weaker notion of indistinguishability is used.

B. Models of Cooperation

A common property of the problems defined is the combining knowledge of a matrix M and of a vector b . As described in Figure 1 three different ways of combining knowledge, with (b) and (c) being the special cases of (d). However, in real life, cases (b) and (c) are more meaningful than (d) because they tend to model the ways of actual cooperation's.

In the matrix algebra problems, M and b usually represent a set of linear constraints. Sometimes the cooperating parties each has its own set of constraints, but sometimes they have to jointly specify each single constraint. Therefore we classify the cooperation to two basic models, the heterogeneous model and the homogeneous model. On the other hand, in this work, we only get concentrated on homogeneous case for the sake of simplicity.

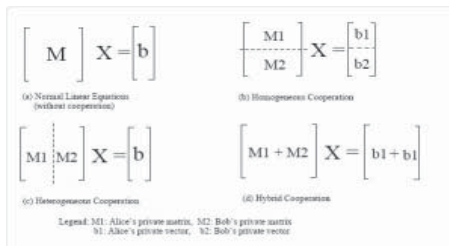


Fig. 1. Different models of cooperative computations

C. Oblivious Polynomial Evaluation

To design a secure protocol for computing a function $f(x, y)$ allows two parties, a receiver who knows x and a sender who knows y , to jointly compute the value of $f(x, y)$ in a privacy preserving way. The fact that for every computable function $f(x, y)$ in polynomial time there exists such a (polynomially-computable) protocol is already achieved in the cryptographic research [13]. In the OPE, the input of the sender is a polynomial P of degree k over some field F . The receiver can get the value $P(x)$ for any element $x \in F$ without learning anything else about the polynomial P and without revealing to the sender any information about x . The input and output for the functionality of OPE as a two party protocol run between a receiver and a sender over a field F as follows:

Input

- Receiver: an input $x \in F$.
- Sender: A polynomial P defined over F .

Output

- Receiver: $P(x)$.
- Sender: nothing.

There are various protocols to solve the OPE yet the protocol given by Naor and Pinkas [14] is preferred for the target algorithms.

IV. DOT PRODUCT PROTOCOL IN THE PRIVACY PRESERVING MANNER

In this section, a protocol for privacy preserving two-party dot product problem (DPP) is designed. A function should be taken as a target to place the terms in the OPE for developing such an algorithm. First we analyze the two-party case then extend it to the multi-party case.

A. Two-Party DPP

Let f be the function for such a computation, its domain set must be n -dimensional vectors for both parties and range set must be a singleton numeric value (dot product). f can be constructed as:

$$f: F^n \times F^n \rightarrow F$$

$$f((x_1, x_2, \dots, x_n), (y_1, y_2, \dots, y_n)) = x_1 \cdot y_1 + x_2 \cdot y_2 + \dots + x_n \cdot y_n$$

The straight forward solution is approximating f by a circuit and using [9] for constructing the protocol for the privacy preserving case. Yet it is well known that the cost for implementing such a circuit is so inefficient that a new solution should be developed for the specific case. We describe the protocol in a top-down fashion.

Steps are as follows:

- i. Define the private bilinear terms summation problem (BTS)
- ii. Produce a protocol for BTS using OPE.
- iii. Find a suitable case for BTS by placing polynomials and field elements for DPP. (Reduction from private-BTS $\rightarrow$ DPP)

BTS: For any finite field F , construct f as

$$f: (F^n[x] \times F) \rightarrow F \times F$$

$$f(P, \alpha) = (P(\alpha), P(\alpha))$$

where $P \in F^n[x]$ (polynomial for party 1) and $\alpha \in F$ (field element of party 2).

Protocol BTS: The construction of BTS via OPE is as follows:

- (1) Party 1 “blinds” the polynomials P by multiplying with a pre-determined field element $\gamma_1 \in F$.
- (2) Party 2 computes $\gamma_1 P(\alpha)$ by OPE.
- (3) Party 2 blinds by multiplying with $\gamma_2 \in F$ and sends the product $\gamma_1 P(\alpha) \gamma_2$ to party 1.
- (4) Party 1 cancels out γ_1 by dividing from the product and sends $\gamma_2 P(\alpha)$ to party 2.
- (5) Party 2 computes $P(\alpha)$, by dividing $(\gamma_2 P(\alpha))/\gamma_2$, and sends it to party 1.

The construction of private-BTS to DPP is stated by placing suitable polynomials and field elements.

Private-BTS to DPP reduction: Recall that party 1 has a vector $(x_1, \dots, x_n)$, and party 2 has $(y_1, \dots, y_n)$. Since the reduction is from BTS, the party 1 needs to construct polynomials and party 2 needs to choose field elements. The polynomials for party 1 are:

$$P(w) = \sum_{i=1}^n R_i(w)$$

$$R_i(w) = wx_i$$

Note that all polynomials are linear and coefficients are known by party 1. P is formed as a summation of sub-polynomials R_i 's for each bilinear terms in it. On the other hand, the field elements for party 2 are:

$$\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$$

$$\alpha_i = y_i$$

After the desired function f is constructed, the lemmas and the theorem in the work of [ours] can be manipulated to prove that reduction can be done in polynomial time and f privately computes the DPP.

Two lemmas are critical for the proof that f computes the overall mean privately. The former belongs to Canetti et. al. [2] and the latter is already given.

Lemma 1 (Composition Theorem for Passive Adversary): If g is privately reducible to f and there exists a protocol for computing f privately then there exists a protocol for computing g privately.

Lemma 2 (Private-BTS): The protocol $P_{\text{BTS}}((R_1, \dots, R_n), (\alpha_1, \dots, \alpha_n))$ is a privacy preserving protocol for private-BTS problem.

Proof: The views of the two parties are

$$\text{VIEW}_1(R_1, \dots, R_n) = (R_1, \dots, R_n, R_1(\alpha_1), \dots, R_n(\alpha_n))$$

$$\text{VIEW}_2(\alpha_1, \dots, \alpha_n) = (\alpha_1, \dots, \alpha_n, \gamma R_1(\alpha_1), \dots, \gamma R_n(\alpha_n))$$

The view of party 1 consists of its input $(R_1, \dots, R_n)$ and output $(R_1(\alpha_1), \dots, R_n(\alpha_n))$. so there is nothing to prove (see definition 1, we can use S_1 as the identity function). The input and output of party 2 are $(\alpha_1, \dots, \alpha_n)$ and $(\gamma R_1(\alpha_1), \dots, \gamma R_n(\alpha_n))$, respectively. It is time to determine probabilistic polynomial-time algorithm S_2 such that $S_2(\alpha_1, \dots, \alpha_n, \gamma R_1(\alpha_1), \dots, \gamma R_n(\alpha_n))$ and $\text{VIEW}_2(\alpha_1, \dots, \alpha_n)$ are statistically indistinguishable. Let δ be a random element of F and $S_2(\alpha_1, \dots, \alpha_n, \delta R_1(\alpha_1), \dots, \delta R_n(\alpha_n))$ be defined as follows:

$$(\alpha_1, \dots, \alpha_n, \delta R_1(\alpha_1), \dots, \delta R_n(\alpha_n), \delta')$$

It is trivial to see that the following two ensembles are statistically indistinguishable:

$$(\alpha_1, \dots, \alpha_n, \delta R_1(\alpha_1), \dots, \delta R_n(\alpha_n), \delta')$$

$$(\alpha_1, \dots, \alpha_n, \gamma R_1(\alpha_1), \dots, \gamma R_n(\alpha_n))$$

This is because if δ is a random element of F then $\gamma R_i(\alpha_i)$ is a random element of F as well, for $i=1, \dots, n$.

Theorem 1 (Two-party DPP): The protocol formed by f yields a privacy-preserving protocol for two-party DPP.

Proof: It is clear that DPP is privately reducible to BTS by choosing the given numerator and the denominator and there exists a protocol for private-RPE (Lemma 2) then by Lemma 1, given protocol is privately computes two-party DPP.

B. Multi-Party DPP

In the multi-party case, the BTS protocol should be applied $(m-1)$ times if there are m parties are joined in. The following construction summarizes the reduction of multi-party DPP to two-party DPP. The key point about the calculation is all the coefficients of the target polynomial can be gathered from traversing all the parties except the last one. Hence rather than a single blinding factor for the step(2) of BTS protocol, there exist a multiplication of blinding factors, a new one is added at each iteration traversing from one to other.

Multi-party DPP Protocol: The protocol for multi-party DPP can be designed from two-party DPP in the following way:

(1) Parties are ordered from 1 to k in a manner that consecutive parties are involved in two-party DPP computation. This can be done with a common share or coin-tossing into well protocol [9]. Hence the last party can be differed from previous attempts.

(2) Between party i and $i+1$, $0 < i < k$, the two-party DPP protocol works and R_i (polynomial regarding to i^{th} feature of the input vectors) can be iterated as:

$$R_i(w) = \left(\prod_{j=1}^t \alpha_{ji} x_{ji} \right) w \rightarrow R_{i+1}(w) = R_i(w) (\alpha_{(t+1)i} x_{(t+1)i}) w$$

Note that α_{ji} 's are the blinding factors.

(3) Hence for the i^{th} feature of the input vectors, the product is computed by multiplying all i^{th} coefficients except the last:

$$R_i(w) = \left(\prod_{j=1}^{k-1} \alpha_{ji} x_{ji} \right) w$$

(4) Summing up into all dimensions (features);

$$P(w) = \left(\sum_{j=1}^n \left(\prod_{i=1}^{k-1} \alpha_{ji} x_{ji} \right) \right) w$$

(5) The field elements are determined by the last party;

$$\beta = (\beta_1, \beta_2, \dots, \beta_n)$$

$$\beta_i = x_{ki}$$

Total computation is quadratic in size and at the end of the computation; the last party (i.e. party k) gets the **blinded** dot product together with total sample size with remaining parties.

(6) In accordance with step (3) of BTS, the blinded dot product is traversed from all party k to party 2 backwards by dividing with corresponding blinding factor. Thus, the first party gets the dot product and send to other parties.

The unimportant gap of the protocol is the first party is more privileged than others yet this can be overcome by choosing the order in a circular round-robin fashion so the order of consecutive parties are preserved but only the first party changes. The probability to be the first party is $1/k$ which is Pareto-optimal for such a scheme.

V. HOMOGENEOUS MATRIX ALGEBRA PROTOCOLS

In this section, multi-party determinant, trace, eigenvalue problems are discussed, respectively. Multi-party DPP protocol is used with *specific* input vectors in each of them.

A. Multi-Party Determinant Protocol

In this subsection, we show how the determinant of an $n \times n$ matrix can be computed using the permutations of the sequence $\{1 \dots n\}$ by the famous Leibnitz's formula.

Theorem 2 (Determinant of a matrix based on permutations): Let A be an $n \times n$ matrix and V_i be a $1 \times n$ matrix where for all $j \neq i$, $v_{i,j} = 0$ and $v_{i,i} = 1$. Let $S(n)$ be the set of all permutations on the sequence $\{1, \dots, n\}$ with $n!$ elements and $\sigma_1(i), \dots, \sigma_n(i)$ represent each of the possible permutations of the sequence $\{1, \dots, n\}$ so that for all $\sigma(i) \in S(i)$, there exists k such that $\sigma(i) = \sigma_k(i)$.

Then;

$$\det(A) = \sum_{k=1}^n \left\{ \text{sgn}(\sigma_k) [a_{1,\sigma_k(1)}, \dots, a_{n,\sigma_k(n)}] \right\}$$

Suppose that we have a $k \times k$ matrix, A , then an **elementary product** from this matrix will be a product of k entries from A and none of the entries in the product can be from the same row or column. Thus, each permutation corresponds to a signed elementary product. Some remarks have to be done since there is an analogy between dot product and determinant computations. The sign is always positive and total number of n -tuple products is n in dot product, on the contrary in determinant; the sign is alternating with the parity of permutation and $n!$ copies of elementary products are involved

in computation. Yet the multi-party dot protocol can be modified in the following way to handle multi-party determinant computation problem in the light of our first assumption. So there are N parties which form the rectangular $k \times k$ matrix zero-padded matrix.

Multi-party Determinant Protocol: The protocol for multi-party determinant protocol where all that needs to be done is to calculate the product of every possible permutation and then sum them up can be designed from multi-party DPP. We have two define a number of algorithms to get the notion.

```

1 Calculate_Determinant(Input Matrix, Output
  Determinant)
2 {
3   Check for invalid conditions (not square etc)
4   If number of rows = 1 Then return only element
5   Initialize determinant value to zero
6   While not used all permutations
7   {
8     Get next permutation vector
9     Calculate the elementary product of the
      current permutation
10    If the current permutation is even Then
11      Add the product to the determinant
        value
12    Else
13      Subtract the product from
        determinant value
15  }
16 Return determinant value
17 }
```

Algorithm I. Determinant Calculation

The Johnson-Trotter algorithm offers a clever way to directly generate permutations of the required length without computing shorter permutations. The algorithm requires the definition of a directed integer is said to be *mobile* if it is greater than its immediate neighbor in the direction it is looking at.

The Johnson-Trotter algorithm can now be described in five lines:

```

1 Initialize the first permutation with <1 <2 ... <n
2 While there exists a mobile integer
3 {
4   Find the largest mobile integer k
5   Swap k and the adjacent integer it is looking
6   Reverse the direction of all integers larger
   than k
7 }
```

Algorithm II. Johnson-Trotter Algorithm for Permutation Calculation

The Algorithm I should be modified in order to handle multi-party case:

(1) Parties are ordered from 1 to k in a manner that consecutive parties are involved to two-party DPP computation. This can be done with a common share or coin-tossing into well protocol [9]. Hence the last party can be differed from previous attempts.

(2) Lines 2, 3 and 4 are handled by the first party.

(3) The **while** loop should be managed in the coordination of the first party. All the permutations are calculated by the

result of Johnson-Trotter Algorithm for all parties in parallel at line 8.

(4) Calculation of the current permutation should be handled by using multi-party DPP protocol. *For each calculation while the parties are being traversed, each party includes his/her term(s) exist(s) in the formation of permutation for the target elementary product in the direction of the DPP protocol. The vectors given as input to the protocol are partially created and should have all-zero values in all the dimensions except the first one which has the target term.*

(5) Lines 10-13 are handled by the first party and the determinant result stored in the return value is distributed to the parties.

Example I: Let Alice, Bob and Cindy are involved in a determinant computation where Alice and Cindy have single vectors yet Bob has two vectors. Each vector has 4 dimensions suitable with our Assumption 1. There are totally 4! permutations that form the determinant computation. An elementary product corresponding to the permutation $\sigma_{3412}=(A_3B_4B_5C_2)$ is illustrated which is the eleventh element in the Johnson-Trotter order. The vectors from x_1 to x_4 are partially created which are given as input to multi-party DPP protocol. The D matrix is also used in the following examples.

$$D = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ b_5 & b_6 & b_7 & b_8 \\ c_1 & c_2 & c_3 & c_4 \end{pmatrix}$$

$$|D| = \text{sgn}(\sigma_{a_1b_1b_1c_1})a_1b_1b_1c_1 + \dots + \text{sgn}(\sigma_{a_3b_4b_5c_2})a_3b_4b_5c_2 + \dots$$

$$\Rightarrow \{(a_3, 0, 0, 0), (0, b_4, 0, 0), (0, 0, b_5, 0), (0, 0, 0, c_2)\}$$

$$\Rightarrow a_3b_4b_5c_2$$

B. Multi-Party Trace Protocol

In linear algebra, the trace of an n-by-n square matrix A is defined to be the sum of the elements on the main diagonal (the diagonal from the upper left to the lower right) of A, i.e.,

$$\text{tr}(A) = a_{11} + a_{22} + \dots + a_{nn} = \sum_{i=1}^n a_{ii}$$

where a_{ij} represents the entry on the i^{th} row and j^{th} column of A.

Multi-party Trace Protocol: The idea for trace computation is based on selecting the target vectors given as an input to DPP in the form of $(1, 1, \dots, d_{ii}, \dots, 1, 1)$ where d_{ii} is the diagonal element which corresponds to the identity permutation.

```
1 Calculate_Trace(Input Matrix, Output Trace)
2 {
3   Check for invalid conditions (not square etc.)
4   If number of rows = 1 Then return only element
5   Initialize trace value to zero
6   Get identity permutation vector,  $\sigma_{id}$ 
7   Calculate the elementary product of  $\sigma_{id}$  via
```

```
8   Return trace value
9 }
```

Algorithm III. Multi-party Trace Calculation

The algorithm is the reduced version of determinant protocol where parties are traversed just once with the identity permutation. Hence the input vectors are formed of all 1's except the diagonal element.

Example II: Regarding the previous example while taking another permutation into account $\sigma_{1234} = (A_1B_2B_7C_4)$ which yields the trace, x_1 to x_4 are formed and the trace value is computed.

$$\{x_1 = (A_1, 1, 1, 1), x_2 = (1, B_2, 1, 1), x_3 = (1, 1, B_7, 1), x_4 = (1, 1, 1, C_4)\}$$

$$\Rightarrow \text{tr}(D) = A_1 + B_2 + B_7 + C_4$$

C. Multi-Party Eigenvalue Protocol

Consider the square matrix A. It is said that λ is an eigenvalue of A if there exists a non-zero vector x such that $Ax = \lambda x$. In this case, x is called an eigenvector (corresponding to λ), and the pair (λ, x) is called an eigenpair for A. A nontrivial solution of this equation is possible if and only if the coefficient matrix $A - \lambda I$ is singular. Such a condition can be expressed as the vanishing of the determinant

$$|A - \lambda I| = 0$$

When this determinant is expanded, we obtain an algebraic polynomial equation in λ of degree n :

$$P(\lambda) = \lambda^n + \alpha_1\lambda^{n-1} + \dots + \alpha_n = 0$$

This is known as the *characteristic equation* of the matrix A. The algorithm for eigenvalue computation is quite similar to determinant computation yet the terms of elementary products include indeterminate λ values as well. Hence, the first party can compute the characteristic equation of the matrix instead of exact determinant. The eigenvalues can be obtained solving the characteristic equation for λ .

The vectors given as input to the protocol are partially created and should have all-zero values in all the dimensions except the first one which has the target term decremented by indeterminate. The following example summarizes the point.

Example III: For the matrix D, in example I, the partially created vectors for the permutation $\sigma_{3412}=(A_3B_4B_5C_2)$ to compute eigenvalues are as follows:

$$\{(a_3 - \lambda, 0, 0, 0), (0, b_4 - \lambda, 0, 0), (0, 0, b_5 - \lambda, 0), (0, 0, 0, c_2 - \lambda)\}$$

$$\Rightarrow (a_3 - \lambda)(b_4 - \lambda)(b_5 - \lambda)(c_2 - \lambda)$$

VI. CONCLUSION AND FUTURE WORK

In this paper, the application of the oblivious polynomial evaluation technique to secure multiparty computation problems is shown via presenting privacy preserving algorithm for dot product and matrix algebra problems. To form a basis, the two-party case and generalized multi-party version of

private dot product protocol are also presented to be used as a component of matrix algebraic protocols. Namely, a group of people may form a homogeneous matrix and can compute the determinant, trace and eigenvalues of the matrix without grasping each others input yet just concentrated on the results. The related validity and security proofs are already made out.

Two crucial points should be noted out which can cause a trade-off between computational complexity and security aspects. The former is, unfortunately, the private determinant and private eigenvalue algorithms have complexity $O(n!)$ since there exist a traversal of all possible permutations. On the other hand, trace algorithm is polynomial. It can be overcome by revealing a number of intermediate terms which can cause a number of security gaps or altering the algorithm from all permutations to Gaussian elimination. Even though complexity can be decreased to $O(n^3)$ yet the cooperative computation of course gets enormously larger in such a case. Since the proof of security is quite more important for our goal, $O(n!)$ is quite affordable unless there is a breach in privacy. The latter is, the algorithms are valid if and only if all the parties are at most honest but curious. If one of them may turn out to active adversary then all the algorithms can fail. It is an open problem to find out a solution to matrix algebraic computations in totally dishonest model. There are some empirical related works on the subject but it is too far away from realization.

In our future directions, we have to adapt the private-DPP and private matrix algebraic problems to a specific case, especially in data mining or machine learning. Principal Component Analysis [7] is chosen as a test bed which suits to the problem well since the mean, the determinant and eigenvalue computations are done before forming the covariance matrix. The controlled experiments can guide us to justify that the protocol works without trouble.

Besides, as an alternative approach, the homomorphic encryption schemes (HES) can be designed to solve the given problems. The scheme developed by Paillier [16] can be considered to be the alternatives for such a mechanism. A testing environment for the comparison of the performance analysis between OPE and HES determines the efficient algorithm under given security assumptions

ACKNOWLEDGMENT

Our thanks to all cryptography group members of Institute of Applied Mathematics, Middle East Technical University who encourage us to work on a heavily cryptographic subject.

REFERENCES

- [1] Atallah M. J. and Du W.. Secure Multi-Party Computational Geometry. In Proceedings of 7th International Workshop on Algorithms and Data Structures (WADS 2001), 165-179.
- [2] Canetti. R.. Security and Composition of Multi-party Cryptographic Protocols. Journal of Cryptology, (2000) 13(1):143-202.
- [3] Du W. and Atallah M. J.. Privacy-Preserving Cooperative Statistical Analysis. In Annual Computer Security Applications Conference (ACSAC) (2001) 102-110.
- [4] Du W. and Atallah M. J.. Privacy-Preserving Cooperative Scientific Computations. In 14th IEEE Computer Security Foundations Workshop, (2001), 273-282.
- [5] Du W. and Atallah M. J.. Secure Multi-Party Computation Problems and their Applications: Review and Open Problems. In New Security Paradigms Workshop (2001), 11-20.
- [6] Du W. and Atallah M. J.. A Practical Approach to Solve Secure Multi-party Computation Problems. In New Security Paradigms Workshop (2002), 127-135.
- [7] Duda R.O., Hart P.E. and Stork D.G.. Pattern Classification. John Wiley & Sons, (2001).
- [8] Goethals B., Laur S., Lipmaa H. and Mielikäinen T. On Private Scalar Product Computation for Privacy-Preserving Data Mining. The 7th Annual International Conference in Information Security and Cryptology (ICISC 2004), volume 3506 of Lecture Notes in Computer Science, 104-120.
- [9] Goldreich O., Micali S. and Wigderson A.. How to play any mental game - a completeness theorem for protocols with honest majority. In 19th Symposium on Theory of Computer Science, (1987), 218-229.
- [10] Goldreich O.. Foundations of Cryptography: Volume 2, Basic Applications. Cambridge University Press, (2004).
- [11] Jha S., Kruger L. and McDaniel P.. Privacy Preserving Clustering. 10th European Symposium on Research in Computer Security (ESORICS), Milan, (2005).
- [12] Lindell Y. and Pinkas B.. Privacy preserving data mining. In Advances in Cryptology (Crypto 2000), 36-54.
- [13] Naor M. and Pinkas B.. Oblivious transfer and polynomial evaluation. In 31st Symposium on Theory of Computer Science, (1999) 245-254
- [14] Naor M. and Pinkas B.. Computationally Secure Oblivious Transfer. Journal of Cryptology, Vol. 18, No. 1, 2005
- [15] Özarar M. and Özgüt A.. Secure Multiparty Overall Mean Computation via Oblivious Polynomial Evaluation, Security of Information and Networks, Proc. First International Conference on Security of Information and Networks (SIN 2007), Gazimagusa, TRNC, May 2007, 84-95.
- [16] Paillier P.. Public-key cryptosystems based on composite degree residuosity classes. In Proceedings of Advances in Cryptology (EUROCRYPT'99).
- [17] Pinkas B.. Cryptographic Techniques for Privacy-Preserving Data Mining SIGKDD Explorations, the newsletter of the ACM Special Interest Group on Knowledge Discovery and Data Mining, (2003).
- [18] Rabin M.. How to exchange secrets by oblivious transfer. Technical Report Tech. Memo TR-81, Aiken Computation Laboratory, 1981.
- [19] Yao A.C.. How to generate and exchange secrets. In 27th IEEE Symposium on Foundations of Computer Science, (1986).
- [20] Yan-Cheng Chang and Chi-Jen Lu.. Oblivious polynomial evaluation and oblivious neural learning. In ASIACRYPT, volume 2248 of LNCS, pages 369-384. Springer, 2001.

Mert Özarar is a senior Ph.D. student in Department of Computer Engineering at Middle East Technical University (METU). His research focuses on using algorithmic techniques from cryptography and secure multiparty computation to design and model secure protocols for data exchange and networking. His primary academic interests are cryptography, security, algorithms, and machine learning. Other academic interests include complexity theory, pattern recognition and game theory. In 2004, he opted to join a startup company, TÜRKTRUST Inc. which is one of the leading certification authorities and IT-Security firms in Turkey.

He obtained his Master's degrees in Computer Engineering, in 2003 as valedictorian and in Cryptography, in 2004 both from METU. As an undergraduate, he attended METU as well where he obtained degrees in Computer Engineering and Mathematics in the double major program. In the past, he has worked for IBM, ZIB, TU-Darmstadt and METU.

Attila Özgüt is a faculty member in Department of Computer Engineering at Middle East Technical University (METU). His research focuses on data security, operating systems and computer networks. Other academic interests include computer architecture and cryptography.

Pasif Ağ Verileri Üzerinden Düzensizlik Tespiti

Devrim SERAL, Beyhan ÇALISKAN

Abstract—Through the history, people have used several different ways to communicate. Over the few decades, Internet has become the primary source of information and important media for communication. This makes the sustainability of Internet crucial. On the other hand, the problems encountered on networks of various sizes that make up the Internet can seriously effect the performance of Internet. These problems usually originate from the anomalies of the networks and the immediate detection of anomalies in high capacity networks is a very resource consuming effort. This paper focuses on methods for anomaly detection which will require less resources by making use of netflow data.

Keywords — Site security monitoring, Networks, Computer Network Security

Özet—İnsanoğlu çağlar boyu bilgi edinmek ve haberleşmek için değişik yöntemlere başvurmuştur. Günümüzde ise İnternet, hem bilgi edinmek hemde haberleşmek için kullanılan en önemli araçlardan biri haline gelmiştir. Bu yüzden İnternetin sürekliliği büyük önem taşımaktadır. İnterneti meydana getiren değişik büyüklükteki ağlar üzerinde meydana gelen sorunlar, İnternete erişimi etkileyebilmektedir. Ağlar üzerinde meydana gelen sorunlar, genelde ağ düzensizliklerinden kaynaklanmaktadır. Yüksek hızlı ağlarda, anlık düzensizlik tespiti yapmak çok fazla kaynak gerektiren bir işlemdir. Bu çalışmada daha az kaynak gerektiren pasif ağ verileri kullanarak düzensizlik tespiti yapma yöntemleri ele alınacaktır.

Anahtar Kelimeler— Ağ güvenliği, Bilgisayar Ağ Güvenliği, Düzensizlik Tespiti

I. GİRİŞ

Ağ sistemlerine erişim, donanımsal nedenlerin dışında ağa kötüye kullanıma yada ağ üzerinde düzensizlik yaratılarak kesintiye uğratılabilir. Bunların önüne geçmek için ağ trafiğini izlemek ve analiz etmek önem kazanmaktadır. Hızlı ve verimli çalışan analiz sistemlerinin varlığı, bu sorunların etkin bir şekilde ağı zarar vermesini engelleyebilmektedir. Bu şekilde çalışan sistemlere saldırı tespit sistemleri adı verilmektedir [1]. Ağ saldırı tespit sistemleri, imza tabanlı ve düzensizlik tabanlı olarak sınıflandırılabilirler [2]. İmza tabanlı sistemler, bilinen saldırı türlerine göre yazılan kurallar ile çalışırlar [3]. Ancak bu sistemlerde yeni saldırılar için gerekli olan kurallar, sadece güvenlik uzmanları tarafından güncellenebilmektedir.

Devrim Seral, Uluslararası Kıbrıs Üniversitesi, Mühendislik Fakültesi, Bilişim Sistemleri Mühendisliği, Lefkoşa-Kıbrıs'ta öğretim görevlisidir. (e-mail: dseral@ciu.edu.tr)

Beyhan Çalıskan, ULAKBİM, Ankara'da sistem yöneticisi olarak çalışmaktadır (e-mail: beyhan@ulakbim.gov.tr)

Bu durum, imza tabanlı sistemleri sıfır gün saldırıları (zero day attack) karşısında etkisiz bırakabilmektedir [4]. İmza tabanlı sistemler, analiz sırasında paket verisinin tümünü kullanmak zorundadırlar. Bundan dolayı yüksek hızlı ağlarda performansı azaltıp maliyeti artırdığından çok fazla tercih edilmezler. Gelişen teknoloji ile ağ hızları Gbps seviyelerine ulaşmış ve imza tabanlı sistemler yerine düzensizlik tabanlı sistemler önem kazanmıştır [5]. Düzensizlik tespiti için güvenlik uzmanları tarafından yazılmış kurallara gereksinim duyulmaz ve yeni saldırı türleri tespit edilebilir. Ancak bu tür sistemler, paket verileri (payload) ile ilgili olmadıkları için saldırıların özelliklerine ait bilgiler veremezler ve imza tabanlı sistemlere göre hatalı uyarı (false alarm) verme ihtimalleri daha fazla olabilmektedir.

Bu makalede, pasif ağ verileri üzerinden düzensizlik tespiti yöntemleri verildikten sonra örnek akış verisi üzerinde uygulaması anlatılacaktır. Pasif ağ verileri akış veri standardı olan NetFlow [6] formatında yönlendirici üzerinden alınacaktır. NetFlow, IP trafiğini özelliklerine göre ayırmakta, kaynak adresi, varış adresi, süre ve port bilgilerini detaylı şekilde verebilmektedir. Bu özellikler, ağ saldırılarından kaynaklanan düzensiz trafiği tespit etmekte kullanışlı olmaktadır. Makalenin ilk bölümünde düzensizlik tespitinde istatistiksel yöntemler incelenmiş, ikinci bölümünde ise yapay sinir ağları ile düzensizlik tespiti yöntemleri değerlendirilmiştir. Son bölümde Ulusal Akademik ağ trafiğinden alınan örnek verilerden yararlanarak saldırı tespiti yapılmıştır.

II. DÜZENSİZLİK TESPİTİNDE İSTATİSTİKİ YÖNTEMLER

Ağ trafiğinde oluşan düzensizliği inceleyerek, saldırı tespit etmek için değişik çalışmalar yapılmıştır. Bu çalışmaların birçoğunda istatistikî yöntemler ve trafik örnekleme (sampling) kullanılarak sonuç elde edilmeye çalışılmıştır [7],[8]. Yönlendiricilerden toplanan akış verileri (flow) ve ip paket başlıkları bu araştırmaların temelini oluşturmaktadır. Her iki yöntemde de paketlerin veri kısmına bakılmaksızın yönlendirme bilgisi, kaynak adresi, varış adresi, kaynak portu, varış portu, aktarılan veri büyüklüğü (byte) gibi bilgilerden faydalanarak modellemeler yapılmıştır [9]. Bu makalede akış verileri kullanılarak düzensizlik tespiti yöntemleri irdelenmiş ve istatistik yöntemler genel olarak iki başlık altında toplanmıştır; *En Çok ve Baz Değer, İz Eşleştirme*.

A. En Çok ve Baz Değer

Baz değer, geçmişte kaydedilen ağ trafiğine göre oluşturulmuş şablondur. Bu şablon normal ağ trafiğini temsil eder. Ağ trafiğinde meydana gelen ve baz değerden farklı olan her türlü trafik düzensiz olarak kabul edilir. Düzensiz trafiğin incelenmesinde kullanılan genel yöntem akış içerisindeki değişimleri tespit etmektir. Belirli bir zaman diliminde en fazla değişimi tespit etmek *en çok* yöntemi olarak tanımlanmaktadır.

En çok yönteminde, meydana gelen düzensizlikleri tespit ederken iki ayrı yöntem izlenebilir. En çok oturum yönteminde; belirli bir zaman dilimindeki oturum sayısı (session) temel alınır. En çok veri yönteminde ise; belirli bir zaman diliminde aktarılan veri miktarı (byte) temel alınır.

En Çok Oturum

Belirli bir istemci veya sunucuya ait ağ trafiğinde meydana gelen ani oturum sayısı artışı DoS/DDoS, solucan aktivitesi, ağ taraması gibi birçok sebepten kaynaklanabilir. En fazla oturumun açıldığı sunucu veya ağ'daki oturum sayısı ile baz değer karşılaştırılınca olası saldırı tespit edilebilir.

Ağdaki herhangi bir bilgisayar servis bağlantısı yaparken kabul edilebilir sıklıkta oturum açar. Eğer oturum sayısında çok hızlı ve ani artışlar gözleniyorsa, bilgisayarın bir solucan tarafından etki altına alındığı ve başka bilgisayar veya ağlara doğru yayılmaya çalıştığı söylenebilir. Solucanların ağdaki faaliyetleri, konak bilgisayardan diğer kurbanları ararken ağı normal ağ karakteristik yapısında farklılıklar oluşturur. Bu farklılık akış verilerindeki artıştan tespit edilebilir.

Bir diğer durum ise belirli bir sunucu veya ağa yönelik akış sayısındaki ani artıştır. Genellikle bu tür artışlar servis veren sunuculara yöneliktir. DoS/DDoS saldırıları servis veren sunucu veya ağı karakteristik yapısını değiştirdiği için yine akış verileri yardımıyla saldırı tespit edilebilir.

En Çok Veri

Sunucu veya istemcilerin belirli bir zaman diliminde bant genişliğini hızlıca tüketmeleri normal bir durumu değildir. Düzensiz trafiği analiz etmek için bu konuda çalışmalar yapılmıştır [10]. Baz değerden farkı açıkça gözlenebilen bu tür trafiğin kaynağı yine solucan veya servis engelleme saldırıları olabilmektedir. Bu saldırıları tespit etmek çok kolay olmakla birlikte hatalı uyarı alma ihtimali daha fazladır. Bunun nedeni yedekleme veya dosya transferi gibi uygulamalardan kaynaklanan ve ağ trafiğinde oluşan ani ve yüksek veri akışları sayılabilir.

B. İz Eşleştirme

İz eşleştirme, normal dışı trafiğin tespit edilmesinde bir diğer yöntemdir. Bu yöntemde motivasyon ağda bilinen servis ve ip bloklarının akış verileri ile karşılaştırılmasına dayanır. Mevcut servislere ait port ve ip bilgileri oluşturulan bir veritabanı yardımıyla akış verileri ile karşılaştırılır. Veri tabanında bulunmayan port veya ip adreslerine gelen veya giden trafik şüpheli olarak değerlendirilebilir. Örneğin sadece 80 portundan hizmet veren bir sunucunun 3306 portuna bir istek gönderildiğinde uyarı sistemi devreye girip şüpheli

durumu bildirebilir. Bu yöntem ağ tarama tespitinde kolayca kullanılabilir.

İz eşleştirmede bir diğer yaklaşım, TCP bayraklarından (flags) yararlanarak örnekleme veritabanı oluşturmaktır. TCP Protokolünde, Three-way-handshake [11] prosedürünü tamamlamayan, sürekli SYN paketleri gönderen istemciler veya sürekli SYN paketi alan sunucular normal olmayan trafiğin habercisidir. Akış verilerindeki TCP bayrakları ile karşılaştırma yapıldığında belirli bir eşik değerin üzerindeki paket türleri düzensiz olarak kabul edilebilir. Genellikle böyle bir durum DoS veya DDoS saldırısını işaret eder.

Port ve TCP bayrağı yaklaşımına benzer bir yaklaşım IP adresleri için de uygulanabilir. Kaynak adresi IANA tarafından rezerve edilmiş ip kümelerinden [12] gelen trafik düzensiz olarak değerlendirilebilir. Ayrıca ağa ait fakat kullanılmayan ip adreslerine doğru yapılan trafik ağ taraması veya solucan aktivitesini işaret edebilir. IP veritabanı örnekleme dışarıdan gelen saldırılara karşı etkili olabildiği gibi aynı yaklaşımla iç ağdan yapılan saldırıların da tespitinde önemli rol oynayabilir.

III. YAPAY SİNİR AĞLARI İLE DÜZENSİZLİK TESPİTİ

Ağlar üzerinde oluşan düzensizlikleri tespit etmek için yapay sinir ağlarını kullanmak bir diğer yöntemdir. Bu sistemler yapay sinir ağlarının, önceden kaydedilmiş problem oluşturan düzensizlik verileri yardımıyla eğitilmesine dayanır [13]. Bu sistemler hem yanlış kullanım hemde düzensizlik tespit sistemleri ile birlikte anılır.

Yapay sinir ağlarının Çok katmanlı Algılama (Multilayer Perception) [14] ve Kendinden Teşekküllü Haritalar (Self-organizing Map) gibi farklı yaklaşımları da kullanılmaktadır [15].

Yapay sinir ağlarında Kendinden Teşekküllü Haritalar (KTH) öncelikle normal davranış gösteren ağ trafiğini öğrenme periyodundan geçirdikten sonra düzensizlik hareketlerini tespit edebilmektedir. Ancak bu sistemin en büyük kısıtlaması neron sayısının ağ performansını etkilemesidir. Çıkış düğümlerinin sayısını artırmak haritanın çözünürlüğünü artırmakla beraber veri işleme süresi dramatik bir biçimde artırmaktadır.

Yapay sinir ağları, ağ saldırı tespitinde kullanılırken bir diğer sorunu da zaman gecikmeli saldırıları tespit edememesidir [16].

Tüm yöntemlerde istenen yanlış uyarı miktarını mümkün olduğunca aşağıya çekmektir.

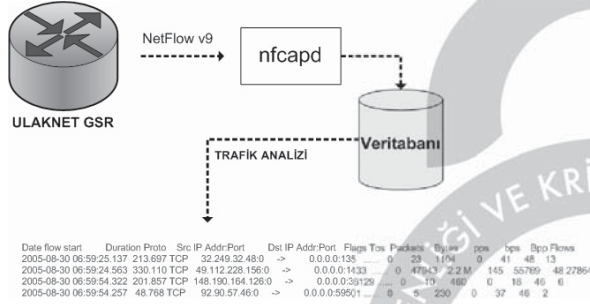
IV. AKADEMİK AĞDA DÜZENSİZLİK TESPİTİ

ULAKNET; Türkiye'deki tüm akademik kurumları, Türk Tarih Kurumu, Milli Kütüphane, YÖK, ÖSYM, TÜBİTAK, Türkiye Atom Enerjisi Kurumu ve Türk Silahlı Kuvvetleri'nin Ar-Ge birimlerinden oluşan geniş bir ağa hizmet sunmaktadır. Bu uçlarda bulunan yaklaşık 89300 öğretim görevlisi, araştırmacı ve 2.000.000 üzerinde üniversite öğrencisinin İnternet bağlantısı ULAKBİM tarafından sağlanmaktadır [17].

A. Yöntem

Düzensizlik tespiti için ULAKNET ağından alınan bir aylık akış verisi üzerinde çalışılmıştır. Akış verileri, 3Gbps bant genişliğine sahip akademik ağın ana omurga yönlendiricisi üzerinden Cisco NetFlow v9 standardında alınmıştır. Şekil 1'de gösterildiği gibi, akış şemaları, açık kaynak kodlu nfcapd [18] yazılımı ile toplanmış ve verilerin hızlı işlenmesi için Perl [19] betikleri yardımıyla MySQL [20] veritabanına kaydedilmiştir.

ULAKNET ağında düzensizlik tespiti için kullanılan yöntemler makalenin birinci bölümünde anlatılan istatistik temelli yaklaşımlara dayanmaktadır. Bu çerçevede deneyler en çok yöntemi ve iz eşleştirme olarak iki başlık altında toplanmıştır. Yapılan çalışma saldırı şüphesi olan trafiği ağ ve sistem yöneticileri tarafından görünür kılmaya yöneliktir [21]. Daha sonra gerekli modelleme yaklaşımları ile otomatik uyarılar üretme ve saldırıları engelleyen bir sistem geliştirilebilir.



Şekil 1. Netflow akış verilerinin alınması

En Çok Yöntemi Uygulaması

İnceleme yapılan bir aylık akış verisi 5, 10, 30 ve 60 dakikalık periyotlarla analiz edilmiştir. Farklı periyotlarda inceleme yapılmasının temel nedeni, en çok yönteminde saldırıların tespiti için bir eşik değeri öngörülmesidir.

Deneyin ilk kısmında 5, 10, 30 ve 60 dakikalık zaman dilimleri kullanılarak akış verisi içerisinde en çok oturum açan istemciler tespit edilmiştir. Yapılan inceleme sonucu, analiz periyodu uzadıkça en çok akış yöntemine ait başarının düştüğü hatta etkisini kaybettiği gözlemlenmiştir. Bu durumun nedenini araştırıldığında, 3Gbps gibi yüksek bir bant genişliğinde normal trafiğin şüpheli trafiğe göre daha fazla yer almasından kaynaklandığı tespit edilmiştir. Bu çerçevede en çok akış yöntemleri uygulanırken, kısa zaman dilimlerinde analiz yapmanın, anlık artışları ve düzensizliği tespit etmekte etkili olacağından hareket edilmiştir. Bu yüzden 5 dakikalık periyotlarla trafik analizi yapılmıştır. En çok oturum yöntemi uygulanarak tespit edilen bir düzensizlik aşağıda gösterilmiştir.

TCP 194.27.X.X:80 -> 20.95.31.62:1024 .A..S. 1 44 0 0 44 1
 TCP 194.27.X.X:80 -> 3.110.217.64:3072 .A..S. 1 44 0 0 44 1
 TCP 194.27.X.X:80 -> 85.255.5.60:3072 .A..S. 1 44 0 0 44 1
 TCP 194.27.X.X:80 -> 138.163.116.123:1024 .A..S. 1 44 0 0 44 1
 TCP 194.27.X.X:80 -> 35.53.251.68:1024 .A..S. 1 44 0 0 44 1
 TCP 194.27.X.X:80 -> 44.77.161.38:3072 .A..S. 1 44 0 0 44 1
 TCP 194.27.X.X:80 -> 181.46.18.16:3072 .A..S. 1 44 0 0 44 1

TCP 194.27.X.X:80 -> 176.116.55.102:1024 .A..S. 1 44 0 0 44 1
 TCP 194.27.X.X:80 -> 201.208.253.34:1024 .A..S. 1 44 0 0 44 1
 TCP 194.27.X.X:80 -> 122.121.178.35:1024 .A..S. 1 44 0 0 44 1

Örnek diyagram sırasıyla; protokol, kaynak ip ve kaynak port, hedef ip ve hedef port, tcp bayrağı, paket sayısı, paket büyüklüğü (byte), saniyedeki bit sayısı, paket başına byte ve oturum sayısını göstermektedir. En çok oturum yöntemi ile tespit edilen bu trafiğin normal olmadığı hemen görülebilmektedir. 194.27.X.X ip adresine sahip 80 numaralı porttan hizmet veren web sunucusu birçok farklı ip adresine SYN-ACK paketleri göndermekte ve hedef portları da sürekli 1024 ve 3072 olmaktadır (Sunucu adresi gizlenmiştir). Tespit edilen bu düzensizlik ilgili web sunucusuna yapılan SYN flood saldırısına aittir. En çok akış yöntemi, ağ trafiğinin karakteristik yapısında belirgin değişiklikler yapan, yukarıda incelediğimiz saldırıyı tespit edebilirken, aynı zaman dilimi içinde yer alan bir başka saldırıyı tespit etmekte başarısız olabilir. Bu varsayımın temelinde, yüksek bant genişliğinde düzensiz trafiği normal trafikten ayırt edecek paket ve akış sayısının çok fazla olması gerektiği düşüncesi vardır. Bu varsayımı doğrulamak için en çok akış yöntemine TCP filtreleri yazılmıştır.

Aşağıda verilen akış verileri bir önceki akış verileri ile aynı zaman aralığından elde edilmiştir. TCP bayrağında SYN paketi olan istemcilere, en çok oturum yöntemi uygulanarak elde edilen veriler, 193.140.X.X ip adresli istemciden kaynaklanan ve 135 port adresini hedef alan faaliyetleri tespit etmiştir. Bu faaliyetin bir solucan saldırısı olduğu hemen fark edilmektedir.

TCP 193.140.X.X:2907 -> 193.140.53.155:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:2926 -> 193.140.53.164:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:2934 -> 193.140.231.7:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:2971 -> 193.140.177.80:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:2978 -> 193.140.53.187:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:2984 -> 193.140.53.190:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:3007 -> 193.140.53.202:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:3027 -> 193.140.53.212:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:3030 -> 193.140.177.91:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:3045 -> 193.140.53.221:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:3061 -> 193.140.231.42:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:3074 -> 193.140.231.49:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:3077 -> 193.140.177.111:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:3099 -> 193.140.53.232:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:3104 -> 193.140.231.60:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:3114 -> 193.140.231.65:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:3127 -> 193.140.177.131:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:3118 -> 193.140.231.67:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:3147 -> 193.140.231.75:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:3154 -> 193.140.53.252:135S. 1 48 0 0 48 1
 TCP 193.140.X.X:3161 -> 193.140.177.137:135S. 1 48 0 0 48 1

Bir diğer en çok yöntemi olan paket büyüklüğüne göre düzensiz trafik tespiti ULAKNET akademik ağında başarısız olmuştur. Bu yöntemdeki motivasyon saldırıların bant genişliğini hızlıca doldurabileceği varsayımına dayanmaktadır. Fakat ULAKNET gibi çok uçlu ve yüksek bant genişliğine sahip bir ağda, normal trafik karakterinin fazla oluşu şüpheli trafiği en çok veri yönteminden gizleyebilmektedir. Bu yöntemin geniş süreli uygulamasından verimli sonuç

alınmayınca daha önce en çok oturum yöntemi ile tespit edilen saldırıya ait zaman aralığı TCP filtreleri de kullanılarak taranmıştır. Elde edilen sonuçlar etkin düzensizlik tespiti için yeterli olmamıştır.

Bu yöntemin mevcut durumda kullanılabilmesi istatistik yöntemlerden daha çok yapay sinir ağlarıyla mümkün olabilir. Yapay sinir ağı eğitilip ULAKNET ağına bağlı her bir uç için baz değer veritabanı oluşturulabilir. Ağda baz değer üzerinde veri akışı gerçekleşirse düzensiz trafik tespit edilebilir. Daha önce de belirtildiği gibi bu yöntemin hatalı uyarı verme ihtimali yedekleme ve dosya transferi gibi sebeplerden dolayı yüksek olması beklenebilir.

İz Eşleme Yöntemi Uygulaması

ULAKNET ağına iz eşleme yöntemi ile düzensizlik tespit uygulaması, istatistik yöntemlerin en başarılısı olmuştur. Akış şemalarından elde edilen veriler IANA tarafından rezerve edilen ip blokları ile karşılaştırılmıştır. Bu çalışmada IANA tarafından rezerve edilen ip adreslerinin, asla geniş alan ağlarında bulunmaması gerektiğinden yola çıkılmıştır. Bu varsayıma uymayan bütün trafik düzensiz olarak kabul edilir. Aşağıdaki diyagramlarda iz eşleme yöntemi ile tespit edilen şüpheli trafikler gösterilmiştir.

TCP 193.140.X.X:49960 -> 192.168.163.169:515S. 1 52 0 0 52 1
TCP 193.140.X.X:49969 -> 192.168.163.170:2191S. 1 52 0 0 52 1
TCP 193.140.X.X:49972 -> 192.168.163.170:81S. 1 52 0 0 52 1
TCP 193.140.X.X:49977 -> 192.168.163.172:515S. 2 100 0 88 50 1
TCP 193.140.X.X:49979 -> 192.168.163.172:2191S. 1 52 0 0 52 1
TCP 193.140.X.X:49984 -> 192.168.163.173:515S. 1 52 0 0 52 1
TCP 193.140.X.X:49986 -> 192.168.163.173:2191S. 1 52 0 0 52 1
TCP 193.140.X.X:49988 -> 192.168.163.173:443S. 1 52 0 0 52 1
TCP 193.140.X.X:49993 -> 192.168.163.171:2191S. 1 52 0 0 52 1
TCP 193.140.X.X:49995 -> 192.168.163.171:443S. 1 52 0 0 52 1

Diyagramdan açıkça görüldüğü üzere 193.140.X.X ip adresli istemciye gelen trafik IANA tarafından rezerve edilmiş 192.168.0.0/16 ağı kaynaklıdır. Bu akış şemasından, ip adresini değiştirmiş saldırganın port tarama saldırısı gerçekleştirdiği görülmektedir. Tespit edilen bir diğer şüpheli trafik ise aşağıdaki akış diyagramına aittir. Web sunucusuna yapıldığı ve servis engelleme amaçlı olduğu açıkça belli olan bu saldırı 0.0.0.0/8 ağ kaynaklı olarak gözükmemektedir. Fakat bu ağ IANA tarafından rezerve edilmiştir ve iz eşleme yöntemi tarafından saldırı tespit edilmiştir.

TCP 193.140.X.X:5823 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:2678 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:35671 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:12301 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:62520 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:32299 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:38133 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:35579 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:27852 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:56331 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:19893 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:14261 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:14736 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:12718 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:52480 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:58488 -> 0.39.15.0:80S. 1 48 0 0 48 1

TCP 193.140.X.X:28680 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:23348 -> 0.39.15.0:80S. 1 48 0 0 48 1
TCP 193.140.X.X:9118 -> 0.39.15.0:80S. 1 48 0 0 48 1

V. SONUÇ

Günümüzde İnternetin kesintisiz olarak çalışması hayati önem taşımaktadır. Bunun nedeni ise artık birçok kurumun ve bireyin hızlı ve zahmetsizce işlerini İnternet üzerinden halledebilmesidir. Erişimin herhangi sebepten dolayı kesilmesi zaman, maliyet ve iş kayıplarına neden olabilmektedir.

İnternet'in donanım sorunları dışında başka nedenlerle kesintiye uğraması genelde ağlar üzerinde görülen düzensizliklerden kaynaklanmaktadır.

Bu çalışmada, yüksek hızlı ağlarda düzensizlik tespitinde kullanılan yöntemler ele alınmış ve ULAKBİM gibi büyük bir ağdaki verilerden yararlanarak, temel düzensizlik bulgularının nasıl tespit edileceği gösterilmiştir.

Bu çalışma yazılım tabanlı uygulamalar geliştirerek daha kapsamlı bir sistem haline getirilebilir. Böyle bir sistemin anlık veri akışları üzerinde düzensizlik tespit edip uyarılar üretmesi bir sonraki çalışma konusu olabilir.

TEŞEKKÜR

Bu çalışmada bizlere ağ akış verilerini ve analiz yapabilmemiz için gerekli olan donanımı sağladığı için ULAKBİM'e teşekkür ederiz.

KAYNAKLAR

- [1] D.E. Denning, "An Intrusion Detection Model", IEEE Transactions on Software Engineering, SE-13:222-232, 1987.
- [2] N. J. Puketza, K. Zhang, M. Chung, "A Methodology for Testing Intrusion Detection Systems", IEEE Transactions on Software Engineering, Volume 22, Issue 10, pp. 719 – 729, 1996.
- [3] Novikov, D. Yampolskiy, R.V. Reznik, L., "Anomaly Detection Based Intrusion Detection", ITNG 2006, pp. 420-425, 2006.
- [4] K. Wang, S. J. Stolfo, "Anomalous payload-based network intrusion detection", RAID, pp. 203-222, Sept., 2004.
- [5] B. Choi, S. Bhattacharyya, "Observations on Cisco Sampled Netflow", ACM SIGMETRICS Performance Evaluation Review, Volume 33, Issue 3, pp.18 – 23, 2005.
- [6] Cisco Netflow, http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html.
- [7] S. S. Kim, A. L. N. Reddy, "Statistical Techniques for Detecting Traffic Anomalies Through Packet Header Data", IEEE/ACM Transactions on Networking, vol.16, pp. 562-575, June 2008.
- [8] A. Lakhina, M. Crovella, C. Diot, "Characterization of Network-Wide Anomalies in Traffic Flows", in Proc. 4th ACM SIGCOMM conference on Internet measurement, Taormina, 2004, pp. 201-206.
- [9] G. Dewaele, K. Fukuda, P. Borgnat, P. Abry, K. Cho, "Extracting Hidden Anomalies using Sketch and NonGaussian Multiresolution Statistical Detection Procedures", in Proc. 2007 workshop on Large scale attack defense, Kyoto, 2007, pp. 145-152.
- [10] Matthew V. Mahoney, "Network Traffic Anomaly Detection Based on Packet Bytes", in Proc. ACM symposium on Applied computing, Florida, 2003, pp. 346-350.
- [11] D. Katz, R. Saluja, Three-Way Handshake for Intermediate System to Intern, IETF RFC 3373, 2002
- [12] IPv4 Global Unicast Address Assignments, <http://iana.org/assignments/ipv4-address-space>
- [13] J. Z. Lei, A. Ghorbani, "Network Intrusion Detection Using an Improved Competitive Learning Neural Network", Communications Networks and Services Research Conference, pp. 190 - 197, 2004.

- [14] A. K. Ghosh, A. Schwartzbard, "A study in using neural networks for anomaly and misuse detection", In Proceedings of USENIX Security Symposium, 1999.
- [15] B. C. Rhodes, J. A. Mahaffey, and J. D. Cannady, "Multiple self-organizing maps for intrusion detection", In Proceedings of the 23rd National Information Systems Security Conference, 2000.
- [16] Y. Yaho, Y. Wei, F. Gao, G. Yu, "Anomaly Intrusion Detection Approach Using Hybrid MLP/CNN Neural Network", ISDA'06, pp. 1095-1102, 2006
- [17] ULAKNET, <http://www.ulakbim.gov.tr/hakkimizda/tarihce/ulaknet>
- [18] nfdump, <http://nfdump.sourceforge.net>
- [19] Perl, <http://www.perl.org>
- [20] MySQL, <http://www.mysql.com>
- [21] G. Conti, K. Abdullah, "Passive Visual Fingerprinting of Network Attack Tools", in *Proc. ACM workshop on Visualization and data mining for computer security*, Washington, 2003, pp. 45-54.



IPv6 İkili Yığın Geçiş Yönteminde Uygulamaların Saldırı Altında Performans Analizi

Beyhan ÇALIŞKAN, Onur BEKTAŞ

Abstract— IPv6, being the next generation Internet protocol to replace IPv4, will be the primary network layer protocol in 21st century networks. The IPv6 transition studies which initially started in research and education networks are now shifting towards the commercial networks due to the expectation that the IPv4 address range will be totally exhausted by the end of 2010. For IPv6 to become more widespread, it has to prove that it fulfills the critical performance and security expectations of commercial networks especially in the transitions phase. This paper analyzes IPv6 stack performance under denial of service attacks for dual stack IPv6 network, which is one of the major types of the IPv6 transition methods. For comparison, native IPv4 and IPv6 performance with and without attacks are also given.

Keywords —Apache benchmark, dual stack, IPv6 performance, security

Özet— IPv6'ün yerini almak için geliştirilen IPv6, 21 yüzyılda internetin temel bağlantı protokolü olacaktır. Araştırma ağlarında ve test yataklarında başlayan IPv6 geçiş çalışmaları, IPv4 adreslerinin 2010 yılı sonunda tükeneceği beklentisi ile birlikte ticari ağlara doğru kaymıştır. IPv6'nın yaygınlaşması için ticari ağların beklentilerini karşılayacak şekilde kendisini kanıtlaması gerekmektedir. Ticari ağların IPv6'ya geçişinde güvenlik ve performans iki önemli kistas olacaktır. Bu makalede IPv6 geçiş yöntemlerinden biri olan ikili yığın metodunun servis dışı bırakma saldırısına karşı performansı incelenmiştir. Geçiş metodunun yanında, yalnız IPv4 ve yalnız IPv6 performansları normal durumda ve saldırı altında araştırılmıştır.

Anahtar Kelimeler— Apache performansı, ikili yığın, IPv6 performansı

I. GİRİŞ

IPv6, IETF (Internet Engineering Task Force) tarafından IPv4'ün yerini almak için geliştirilen yeni nesil internet protokolüdür. IPv6'nın çıkış noktası internet protokolünün günün ihtiyaçlarının karşılayacak şekilde yenilenmesidir. Yeni

Beyhan Çalışkan, TÜBİTAK Ulusal Akademik Ağ ve Bilgi Merkezinde sistem yöneticisi olarak çalışmaktadır. Telefon: 312-2989376; faks 312-2989393; Eposta: beyhan@ulakbim.gov.tr

O. Bektaş TÜBİTAK Ulusal Akademik Ağ ve Bilgi Merkezinde uzman araştırmacı olarak çalışmaktadır. Telefon: 312-2989367; faks 312-2989393; Eposta: onur@ulakbim.gov.tr

nesil IP (Next Generation IP, IPng) ismi altında başlayan IPv6 geliştirme çalışmaları sonucunda protokol temel tanımlarını içeren RFC 2460 [1] ise 1998 yılında yayınlanmıştır. IPv6'nın yakın bir gelecekte internete bağlanmak için yeni standart olması beklenmektedir.

IPv4 adres dağıtımının geçmiş yıllardaki hızı modellenerek yapılan tahminler IPv4 adreslerinin 2010 yılı sonlarına doğru tükeneceği göstermektedir [2]. IPv6 uzun süren tasarım aşamaları ve araştırma ağlarında yapılan denemelerden sonra günümüzde ticari ağlara doğru geçiş sürecindedir. IPv6'ya geçiş sürecinde mevcut olan IPv4 altyapısı bir anda bırakılmayacağından iki protokolünde internete aynı anda bulunması kaçınılmazdır. IPv6 tasarlayıcıları tarafından geçiş sürecinin en optimum gerçekleştirilmesi için çeşitli yöntemler önerilmiştir. Bu yöntemler 3 başlık altında toplanabilir [3].

İkili yığın

Bu yöntemde cihazların geçiş sürecinde IPv4 ve IPv6 protokollerini de aynı anda desteklemesi söz konusudur. İkili yığın destekli cihazlarda bağlantı aşamasında ilk olarak IPv6 adresi ile bağlantı yapılmaya çalışılır. Bağlantının gerçekleşmemesi durumunda IPv4 adresi kullanılır.

Tünelleme

Tünelleme yöntemi, IPv6 ağlarının diğer IPv6 ağlarına ulaşmaları için IPv4 ağlarının kullanılmasıdır. Bu yöntemde IPv6 trafiği IPv4 paketleri içinde taşınır. Bir diğer yöntem ise IPv4 trafiğinin IPv6 paketleri ile taşınmasıdır. İstemciden istemciye, istemciden yönlendiriciye, yönlendiriciden istemciye, yönlendiriciden yönlendiriciye olmak üzere tünelin açılış şekline göre 4 grup altında sınıflandırılabilir.

Yalnız IPv6

Sadece IPv6 adresine sahip olan cihazların IPv4 cihazları ile haberleşmesi için araya bir çevirici (translator) konulması yöntemidir. Bu yöntemde IPv6 <-> IPv4 ve IPv4 <-> IPv6 çevrimi OSI referans modelinin ağ, ulaşım veya uygulama katmanlarında gerçekleştirilebilir.

IPv6 ile ilgili yapılan çalışmaların birçoğu test ortamlarında ve araştırma ağlarında gerçekleştirilmiştir. IPv6'nın ticari ağlardaki performansı ile ilgili çok fazla araştırma

yapılmamıştır [4]. Ağın performansı ticari ağlar için kritik olan bir özelliktir. IPv6 ağlarında performans ile ilgili çalışmalar, işletim sistemlerinde IPv6 yığın performansının incelenmesi ve ticari IPv6 internet performansının IPv4 ile karşılaştırılması konularında yoğunlaşmıştır.

İlk grupta yer alan araştırmalar işletim sistemlerindeki IPv6 yığın performansını ölçmeye yöneliktir. Windows 2000 ve Solaris 8 işletim sistemlerinde IPv4 ve IPv6 protokollerinin ağ performansının ve sistem yükünün incelendiği çalışmada [5], Solaris 8 işletim sisteminin 256 bayttan küçük TCP paketleri için ağ katmanında IPv4 kullanımının IPv6 kullanıma göre 3 kat daha hızlı olduğu görülmüştür. Yine aynı çalışmada, Windows 2000 işletim sisteminde IPv6 TCP performansının 1 Kbayt'tan büyük paketler için IPv4'e göre %25 daha düşük olduğu gözlenmiştir. İki protokolün sistem kaynakları kullanımını incelendiğinde ise IPv6 üzerinden TCP protokolü kullanımının IPv4'e göre ortalama %20 daha fazla işlemci kaynağı kullandığı saptanmıştır. IPv6 kullanan yazılımların performans araştırmasında Web sunucularının performansı karşılaştırılmıştır. Solaris 8 işletim sisteminin web sunucu performansının Windows 2000'e göre 4 kat daha fazla olduğu tespit edilmiştir. İşletim sistemlerinin yığın performansı ile ilgili diğer bir çalışma Windows 2003, RedHat 9.0 ve FreeBSD 4.9 işletim sistemlerinin karşılaştırılmasıdır [6]. Çalışmada, farklı paket büyüklükleri için IPv4 ve IPv6 performansları arasında benzer sonuçlara ulaşılmış fakat işletim sistemleri arasında farklılıklar gözlenmiştir. Redhat işletim sistemi loopback üzerinde yapılan testlerde ilk sırayı almış, Windows 2003 arada bir cihaz olmadan doğrudan kablo ile yapılan testlerde en iyi performansı göstermiştir.

Performans üzerinde yapılan diğer çalışmalar son kullanıcı tarafından IPv6 ağlarında hissedilecek olan performansı ölçmeye yöneliktir [4],[7]. Çalışmalarda, ilk olarak ikili yığın yapısında çalışan web sunucuların listesi çıkarılmıştır. İkinci aşamada tespit edilen sunuculara IPv4 ve IPv6 üzerinden bağlanılarak bant genişliği, paket kaybı, paket gidiş geliş süresi benzeri ağ performansı parametreleri gözlenmiştir. Elde edilen bulgulardan ilki IPv6 ağlarında IPv4 ağlarına göre daha fazla sayıda paket kaybı yaşanmasıdır. Ayrıca, deneysel ağlarda yapılan çalışmalarda bulguların aksine tünellenmiş IPv6 trafiği ile tünellenmemiş trafik arasında performans açısından fark olmadığı tespit edilmiştir. Diğer bir gözlem, IPv6 kullanımının yaygın olmamasının bir sonucu olarak IPv6 için ayrılan bant genişliğinin boş olduğudur. Bunun sonucu olarak testlerde IPv6 istemcilerinin IPv4'e göre daha hızlı veri alıp gönderebildikleri saptanmıştır.

Ticari ağlarda önemli olan diğer bir kıstas IPv6'nın güvenlik özellikleridir. Bu konuda yapılan araştırmalar iki grup altında toplanabilir. İlk grupta, IPv4 ağlarındaki mevcut güvenlik risklerinin IPv6 ağlarındaki durumu incelenmiştir [8]-[10]. İkinci grupta IPv6'nın IPv4'ten farklı olan adres yapısı, dolaşılabilirlik, ek-başlık desteği gibi özelliklerin güvenliği irdelenmiştir [11]-[14].

Literatürde IPv6 performans ve güvenlik özellikleri konusunda araştırmalar yapılmış ise de, uygulamaların servis dışı bırakma saldırısı benzeri güvenlik riskleri karşısında durumları incelenmemiştir. Diğer bir değişle, IPv6 yığın yapısının IPv4'e göre saldırı altındaki performansları karşılaştırılmamıştır.

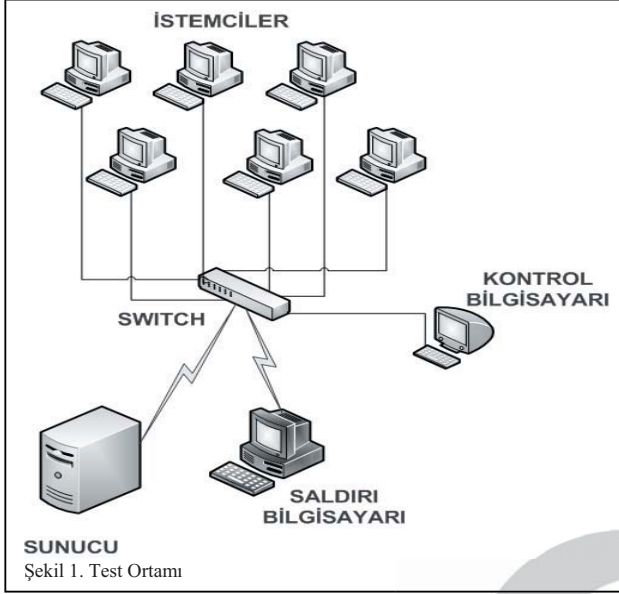
Bu makalede, FreeBSD işletim sistemi üzerine çalışan apache web sunucusunun saldırı altında IPv4 ve IPv6 yığınlarının performansı incelenmiştir. Makalenin ikinci bölümünde test yatağı özellikleri ve ölçüm metodolojisine değinilmiştir. Üçüncü bölümde, test sonuçlarından elde edilen veriler incelenmiş ve son olarak dördüncü bölümde makale sonuçları özetlenmiştir.

II. DENEY DÜZENEGİ VE ÖLÇÜM SÜRECİ

Kullanılan yöntem, uygulamaların IPv4-IPv6 ve ikili yığın performansını ortaya koymaya yöneliktir. Bu çalışmada seçilen uygulama Apache web sunucusudur. Apache web sunucusu, netcraft araştırma sonuçlarına göre dünya üzerindeki web sunucularının %53,3'ünde kullanılmaktadır [15]. Günümüzde internet trafiğinin büyük bir kısmı web trafiği oluşturmaktadır. Web sunucuları sağladığı içerik ile birlikte kurumların vitrini ve saygınlık göstergesi haline gelmiştir. Bankacılık, kurumsal veritabanı, e-devlet uygulamaları benzeri kritik yazılımların web sunucuları üzerinden çalışmaları bu serviste meydana gelecek kesintilerin kullanıcılar ve kurumlar tarafından önemini arttırmaktadır. Bununla birlikte asp, php benzeri web programlama dillerinin gelişimi bu eğilimi artırıcı yönde etki yapmaktadır.

A. Test Ortamı

Apache web sunucusunun IPv6 ve ikili yığın yapıda performansı ölçülümü Şekil 1'de gösterilen ağ topolojisi üzerinden gerçekleştirilmiştir. Test ortamında, aynı özelliklere sahip 6 istemci bilgisayar, 1 adet sunucu, 1 adet kontrol bilgisayarı, 1 adet saldırı bilgisayarı ve Cisco 3550 serisi anahtarlama cihazı bulunmaktadır. İstemci bilgisayarlar ve kontrol bilgisayarı, Intel Pentium 4 2.66GHz işlemci, 512MB bellek, 80GB Sata sabit disk ve 100Mbit ethernet kartı donanımlarına sahiptir. Sunucuda, 2 adet Intel Xeon Quad Core 1.86GHz işlemci, 8Gbayt bellek, 80Gbayt Sata sabit disk ve PCI-X Intel Pro 1000 gigabit ethernet kartı donanımları bulunmaktadır. Saldırı bilgisayarının anakart ve işlemci donanımı istemci bilgisayarları ile aynıdır. Bunların birlikte istemci bilgisayarlarından farklı olarak Broadcom gigabit ethernet kartı ve 1512MB bellek kullanılmıştır. İstemci ve kontrol bilgisayarları Cisco 3550 anahtarlama cihazının 100 Mbit hızındaki ethernet portlarına, sunucu ve saldırı bilgisayarları ise 1 Gbit hızındaki portlarına CAT5e kablolar ile doğrudan bağlanmıştır. İstemciler, sunucu, saldırı ve kontrol bilgisayarı aynı ağda olacak şekilde yapılandırılmıştır.



B. İşletim Sistemleri

İstemci, saldırı ve kontrol bilgisayarlarına x86 Debian Etch 4.0_r4 sürümlü işletim sistemi yüklenmiştir. Sistemler üzerinde çalışan Linux çekirdek sürümü 2.6.24'tür. Sunucu üzerine AMD64 FreeBSD 7 işletim sistemi bulunmaktadır. Apache web sunucusu FreeBSD port koleksiyonundan kurulmuştur ve sürümü 2.0.63'tür. Sunucu ve istemci bilgisayarlar üzerinde yapılan ince ayarlar aşağıda verilmiştir. Linux sistemler;
ulimit -t 10000

FreeBSD sistemi sysctl.conf ayarları;
vm.pmap.pv_entry-max=90000000
vm.pmap.shpgperproc=500000

FreeBSD üzerine portlardan kurulan Apache web sunucusu mpm prefork modülü [16] ile çalıştırılmıştır. Yapılan httpd.conf ayarları aşağıda listelenmiştir;
ServerLimit 15000
StartServer 2000
MinSpareServers 1000
MaxSpareServers 1000

C. Ölçüm Araçları

Web sunucusunun performansı apache benchmark (ab) [17] ile ölçülmüştür. Ab yazılımı Apache sunucusunun saniyede cevap verebildiği istek sayısının ölçümü için geliştirilmiştir. Her bir istemciye ab yazılımı kurulmuş ve yazılan betikler yardımıyla sonuçlar kontrol bilgisayarı tarafından toplanmıştır. Ab uygulaması -n 1600 -c 20 parametreleri ile çalıştırılmış ve sabit içeriğe sahip olan html sayfasına erişim süreleri kaydedilmiştir. Test sonuçlarının karşılaştırılabilir olması için bütün istemcilerden aynı sayıda istek (1600) gönderilmiştir.

FreeBSD işletim sisteminde, testler sırasında oluşan işlemci ve ethernet yükleri, vmstat [18] yazılımıyla tespit edilmiş ve yazılan betik yardımıyla kaydedilmiştir.

D. Ölçüm Sonuçlarının Toplanması

Performans testlerinin aynı şartlar altında tekrarlanması için istemci bilgisayarların hepsine bir kabuk betiği yazılmıştır. Bu betik kontrol bilgisayarı tarafından Clusterssh [19] yazılımıyla tüm istemcilerde aynı anda çalıştırılmıştır. Her testten sonra sunucu ve istemciler yeniden başlatılmıştır. Ölçümler 3'er kez tekrarlanmış ve sonuçların aritmetik ortalaması alınmıştır.

E. Ölçüm Sonuçlarının Anlamlı Hale Getirilmesi

Kontrol bilgisayarında toplanan ham veriler Perl [20] betikleri yardımıyla işlenmiştir. Sonuçların anlamlı bir hale getirilmesinden sonra Gnuplot [21] uygulaması ile grafikler çizilmiştir.

III. ÖLÇÜMLERİN YAPILMASI

IPv6 ve ikili yığın yapının uygulama performansının IPv4 uygulama performansı ile karşılaştırılması aşağıdaki ölçüm yöntemleriyle yapılmıştır:

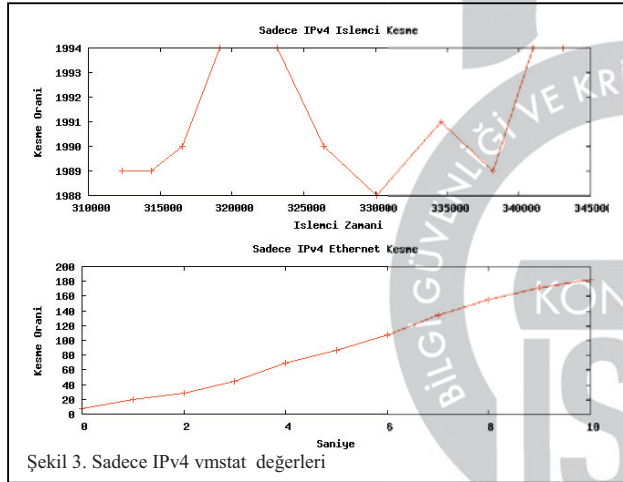
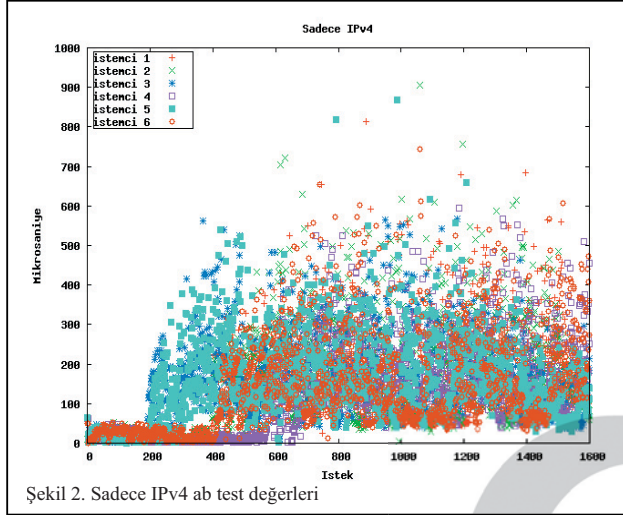
- 6 istemci ve web sunucusunda sadece IPv4 adresleri kullanılarak,
- 6 istemci ve web sunucusunda sadece IPv6 adresleri kullanılarak,
- 3 istemcide sadece IPv4 adresi, 3 istemcide sadece IPv6 adresi ve web sunucusunda ikili yığın yapı kullanılarak,

Yukarıdaki her bir adım saldırı altında tekrarlanarak toplamda 6 adımda ölçümler tamamlanmıştır. Bu 6 adım *Normal Durumda Test* ve *Saldırı Altında Test* olmak üzere iki grupta incelenmiştir.

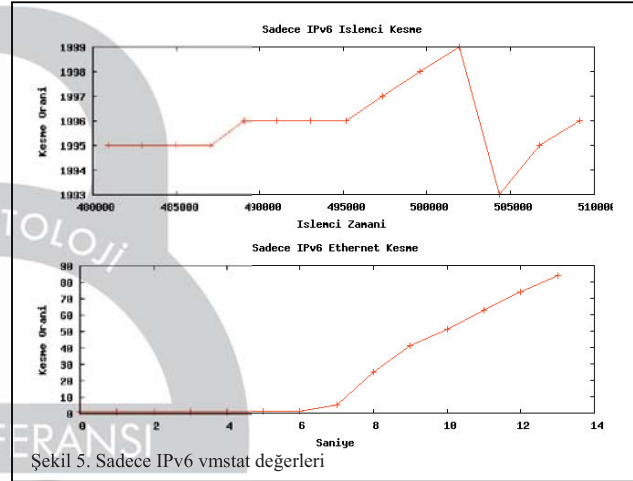
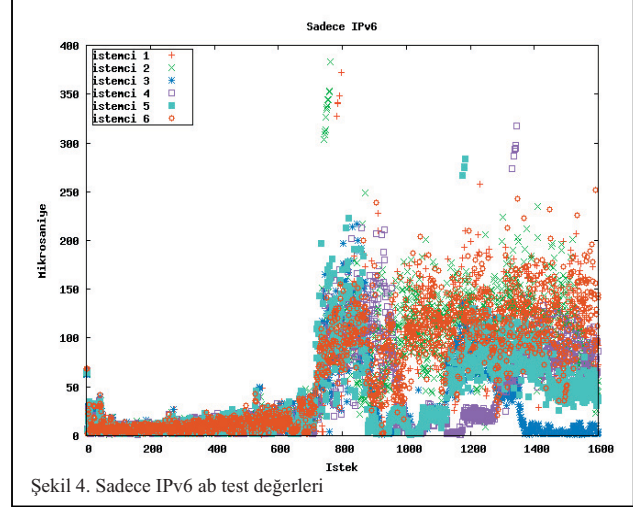
Normal Durumda Test

Ölçüm sonuçlarının grafiksel gösterimi için apache benchmark sonuçları ve VMSTAT çıktıları kullanılmıştır. Ab grafiklerinde yatay eksen sunucuya yapılan istek sayısını, dikey eksen istemcilerin aldığı cevap süresini mikrosaniye olarak göstermektedir. VMSTAT grafikleri işlemci ve ethernet üzerinde oluşan kesme oranını (interrupt rate) göstermektedir. Kesme oranı; ethernet kartı için işlemciye gönderilen kesme isteği sayısını, işlemci için ise tüm giriş/çıkış (I/O) ve programlardan gelen toplam kesme isteği sayısını göstermektedir. İşlemci kesme oranını gösteren grafikte yatay eksen işlemci zamanı, dikey eksen kesme oranı gösterilmiştir. İşlemci zamanı ve kesme oranı her test için farklı başlangıç değerlerinde olabilmektedir. Bu nedenle işlemciye ait grafik yorumu dikey ve yatay eksenindeki sayısal değerlerin büyüklüğüne göre değil, grafik altında kalan alan değerlendirilerek yapılmalıdır. Ethernet kesme oranını gösteren grafikte yatay eksen zamanı (saniye), dikey eksen kesme oranını göstermektedir. Şekil 2 ve Şekil 3'te istemcilerin ve web sunucusunun sadece IPv4 adresi kullandığı testin sonuçları gösterilmiştir. Test sonuçları,

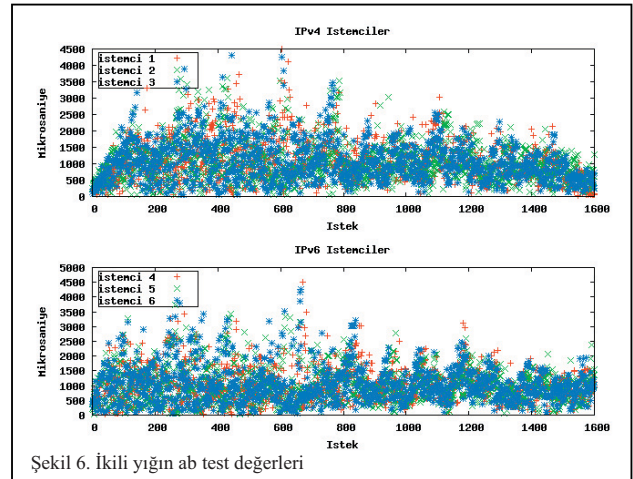
beklendiği gibi zamanla işlemci ve ethernet yükünün arttığını ortaya koymaktadır. Apache sunucusunun ise istek sayısı artışıyla birlikte cevap verme süresinin arttığı görülmektedir.

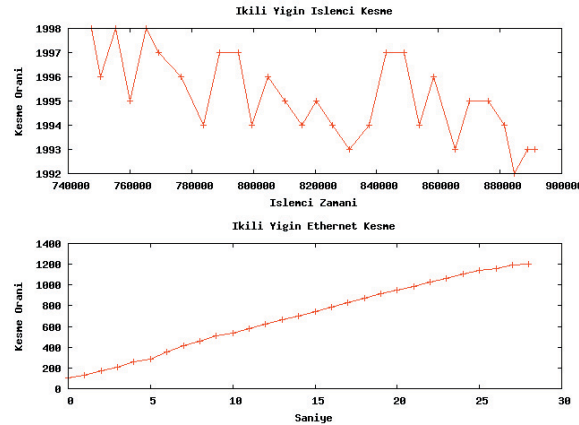


İstemcilerin ve sunucunun sadece IPv6 kullandığı test sonuçları Şekil 4 ve Şekil 5'te gösterilmiştir. Sadece IPv6 kullanıldığında Apache sunucusunun yaklaşık 750 isteğe kadar cevap verme süresi en çok 50 mikrosaniye seviyesinde iken sadece IPv4 ile 200 isteğe kadar bu seviyede kalabilmiştir. Genel olarak bakıldığında isteklere cevap süresi IPv6 ile daha az görünmektedir. Şekil 5'te gözlemlenen ethernet yükünün bir süre sonra hızla tırmanışı IPv6 paket sayısına bağlı olarak sunucunun performansındaki değişimi ortaya koymaktadır.

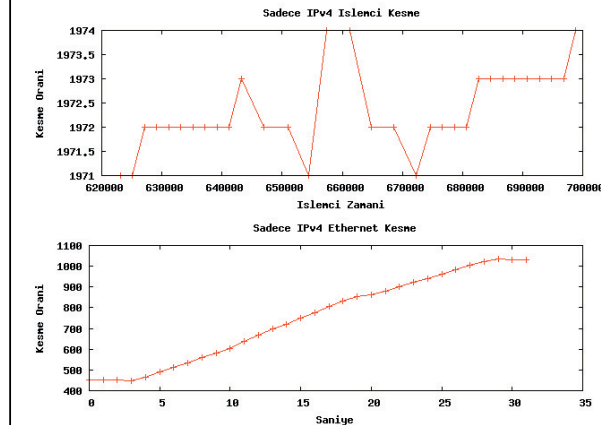


İkili yığın yapısı testleri Şekil 6 ve Şekil 7'de gösterilmiştir. Bir önceki testlerle kıyaslandığında Apache sunucusunun isteklere cevap verme süresinin artışı açıkça görülmektedir. Bu seviye 250-500 mikrosaniye seviyesinden 1500 mikrosaniye seviyesine kadar çıkmıştır. Buna paralel olarak ab testinin tamamlanma süresi 10-13 saniye seviyesinden 27-28 saniye seviyesine çıkmıştır. Bir diğer önemli nokta ise ethernet yükünün 10 kata kadar artması olmuştur. Bu süreçte işlemci yükü de gözle görülür artış göstermiştir.





Şekil 7. İkili yığın vmstat değerleri

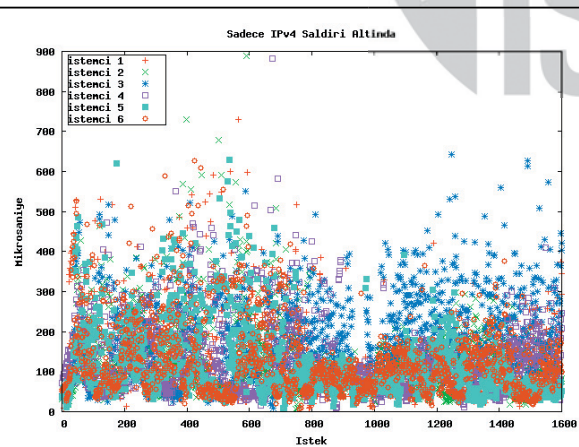


Şekil 9. Saldırı altında sadece IPv4 vmstat değerleri

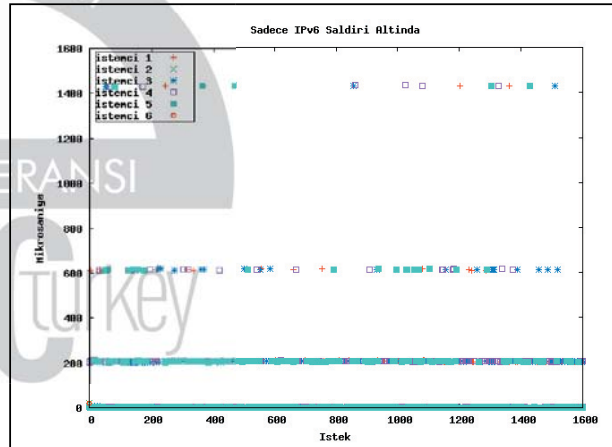
Saldırı Altında Test

Saldırı altında yapılan ölçümlerde pktgen [22] uygulaması kullanılmış ve normal durumda yapılan 3 test sırasıyla tekrarlanmıştır. Pktgen, Linux çekirdek seviyesinde çalışan bir paket üretici yazılımdır. Saldırı bilgisayarının sunucu üzerindeki etkisini arttırmak için donanımında istemci bilgisayarlardan farklı olarak PCI gigabit ağ kartı ve 1512 MB bellek kullanılmıştır. Saldırı bilgisayarı, sadece IPv4 kullanılan ortama IPv4 paketleri, sadece IPv6 kullanılan ortama IPv6 paketleri ile saldırmıştır. İkili yığın yapıya yapılan saldırılarda önce IPv4 sonra IPv6 paketleri kullanılmıştır.

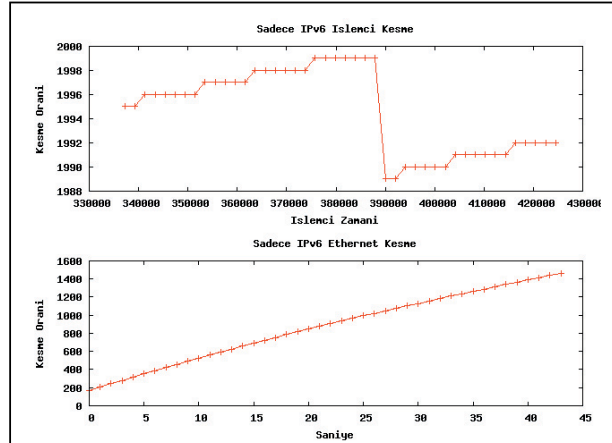
Şekil 8 ve Şekil 9'da saldırı altında sadece IPv4 kullanıldığı durum gösterilmiştir. Beklendiği gibi sunucu sistemin işlemci ve ethernet yükü normal duruma göre daha çok artmış ve buna paralel olarak Apache sunucusunun isteklere cevap verme süresi de artmıştır.



Şekil 8. Saldırı altında sadece IPv4 ab değerleri

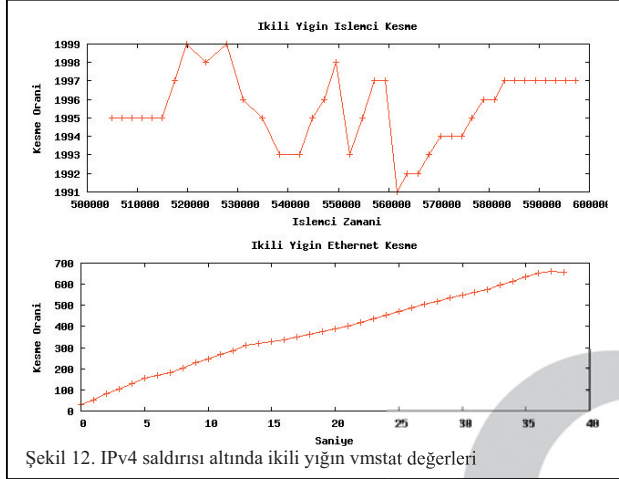


Şekil 10. Saldırı altında sadece IPv6 ab değerleri

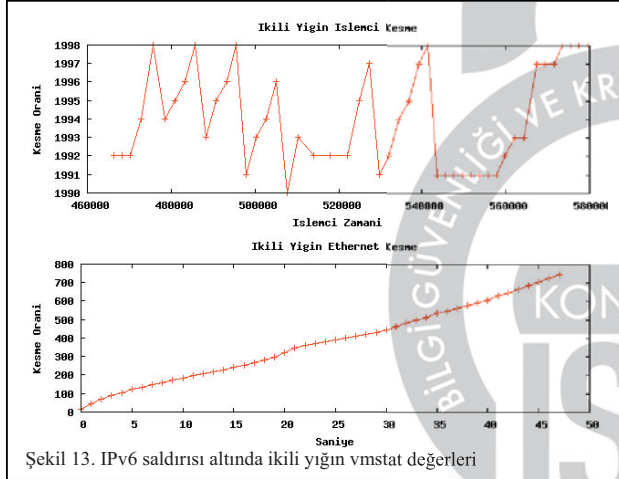


Şekil 11. Saldırı altında sadece IPv6 vmstat değerleri

İkili yığın yapıya önce IPv4 paketleri sonra IPv6 paketleri ile saldırılmıştır. İstemcilerin hiçbiri ab testini her iki durumda da tamamlayamamıştır. Şekil 12’de IPv4 paketleri ile saldırıldığında, Şekil 13’te ise IPv6 paketleri ile saldırıldığında sunucuda oluşan yük gösterilmiştir.



Şekil 12. IPv4 saldırısı altında ikili yığın vmstat değerleri



Şekil 13. IPv6 saldırısı altında ikili yığın vmstat değerleri

IV. SONUÇLAR

Bu makalede işletim sistemlerinde IPv4, IPv6 ve ikili yığın yapısında çalışan servislerin performansları ölçülmüştür. Servis performansının gözlenmesi için uygulama olarak Apache web sunucusu kullanılmıştır. Ayrıca, saldırı altında protokol yığını ve uygulama performansındaki değişim de incelemiştir.

Elde edilen bulgular iki başlık altında yorumlanabilir. İlki, IPv4, IPv6 ve ikili yığın yapısında çalışan servisler ve işletim sistemlerinin performans sonuçlarıdır. Araştırma bulguları düşük istek sayısında, IPv6’nın IPv4’e göre daha iyi bir performans gösterdiğini ortaya koymuştur. Bununla birlikte her iki protokolünde aynı anda desteklendiği ikili yığın yapı performansının sadece IPv6 veya sadece IPv4 kullanan

sistemlere göre oldukça düşük olduğu görülmektedir.

İkinci kısımda servis dışı bırakma saldırısının performans üzerine etkileri incelenmiştir. Elde edilen veriler ışığında, IPv6 kullanan sistemlerin IPv4 kullanan sistemlere göre servis engelleme saldırılarından daha çok etkilendiği görülmüştür. Bu durum ikili yığın yapıda çalışan bir sunucu için daha dramatik bir hal almakta ve sunucu servis veremez hale gelmektedir.

Elde edilen sonuçlar, IPv6 geçiş sürecinde ikili yığın yapılandırmasının performans problemleri yaşanmasına neden olacağını göstermiştir. Bu problemin çözümü için yüksek yük altında çalışan servislerin ikili yığın yerine yalın olarak IPv4 ve IPv6 desteği olan ayrı sunucularda çalıştırılması önerilebilir.

Bu konuda yapılacak ileriki çalışmalarda farklı işletim sistemlerindeki yığın performansının gözlenmesi için FreeBSD işletim sistemi ile birlikte Linux ve Windows işletim sistemleri de kullanılabilir. Ayrıca, Bind DNS, Windows IIS ve benzeri uygulamalar ile makale sonuçları farklı yapılandırmalarda test edilebilir.

KAYNAKLAR

- [1] RFC 2460, Internet Protocol, Version 6 (IPv6) Specification
- [2] IPv4 Address Report, “http://www.potaroo.net/tools/ipv4/index.html”
- [3] 6Net IP Deployment Guide <http://www.6net.org/book/deployment-guide.pdf>
- [4] Y. Wang, S. Ye, X. Li, “Understanding current IPv6 performance: a measurement study,” Proceedings. 10th IEEE Symposium on Computers and Communications, Cartagena, 2005, 71-76
- [5] Z. Zeadaly, I. Raicu, “Evaluating IPv6 on Windows and Solaris,” IEEE Internet Computing, vol 7, sayfa 51-57, Mayıs-Haziran. 2003
- [6] S. S. Mohamed, A. Y. M. Abusin, D. Chieng, “Evaluation of IPv6 and comparative study with different operating systems,” International Conference on Information Technology and Applications, vol 2, sayfa 665-670, Haziran. 2005
- [7] Y. N. Law, M. Lai, W. L. Tanand, W. C. Lau, “Empirical Performance of IPv6 vs. IPv4 under a Dual-Stack Environment,” IEEE International Conference on Communications, Beijing, 2008, 5924 – 5929
- [8] D. Zagar, K. Grgic, R. Snjezana, “Security aspects in IPv6 networks implementation and testing,” Computers and Electrical Engineering, vol. 4, sayfa 425-437, Eylül. 2007
- [9] Y. Xinyu, M. Ting, S. Yi, “Typical DoS/DDoS threats under IPv6,” Computing in the Global Information Technology, Guadeloupe, 2007, 55 – 61
- [10] H. Oh, K. Chae, H. Bang, J. Na, “Comparisons analysis of Security Vulnerabilities for Security Enforcement in IPv4/IPv6,” Advanced Communication Technology, vol 3, sayfa 1583 – 1585. Şubat. 2006
- [11] K. Elgoarany, M. Eltoweissy, “Security in mobile IPv6 a survey,” Information Security Tech. Report, vol 4, sayfa 32-43, Ocak. 2007
- [12] J. Kempf, J. Arkko, P. Nikander, “Mobile IPv6 security,” Wireless Personal Communication, vol 29, sayfa 389-414, 2004
- [13] J. Lim, Y. Kim, “Protection algorithm against security holes of IPv6 routing header,” Advanced Communication Technology, vol 13, sayfa 2004 -2007, Şubat. 2006
- [14] J. Arkko, T. Aura, J. Kempf, V. Mäntylä, P. Nikander, M. Roe, “Securing IPv6 neighbor and router discovery,” Proceedings of the 1st ACM workshop on Wireless security, Atlanta, 2002, 77-86
- [15] Netcraft, October 2008 Web Server Survey, http://news.netcraft.com/archives/web_server_survey.html
- [16] Apache MPM prefork, <http://httpd.apache.org/docs/2.0/mod/prefork.html>

- [17] Apache HTTP server benchmarking tool,
<http://httpd.apache.org/docs/2.0/programs/ab.html>
- [18] VMSTAT,
<http://www.freebsd.org/cgi/man.cgi?query=vmstat&manpath=FreeBSD+7.0-RELEASE>
- [19] Cluster SSH, <http://clusterssh.wiki.sourceforge.net/Main+Page>
- [20] Perl, <http://www.perl.org>
- [21] Gnuplot, <http://www.gnuplot.info>
- [22] R. Olsson, pktgen the linux packet generator, Linux Symposium 2005,
http://www.linuxsymposium.org/2005/linuxsymposium_procv2.pdf



Kablosuz Algılayıcı Ağlarda Güven ve Zaman Tabanlı Solucan Deliği Tespit Algoritması

Suat ÖZDEMİR¹, Majid MEGHDADI², İnan GÜLER³

Özet— Günümüzde Kablosuz Algılayıcı Ağ (KAA)'lar çok geniş uygulama alanları bulmaktadır. Kısıtlı kaynakları ve genelde dost olmayan ortamlarda kullanılmaları sebebiyle KAA'lar güvenlik açısından hassastırlar. Geleneksel güvenlik mekanizmalarının KAA'lara özgü güvenlik ataklarına karşı sağlayamadığı kanıtlanmıştır. Bu çalışmada ele alınarak çözüm getirilen solucan deliği (wormhole) saldırısı da bu ataklardan birisidir. Önerilen çözüm zaman tabanlı bir sistem olup, aynı zamanda yanlış bilgi veren kötücül düğümleri tespit edebilmek için bir güven mekanizması da içermektedir. Bilgilerimiz dahilinde, literatürdeki zaman tabanlı solucan deliği bulma mekanizmaları kötücül düğümlerin yanlış bilgi aktarmaları durumunda doğru sonuç verememektedirler. Bu problemi ortadan kaldırmak için, bu çalışmada zaman tabanlı bir sistem ile düğümler arasındaki güven/itibar ölçümünü yapabilen bir güven mekanizması birleştirilmiştir. Performans analiz sonuçları önerilen çözümün, solucan deliği saldırısı belirlemede literatürdeki zaman tabanlı sistemlere göre daha doğru sonuçlar verdiğini göstermektedir.

Anahtar Kelimeler— Kablosuz Algılayıcı Ağlar, Solucan Deliği Saldırısı, Güven Sistemleri.

Abstract— Wireless sensor networks (WSN) are being used in many application areas. As WSNs are deployed in hostile environments, security is an important issue for these networks. Traditional security mechanisms are not applicable against attacks in WSNs such as wormhole attack. In this paper, a time and trust based wormhole detection mechanism is proposed. To the best of our knowledge, existing wormhole attack detection protocols may fail when compromised nodes falsify routing information. The proposed technique combines a time based system with a trust based mechanism to detect compromised nodes that send false information. Performance analysis shows that the proposed technique is more effective than existing wormhole detection protocols.

Keywords— Wireless sensor networks (WSN)

I. GİRİŞ

Kablosuz Algılayıcı Ağ (KAA) kavramı ilk kez 1980'lerin başlarında karşımıza çıkmıştır. Mikro elektronik ve kablosuz haberleşme teknolojilerindeki gelişmeler küçük boyutlu, hareketli, düşük maliyetli, düşük enerji gereksinimli ve çok fonksiyonlu algılayıcı düğümlerinin yaygın olarak kullanılmasına olanak sağlamıştır [1]. Son yıllarda KAA'ları

çok geniş uygulama alanları bulmaktadır ve bu ağların kullanımı, ortam izleme, sağlık, askeri ve meteoroloji gibi birçok alanda yaygınlaşmaktadır. Bu tür ağlar temel olarak algılayıcılar ve bu algılayıcılardan gelen verileri toparlayan düğüm istasyonlarından oluşmaktadır. Algılayıcılar pil ile çalışan ve kısıtlı ömre sahip olan kablosuz iletişim cihazlarıdır [1], [2].

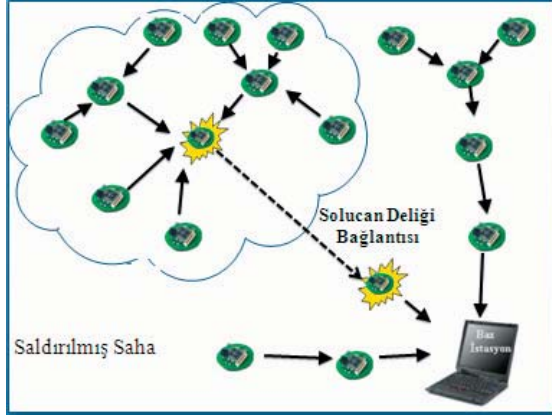
KAA'lar genelde dost olmayan kötücül ortamlarda kullanılmaları nedeniyle ağ güvenliği açısından hassastırlar. KAA'larda algılayıcılar bir işbirliği içerisinde çalışmaktadırlar. Dolayısıyla düğümler kendi aralarında sürekli iletişim halinde olmaktadır. Dışarıdan dinlenilmeye son derece açık olan bu tür sistemler güvenlik problemini de beraberinde getirmektedir. Yayın yoluyla yapılan haberleşme dışarıdan dinlenilmeye açık olup saldırıya karşı son derece zayıf bir altyapı sunmaktadır. Ayrıca KAA'lardaki algılayıcı elemanlar sınırlı bant genişliğinde bir iletişim becerisine, sınırlı bir işlemci gücüne, düşük kapasiteli bir hafızaya ve düşük enerjili bir bataryaya sahiptir. Dolayısıyla sınırlı kaynaklara sahip olan KAA yapılarında diğer ağ yapılarında kullanılan etkili güvenlik algoritmaları direkt olarak kullanılamamaktadır. Kaynakları kısıtlı algılayıcı düğümleri sebebiyle, literatürdeki araştırmalar geleneksel güvenlik mekanizmalarının KAA'larda çözüm sağlayamadığını ortaya koymuştur [3],[4]. Özellikle askeri ve sağlık uygulamaları gibi güvenlik yönünden hassas veri iletiminin yapıldığı KAA'larda veri gizliliğini ve bütünlüğünü sağlayacak güvenlik mekanizmalarına fazlasıyla ihtiyaç vardır. Daha da önemlisi, KAA'ların kendilerine has özellikleri sebebiyle bu güvenlik mekanizmaları sistem tasarımı aşamasında geliştirilmelidir. KAA'ların özgün yapısı geleneksel ağlarda görülmeyen birçok saldırı tipini ortaya çıkarmıştır. Bu çalışmada bu tür saldırılardan birisi olan solucan deliği saldırısı ele alınmış ve bu saldırıya karşı bir savunma mekanizması önerilmiştir.

Solucan deliği saldırısında iki kötücül düğüm birbirleri arasında yüksek iletişim kalitesine sahip bir kanal oluştururlar. Bu kanal bir kablolu ya da kablosuz ortam olabilir [2],[3]. Daha sonra yönlendirme için bu yüksek kaliteli kanalın reklamını yaparak çevredeki algılayıcılardan baz istasyonuna gönderilmek üzere veri toplarlar (Şekil 1). Amaç, toplanan bu verinin baz istasyonuna erişiminin engellenmesi ya da bozularak iletilmesidir. Bu sebeple baz istasyonu yakınındaki kötücül düğüm toplanan veriyi baz istasyonuna iletmeyebilir ya da verileri değiştirerek baz istasyonuna gönderebilir [5], [6]. Saldırı sonucunda ağın veri toplama performansı ve toplanan verinin doğruluğu/hassasiyeti azalır.

¹ Bilgisayar Mühendisliği Bölümü, Mühendislik Mimarlık Fakültesi, Gazi Üniversitesi, Ankara, Türkiye

² Bilgisayar Mühendisliği Bölümü Mühendislik Fakültesi, Zanjan Üniversitesi, Zanjan, İran

³ Elektronik-Bilgisayar Bölümü, Teknik Eğitim Fakültesi, Gazi Üniversitesi, Ankara, Türkiye
suatozdemir@gazi.edu.tr, meghdadi@mail.znu.ac.ir, iguler@gazi.edu.tr



Şekil 1. Solucan deliği (Wormhole) saldırısı - iki kötücül düğüm baz istasyonuna doğru yüksek kaliteli bir veri iletim hattının reklamını yaparlar ve veri toplarlar.

Bu makalede solucan deliği atağına karşı önerilen çözüm tabanlı bir sistem olup, aynı zamanda yanlış bilgi veren kötücül düğümleri tespit edebilmek için bir güven mekanizması da içermektedir. Literatürdeki zaman tabanlı solucan deliği bulma mekanizmaları kötücül düğümlerin yanlış bilgi aktarma ihtimallerini göz önüne almadıklarından saldırı tespit etkinlikleri düşüktür [7],[8]. Bu çalışmada zaman tabanlı bir sistem ile düğümler arasındaki güven ölçümünü yapabilen bir güven mekanizması ile birleştirilerek bu problem ortadan kaldırılmıştır. Yapılan performans analiz sonuçları önerilen çözümün, solucan deliği saldırısı belirlemede literatürdeki zaman tabanlı sistemlere göre daha doğru sonuçlar verdiğini göstermektedir.

Tablo 1. Solucan Deliği ile ilgili önemli çalışmalar.

	Yıl	Modelin Adı	Kullanılan Metot
Hu et al.[9]	2001	TIK	Paketlerin en çok iletimini sınırlamak
Capkun et al.[10]	2003	SECTOR	Her düğüm bir özel donanım ile teçhiz edilmek.
Wang et al.[11]	2004	MDS_VOW	Multi Dimensional Scaling algoritması, Dijkstra algoritması
Song et al.[12]	2005	SAM	Çoklu yol Yönlendirme (Multi Path Routing)
Pirzada et al. [13]	2005	Trust Base	Güven puanı, Komşuları izlemek
Ngai et al.[14]	2006		Bilgi Tutarlılığı, Şebekenin Akım Bilgisi Analizi
Yun et al.[15]	2007	WODEM	Sınırlı sayıda düğümleri yer bulma aygıtlara ve uzun ömürlü pil ile teçhiz etmek

II. İLGİLİ ÇALIŞMALAR

Tablo 1’de bu konuda bazı araştırmalar ve o çalışmalarda kullanılan metotlar gösterilmektedir.

Hu ve arkadaşları paketlerin en çok iletimini sınırlamak metodu ile solucan deliği saldırısına karşı bir yöntem oluşturmuşlardır [9]. Bu yöntemde düğümler komşularını sürekli izlemektedirler. Bu yöntemde fazla veri paketlere ekleme ile paketlerin adım sayısını ağda belirtir ve böylece paketlerin gittiği adımları ağda sınırlandırmışlar. Ayrıca paketlerin gönderildiği zaman ve gönderen düğümün yerini paketlere eklemiştirler. Böylece alıcı bu bilgileri incelemeye gelen paketlerin normal durumda gelip gelmediğini incelemektedir.

Solucan deliği saldırısına karşı, Capkun ve arkadaşları tarafından önerilen The Secure Tracking of Node Encounters in Multi-hop Wireless Networks (SECTOR) protokolü bir kaç metodun bir araya gelmesinden oluşmuştur [10]. SECTOR hiçbir saat senkronizasyonu veya konum bilgisine gerek duymaz ve düğümlerin uzaklığını bulmak için MAD (Mutual Authentication with Distance-bounding) protokolünü kullanır. MAD protokolünde her düğüm bir özel donanım ile teçhiz edilmiştir. MAD protokolü paketlerin bütünlüğünden emin olmak için Hash-Tree ve One-Way-Hash zincirinden yararlanır. Mesajları doğrulamak için MAC (Message Authentication Code) ’den yararlanır. KAA’larda düğüm sayısı pek çok olduktan, düğümlerde kullanan donanım bu metot için bir dezavantajdır.

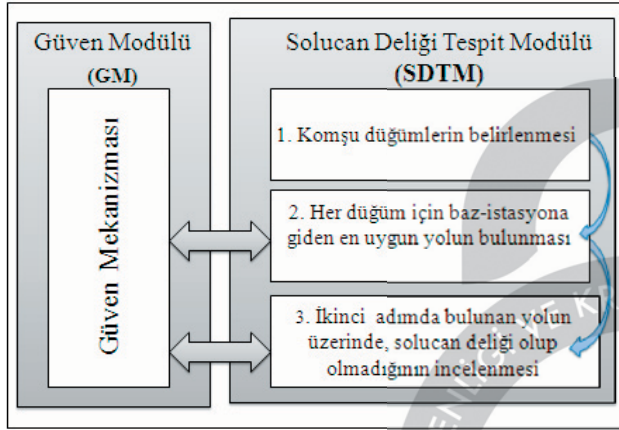
Solucan deliği saldırısına karşı, Wang ve arkadaşları Multi Dimensional Scaling Visualization of Wormhole (MDS_VOW) adlı mekanizma yardımıyla, bir çözüm sunmuşlardır [11]. Bu çalışmada her düğüm komşularından gelen sinyal gücünü ölçüp, uzaklığını onlardan tahmin ederken bu uzaklıkları baz istasyona gönderir. Daha sonra baz istasyonda Dijkstra algoritması [16] yardımı ile tüm düğümlerin komşularından uzaklığı hesaplanır. Baz istasyon MSD algoritmasını kullanarak düğümlerin gerçek konumlarını bulmaya çalışıp bir düzleme (Smoothing) fonksiyonu kullanarak hataları hesaplar. Eğer elde edilen harita düz olursa şebekede solucan deliği saldırısı bulunmamaktadır ama eğer iki düğüm arasındaki yüzey (surface) eğri olursa solucan deliği saldırısının olduğunu gösterir. Bu durumda baz istasyon, solucan deliği saldırısının uzaklığını başka düğümlerden hesaplar ve böylece kötücül düğümün konumunu belirttikten sonra normal düğümler kötücül düğümlerle iletişim kurmazlar.

Ngai ve arkadaşları solucan deliği saldırısına karşı bir algoritma geliştirmişlerdir [14]. Bu algorithmada her bir düğümün farklı bir tanımlayıcı ID numarasına sahip olduğu farz edilmiştir. Algoritma iki aşamadan oluşur. Birinci aşamada veri tutarlılığı (Data Consistency) yardımıyla, şüpheli düğümlerin listesini bulunur hale getirilir. İkinci adımda, Ağ Akım Bilgisinin (Network Flow Information) analizini yardımıyla bu listeden kötüsel kişiler bulunur. Algoritma kötücül düğümlerin sayısının birden fazla olduğu ya da işbirliği yapan kötücül düğümlerin bulunduğu durumlarda da başarılı olarak çalışabilmektedir.

[15]'te Yun ve arkadaşları solucan deliği saldırısına karşı bir algoritma geliştirmişlerdir. Bu çalışmada sınırlı sayıda özel algılayıcı düğümünün yer bulma aygıtlarına sahip oldukları kabul edilmiştir. Ayrıca bu düğümlerin pillerinin normal düğümlere göre daha uzun ömürlü oldukları kabul edilmiştir. Simülasyon sonuçları, yaklaşık 400 düğümlü bir algılayıcı ağda 10 tane yer bulma aygıtına sahip düğüm bulunduğunda, solucan deliği saldırılarının %90 oranında tespit edilebildiğini göstermiştir.

III. ÖNERİLEN YÖNTEM

Bu çalışmada önerilen çözüm paralel çalışan iki modülden oluşmaktadır: "Güven Modülü (GM)" ve "solucan deliği Tespit Modülü (SDTM)". Sistem yapısı Şekil 2 de gösterilmiştir. SDTM üç aşamadan oluşmaktadır.



Şekil 2. Önerilen çözümün sistem yapısı

Bu modülün birinci adımında, her düğüm için komşu düğümler belirtilmektedir. İkinci adımda ise her düğüm için baz istasyona giden en uygun yol bulunmaktadır. Üçüncü adımda, baz istasyona giden yollar üzerinde solucan deliği olup olmadığını incelenmektedir. Ancak, yol üzerindeki kötücül düğümler yanlış bilgi vererek SDTM'yi yanıltıp solucan deliği saldırısının tespitini önleyebilirler. Bunu engellemek için GM sürekli SDTM'nin ikinci ve üçüncü aşamasını gözlemleyerek, baz-istasyona giden yollar üzerindeki düğümler için güven/itibar değerleri hesaplar. Bu güven/itibar değerlerini kullanarak solucan deliği saldırısı ihtimali olan yolların değiştirilmesini sağlar.

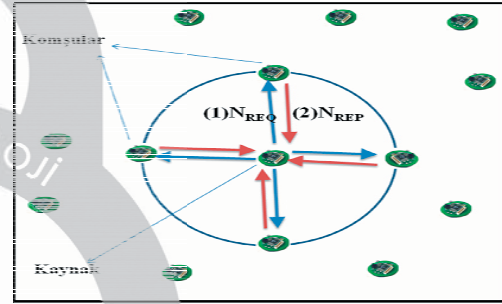
A. Komşu düğümlerin belirlenmesi

Bu aşamada her düğüm N_{REQ} - Neighbor Request adlı özel bir mesajı tüm komşularına gönderir. N_{REQ} mesajını alan bütün komşu düğümler, bu mesajın cevap olarak N_{REP} - Neighbor Reply mesajını gönderir. N_{REQ} mesajını gönderen düğüm N_{REP} mesajları aldıktan sonra komşularını tanıır ve bunlarla bir çizelge oluşturur ve komşuların sayısı belirtilir. Örneğin şekil 3'teki düğüm, 4 tane N_{REP} aldıktan dolayı 4 tane komsusu olduğunu fark etmektedir. Bu çalışmada bu sayı N ile adlandırılmış.

B. Baz-istasyona giden en uygun yolun bulunması

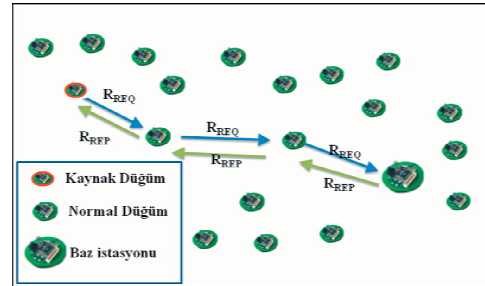
Bu aşamada her düğüm kendisi ile baz istasyon arasındaki en kısa yolu bulmaktadır. Bu işlemi yapabilmek için her düğüm Yol Bulma (R_{REQ} - Route Request) paketi tüm komşularına gönderir ve bu mesajın gönderilme zamanını kayıt eder (T_{REQ} -Time of Request). Bu paketi alan komşular bu paketi sonraki düğüme gönderir ve onlarda bu paketi gönderme zamanını kayıt ederler. Böylece bu paket ağda yayılır ve sonunda bu paket baz istasyona ulaşır. Baz istasyonu bu paket aldıktan sonra Yol Yanıtı (R_{REP} - Route Reply) paketi ile R_{REQ} paketini gönderen düğümü yanıtlar. Bu paket, kaynaktan baz istasyona kadar tüm bulunan düğümleri içermektedir. Bu paket her düğüme vardığında o paketin yanıt zamanını (T_{REP} -Time of Reply) kayıt eder. Her düğümde bu paketin gidiş dönüş zamanlarının farkı (RTT - Round Trip Time) kayıt edilir. RTT değeri aşağıdaki formül ile hesaplanmaktadır.

$$RTT = T_{REP} - T_{REQ} \quad (1)$$

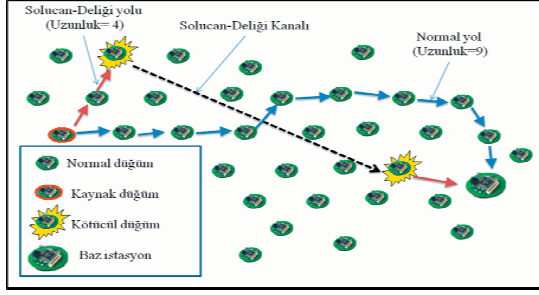


Şekil 3. Komşu düğümlerin belirlenmesi

Tüm aradaki düğümler RTT bilgisini hesapladıktan sonra baz istasyona göndermektedirler. R_{REP} paketinin kaynağa ulaşması baz istasyonu ile kaynak arasında bir yol oluşturduğu anlamına gelir (Şekil 4). Baz istasyonu gelen her R_{REQ} mesajını yanıtladığı için, kaynak, gelen R_{REP} mesajlarının RTT değerlerini inceledikten sonra baz istasyonu ile arasındaki en kısa yolu seçmektedir. Şekil 5'te gösterildiği gibi yol seçimi yapılırken kötücül daha kıs bir yolun reklamını yaparak solucan deliği saldırısı gerçekleştirebilirler ve paket iletimini engelleyebilir ya da içeriklerini değiştirebilirler. SDTM'nin üçüncü basamağı bu saldırıları tespit eder.



Şekil 4. Yol Bulma paketleri



Şekil 5. KAA’larda bir solucan deliği saldırısı

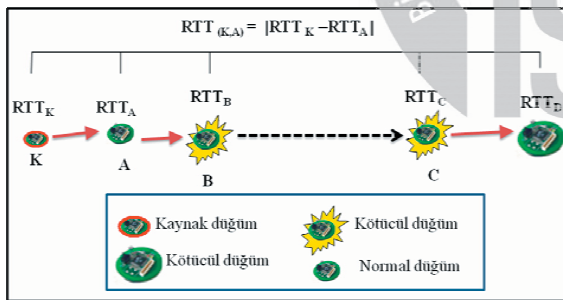
C. Solucan deliği saldırılarının tespiti

Bu aşamada kaynak düğüm, yoldaki bütün düğümlerin gönderdiği RTT değerlerini inceleyip bu yolda solucan deliği saldırısı olup olmadığını anlamaktadır. Bu işlemi yapabilmek için yol üzerindeki her iki ardışık düğümün arasındaki RTT farkından faydalanılır. Normal düğümle için bu fark bir eşik (threshold) değerden fazla olmaması gerekir. İki ardışık düğüm **A** ve **B** arasındaki RTT farkı ($RTT_{(A,B)}$) Formül 2 ile tanımlanmaktadır [13].

$$RTT_{(A,B)} = |RTT_A - RTT_B| \quad (\mathbf{A, B} \text{ ardışık düğümler}) \quad (2)$$

$RTT_{(A,B)}$ = Paketlerin **A** düğümünden **B** düğümüne ulaşma zamanı

Eğer iki ardışık düğümün RTT farkları başka düğümler arasındaki RTT farkından çok fazlaysa, bu solucan deliği saldırısının bir göstergesidir. Kötücul düğümler arasındaki mesafe uzun olduğundan, kötücul düğümler arasındaki RTT farkı diğer düğümlere göre fazla olacaktır. Şekil 6’daki örnekte görüldüğü gibi $RTT_{(B,C)}$, yol üzerindeki başka RTT ’lere göre çok daha büyüktür, çünkü **B**, **C** düğümleri arasındaki mesafe diğer düğümler arasındaki mesafelerden daha uzundur.



Şekil 6. RTT değerlerinin farkı iki normal düğüm ve iki kötücul düğüm arasında

Önerilen zaman tabanlı solucan deliği bulma mekanizması, kötücul düğümler arasındaki paket iletim zamanından yararlanmaktadır. Eğer iki düğüm arasındaki paket iletim zamanı bir belli eşikten fazlaysa bu bir anomali demektir. Bu durumda kötücul düğümler eğer kaynağa yanlış bilgi iletseler zaman tabanlı algoritma her zaman doğru sonuca varamaz. Bu problemi ortadan kaldırabilmek için, bu çalışmada zaman tabanlı bir modül ile düğümler arasındaki güven (itibar) tahmin edebilen, güven mekanizması ile bileştirilmiştir ve

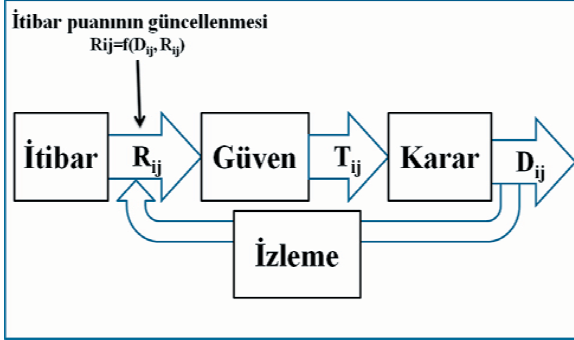
böylece solucan deliği saldırıları daha yüksek performansta bulunabilmektedir. Bu işlemi yapabilmek için bir izleme modülü tasarlanmıştır. Bu modül bir Güven mekanizmasını içermektedir. Bu bölümün devamında bu mekanizma anlatılmaktadır.

Tablo2. Kullanılan simgeler ve açıklamaları

Simge	Açıklama
RTT	Paketin gediş dönüş zamanı (Round Trip Time)
T_{REP}	Paketin yanıt zamanı (Time of Reply)
T_{REQ}	Paketin gönderme zamanı (Time of Request)
R_{REQ}	Yol bulma Paketi(Route Request Packet)
R_{REP}	Yol Yanıt Paketi (Route Reply Packet)
R_{ij}	j’inci komşuya i’inci düğümün verdiği itibar Puanı $0 \leq R_{ij} \leq 1$
D_{ij}	j’inci komşuya i’inci düğümün verdiği en son Karar $K_{ij}=0$ yada $K_{ij}=1$
T_{ij}	j’inci komşuya i’inci Düğümün güven puanı $0 \leq T_{ij} \leq 1$
f()	f fonksiyonu R_{ij} değerini güncellemektedir
θ	Gelecek iletişimin başarı olma ihtimali
α_{ij}	j’inci komşuya i’inci düğüm gönderen paketlerin başarılı olan paketlerin sayısı
β_{ij}	j’inci komşuya i’inci düğüm gönderen paketlerin başarısız olan paketlerin sayısı

D. Güven Mekanizması

Eğer kötücul düğümler yanlış bilgi göndermezler, SDTM’nin üçüncü aşamasında ağda solucan deliğinin olup olmadığı kolayca anlaşılmaktadır. Ancak kötücul düğümler tarafından paketlerdeki RTT değerleri, değiştirilirse ve yanlış değerler kaynağa ulaşırsa, SDTM’nin performansı azaltılmaktadır. GM her düğümde sürekli çalışmaktadır. GM çalışırken komşulardan alınan RTT değerleri, beklenen eşik değeri ile karşılaştırılıp ve her komşuya bir güven/itibar (Reputation) puanı (R_{ij} = j’inci komşuya i’inci düğüm tarafından verilen güven/itibar puanı) verilmektedir. Bu bölümde kullanılan simgeler ve açıklamaları Tablo2’de verilmiştir). Güven puanı zaman içerisinde değiştirilmektedir. Başlangıçta tüm düğümler için 0.5 değeri alan güven puanı kötücul düğümlerin gönderdikleri her eşik değere göre yanlış RTT için beta dağılımına göre düşürülür (beta dağılımı birazdan açıklanacaktır). Güven puanının 1 değerini alması “güvenin tam olması” anlamındadır. Başka söyleyişle bir paketi bu komşu aracı ile göndermek güvenilirdir ve bu yolda solucan deliği saldırısı olma ihtimali küçüktür. Güven puanının sıfır olması “asla bu komşu güvenilir değil” anlamındadır. Başka söyleyişle bir paketi bu komşu aracı ile göndermek güvenilir değildir ve bu yolda saldırı olma ihtimali yüksektir. GM ile komşular sürekli izlenir ve güven/itibar puanları sürekli güncellenir (Şekil 7).



Şekil 7. Güven modülünde itibar puanı güncellenmesi

Şekil 7’de görüldüğü gibi R_{ij} izlemenin sonuçlarına göre sürekli güncellenmektedir (Formül 3). Güven puanı (T_{ij}), itibar puanının (R_{ij}) beklenen değeridir (Formül 4).

$$R_{ij} = f(D_{ij}, R_{ij}) \quad (3)$$

$$T_{ij} = E(R_{ij}) \quad (4)$$

Güven modellerini ifade etmek için birçok matematiksel dağılımdan yararlanabiliriz. Örneğin, Beta, Gaussian, Poisson, Binomial dağılımları vb. Bu çalışmada söz ettiğimiz dağılımlardan esnekli ve kolaylık göz önüne alınarak Beta dağılımı seçilmiştir. Beta dağılımı iki parametre ile (α, β) ifade edilir (Formül 5) [13].

$$P(x) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha) \times \Gamma(\beta)} x^{\alpha-1} \times (1-x)^{\beta-1} \quad (5)$$

$$\forall 0 \leq x \leq 1, \alpha \geq 0, \beta \geq 0$$

Bu çalışmada beta dağılımından yararlanmak için α başarılı olan iletişimleri ve β başarısız olan iletişimleri ifade etmektedir. Şimdiye kadar $n+m$ paket gönderildiğini farz edelim. Başarılı olan iletişimlerin sayısı n ve başarısız olan iletişimlerin sayısı m olsun. Sonraki iletişimde başarılı bir iletişim olma ihtimali (θ) ne kadardır? Geçmişten bir bilgi olmazsa θ bir uniform dağılım olmalıdır ($0 \leq \theta \leq 1$). Bu nedenle $P(\theta) = \text{uni}(0,1) = \text{beta}(1,1)$ denilebilir. Buna göre gelecek seferdeki iletişimde başarılı olma ihtimalini Formül 6 gibi yazabiliriz [13].

$$P(\theta) = \frac{\text{Bin}(m+n, m) * \text{Beta}(1,1)}{\text{Normalizasyon}} = \text{Beta}(m+1, n+1) \quad (6)$$

Formül 6 gösteriyor ki θ ’nin gelecekteki dağılımı beta dağılımı olabilir. R_{ij} (i’inci düğümün j’inci düğüm için hesapladığı itibar değeri) beta dağılımı yardımıyla Formül 7 deki gibi yazılmaktadır.

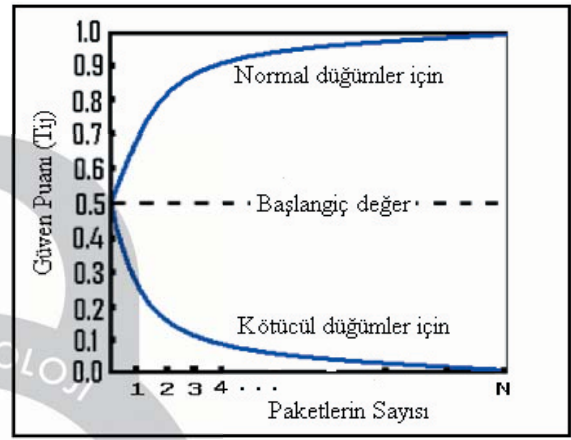
$$R_{ij} = \text{Beta}(\alpha_{ij} + 1, \beta_{ij} + 1) \quad (7)$$

Eğer daha önceden hiçbir bilgi olmazsa $\alpha_{ij} = \beta_{ij} = 0$ olmalıdır. Bu nedenle görüldüğü gibi $R_{ij} = \text{uni}(0,1)$ olmalıdır.

$$R_{ij} = \text{Beta}(\alpha_{ij} + 1, \beta_{ij} + 1) = \text{Beta}(1,1) = \text{uni}(0,1) \quad (8)$$

Güven (T_{ij}), itibarın (R_{ij}) istatistiksel olarak beklenen değeridir ve şöyle ifade edilebilir [13].

$$T_{ij} = E(R_{ij}) = E(\text{Beta}(\alpha_{ij} + 1, \beta_{ij} + 1)) = \frac{\alpha_{ij} + 1}{\alpha_{ij} + \beta_{ij} + 2} \quad (9)$$



Şekil 8. Güven puanının değiştirilmesi

Eğer bir düğümün komşusu tüm paketlerin iletilmesine tam yardım ederse (yolda saldırı olmama durumunda) ve RTT değerlerini belirlenen eşik değerine yakın verirse bu komşu düğümün güven puanı en sonunda bir olmaktadır. Başka söyleyişle paketlerin gönderildiği yolda kötücül düğüm bulunmamaktadır. Aksi takdirde eğer bir komşu asla paketlerin iletimi için yardım etmezse, güven puanı sıfır olmaktadır. Şekil 8’de görüldüğü gibi güven puanının başlangıç değeri tüm komşulara 0.5 tir. Sistem çalıştıktan sonra bu puan her komşu için değiştirilmektedir.

GM modülü tarafından üretilen güven puanlarından faydalanılarak, SDTM’nin üçüncü adımında kötücül düğümlerin yanlış bilgi verdiği durumlarda da solucan deliği saldırıları tespit edilebilmektedir. Paket gönderiminde rol alan bütün düğümler periyodik olarak komşularını gözlemler ve onlara ait güven puanlarını hesaplar.. Her düğüm kendi komşularının güven puanlarını ve RTT değerleri inceler, eğer RTT değerlerinde herhangi bir anormallik varsa o komşuya ait güven puanını düşürür. Böylece her düğüm komşularının solucan deliği saldırısında yer alıp almadığını tahmin etmeye çalışır. Eğer bir düğümün güven puanı 1’e yaklaşıyorsa solucan deliği saldırısında yer alma ihtimali 0’a yaklaşmaktadır. Güven puanlarına göre solucan deliği saldırısında bulunduğu düşünülen düğümler paket gönderiminde kullanılmaz ve böylece paketlerin baz istasyona ulaşma olasılığı artırılır.

IV. SONUÇ VE GELECEK ÇALIŞMALAR

Bu çalışmada KAA'larda solucan deliği saldırısı ele alınmış ve bu saldırıya karşı bir savunma mekanizması önerilmiştir. Önerilen çözüm zaman tabanlı bir sistem olup, aynı zamanda yanlış bilgi veren kötücül düğümleri tespit edebilmek için bir güven mekanizması da kullanılmaktadır. Önerilen savunma mekanizmasının tasarım aşaması bitmiştir ve şuan itibarı ile ns2 ağ simülatörü [17] kullanılarak gerçekleştirilmektedir. GM ve SDTM'nin detayları ve önerilen savunma mekanizmasının gerçekleştirilmesinden elde edilecek sonuçlar bu bildirinin genişletilmiş versiyonunda yer alacaktır.

KAYNAKLAR

- [1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine vol.40 , no.8 pp.102-114. , 2002.
- [2] M. Meghdadi, S. Özdemir, İ. Güler, "Security in Wireless Sensor Networks: Problems and Solutions" (Manuscript in Turkish), Journal of Informatics Technologies , Gazi University, Ankara, Turkey , vol. 1, no.1, pp. 35-42, 2008.
- [3] C. Ceken. "An Energy Efficient and Delay Sensitive Centralized MAC Protocol for Wireless Sensor Networks", Computer Standards & Interfaces, vol.30, no.1-2, pp. 20-31, 2008.
- [4] M. Meghdadi, S. Özdemir, İ. Güler, "An Algorithm for Defending Black-Hole Attacks in Wireless Sensor Networks", (Manuscript in Turkish), in Proc. of HABTEKUS 08, Istanbul, Turkey, pp. 71-76, October 22-24, 2008.
- [5] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September, pp. 293-315, 2003.
- [6] S. S., Kulkarni, M. G., Gouda, A. Arora, "Secret instantiation in adhoc networks", Special Issue of Elsevier Journal of Computer Communications on Dependable Wireless Sensor Networks, pp.1-15, 2005.
- [7] T. V. Phuong, L. X. Hung, Y. K. Lee, S. Lee, H. Lee, "TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks", 4th IEEE Consumer Communications and Networking Conference , pp. 593-598, 2007.
- [8] T. V. Phuong, N. T. Canh, Y. K. Lee, S. Lee, H. Lee, "Transmission Time-Based Mechanism to Detect Wormhole Attacks", Proceedings of the The 2nd IEEE Asia-Pacific Service Computing Conference pp.172-178, 2007.
- [9] Y. C. Hu, A. Perrig, D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE, vol.3 no.1, pp.1976-1986, 2001.
- [10] S. Capkun, L. Buttyan, J. Hubaux, "Sector: secure tracking of node encounters in multi-hop wireless networks" Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks, vol.1, no.1 pp 1-11, 2003.
- [11] Wang, X., Gu, W., Schosek, K. Chellappan, S. Xuan, D. "Sensor network configuration under physical attacks". Technical Report Technical Report (OSU-CISRC-7/04-TR45), 2004.
- [12] Song, N., Qian, L. and Li, X., "Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach", Proceedings. 19th IEEE International Parallel and Distributed Processing Symposium, vol. 1, no. 1 pp. 1-11, 2005.
- [13] A. Pirzada, C. McDonald, "Circumventing Sinkholes and Wormholes in Wireless Sensor Networks", International Workshop on Wireless Ad-hoc Networks, 2005.
- [14] E. C. H. Ngai, J. Liu, M. R. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor Networks", ACM Transaction on Sensor Networks, Vol. V, No. N, 2007.
- [15] J. H. Yun, I. H. Kim, J. H. Lim, S. W. Seo, "WODEM: Wormhole Attack Defense Mechanism in Wireless Sensor Networks" book chapter in Lecture Notes in Computer Science, vol. 4412 pp. 200-209, 2007.
- [16] E. W. Dijkstra, "A note on two problems in connection with graphs", Numerische Mathematik, vol. 1, no. 1, pp.83-89, 1959.
- [17] S. McCanne and S. Floyd. ns-Network Simulator. Available at: <http://www.isi.edu/nsnam/ns/>

Güvenlik Penceresinden IPv4/IPv6 Karşılaştırılması

Şeref SAĞIROĞLU, Onur BEKTAŞ, Murat SOYSAL

Özet—IPv4'ün yerini almak için tasarlanmış olan IPv6 yakın bir gelecekte internete bağlanmak için yeni standart olacaktır. IP adreslerinin dağıtımından sorumlu kurumların IPv4 adres aralığının bitiş tarihinin 2010 yılı sonlarına doğru olacağını tahmin etmeleri IPv6'ya geçiş çalışmalarının son yıllarda tüm ülkelerde ivmelenmesine neden olmuştur. IPv6'nın IPv4'te desteği sorunlu olan adres kapasitesi, çoklu dağıtım, servis kalitesi ve dolaşılabilirlik problemlerine çözüm olacağı öngörülmektedir. IPv6'nın bu özellikleri yanında ön plana çıkarılan diğer bir özelliği de IPv4'e göre güvenlik konusunda getirdiği yeniliklerdir. IPv6 ile birlikte IPv4'te seçimlik olan IPsec desteğini zorunlu tutulması, adreslenebilecek uç sayısının artırılması, başlık yapısının sadeleştirilmesi, ara düğümlerde paket parçalanmasına izin vermemesi benzeri iyileştirmelerinin yapılması yeni nesil internet protokolünün daha güvenli olarak sunulmasını sağlamıştır. Bununla birlikte henüz geliştirilme ve deneme aşamasında olan IPv6'nın kullanım oranının çok yüksek olamaması, protokolün internetin güvenliğine yapacağı katkı ve yaratacağı muhtemel güvenlik riskleri konularında ki belirsizliği henüz kaldıramamıştır. Bu makalede ilk olarak IPv4'te karşılaşılan güvenlik riskleri ve saldırı türlerinin IPv6 kullanımı ile birlikte durumları incelenecek ve daha sonra IPv6 kullanımı ile ortaya çıkabilecek IPv6'ya özel güvenlik problemlerini konusunda bilgi verilecektir.

Anahtar Kelimeler —IPv4, IPv6, IPv6 Güvenliği, Gezinir IPv6, IPv6 Saldırı Türleri

Abstract— IPv6 is expected to become the new standard for Internet connection in the forthcoming years. There is a transition progress all over the world towards the IPv6 since IPv4 address space is expected to be exhausted by the end of 2010. IPv6 brings many improvement opportunities in terms of address space, auto configuration, quality of service, routing speed, mobility and security. In comparison to IPv4, IPv6 was designed with security in mind and offers many improvements on network layer security. Despite these improvements, IPv6 is not widely deployed yet and still in the phase of development and early integration. As a result, IPv6 security features are not extensively tested in real environments and it is likely that IPv6 usage in operational networks may pose risks and introduce potential vulnerabilities in addition to those experienced in IPv4 networks.

Ş. Sağiroğlu, Gazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Maltepe, Ankara.

Telefon/fax: 312-2306503; E-posta: ss@gazi.edu.tr

O. Bektaş TÜBİTAK Ulusal Akademik Ağ ve Bilgi Merkezinde uzman araştırmacı olarak çalışmaktadır. Telefon: 312-2989367; faks 312-2989393; E-posta: onur@ulakbim.gov.tr

M. Soysal TÜBİTAK Ulusal Akademik Ağ ve Bilgi Merkezinde uzman araştırmacı olarak çalışmaktadır. Telefon: 312-2989310; faks: 312-2989393; E-posta: msoysal@ulakbim.gov.tr

This paper analyses the major security threads in IPv6 networks in two categories. First part focuses on the attacks which are common to both protocols. Second part examines types of attacks that will change in IPv6 networks and security threads which are IPv6 specific.

Keywords —IPv4, IPv6, IPv6 Security, Mobile IPv6

I. GİRİŞ

İNTERNETİN temel protokolü olan IPv4 25 yıldan daha uzun süredir kullanılmaktadır. IPv4, tasarımının yapıldığı 80'li yıllardan günümüze kadar teknolojinin getirdiği gereksinimler doğrultusunda yapılan eklentiler ile günün ihtiyaçlarını karşılar hale getirilmeye çalışılmıştır. 1990'lı yılların başından itibaren IETF (Internet Engineering Task Force) tarafından IPv4'ün internetin gelişimde engel oluşturmaması için yerini alacak yeni bir protokole ihtiyaç duyulduğu uyarıları yapılmış ve çalışmalar başlatılmıştır [1]. Çalışmaları yeni nesil IP protokolü (Next Generation IP, IPng) ismi altında başlayan IPv6 ile ilgili temel tanımlarını içeren RFC 2460 [2] 1998 yılında yayınlanmıştır.

IPv6'nın çıkış noktası internet protokolünün günün ihtiyaçlarının karşılayacak şekilde yenilenmesidir. Günümüze internetin geldiği noktada IPv4 geliştiricilerinin öngöremediği gereksinimlerin ortaya çıkması IPv6'ya olan ihtiyacı tetiklemektedir. IPv6, adres kapasitesi artırımı, çoklu dağıtım, servis kalitesi, dolaşılabilirlik gibi IPv4 ile sağlanması güç olan teknolojilerin çözümlerini içeren yapısı ile günümüz ihtiyaçları ve yeni nesil internet uygulamalarının gereksinimleri karşılayacak şekilde tasarlanmıştır. Uzun süredir kullanımda olan IPv4 adreslerinin 2010 yılı sonlarına doğru tükeneceği hesaplanmaktadır [3]. IPv4 adreslerinin dağıtımını sırasında Amerika'nın protokolü geliştiren ülke olması nedeni ile elde ettiği avantaj adreslerin dünya ülkelerinde eşit dağıtılmamasına neden olmuştur [4]. Bunun sonucunda özellikle Uzak Doğu ülkelerinde IPv4 adres sıkıntısı oluşmuş ve IPv6 geçişi ile ilgili çalışmalar Uzakdoğu ülkelerinde Amerika ve Avrupa'ya göre daha önce başlamıştır. Tüm dünyada IPv4'den IPv6'ya geçiş için yapılan çalışmalarda IPv6'nın yeni nesil teknolojilerin uygulanmasında sağladığı kolaylıklar yanında IPv6'nın güvenlik özellikleri geçiş nedenlerinden bir olarak öngörülmektedir.

İnternette en çok karşılaşılan saldırılar OSI referans modeli uygulama seviyesi saldırılardır. Buna karşın ağ katmanında ki

saldırıların karşı önlemlerinin alınması, fark edilmeleri ve engellenmeleri çok daha güç olabilmektedir. Ağ katmanı güvenliğinde yaşanacak sorunlar dünya çapında servis kesintilerine neden olabilecek seviyede yaygınlığa ve tüm haberleşmenin kesintiye uğraması, dinlenmesi, sahte bir hedefe yönlendirilmesi benzeri durumlar ile sonuçlanabilecek güvenlik risklerinin oluşmasına neden olabilir.

Bir ağ seviyesi protokolü olan IPv6'nın güvenliği ile ilgili olarak literatürde birçok çalışma mevcuttur [8], [12], [16], [18], [25], [26], [27], [29], [30]. Yapılan araştırmalar iki grup altında toplanabilir. İlk grupta IPv4 ağlarındaki mevcut güvenlik risklerinin (solucan dağılımı, ortadaki adam saldırısı vb) IPv6 ağlarındaki durumu incelenmiştir. İkinci grupta IPv6'nın IPv4'ten farklı olan adres yapısı, dolaşılabilirlik, ek-başlık desteği gibi özelliklerin güvenliği irdelenmiştir.

IPv6 kullanımı ile birlikte ağ seviyesi saldırılarının güvenlik riskleri analiz edildiğinde yeni bir protokole geçilmesinin bir sonucu olarak IPv4'e göre farklılıklar olduğu gözlenmektedir. Mevcut güvenlik riskleri ve saldırıların incelendiğinde bazı saldırı türlerinin IPv6 ile gerçekleştirilme zorluklarının arttığı ve bazılarının da azaldığı görülmektedir. IPv6 güvenlik açısından değerlendirildiğinde özellikle dolaşılabilirlik ve yerel ağda IPv6 kullanımında potansiyel güvenlik risklerinin olabileceği öngörülmüştür.

Bu çalışmanın sunuş sırası şu şekildedir. IPv4 ve IPv6 arasında benzerlik gösterilen güvenlik riskleri Bölüm 2'de irdelenmiştir. IPv6'nın kullanılması ile birlikte IPv6'ya özel hangi güvenlik riskleri ile karşı karşıya kalılabileceği Bölüm 3'de açıklanmıştır. İki protokol arasında güvenlik risklerin karşılaştırması Bölüm 4'de sunulmuştur. Son bölümde (Bölüm 5) ise çalışma genel olarak değerlendirilmiş ve öneriler sunulmuştur.

II. IPV4 VE IPV6 İÇİN BENZERLİK GÖSTEREN BAZI GÜVENLİK RİSKLERİ

IPv4 ve IPv6 güvenlik riskleri açısından değerlendirildiğinde paket koklamak, taşıma saldırısı, ortadaki adam saldırısı ve uygulama seviyesi saldırıları karşılanabilecek güvenlik risklerinin başında gelmektedir. Bu hususlar aşağıda alt başlıklar halinde açıklanmıştır. Tablo 1'de IPv4 ile IPv6 arasındaki benzerlik gösteren güvenlik riskleri listelenmiştir.

A. Paket koklamak

Paket koklamak ağda dolaşan paketlerin yakalanarak ve içeriğinin incelenmesi şeklinde tanımlanabilir. Açık kaynak kodlu popüler paket koklayıcılardan tcpdump [5] ve wireshark [6] uzun süredir IPv6 desteği vermektedir. IPv6'nın IPsec desteğini zorunlu tutması ağ seviyesinde uçtan uca güvenli iletişimin her cihaz tarafından yapılabilmesinin önünü açmıştır. Paket koklanması saldırısında IPsec kullanılarak şifreleme yapılmaması durumunda paketlerin içeriği açık olduğu için IPv4 ve IPv6 arasında bir fark bulunmamaktadır. IPsec uygulaması ile yakalanan paketlerinin içeriğinin incelenmesinin engellenebilmesine karşın henüz IPsec için

anahtar paylaşımında verimli algoritmalar önerilmediğinden yeni nesil protokolün bu saldırının şekli ve tespitine katacakları şimdilik sınırlıdır [7]. Bu saldırı türünün IPv6 ağlarındaki durumunda IPsec'in kullandığı ISAKMP (Internet Security Association and Key Management Protocol) ve IKE (Internet Key Exchange) protokollerinin şifreleme, mesaj özeti algoritmaları, yetkilendirme yöntemi konularındaki başarıları belirleyici olacaktır.

B. Uygulama seviyesi saldırıları

OSI referans modeli 7. seviyesi olan uygulama katmanı, internette yapılan saldırıların sayıca ve kapsam olarak en büyük kısmını oluşturmaktadır. Uygulama katmanında yapılacak olan saldırılar ağ katmanından çalışan IP sürümünden bağımsız olduğu için hafıza taşıma veya taşıması, SQL enjeksiyonu (SQL injection) benzeri uygulama seviyesi saldırıları yeni nesil internet protokolü kullanımı ile herhangi bir değişiklik göstermeyecektir [8].

C. Ortadaki adam saldırısı

IPv4 ve IPv6 adres başlıklarının hiçbir koruma altında olmaması, ortadaki adam saldırılarından korunmak için iki protokolünde IPsec desteğine ihtiyaç duymalarına neden olmaktadır. Paket koklama saldırılarına benzer olarak IPsec kullanılmaması durumunda bu saldırı türü için IPv4 ve IPv6 arasında bir fark bulunmamaktadır.

TABLO 1

IPV4 İLE IPV6 ARASINDAKİ BENZERLİK GÖSTEREN GÜVENLİK RİSKLERİ

Güvenlik Riski	IPv4	IPv6
Paket Koklamak	Mümkün	IPsec kullanılmazsa mümkün
Uygulama seviyesinde yapılacak saldırılar	Mümkün	Kısmen mümkün
Ortadaki adam saldırısı	Mümkün	Kısmen mümkün
Taşıma hafıza veya Taşıma saldırısı	Mümkün	Kısmen mümkün

D. Taşıma (flooding)

Taşıma saldırıları genel anlamda hedefe baş edebileceğinden daha fazla istegün yönlendirmesiyle yapılır. Bu yönlendirme sonucu hedefin işlemci, bellek, disk kapasitesi ve bant genişliği tüketilerek hizmet vermesi engellenir. Taşıma saldırıları IP adres yapısıyla çok bağlantılı bir saldırı türü olmadığından IPv6 için çok fazla değişikliğe maruz kalmaya beklenmemektedir. Bununla birlikte aşağıdaki problemlerle karşılaşılabilir:

- İkili yığın yapısını destekleyen sunucularda IPv4 ve IPv6 ağ yığınların birlikte kullanılmasının sistem kaynakları tüketimi açısından bir maliyeti olacaktır. İkili yığın çalıştıran cihazlar IPv6 için kaynak ayırmaları nedeni ile sadece IPv4 çalıştıran cihazlara göre daha az istek ile servis veremez hale gelebilirler.
- IPv6 ağlarında geçiş için kullanılan tünel mekanizmaları, saldırganın tüneli açan cihazlara karşı aşırı trafik oluşturarak servis dışı bırakma saldırısı

yapılmasını kolaylaştırabilir.

- ICMPv6 ve IPv6 çoklu gönderim adreslerinin kullanılma şekli ileride bahsedileceği şekilde IPv6 ağlarında taşıma saldırısı yapılmasını kolaylaştırabilir.

III. IPV6 İLE DEĞİŞECEK SALDIRI TÜRLERİ

A. Keşif (Reconnaissance)

Keşif saldırıları bir saldırı türü olmaktan çok saldırı öncesi hedef cihazların tespiti ve kurban aramak için kullanılan çalışmaları içermektedir. IPv4 ağlarında adres aralığının dar olması nmap benzeri tarama programları ve solucanlar tarafından bir ağa ait tüm adres aralığının çok kısa bir zamanda taranmasını mümkün kılmaktadır. IPv6 ile birlikte en düşük alt ağ adresi olan $/64$, 2^{64} adres içermektedir. Alt ağdaki adres sayısındaki bu artış rastgele IP adresi tarama ile hedef bulma olasılığını azaltmaktadır. Adres aralığının getirdiği bu koruma saldırganların rastgele IP adresi aramak yerine DNS mekanizması kullanmaları ile aşılabılır. Hedef ağa ait alan adı altında bulunan bilgisayarların IPv6 adresine ulaşmak, DNS sözlük saldırısı ile desteklenmiş bir DNS kaba kuvvet saldırısı ile mümkündür. DNS kaba kuvvet saldırısı yapan TXdns [9] benzeri uygulamalar bu amaç için kullanılabilir. IPv6 ile birlikte ağda belirli servisleri veren sunucuların ortak çoklu gönderim adresi kullanmaları sunucuların adreslerinin bulunmasını kolaylaştırmaktadır. Örneğin ağdaki tüm EIGRP yönlendiricilerini temsil eden FF02::A [10] adresi bu yönlendiricileri tespit etmek için kullanılabilir.

B. ICMPV6

IPv4'te ICMP protokolü hata ve hat bilgisi iletimi amacı ile kullanılmakta ve bu nedenden güvenlik duvarı tarafından tamamen filtrelenmesi durumunda dahi IPv4 kullanan servislerde kesintiye neden olmamaktadır. RFC 4443 tanımlanan ICMPv6 IPv6 konuşan cihazların hata bildirimde bulunması ve diğer tanısal (diagnostic) bilgileri iletmeleri için tasarlanmıştır [11]. ICMPv6 IPv4'teki ICMP'ye göre çok daha fazla işlem için kullanılmaktadır ve IPv6 üzerinden sunulan servislerin çalışabilmesi için gerekliliktir. IPv6 komşu araştırılması (neighbor discovery), maksimum paket büyüklüğü keşfi (Path Maximum-Transmission-Unit Discovery, PMTU-D) benzeri mekanizmalar ICMPv6 paketlerini kullanmaktadır.

ICMPv6 ile ilgili güvenlik risklerinden ilki ICMPv6'nın hata mesajlarının hedef adresinin çoklu gönderim adresi olarak tanımlanabilmesine izin vermesidir. Bu durumun saldırganlar tarafından kullanılması dağıtık servis dışı bırakma (DDOS) saldırısı için zemin oluşturabilir [12]. Örneğin ağdaki tüm DHCPv6 adreslerini temsil eden FF05::1:3 çoklu gönderim adresi [13] DHCPv6 sunucularına icmpv6 kullanan servis dışı bırakma saldırısı gerçekleştirmek için kullanılabilir.

ICMPv6'nın içerdiği seçeneklerin fazlalığı ve kullanımının zorunlu olması, güvenlik duvarlarında hangi ICMPv6

tiplerinin hangi servislerin çalışması için mutlak gereklilik olduğu konusunda probleme neden olabilir. ICMPv6'nın IPv6'da kullanılması zorunluluğuna ICMPv6 tip 2 (Çok büyük paket, Packet too big) paketleri örnek olarak verilebilir. Bu paketler IPv6 kullanarak haberleşen iki uç arasındaki ağda gönderilebilecek en büyük paketin büyüklüğünü bulmayı amaçlayan maksimum paket büyüklüğü keşfi mekanizmasının işlemesi için mutlak gerekliliktir ve güvenlik duvarı tarafından engellenmemelidir. FreeBSD [14] işletim sisteminin AMD64 sürümünde ICMPv6 tip 2 paket göndererek servis dışı bırakılmasına sebep olabilecek bir açık FreeBSD güvenlik listesine 8 Eylül 2008 tarihinde duyurulmuştur [15]. ICMPv6 tip iki paketlerin güvenlik duvarında engellenmemesi zorunluluğu FreeBSD sunucularını bu saldırıya maruz kalmalarına sebep olabilmektedir.

C. Komşu Araştırılması (neighbor discovery) ve Durum Denetimsiz (stateless) Adres Yapılandırması

IPv6 komşu araştırması paketleri, IPv6 konuşan cihazların yerel alan ağlarındaki diğer uçların bağlantılı yerel adreslerinin öğrenilmesi ve yönlendirici bilgilerinin sorgulanması için kullanılır. Komşu araştırması sürecinin bir parçası olan yinelenmiş adres tespiti (Duplicate Address Detection) işlemi ağda aynı IPv6 adresine sahip olan ucun bulunup bulunmadığı bilgisinin öğrenilmesi amacı ile kullanılır.

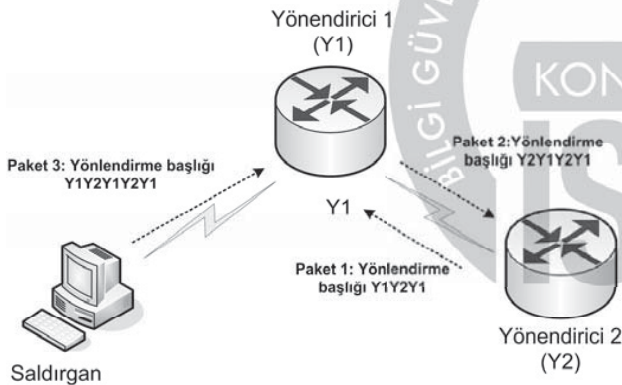
Durum denetimsiz yapılandırma paketleri, yerel alan ağındaki cihazlara IPv6 adresi atanması için kullanılabilecek bir yöntemdir. IPv6'nın komşu araştırması ve durum denetimsiz yapılandırma paketleri tasarlanırken IPv6 kullanımının yerel alan ağlarında erişim kontrolü fiziksel güvenliği sağlanmış linkler üzerinden yapılacağı öngörülmüştür. Günümüzde IPv6'nın kablolu ağlarda kullanılması ile bu durum geçerliliğini kaybetmiştir [16]. Bu sebepten dolayı IPv6 yerel alan ağına katılan tek bir cihaz bile belirtilen tüm güvenliğini tehdit edebilecek potansiyele sahiptir. Yerel alan ağında durum denetimsiz adres yapılandırması mekanizmasını suistimal eden bir saldırgan kendisini yönlendirici olarak göstererek tüm trafiği üzerinden akıtabilir. Windows XP işletim sisteminin IPv6 adresleri için öntanımlı adres isteme biçimi durum denetimsizdir. Ağa yeni katılıp IPv6 yönlendiricisini soran Windows XP işletim sistemini yüklü bir bilgisayarın tüm trafiği kendisini yönlendirici olarak tanıtan bir saldırgan tarafından çok kolayca yakalanıp istenilen noktaya yönlendirilebilir veya analiz edilebilir. IPv6 yerel alan ağlarında diğer bir güvenlik riski yinelenmiş adres tespiti ile adres kontrolü yapan bir cihazın IPv6 adresi almasının engellenebilir olmasıdır. Ağda mevcut olup olmadığı sorulan her IPv6 adresi için saldırgan tarafından ağda olduğu bilgisi dönülmesi ile cihaza hizmet aksattırma saldırısı yapılabilir.

D. Ek başlıklar (Extension headers)

IPv6 ek başlıkları RFC 2460 ta "seçimlik internet seviyesi trafiğinin taşınması için IPv6 ana başlığı ve üst katman (upper layer) başlığı arasına kodlanmış bilgiler" olarak tanımlanmaktadır. Şifreleme, doğruma, paket parçalanması gibi

seçimli işlemler için kullanılırlar. IPv6 ek başlıkları paket büyüklüğünün sabit tutulabilmesi için IPv4'ten farklı olarak ana IP başlığının sonrasına eklenmiştir. Ek başlıklardan yönlendirme başlığı (Routing header) ve Ev adresi (Home address) başlığını tüm IPv6 cihazları tarafından desteklemek zorundadır [17]. Yönlendirme başlığı kullanımı ile IPv6 paketlerinin hangi yönlendiricileri geçerek hedef noktasına varacağı bilgisi ek başlığın içine gömülerek izlenecek yolun paketi gönderen uç tarafından belirlenmesi amaçlanmıştır.

Yönlendirme başlığındaki güvenlik riskleri ile ilgili uyarıları içeren pek çok çalışma mevcuttur [12], [18], [19]. RFC 2460 ve RFC 1883'te yönlendirme başlığı tip 0 içerisinde belirtilen ara düğüm adreslerinin çoklu gönderim adresi olması dışında herhangi bir kısıtlama belirtilmemiştir. Protokoldeki bu tanım ek başlığı içindeki adreslerden birinin üzerinden daha önceden geçilen yönlendiricinin adresi olabilmesine izin vermektedir. Bu açık kullanılarak gerçekleştirilebilecek hizmet aksattırma saldırısının grafiksel gösterimi Şekil 1'de verilmiştir. Saldırının başlatılabilmesi için Y1 yönlendiricisine yönlendirme ek başlığında adres sıralaması olarak Y1Y2Y1Y2Y1 kullanan bir paket yaratılıp gönderilmesi yeterlidir. Bu şekilde yaratılan bir paket yönlendirme ek başlığının izin verdiği en fazla sayı olan 255 tamamlanincaya kadar Y1 ve Y2 yönlendiricileri arasından gidip gelecektir. Bu paketlerden çok sayıda gönderecek bant genişliğini kaplamaya yönelik bir hizmet aksattırma saldırısı gerçekleştirilebilir. Paketlerin iki nokta arasına yönlendirilmesi ile yapılan bu saldırı türü ping-pong olarak isimlendirilmektedir.



Şekil 1. Ping Pong saldırısı 1

E. Programlara IPv6 desteği verilmesi

IPv4'ün 25 yıldan fazla bir süredir kullanılması IPv4 konuşan cihazların üzerindeki yazılımların güvenlik açısından kararlı hale getirmiştir. IPv4 destekleyen cihazların ağ yığınlarına IPv6'yı desteğinin verilmesi sürecinde birçok güvenlik açığı ortaya çıkabilir. İşletim sistemlerinin IPv6 destekler hale getirilmesi için yapılan çalışmalarda ortaya çıkabilecek açıkların yaygın etkileri olmaktadır. Günümüzde en yaygın olarak kullanılan işletim sistemlerinden biri olan Windows'ta IPv6 ile ilgili hizmet aksattırma saldırılarına imkân veren açıklar bulunmaktadır [20]. Linux işletim sisteminde de IPv6 Jumbo paketlerini kullanarak servis dışı bırakma saldırısı

yapılabilecek açık keşfedilmiştir [21]. BSD türevi olan ve felsefesi güvenli bir işletim sistemi sunmak olan OpenBSD işletim sisteminde 10 senede çıkan ikinci açığın sisteme IPv6 desteği verilmesi sırasında ortaya çıkmıştır [22]. Yine bir BSD türevi olan FreeBSD işletim sisteminde de ICMPv6 ve komşu araştırılması yazılım desteklerine açıklar tespit edilmiştir [23].

F. Virüs / Solucan yayılımı

Virüs ve solucanların bulaşma yöntemleri iki başlık altında incelenebilir. İlki yayılmak için e-posta ve virüslü dosyaların paylaşılması benzeri kullanıcı bağımlı veya uygulama seviyesinde metotların kullanılmasıdır. Diğer yöntem ise ağ iletişimi aktivitesi (genellikle tarama) ile güvenlik açığı cihazların taranarak bulaşacak konak aranmasıdır [24].

Yeni hedef tespiti için konak üzerinde bulunan bilgilerin ve depolama ortamlarının kullanılması IP nesline bağlı olmayan bir durumdur. İlk bölümü oluşturan virüs/solucanlar, IP protokolü değişiminden etkilenmeyeceklerdir. Bunun yanında ikinci bölümde yer alan solucanlar için ağ taraması yapma aşamasında, IPv6 ile artan adres sayısı ciddi sorunlar yaratacağı düşünülmektedir. Saldırı araçlarının geçireceği evrim ile yeni nesil solucanlar IPv6 adres aralığının getireceği güvenlik artımını ortadan kaldırabilir [25]. Örneğin IPv6 adreslerinin bulunması için DNS yöntemini kullanan solucanların geliştirilmesi, IPv6 adreslerinin tespit edilmesinin önünü açabilir. Bu konuda yapılan araştırmalarda, DNS servisini IPv6 adresini bulmak için kullanan solucanların mevcut olması durumunda yayılma hızlarının IPv4 ağlarına yakın olabileceğine dair sonuçlar elde edilmiştir [26]. IPv6 geçiş aşamalarında, iki protokolün aynı anda hizmet vermesi solucan dağılımı için uygun zemin hazırlayabilir. IPv6 geçiş yöntemlerinden biri olan ikili yığın yapısında çalışan ağlarda solucan yayılımının yalnız IPv4 çalışan ağlara göre daha hızlı olabileceğine dair bazı araştırma sonuçları mevcuttur [27].

G. IPv6 "herhangi birine gönderim" (anycast) adreslerinin kullanımı

IPv6 herhangi birine gönderim adresleri aynı hizmeti veren sunucular arasında en yakın olanın otomatik olarak bulunabilmesi için kullanılmaktadır

Herhangi birine gönderim adresleri ile ilgili en büyük güvenlik riski bu adreslerin çoklu gönderim adreslerinde olduğu gibi önceden tanımlı bir adres aralığının olmamasıdır. Bu adresleme metodolojisinin bir sonucu olarak tek bir "gönderim adresine" paket gönderilmesi durumunda, bu adresin herhangi birine gönderim adresi "veya" teke gönderim adresi olup olmadığı bilinmemektedir. RFC 3513 [28] IPv6 herhangi birine gönderim adresinin sadece yönlendiricilere verilmesini ve kaynak IPv6 adresi olarak kullanılmamasını önermektedir.

Herhangi birine gönderim yöntemi ile sunucu sorgulamanın getireceği risk istemcinin kendisine cevap dönen sunucunun yetkili bir sunucu olup olmadığını tanımlayan bir mekanizmaya sahip olmamasıdır. Bu açık yetkili sunucu yerine saldırgan tarafından ele geçirilmiş bir bilgisayarın sorguya cevap vermesi yöntemi ile kullanılabilir. Örneğin,

saldırgan herhangi birine gönderim adresine DNS sorgusu gönderildiğinde sorguya cevap vererek kendini yetkili DNS sunucusu olarak gösterebilir.

H. Parçalanmış paket (Fregmentation) Saldırıları

IPv4'te paket parçalanması ara düğümler tarafından yapılmaktadır. IPv6'da IPv4'ten farklı olarak parçalanma işlemi sadece uçtan uca yapılmakta ara düğümlere paket parçalaması işlemi gerçekleştirilmemektedir. Paket parçalanmasının ara cihazlarda yapılmayıp uç noktada ki cihazlarda yapılması yönlendiriciler, güvenlik duvarları benzeri ara ağ cihazları üzerindeki parçalanmış paket saldırısı riskini azaltmıştır. Bununla birlikte uç cihazların parçalama başlığı ile paket parçalama yapabilmesi bu saldırı riskini uç cihazların üzerine çekmiştir.

RFC2460'da parçalanmış paketleri alan uçların paketleri birleştirmek için 60 saniye süresince tampon bellekte tutmaları gerektiğini belirtmektedir. Bu sürenin uzunluğu aynı anda birden fazla noktadan çok sayıda parçalanmış paket gönderilmek sureti ile hedef cihaza servis dışı bırakma saldırısı yapmak için kullanılabilir. RFC belgelerinde IPv6'nın parçalanmış bir paketin parçaları bileştirildikten sonra içinden tekrar bir parçalama başlığı çıkması durumunu tanımlayan yuvalanmış paket parçalama (nested fragmentaion) işlemine izin verilip verilmediği kesin olarak tanımlanmamıştır. Bu tip bir paket alındığında ne yapılacağına karar verilememesi cihazların kilitlenmesine neden olabilir veya iç içe geçmiş paketler saldırıdan güvenli kontrol mekanizmalarını aşmak için kullanılabilir [19].

İ. Tünel mekanizmaları kullanan saldırılar

Tünelleme mekanizması IPv6 trafiğinin IPv4 paketlerinin içinde taşındığı veya IPv4 trafiğinin IPv6 paketlerin içinde taşındığı çözümleri içermektedir. Bu IPv6'ya geçiş aşamalarında kullanılabilecek yöntemlerden birisidir. Tünel mekanizmalarının IPv6 geçiş yöntemlerinden biri olarak kullanılması tünellenmiş trafiğin güvenlik önlemlerinin alınmasını gerektirmektedir.

IPv4 protokolü içerisinde IPv6 trafiği taşınması ve trafiğin IPv4 olarak gözükmesi saldırıdanlar tarafından kendilerini gizleme yöntemi olarak kullanılabilir. Günümüzde kullanılan güvenlik duvarlarının birçoğu kapsüllenmiş trafiğin içeriğini filtreleyememektedir. Bu açığı kullanan saldırıdanlar iç ağda kalan IPv6 destekli cihazların dış ağlara filtresiz erişimi için IPv4 üzerinde açık tek bir portu kullanarak tünel açıp IPv6 trafiğini filtrelenmeden akıtabilirler.

J. Broadcast yükseltgenme saldırısı (Smurf)

Broadcast yükseltgenme saldırıları ICMP echo mekanizmasının kullanıldığı hizmet aksattırma saldırısının bir türüdür. Bu saldırının IPv6'da önüne geçmek için RFC2463'te ICMPV6 hedef adresinin çoklu gönderim, veri bağı çoklu gönderim (link-layer multicast) ve veri bağı broadcast adresi (link-layer broadcast address) olamayacağı belirtilmiştir [29]. Yang ve arkadaşları tarafından yapılan çalışmada RFC2463 uyumlu IPv6 ağ cihazlarında IPv6 yükseltgenme saldırı

yapmanın mümkün olmadığı rapor edilmiştir [30].

K. IPv4- IPv6 geçişi sürecinde çıkabilecek problemler

Yeni nesil internet protokolüne geçiş süresince IPv4 ve IPv6 uzun bir süre internette beraber bulunacaklardır. İki protokolün beraber kullanılması cihaz yönetimi, trafiğin izlenmesi, filtrelenmesi, iletişim bilgilerin ve kütük dosyaların takibi konularını daha karmaşık hale getirecektir. Geçiş sürecinde yaşacak güvenlik risklerinin temel sebeplerinden biri bilgi eksikliği olacaktır. Günümüzde popüler işletim sistemlerinde (Windows Vista, Linux, FreeBSD vb.) IPv6 desteği özdevimli olarak gelmektedir.

Ağ ve güvenlik uzmanların ağlarına IPv6 desteğini vermedikleri durumda IPv6 kullanımının olmayacağı düşüncesine sahip olmaları geçişteki en büyük güvenlik risklerinden biridir. Örneğin Windows Vista yüklü bilgisayarlarda kurulu bir ağ, makalenin daha önceki kısımlarında bahsedilen tünel mekanizması, komşu araştırılması ve durum denetimsiz adres yapılandırması başlıklarında tanımlanan saldırılara açıktır. Ağda kullanan saldırı tespit sistemi, güvenlik duvarı, ağ trafik izleme yazılımlarının IPv6 desteğinin olmaması durumunda, ağda meydana gelen saldırı ve güvenlik ihlallerinin farkına varmak oldukça güç olacaktır.

L. Gezgin (Mobil) IPv6

IPv6 dolaşılabilirlik desteği ile ilgili standartlar RFC 3375'te tanımlanmıştır [31]. Gezgin IPv6 mimarisinin nasıl çalıştığı şekil 2 üzerinde açıklanmıştır.

Gezgin IPv6 mimarisinde her bir hareketli kullanıcı internete bağlı olduğu noktadan bağımsız olarak ev adresi (Home Address, HoA) ile tanımlanır. Gezgin düğüm (Mobile Node, MN) kendi ev ağında olduğu sürece iletişimi ve yönlendirme normal şekilde yapılır. Kullanıcı kendi ağı dışında başka bir ağa geçtiği zaman (1), ağa ait olan bir konuma bağlı IPv6 adresi (Care of Address, CoA) durum denetimsiz adres yapılandırma veya diğer mekanizmalar ile kendisine atanır. (2) Gezgin düğüm misafir ağda aldığı konuma bağlı adresini ev ağındaki yönlendiriciye (Home Agent, HA) bağlama güncellemesi (Binding Update, BU) göndererek bildirir (3). Bu aşamadan sonra gezgin düğüme gönderilen paketler ev ağındaki yönlendirici ile gezgin düğümün konuma bağlı adresi arasında açılan tünel üzerinden iletilir (4) ve ev adresine gelen paketler saydam bir şekilde gezgin düğümün konuma bağlı adresine yönlendirilir. (5) Gezgin IPv6'da kullanılan terminoloji ile ilgili bilgiler Tablo 2'de özetlenmiştir.

Gezgin IPv6'nın güvenliğinin sağlanması IPv6 dolaşılabilirlik özelliklerinin standartlaşmasındaki en önemli engellerden biridir [29]. Gezgin IPv6 ile ilgili oluşabilecek potansiyel güvenlik problemleri ile birçok araştırma mevcuttur [29], [32], [33]. Bununla ilgili olarak yapılan çalışmalar şekilsel olarak verilmiş ve aşağıda alt başlıklarda açıklanmıştır.

içerdiği zaman içinde ortaya çıkacak bir durumdur. IPv6 kullanımı arttıkça saldırganlar tarafından açıklarının daha fazla araştırılması, IPv6 kullanan sistemlerde güvenlik sorunlarına yol açabileceği değerlendirilmektedir.

IPSec protokolünün desteğinin IPv6 ile birlikte zorunlu olması ağda dolaşan şifreli trafiğin miktarının artmasına neden olabilecektir. Bu durumun saldırganlar tarafından kullanılması derin paket analizi metodu kullanarak çalışan saldırı tespit ve önleme sistemlerinin işlerliğini yitirmelerine sebep olabilecektir. Doğal olarak, yeni saldırıların tespit edilmesinde imza tabanlı çözümler yetersiz kalacağından davranışsal (behavioral) tabanlı yöntemlerin kullanımı artabilecektir. IPv6 kullanımına geçiş ve yaygınlaşma sırasında iki protokolün birlikte kullanılması, sorumlu personelin IPv6 güvenliği konusunda yeterince bilgiye ve tecrübeye sahip olmamaları bilgi güvenliğini daha fazla tehdit edebilecek hususlar olarak karşımıza çıkabilecektir.

Sonuç olarak, ülkemizin IPv6'ya geçiş konusunda hazır hale gelmesi, bu konulara ilgi duyan uzman sayısının artması uygulamaların geliştirilmesi, test ortamlarının oluşturulması ve özellikle alt yapının sağlıklı olarak yaygınlaştırılmasına bağlıdır. Bu çalışmamızın ülkemizde yeni yeni yaygınlaşmaya başlayan bu konunun farklı açılardan değerlendirilmesine ihtiyaç duyulmaktadır. Bu çalışmamızın güvenlik açısından farklı kazanımların elde edilmesine katkılar sağlayacağı değerlendirilmektedir.

KAYNAKLAR

- [1] S. Bradner, A. Mankin, The Recommendation for the IP Next Generation Protocol, IETF RFC 1752, 1995
- [2] S. Deering, R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, IETF RFC 2460, 1998
- [3] IPv4 Address Report, <http://www.potaroo.net/tools/ipv4/index.html>
- [4] IPv4 Global Unicast Address Assignments, <http://www.iana.org/assignments/ipv4-address-space>
- [5] Tcpdump paket koklayıcı, <http://www.tcpdump.org>
- [6] Wireshark paket koklayıcı, <http://www.wireshark.org>
- [7] S. Convery, D. Miller, "Cisco IPv6 and IPv4 threat comparison and best practice evaluation (v1.0)"
- [8] D. Zagar, K. Grgic, R. Snjezana, "Security aspects in IPv6 networks implementation and testing," *Computers and Electrical Engineering*, vol. 4, sayfa 425-437, Eylül. 2007
- [9] TXdns multithreaded DNS digger, <http://www.txdns.net>
- [10] S. Deering, R. Hinden, IPv6 Multicast Address Assignments, IETF RFC 2375, 1998
- [11] A. Conta, S. Deering, M. Gupta, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, IETF RFC 4443, 2006
- [12] D. Zagar, K. Grgic, "IPv6 security threats and possible solutions," World Automation Congress, 2006
- [13] R. Droms, J. Bound, B. Voltz, T. Lemon, C. Perkins, M. Carney, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), IETF RFC 3315, 2003
- [14] FreeBSD işletim sistemi, <http://www.freebsd.org>
- [15] Remote kernel panics on IPv6 connections, <http://security.freebsd.org/advisories/FreeBSD-SA-08:09.icmp6.asc>
- [16] J. Arkko, T. Aura, J. Kempf, V. Mäntylä, P. Nikander, M. Roe, "Securing IPv6 neighbor and router discovery," *Proceedings of the 1st ACM workshop on Wireless security*, Atlanta, 2002, 77-86
- [17] P. Savola, IPv6 Routing Header and Home Address Options Internet draft, <http://www.6net.org/publications/standards/draft-savola-ipv6-rh-ha-security-03.txt>
- [18] J. Lim, Y. Kim, "Protection algorithm against security holes of IPv6 routing header," *Advanced Communication Technology*, vol 13, sayfa 2004 -2007, Şubat. 2006

- [19] C. A. Potyraj, "NSA Firewall Design Considerations for IPv6," http://www.nsa.gov/snac/downloads_all.cfm
- [20] Microsoft security bulletin ms06-064, "Vulnerabilities in TVP/IP IPv6 could allow denial of service," <http://www.microsoft.com/technet/security/bulletin/ms06-064.msp>
- [21] Linux Kernel IPv6 Jumbo Bug, <http://www.securiteam.com/exploits/5QP0F15N5Q.html>
- [22] OpenBSD's IPv6 mbufs remote kernel buffer overflow, <http://www.coresecurity.com/content/open-bsd-advisorie>
- [23] IPv6 Neighbor Discovery Protocol routing vulnerability, <http://security.freebsd.org/advisories/FreeBSD-SA-08:10.nd6.asc>
- [24] O. Bektaş, M. Soysal, "IPv6 ağlarında solucan dağılımı," *Haberleşme Teknolojileri Uygulama Sempozyumu*, İstanbul, 2008, 137-141
- [25] S.M. Bellovin, B. Cheswick, A. D. Keromytis "Worm propagation strategies in an IPv6 internet," <http://www.cs.columbia.edu/~smb/papers/v6worms.pdf>
- [26] A. Kamra, H. Feng, V. Misra, A. Keromytis, "The effect of DNS delays on worm propagation in an IPv6 Internet," *Proceedings of IEEE Infocom*, Miami, 2005, 2405- 2414
- [27] Q. Zheng, T. Liu, G. Xiaohong, X. Q. Yu, N. Wang N, "A new worm exploiting IPv4-IPv6 dual-stack networks," *Proceedings of the 2007 ACM workshop on Recurring malware*, Virginia, 2007, 9-15
- [28] S. Deering, R. Hinden, Internet Protocol Version 6 (IPv6) Addressing Architecture, RFC RFC 3513, 2003
- [29] K. Elgoarany, M. Eltoweissy, "Security in mobile IPv6 a survey," *Information Security Tech. Report*, vol 4, sayfa 32-43, Ocak. 2007
- [30] Y. Xinyu, M. Ting, S. Yi, "Typical DoS/DDoS threats under IPv6," *Computing in the Global Information Technology*, Guadeloupe, 2007, 55 - 61
- [31] S. Hollenbeck, Mobility Support in IPv6, IETF RFC 3375, 2002
- [32] J. Kempf, J. Arkko, P. Nikander, "Mobile IPv6 security," *Wireless Personal Communication*, vol 29, sayfa 389-414, 2004
- [33] T. Aura, "Mobile IPv6 Security," Microsoft Research Ltd. <http://research.microsoft.com/users/tuomaura/publications/aura-protocols02.pdf>

Analysis of Attacks towards Turkish National Academic Network

Murat SOYSAL, Onur BEKTAŞ

Abstract— Monitoring unused IP address is an emerging method for capturing Internet security threats. Either an attack or a mis-configuration could generate network traffic towards the unused IP blocks of a network segment. This paper summarizes the method for ascertaining the attacks towards Turkish National Academic Network by the use of modified version of Blackhole concept. In this method Blackhole traffic is captured by using Honeypots and analyzed by using IP header information. The attacks are classified based on source IP address, originating country, operating system and destination port. Moreover, captured traffic originating from Turkey is further evaluated in order to characterize distribution of attacks among the Turkish Internet Service Providers.

Keywords —Blackhole monitoring, Honeypot, network security, ULAKBIM, ULAKNET

I. INTRODUCTION

The security of the national and personal information resources has become more important with the expansion in the use of the internet and the increase in the number of applications such as e-government and electronic banking applications. Moreover, the increase in the number of cyber attacks and cyber terrorism have been threatening especially the security of the national information resources. These circumstances have emerged the urgent establishment of the Computer Security Incident Response Teams. Urged by necessity, Ulak-CSIRT, ULAKNET Computer Security Incident Response Team, has been established in the constitution of the National Academic Network (ULAKNET).

ULAKNET, managed by Turkish Academic Network and Information Center (ULAKBIM) [1], provides network connectivity of universities and research institutes with similar institutions in Turkey and abroad. For ULAKBIM to provide services in order to be able to fulfill its primary duties there is a need for a high-speed reliable backbone and external connections. The main goal of ULAKBIM is to provide network services always one step ahead of the expectations of its users, made up of 100,000 academic personnel and more than 2.2 million university students.

ULAKBIM is a partner of GÉANT2 and ULAKNET backbone is interconnected with the trans-European Research

Network GÉANT2 with 2.5 Gbps capacity and an upgrade on this link is in process. ULAKNET backbone consists of three PoPs located in Ankara, Istanbul and Izmir and the backbone links are 1 Gbps, 500 Mbps and 500 Mbps accordingly.

The CERT/CSIRT units are mainly established in the constitutions of well-organized and superior enterprises managing big networks [2]. Ulak-CSIRT (Computer Security Incident Response Team) is responsible for preventing the potential security violation of external networks to ULAKNET. Ulak-CSIRT also aims ascertaining the attacks and the people in charge and in the same way, preventing the attacks of ULAKNET to the outside world and if there is an attack, ascertaining the people in charge of the attack and sharing the information with the administrators of this network [3].

The method developed in this study is based on Blackhole concept and employs Honeypots in the scope of “ascertaining the attacks towards ULAKNET” mission of Ulak-CSIRT. In ordinary usage, Blackholes, from a network security perspective, are placed in the network where traffic is forwarded and dropped. Systems that monitor unused address space have been called Blackholes [4], darknets [5], network telescopes [6] or Sinkholes [7] and have been under investigation for a long time. Honeypots are kind Intrusion Detection Systems which emulates vulnerable systems or services to attract interest of intruders [8].

ULAKNET Blackhole Attack Detection System includes a Blackhole application based on ULAKNET unused IP blocks and the traffic forwarded to this system is received by a Honeypot. Inclusion of the Honeypot encourages the intruders to continue their attacking behavior which facilitates security experts analyzing the attacks deeper. Whereas, with single stand Blackholes security experts have limited capabilities since the traffic is directly dropped. Although there are some researches in literature focusing on the use of Honeypots in Blackhole applications, implementation in large scale networks is still a challenging study due to the great amount of data required to be analyzed. In addition, ULAKNET Blackhole Attack Detection System is a unique study in Turkey in this scale up to our knowledge. Moreover, our study represents national scale findings since it analyzes the attacks towards whole national academic network. These findings contribute to the analysis of attacks toward Turkey with interesting results such as the most attacking countries, the most attacking Operating Systems, the mostly attacked ports, etc.

Manuscript received November 10, 2008.

M. Soysal. is with the Turkish Academic Network and Information Center (ULAKBIM), Ankara, 06539 Bilkent, phone: 312-298-9367; fax: 312-298-9310; e-mail: msoysal@ulakbim.gov.tr

O. Bektaş. is with the Turkish Academic Network and Information Center (ULAKBIM), Ankara, 06539 Bilkent, e-mail: onur@ulakbim.gov.tr

II. ULAKNET BLACKHOLE ATTACK DETECTION SYSTEM

A. Blackholes

Blackholes, from a network security perspective, are placed in the network where traffic is forwarded and dropped. Once an attack has been detected, blackholing can be used to drop all attack traffic at the edge of an Internet Service Provider (ISP) network, based on either destination or source IP addresses.

Blackholes are used for monitoring unused Internet space to characterize security threats. Systems that monitor unused IP address space have been called Blackhole monitors [4], darknets [5], network telescopes [6] and Sinkholes [7].

Blackholes are capable of identifying configuration errors, routing problems [9], denial of service attacks (DoS) [10], [11], Internet worms [12], [13], [14], [15] and botnets [4]. There are some primitive results even from IPv6 Blackhole applications [16].

B. Capturing and Analyzing Attacks

The Blackhole concept is adapted to detect the attacks by the help of unused IP blocks among ULAKNET. The following IPv4 address blocks are assigned to ULAKNET in Ripe Database [17]:

- 193.140.0.0/16
- 194.27.0.0/16
- 193.255.0.0/16
- 79.123.128.0/17

ULAKBIM assigns sub-blocks of these four IP blocks to the nodes of ULAKNET, using its "Assignment Window", and routes the traffic destined to these sub-blocks to the related node according to these assignments. On the other hand, some sub-blocks are currently not assigned to any node and consequently, nominated as unused IP blocks of ULAKNET. Any network packet whose destination address is in one of the unused IP block ranges belongs to either a malicious activity or a mis-configured traffic. The ULAKNET Blackhole application is mainly based on capturing and analyzing this kind of traffic.

We used a very simple rule of routing to capture this traffic: "The priority of the specific routes over the general ones". First, all four huge IP ranges assigned to ULAKBIM are routed to a ULAKNET Blackhole.

```
ip route 193.140.0.0 0.0.255.255 193.140.82.205
ip route 194.27.0.0 0.0.255.255 193.140.82.205
ip route 193.255.0.0 0.0.255.255 193.140.82.205
ip route 79.123.128.0 0.0.254.255 193.140.82.205
```

Since the smaller blocks assigned to the nodes have more specific entries in the routing tables of backbone routers, they are issued first. All packets having a "used" IP address as a

destination address are distributed to the related nodes. Then, the rest is captured by Blackhole.

After capturing these packets the analysis is done according to the research interests. We assumed that if the captured packets belong to a malicious activity, this is mainly a scan before the actual attack since the destination is not a real victim with a valid IP address. Therefore, we decided to identify the distribution of these hosts according to the ISP hosting the attacker, the country the attacks come from, the destination ports scanned. This information could easily be gathered from the IP header part from the packets, so the deep packet inspection tools are not used in this study. Employing such a tool to identify the attack type more precisely and in more detail was another option, but it will not be cost effective since the captured packets probably belong to the only the scan part. Besides, as the number of packets towards the Blackhole increases, real time deep packet analysis of traffic gets more difficult.

Honeyd [18] is used to gather information from the IP header part of the captured packets. Although honeyd is classified as low interaction honeypot it has advanced features like faking operating system probe scanners. Simplicity, human readable logs and familiarity are the main concerns while choosing honeyd.

Honeyd creates a flow log for all connections request captured. Example log file includes the following lines:

```
2008-06-30-00:00:00.8110 tcp(6) S 10.10.10.12 4270
192.16.2.3 1433 [Windows XP SP1]
2008-06-30-00:00:00.8848 tcp(6) E 220.169.60.35 4021
79.123.148.140 1433: 41 0
2008-06-30-00:00:00.0312 udp(17) - 24.215.24.91 1045
193.255.1.207 1026: 30
```

Fields in the Honeyd log file can be interpreted as follows:

- The first field contains the timestamp of event
- The second field lists the protocol like tcp, udp etc.
- The third field may either be :
 - S start of a new connection
 - E end of a connection (Honeyd logs the amount of data received at the end of line)
 - Packet does not belong to any connection.
- Third field is four tuple of connection in the order of source IP, source port, destination IP and destination port.

Honeyd also logs operating system (OS) of the attacker at the end of the line if it can be identified via passive fingerprinting.

C. Classification of Attacks

In this section, the methodology which is used to classify the attacks will be explained. The attacks are classified according to the ISP which the attacker belongs to, the

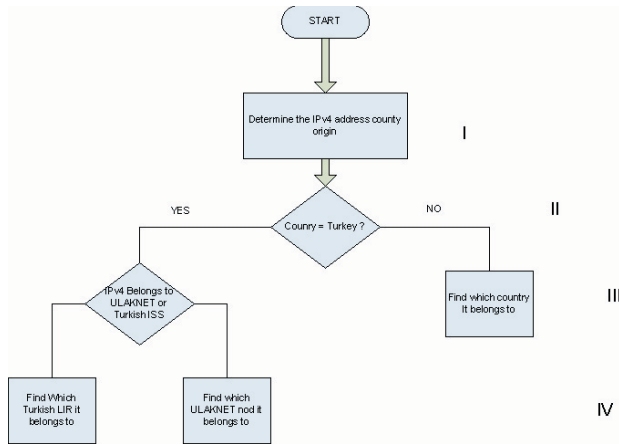


Figure 1. Source IP based analysis

country the attacks come from, the destination ports scanned and the operating system used by the attacker.

The classifications based on the destination port and OS are directly gathered from the honeypot log file. On the other hand, source IP information is further processed to identify the ISP hosting the attacker and the country the attacks come from. This process is given in Figure 1 as a flow chart.

In the first step, the country which the attack comes from is identified by using an open source tool, Maxmind GeoIP [19]. GeoIP is a geographical location database which is mainly used to gather geographical information about their Internet visitors in real-time. An example of GeoIP query/result pair is given below:

Query: `[root@blackhole]$ geoiplookup 75.82.32.12`
Result: `GeoIP Country Edition: US, United States`

In step 2, country origin is determined. Countries other than Turkey are classified using GeoIP database. RIPE membership information [20] is used in order to identify Turkish Local Internet Registers (LIR) and their IP ranges. At step 3 and 4, Turkey originated IP addresses are further classified as ULAKNET and the others. To accomplish this task, membership list further filtered based upon the registry base of LIR's. A LIR is added to "Turkish LIR's List" if its registry base is in Turkey. Attacks from Turkey are classified according to the ISPs hosting the attacker. .

The last classification is made on the attacks coming from ULAKNET nodes. Most of ULAKNET nodes use the IPv4 blocks assigned by ULAKBIM, so it is easy to identify the node owning a source IPv4 address from the local databases. In addition, some nodes of ULAKNET have their own AS numbers and IPv4 addresses assigned directly from RIPE (e.g. METU, ITU). The local database is updated to include all IPv4 addresses used among ULAKNET.

D. Reporting

All the classification results are visualized in a graphical manner and shared via Ulak-CSIRT web page [21]. The graphs include statistics such as the most attacking ULAKNET node, the most attacking countries and the most attacking IP address. This information is publicly published to enable all security teams to identify the most active attackers targeting Turkish Academic Network. Further details are available up on request, since public share could result in more security holes.

III. RESULTS

In this section the classification results of the attacks captured during June 2008 will be given. The log file processed exactly belongs to 30 days. The log file has an approximate size of 18 Gigabytes and over 233 Million lines. The total number of unique IP addresses in the log file is around 500k. 50.000 of these unique IP addresses belongs Turkish ISPs which is a significant number for our internet society. Blackhole application identified 50k compromised machines hosted by Turkish ISP during one month.

A. The Most Attacking IP addresses

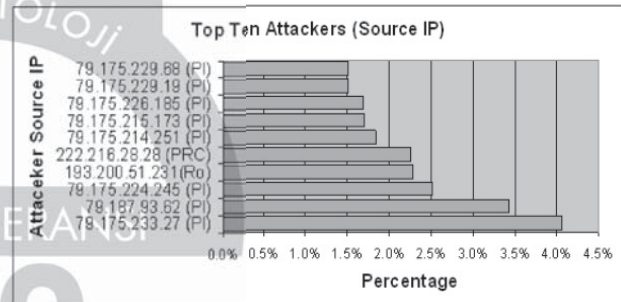


Figure 2. Top Ten Attacking IP Addresses

The list of "Top Ten Attacking IP Addresses" is one of the most beneficial results in network security point of view. This list could be used for dynamically generating Access Control Lists for filtering the most active attackers at the edge of backbone. After detecting IP address, traffic can also be redirected to deep packet intrusion detection systems (IDS) to analyze attack in depth. By using this method load on IDS can be reduced.

B. The Most Attacking Countries

Another type of classification on the attackers is made according to the countries they belong to. This information became much more important after the examples of "cyber wars" following the conflicts between some countries during 2008.

The results in Figure 3 show the ranking according to the sum of all packets received from the attacking country.

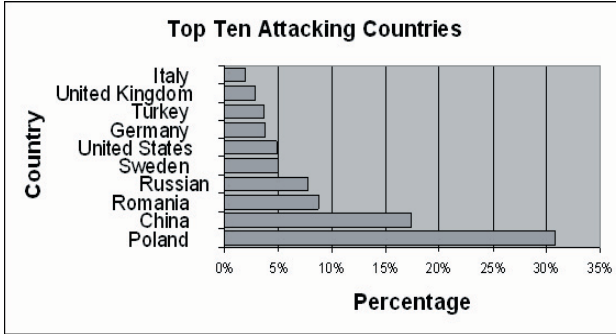


Figure 3. Top Ten Attacking Countries

Evaluations on the “Top Ten Attacking Countries” revealed that summing all the packets would mislead the ranking. A single host scanning the ports of another single destination could burst the country rank. A revised analysis is performed by counting all the traffic between distinct source/destination IP pairs as single hit and result is given in Figure 4. The comparison of Figure 3 and Figure 4 shows that the former is biased by the Polish hosts identified from Figure 2.

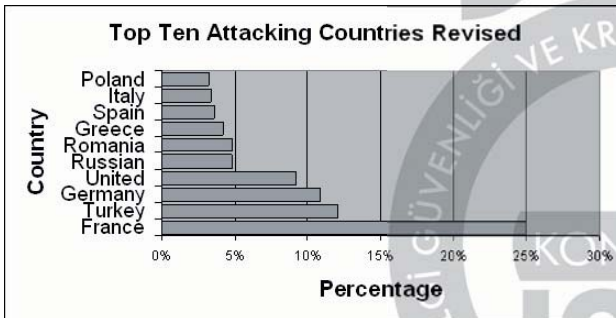


Figure 4. Top Ten Attacking Countries Revised

C. The Mostly Attacked Ports

The “Top Ten Attacked Ports” is given in Figure 5. The port information is valuable since some of the attacks could be identified according to these ports. In addition, the list of the mostly attacked ports is heavily used by network administrators to secure their network by simply blocking the probes to these ports.

A dramatic result from this evaluation is the high share of Port 1433 which is commonly used by Microsoft's SQL server. Two MSSQL worms in May 2002 and January 2003 exploited several known MSSQL flaws [22]. The mostly attacked ports evaluation shows that the scan on this port still has a great amount of activity on Internet. Another interesting result is observation of port 1026 and 1027. These ports are used by Microsoft Windows messaging system which is designed for use by system administrators to notify users about their networks. Nevertheless, spammers use this service to send advertisements [23]. Port number 22 is used for SSH protocol which is used in Unix derivatives for encrypted

remote shell access. Its ranking indicated that ssh probes are the most common attack type performed against Unix derivatives.

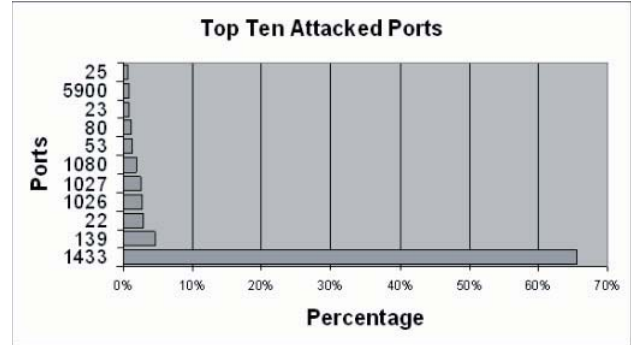


Figure 5. Top Ten Attacked Ports

D. The Most Attacking Operating Systems

Honeyd logs allow us to identify the Operating System used by the attacker. The result of the attacker OS evaluation is as expected (Figure 6). Since most of the internet users are using Windows XP, this operating system has more than 70% share among all the attackers.

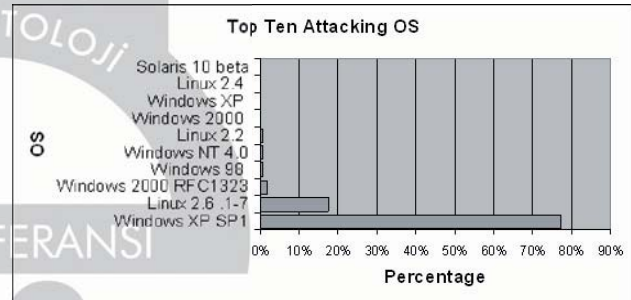


Figure 6. Top Ten Attacking OS

A notable finding of this evaluation could be the 18% share of Linux. Since vast amount of the open source attacking tools are available and Linux is feasible platform for running and improving such tools, a special attention to these attacks are paid. Linux can be used as server operating system. Thus, detection of Linux as attacker OS can be the indication of the more severe security problems like the compromise of DNS or SMTP servers. As a result, if detected OS is a server operating system it should be investigated more closely.

E. Special analysis on the attackers from Turkey

A novel result of this study is based on evaluating the attacks originating from Turkey. This is the first time in literature such a classification is given.

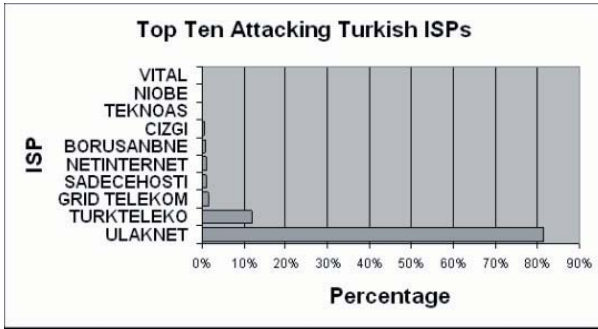


Figure 7. Top Ten Turkish ISPs

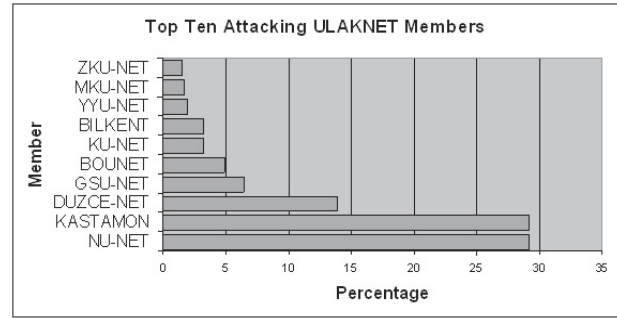


Figure 9. Top Ten Attacking ULAKNET Members

The Turkish ISP ranking is given with two different evaluations similar to the “Most Attacking Countries” is section III.B.

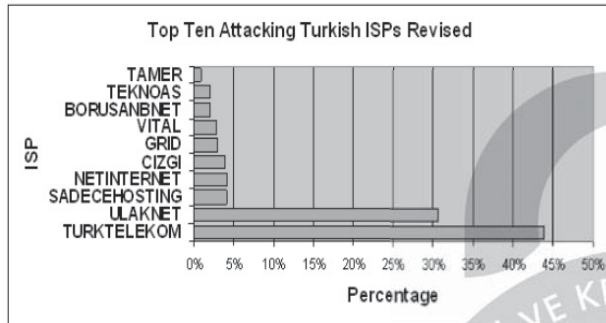


Figure 8. Top Ten Turkish ISPs Revised

It should be noted here that ULAKNET hosts generate a considerable amount of the attacks gathered via the Blackhole. This is mainly based on the worm traffic trying to infect the “nearby” hosts. A worm uses the source IP address and the subnet mask to discover the nearby hosts and scan their related ports.

The lead of “Turk Telekom” is an expected result due to the high share of the ISP in the market. On the other hand, the rank of other ISPs could be beneficial for the security teams of these ISPs to evaluate their position according to their competitors in the market.

F. The Most Attacking ULAKNET members

Since attack ranking of ULAKNET members are visualized and shared via Ulak-CSIRT web page on daily and hourly basis, only one month summary is given in Figure 9.

Attacks were counted as a single hit if source and destination addresses are distinct.

IV. CONCLUSION

In this paper, ULAKNET Blackhole Attack Detection System and its data analysis methodology have been explained. Besides, findings of the system for a one month period are demonstrated. It is also verified that even if the Blackhole traffic is analyzed only in IP header level, significant knowledge can be gained about the attacks towards the monitored networks.

The traffic towards the Blackhole can be the result of either an attack or a configuration error. The results of the detailed analysis on the traffic due to the attacks are presented in this study. Both the ULAKNET Network Operations Center (NOC) and the network administrator of the ULAKNET nodes have gained the general vision on the security threads towards the Turkish Academic Network with the findings of this study. In addition, the analysis over Blackhole data are being performed continuously and results are updated in hourly manner.

The attacks coming from ULAKNET nodes are further processed by Ulak-CSIRT to improve the security level in ULAKNET by identifying the compromised machines in academic network. This identification is automatically turned into security incident by a trouble ticketing system and the system informs security contact point of the node. Severity levels are assigned to each incident with time limits to investigate and resolve the attack.

Two configuration errors causing network traffic towards Blackhole are also discovered in this study. In the first case the Akamai servers, hosted in ULAKBIM and providing the content delivery services to ULAKNET, were discovered to distribute traffic to Blackhole due to BGP routing problem.

The second problem was discovered by the real time monitoring of port anomalies. A configuration error in the DNS server of one of the ULAKNET nodes resulted in excessive amount of traffic to port 53 of an unused IP address (193.140.82.251). This anomaly was detected by the help of “Blackhole Destination Port Daily Analysis”. The

administrator of the node was informed to update the configuration of DNS server and enter the correct IP address (193.140.83.251) to use ULAKBIM DNS forwarder service. This update prevented nodes DNS server from forwarding all uncached DNS queries to Blackhole.

Blackhole system also detected considerable amount of traffic originated from unassigned ULAKNET IP addresses which is a clear indication of IP spoofing. Ulak-CSIRT published a recommendation including technical details of IP spoofing and “ingress filtering” as a possible solution as a result of this observation.

In the future the efficiency of a Blackhole system can be improved by increasing the number of sensors. Moreover, if universities deploy their Blackhole systems monitored data can correlate together to produce better results. Another enhancement can be made by analyzing Blackhole traffic with the deep packet inspection tools. For example Honeynet can be used for this kind of purposes.

REFERENCES

- [1] ULAKBIM The Turkish Academic Network and Information Centre, <http://www.ulakbim.gov.tr>
- [2] RFC 2350, Expectations for Computer Security Incident Response.
- [3] Ulak-CSIRT, Turkish Academic network and information center Computer Security Incident Response Team, <http://csirt.ulakbim.gov.tr/>
- [4] Dug Song, Rob Malan, and Robert Stone, “A snapshot of global Internet worm activity,” presented at the FIRST Conference on Computer Security Incident Handling and Response, June 2002.
- [5] Team Cymru. The darknet project [Online]. Available: <http://www.cymru.com/Darknet/index.html>, November 2008.
- [6] David Moore, Colleen Shannon, Geoffrey M. Voelker, and Stefan Savage, “Network telescopes,” Technical Report CS2004-0795, UC San Diego, July 2004.
- [7] Barry Raveendran Greene and Danny McPherson, “Sinkholes: A swiss army knife isp security tool,” June 2003 [Online]. Available: <http://www.arbor.net/>.
- [8] The Honeynet Project, *Know Your Enemy : Learning about Security Threats*, (2nd Edition), Pearson Education.
- [9] S. Soltani, S. A. Kyaham, H. Radha, “Detecting Malware Outbreaks Using a Statistical Model of Blackhole Traffic,” in *Proc. IEEE International Conference on Communications*, Beijing, 2008, pp. 1593 – 1597
- [10] David Moore, Geoffrey M. Voelker, and Stefan Savage, “Inferring Internet denial-of-service activity,” in *Proceedings of the Tenth USENIX Security Symposium*, Washington, D.C., August 2001, pp. 9–22.
- [11] Evan Cooke, Michael Bailey, Z. Morley Mao, David Watson, and Farnam Jahanian, “Toward understanding distributed Blackhole placement,” in *Proceedings of the 2004 ACM Workshop on Rapid Malcode (WORM-04)*, New York, Oct 2004. ACM Press.
- [12] Michael Bailey, Evan Cooke, David Watson, Farnam Jahanian, and Jose Nazario, “The Blaster Worm: Then and Now,” *IEEE Security & Privacy*, 3(4):26–31, 2005.
- [13] David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, and Nicholas, “Weaver. Inside the Slammer worm,” *IEEE Security & Privacy*, 1(4):33–39, 2003
- [14] Colleen Shannon and David Moore, “The spread of the Witty worm,” *IEEE Security & Privacy*, 2(4):46–50, July/August 2004.
- [15] Colleen Shannon, David Moore, and Jeffery Brown, “Code-Red: a case study on the spread and victims of an Internet worm,” in *Proceedings of the Internet Measurement Workshop (IMW)*, December 2002
- [16] M. Ford, J. Stevens, J. Ronan, “Initial Results from an IPv6 Darknet Internet Surveillance and Protection,” in *International Conference on Volume , Issue 2006*, pp:13 – 13.
- [17] RIPE network coordination centre, <http://www.ripe.net>
- [18] Honeyd virtual honeypot, <http://www.honeypot.org>
- [19] Geoip Geolocation IP finder <http://www.maxmind.com>
- [20] Local Internet Registries offering service in Turkey. Available: <http://www.ripe.net/membership/indices/TR.html>
- [21] ULAKNET honeypot statistics, [Online]. Available: <http://www.ulakbim.gov.tr/ulaknet/istatistik/balkupu>
- [22] Port 1433 details, [Online]. Available: <http://isc.sans.org/port.html?port=1433>
- [23] Disabling Messenger Service in Windows XP, [Online]. Available: <http://www.microsoft.com/windowsxp/using/security/learnmore/stopspace.m.mspx>

Pairing-Based Cryptography : A Survey

Sedat AKLEYLEK, Barış Bülent KIRLAR, Ömer SEVER, Zaliha YÜCE

Abstract—Pairings, bilinear maps, help to transform a discrete logarithm problem on an elliptic curve to the discrete logarithm problem in finite fields. They started to be used in cryptography during 1990's. At the beginning, they are used to build as attacks on elliptic curve digital signature algorithm. Nowadays, pairings are popular to construct cryptographic protocols. The purpose of this paper is to introduce bilinear pairings in cryptography and to show how to construct protocols in pairing-based cryptography.

Keywords —bilinear map, pairing-based cryptographic protocols, Weil and Tate pairing.

I. INTRODUCTION

Over the last years, there has been an increasing interest in pairing-based cryptography. The primitives of pairing based cryptosystems are three groups in which the discrete logarithm problem (DLP) is believed to be hard. Moreover, one requires the existence of an efficiently computable, so-called non-degenerate pairing map. This additional structure allows many interesting protocols for all kind of different applications [6], [8], [12]. Pairings in elliptic curve cryptography are functions which map a pair of elliptic curve points to an element of the multiplicative group of a finite field.

Earlier bilinear pairings, namely Weil pairing and Tate pairing were used in cryptography for the Menezes-Okamoto-Vanstone (MOV) [13] and Frey-Rueck (FR) [10] attacks, respectively. MOV and FR attack reduces elliptic curve discrete logarithm problem (ECDLP) to DLP in a finite field. They use bilinearity of the pairings. The basic idea of MOV and FR attack is to find an isomorphism between r -torsion point and r -th roots of unity of $\mathbb{F}_{q^k}$, where k is the embedding degree of r -torsion points. When k is small enough, i.e., $k \leq (\log q)^2$, there is a sub-exponential time algorithm such as index calculus and function field sieve algorithms that can be used to solve DLP on a finite field. For supersingular curves, ECDLP is easy to solve since MOV or FR attack is applicable.

Most of the protocol researchers use the fascinating properties of the bilinear pairings to design new cryptographic protocols. They just focus on the efficiency of the pairing but skip the details of pairings. On the other side, the security of the protocol must be based on a hard problem which depends on the mathematical properties of the pairing. In this respect Galbraith, Paterson and Smart [11] give a good guidance to

non-specialists who are interested in using pairings to design cryptographic schemes focusing on efficiency, bandwidth and security.

Pairing-based protocols primarily achieve two main objective; to construct methods which can not be constructed using other techniques (ID-based encryption, etc) and methods which can be done using other techniques, but for which pairings provide improved functionality (short signature, tri partite key exchange in one round, etc).

For pairing-based cryptography, it is a general problem of choosing elliptic curves together with bilinear mappings. To find a suitable elliptic curve one needs with a prime $r \geq \sqrt{q}$ dividing $\#E(\mathbb{F}_q)$ and the embedding degree of E , k , small enough so that arithmetic on $\mathbb{F}_{q^k}$ is feasible and large enough that DLP on $\mathbb{F}_{q^k}^*$ is as hard as the ECDLP on $E(\mathbb{F}_q)[r]$.

In this paper, a survey on pairing-based cryptography is given. Section II briefly explains the cryptographic bilinear map, Bilinear Diffie-Hellman Problem and describes the pairing-based cryptographic protocols. The Weil and Tate pairings, the basic elements in protocols, are discussed with their use in Section III. The suitable elliptic curves with the given embedding degree for pairing-based cryptography are explained in Section IV. Finally, we conclude in Section V.

II. PAIRING-BASED CRYPTOGRAPHY

A. Bilinear Pairings

Definition 1. Let $(G_1, +)$ and $(G_2, +)$ be abelian groups of order n . Let $(G_3, \cdot)$ be a cyclic group of order n . A bilinear pairing is an efficiently computable map $e : G_1 \times G_2 \rightarrow G_3$ which satisfies the following additional properties:

- 1) (bilinearity) For all $P, R \in G_1$ and all $Q, S \in G_2$, we have $e(P+R, Q) = e(P, Q)e(R, Q)$ and $e(P, Q+S) = e(P, Q)e(P, S)$.
- 2) (non-degeneracy) For all $P \in G_1$, with $P \neq Id_{G_1}$, there is some $Q \in G_2$ such that $e(P, Q) \neq 1$. For all $Q \in G_2$, with $Q \neq Id_{G_2}$, there is some $P \in G_1$ such that $e(P, Q) \neq 1$. When $G_1 = G_2$ and n is prime, $e(P, P)$ is a generator of G_3 for all $P \neq Id_{G_1}$.

Weil and Tate pairings on elliptic curves over finite fields can be given as an example of pairings. For the use in cryptography it is assumed that DLP on G_1 , G_2 and G_3 are hard to solve. This bilinear property has many applications and it was first used for DLP in [13]. For instance, choosing $G_1 = G_2 = E(\mathbb{F}_q)$ and $G_3 \subset \mathbb{F}_{q^k}^*$ with k an embedding degree, defines bilinear pairing.

The following lemma which is related to the properties of bilinear pairings can be easily verified.

Lemma 2. Let $e : G_1 \times G_2 \rightarrow G_3$ be a bilinear pairing. Let $P \in G_1$ and $Q \in G_2$. Then

Manuscript received November 10, 2008.

S. Akleyek, B. B. Kirlar, Ö. Sever, Z. Yüce are with the Institute of Applied Mathematics, METU, Ankara, Turkey, e-mail: {akleyek,kirlar}@metu.edu.tr, severomer@yahoo.com, zyuice@stn.com.tr

S. Akleyek is also with the Department of Computer Engineering, Ondokuz Mayıs University, Samsun, Turkey

B. B. Kirlar is also with the Department of Mathematics, Süleyman Demirel University, Isparta, Turkey

Z. Yüce is a software engineer in STM A.Ş.

* This research is partially supported by ASELSAN A.Ş.

- 1) $e(P, 0) = e(0, Q) = 1$
- 2) $e(-P, Q) = e(P, -Q) = e(P, Q)^{-1}$
- 3) $e(kP, Q) = e(P, kQ) = e(P, Q)^k$ for all $k \in \mathbb{Z}$.

We will now give the Bilinear Diffie Hellman Problem that has been widely studied in recent years.

B. The Bilinear Diffie-Hellman Problem (BDHP)

Security of the some of the applications of bilinear pairings in cryptography relies on the difficulty of bilinear Diffie-Hellman problem which was first stated in [7].

Definition 3. Let G be a finite cyclic group of order n with a generator g , and let a, b, c be integers. The BDHP is to compute the value of the bilinear pairing $e(g^{abc}, g)$, whenever g^a, g^b and g^c are given.

There is a close relation between BDHP and DHP which are defined on elliptic curve. The following fact is easy to prove.

Lemma 4. BDHP is no harder than either the elliptic curve Diffie-Hellman problem or any finite field Diffie-Hellman problem.

We presents three fundamental pairing-based protocols that the security of them depends upon the BDHP.

C. Pairing-Based Cryptographic Protocols

Protocols from pairings can be classified into two types :

- 1) Construction of primitives which can be constructed using other techniques, however by using pairings efficiency is gained.
- 2) Construction of primitives which cannot be constructed by using other cryptographic techniques.

Three party key agreement in one round and short signature protocols are the examples for the first class. Identity-Based encryption which eliminates the public key distribution is the example of the second class

1) *Joux's One Round Three Party Key Agreement Protocol* [12]: Key agreement, one of the fundamental cryptographic primitives, is required when two or more parties want to share a message securely. Three party key agreement in a single round proposed by Joux was the first application of bilinear pairings in cryptography.

Protocol:

Let $(G_1, +)$ and $(G_2, \cdot)$ be cyclic groups of prime order n , $P \in G_1$, $G_1 = \langle P \rangle$ and $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear map. Consider three parties A, B, C with secret keys $a, b, c \in \mathbb{Z}_n$

- A broadcasts aP to both B, C
- B broadcasts bP to both A, C
- C broadcasts cP to both A, B
- A computes $e(bP, cP)^a$
- B computes $e(aP, cP)^b$
- C computes $e(aP, bP)^c$
- Common agreed key is $e(P, P)^{abc}$

2) *Short Signatures* [6]: Digital signatures are the most important cryptographic primitive for the daily life. Short signatures are needed in environments with space and bandwidth constraints. So far, the best known shortest signature is obtained by using the Digital Signature Algorithm (DSA) over a finite field $\mathbb{F}_q$. The length of the signature is approximately $2\log q$. On the other hand, when the following pairing-based protocol is used the length of the signature is about $\rho \log q$, where $\rho = \log q / \log r$ and r is the largest prime divisor of the number of the points in the elliptic curve. For example, if one uses RSA signature 1024 bit modulus, ECDSA signature is 320 bit long for the same security level. However, short signature provides the same security level only for 160 bits for the best choose. This case corresponds finding a suitable elliptic curve $E(\mathbb{F}_q)$, for which r is close to q and it is a general problem to find such suitable elliptic curves having this property [2].

Protocol:

Let $(G_1, +)$ and $(G_2, \cdot)$ be cyclic groups of prime order n , $P \in G_1$, $G_1 = \langle P \rangle$ and $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear map.

- **Public Key Generation** : Let $H : \mathbb{Z}_2^\infty \rightarrow G_1$ be a map to point hash function. The secret key is $k \in \mathbb{Z}_n^*$ and public key is kP for a signer.
- **Sign** : Given a secret key k and a message $m \in \mathbb{Z}_2^\infty$, compute the signature $\sigma = kH(m) \in G_1$
- **Verify** : Given a public key kP , a message m and a signature σ , verify $e(P, \sigma) = e(kP, H(m))$.

3) *Identity-Based (ID-B) Cryptosystems* [7]: This was firstly suggested by [17] that a public key encryption scheme can be run with the identity of receiver. In other words, for ID-B encryption provides the simplification of certificate management in e-mail systems. By this way, management of keys and certificates gets more and more easier. The most used ID-B cryptosystem was proposed by [7] in 2001. The main advantage of ID-B cryptosystems is to eliminate the need for certificates. Moreover, ID-B cryptosystems remove the certificate lookup, lifecycle management and certificate revocation lists.

Protocol:

Let $(G_1, +)$ and $(G_2, \cdot)$ be cyclic groups of prime order n , $P \in G_1$, $G_1 = \langle P \rangle$ and $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear map.

- **Public Key Generation** : Let $H_1 : \{0, 1\}^* \rightarrow G_1^*$ and $H_2 : G_2 \rightarrow \{0, 1\}^l$, where l is the length of the message m be the cryptographic hash functions. Let $s \in \mathbb{Z}_n^*$ and $S = sP$.
- **Encrypt** : Choose a random $r \in \mathbb{Z}_n^*$, then the ciphertext for the message $m : C = \langle rP, m \oplus H_2(e(H_1(ID), S)^r) \rangle$
- **Decrypt** : Compute $V \oplus H_2(e(sH_1(ID), U))$ for given $C = \langle U, V \rangle$.

In practice, elliptic curves are the only groups used to implement pairings.

III. WEIL AND TATE PAIRINGS

A. Elliptic Curves and Divisors

A cubic equation in Weierstrass form is given by the expression

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (1)$$

where the coefficients a_i are in the field $\mathbb{F}_q$. The projective non-singular curve defined by the affine equation (1) over the algebraic closure $\overline{\mathbb{F}_q}$ is called an elliptic curve over $\mathbb{F}_q$. This curve is denoted by E and it has an additive group structure determined by the fact that $P, Q, R \in E : P+Q+R = \text{identity} \Leftrightarrow R$ lies in the line joining P to Q in the projective space. We denote the identity element of E by ∞ , and it is well-known that the set of $\mathbb{F}_{q^k}$ -rational points of E is a subgroup of E for any $k \geq 1$. This subgroup is denoted by $E(\mathbb{F}_{q^k})$. In fact, $E(\mathbb{F}_{q^k})$ consists of all solutions of (1) in $\mathbb{F}_{q^k} \times \mathbb{F}_{q^k}$ together with ∞ .

The divisor group of a curve E , denoted by $\text{Div}(E)$, is the free abelian group generated by the points of E . Therefore, a divisor $D \in \text{Div}(E)$ is a formal sum given by

$$D = \sum_{P \in E} n_P(P)$$

with $n_P \in \mathbb{Z}$ and $n_P = 0$ except for finitely many $P \in E$. The degree of a divisor D is defined by

$$\deg(D) = \sum_{P \in E} n_P.$$

The support of a divisor D , $\text{supp}(D)$, is the set of points $P \in E$ for which $n_P \neq 0$.

The divisors of degree zero form a subgroup of $\text{Div}(E)$, that is denoted by

$$\text{Div}(E) = \{D \in \text{Div}(E) \mid \deg(D) = 0\}.$$

Let $f \in \overline{\mathbb{F}_q} = \overline{\mathbb{F}_q} \setminus \{0\}$ be a rational function. Then, the divisor of a function f is $\text{div}(f) = \sum_{P \in E} \text{ord}_P(f)(P)$, where $\text{ord}_P(f)$ is the multiplicity of f at P . It is a well-known fact that $\deg(\text{div}(f)) = 0$. A divisor D is called *principal* if $D = \text{div}(f)$ for some rational function $f \in \overline{\mathbb{F}_q}^*$. This is denoted by

$$\text{Prin}(E) = \{D \in \text{Div}(E) \mid D = \text{div}(f), f \in \overline{\mathbb{F}_q}^*\}.$$

$\text{Prin}(E)$ is a subgroup of $\text{Div}(E)$ since for all rational functions $f, g \in \overline{\mathbb{F}_q}^*$, $\text{div}(fg) = \text{div}(f) + \text{div}(g)$ and $\text{div}(f/g) = \text{div}(f) - \text{div}(g)$.

Theorem 5. A divisor $D = \sum_{P \in E} n_P(P)$ is principal if and only if $\deg(D) = 0$ and $\sum_{P \in E} n_P P = \infty$.

The divisor class group (or Picard group) $\text{Pic}(E)$ of E is the quotient of the group of degree zero divisors $\text{Div}(E)$ by the principal divisors $\text{Prin}(E)$, i.e.,

$$\text{Pic}(E) = \text{Div}(E) / \text{Prin}(E).$$

It is known that for every divisor $D \in \text{Div}(E)$, there is a unique point $Q \in E$ such that $D \sim (Q) - (\infty)$. This gives a one-to-one correspondence between $\text{Pic}(E)$ and the group of points of E .

Let $P, Q \in E$. Suppose the line between P and Q (tangent line if $P = Q$) has an equation $l(x, y) = 0$. By Bezout's theorem, this line l intersects E at a third point $R = (x_R, y_R)$. Then, the divisor of l is $\text{div}(l) = (P) + (Q) + (R) - 3(\infty)$. The vertical line $v(x) = (x - x_R)$ passes through the points R and $S = P + Q$. Then, $\text{div}(v) = (R) + (S) - 2(\infty)$. Therefore, the equation $S = P + Q$ corresponds to the divisor equality $\text{div}(l/v) = (P) + (Q) - (S) - (\infty)$.

If $D = \sum_{P \in E} n_P(P) \in \text{Div}(E)$ and $f \in \overline{\mathbb{F}_q}^*$ is a rational function such that $\text{supp}(D) \cap \text{supp}(\text{div}(f)) = \emptyset$, then the value of f at D is defined to be the following equation:

$$f(D) = \prod_{P \in E} f(P)^{n_P}.$$

B. Weil and Tate Pairings [5]

Let E be an elliptic curve over $\mathbb{F}_q$ and $\overline{E}$ be the corresponding elliptic curve over the algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$. For a positive integer r , $E[r]$ denotes the group of r -torsion points of E , namely $E[r] = \{P \in E \mid rP = \infty\}$.

Definition 6. The embedding degree of $E[r]$ is the smallest k such that $E[r] \subset E(\mathbb{F}_{q^k})$.

Theorem 7. (Balasubramanian, Koblitz [2]) Let E be an elliptic curve defined over $\mathbb{F}_q$ and suppose that E has a subgroup $\langle P \rangle$ of order r with $\gcd(r, q-1) = 1$. Then, $E[r] \subset E(\mathbb{F}_{q^k})$ if and only if $r \mid q^k - 1$.

Let $P, Q \in E[r]$ and let $R, S \in E(\mathbb{F}_{q^k})$ such that $S \notin \{R, P+R, P+R-Q, R-Q\}$. Let $D = (P+R) - (R)$ and $D' = (Q+S) - (S)$. Then, by theorem (5) the divisors rD, rD' are in the form $rD = \text{div}(f)$ and $rD' = \text{div}(g)$ for some rational functions $f \neq 0, g \neq 0$. Let μ_r be the group of r -th roots of unity in $\overline{\mathbb{F}_q}^*$.

Definition 8. The bilinear map

$$e_r : E[r] \times E[r] \rightarrow \mu_r \subset \overline{\mathbb{F}_q}^*$$

defined by

$$e_r(P, Q) = (-1)^r \frac{f(D')}{g(D)} = (-1)^r \frac{f(Q) \cdot S / f(R)}{g(P) \cdot R / g(S)}.$$

is called Weil pairing. This map is well-defined, i.e., $e_r(S, T)$ is independent of the choice of D, D', f and g for all $S, T \in E[r]$.

Theorem 9. (Properties of Weil Pairing) Let E be an elliptic curve defined over $\mathbb{F}_q$. Then, the Weil pairing e_r satisfies the following properties :

- 1) (identity) $e_r(S, S) = 1$ for all $S \in E[r]$
- 2) (alternation) $e_r(S, T) = e_r(T, S)^{-1}$ for all $S, T \in E[r]$
- 3) (bilinearity) e_r is bilinear in each variable; $e_r(S+T, P) = e_r(S, P)e_r(T, P)$ and $e_r(S, T+P) = e_r(S, T)e_r(S, P)$ for all $S, T, P \in E[r]$
- 4) (non-degeneracy) If $e_r(S, T) = 1$ for all $S \in E[r] - \infty$, then $T = \infty$ and if $e_r(S, T) = 1$ for all $T \in E[r] - \infty$, then $S = \infty$
- 5) (compatibility) For all $S, T \in E[r]$, $e_r(\alpha(S), \alpha(T)) = e_r(S, T)^{\deg \alpha}$, for any endomorphism $\alpha : E \rightarrow E$

6) If $E[r] = \langle P \rangle \oplus \langle R \rangle$, then $e_r(P, R) = \xi$ is a primitive r -th root of unity.

The following algorithm developed by Miller computes $e_r(P, Q)$ in a polynomial time, efficiently. This algorithm for Weil pairing aims to construct rational functions f and g associated to the point P and Q and evaluate at divisors $D' = (Q + S) - (S)$ and $D = (P + R) - (R)$, respectively. The functions f and g can be efficiently computed by double and add procedure. This idea is to define functions f_i, g_i , where $1 \leq i \leq r$ and $f_r = f, g_r = g$, recursively. These functions are computed by the following way :

$$f = \frac{v_P R}{l_{P,R}}, f_i = f_i f_j \frac{l_{iP,jP}}{v_{iP} v_{jP}}, f_i = f_i \frac{t_{iP}}{v_{iP}}$$

where v_P is the vertical line at P , t_R is the tangent line at R and $l_{P,Q}$ is the line passing through the points P and Q .

Let $P, Q \in E[r]$ and let $f \in \mathbb{F}_q^*$ be a function with $\text{div}(f) = r(P) - r(\infty)$. Let $R \in E(\mathbb{F}_{q^k})$ such that $R \notin \{\infty, P, -Q, P - Q\}$, and let $D_Q = (Q + R) - (R)$. Let k be the embedding degree and let $E(\mathbb{F}_{q^k})[r] = E(\mathbb{F}_{q^k}) \cap E[r]$. Note that $\text{supp}(D_Q) \cap \text{supp}(\text{div}(f)) = \emptyset$ due to the choice of R .

Definition 10. The bilinear map

$$\langle \cdot, \cdot \rangle : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \rightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r \rightarrow \mu_r$$

defined by

$$\langle P, Q \rangle = f_P(D_Q)^{q^k - 1/r} = (f_P(Q + R)/f_P(R))^{q^k - 1/r}$$

is called Tate pairing. This map is well-defined, i.e., $\langle \infty, Q \rangle = 1$ for all $Q \in E(\mathbb{F}_{q^k})$ and $\langle P, Q \rangle \in (\mathbb{F}_{q^k}^*)^r$ for all $P \in E(\mathbb{F}_{q^k})[r]$ and all $Q \in rE(\mathbb{F}_{q^k})$.

Theorem 11. (Properties of Tate Pairing) Let E be an elliptic curve defined over $\mathbb{F}_q$. Let $r > 0$ and $\gcd(r, q - 1) = 1$, and let k be the embedding degree of $E[r]$. Then, the Tate pairing satisfies the following properties :

- 1) (bilinearity) For all $P, P', P'' \in E(\mathbb{F}_{q^k})[r]$, and $Q, Q', Q'' \in E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$, $\langle P + P', Q \rangle = \langle P, Q \rangle \langle P', Q \rangle$ and $\langle P, Q + Q' \rangle = \langle P, Q \rangle \langle P, Q' \rangle$.
- 2) (non-degeneracy) For all $P \in E(\mathbb{F}_{q^k})[r] - \infty$, there is some $Q \in E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ such that $\langle P, Q \rangle \neq 1$. Similarly, for all $Q \in E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ with $Q \notin rE(\mathbb{F}_{q^k})$ there is some $P \in E(\mathbb{F}_{q^k})[r]$ such that $\langle P, Q \rangle \neq 1$.

The Tate pairing $\langle P, Q \rangle$ is computed by a function $f_P = f_r$ at the divisor $D_Q = (Q + R) - (R)$ using double and add method in the following way:

$$f = 1, f_i = f_i \frac{l_{iP,P}}{v_i v_P}, f_i = f_i \frac{t_{iP}}{v_i v_P}$$

By raising $f_P(D_Q)$ to the power $(q^k - 1)/r$, one obtains an r -th roots of unity μ_r in $\mathbb{F}_{q^k}^*$.

The main differences between the Weil and Tate pairings are the symmetric property and exponentiation. The Weil pairing also requires more computation time than the Tate pairing.

IV. CURVE SELECTION

This section describes the elliptic curves that are suitable for implementing pairing-based protocols. It is well-known that the number of points of the elliptic curve E over $\mathbb{F}_q$ is defined by $\#E(\mathbb{F}_q) = q + 1 - t$ and by Hasse's Theorem [18] that $|t| \leq 2\sqrt{q}$. if p divides t , E is said to be supersingular. Otherwise, it is called ordinary. The following theorem, where the proof can be found in [13] shows the classification of supersingular curves over any finite field for pairing-based cryptography.

Theorem 12. Let E be a supersingular elliptic curve over $\mathbb{F}_q$ of order $q + 1 - t$, where $q = p^m$. Then, there are six families of supersingular curves with embedding degree $k \leq 6$.

- 1) $k = 1$: $t^2 = 4q$ and m is even
- 2) $k = 2$: $t = 0$ and $E(\mathbb{F}_q) \cong Z_{q+1}$.
- 3) $k = 2$: $t = 0$ and $E(\mathbb{F}_q) \cong Z_{(q+1)/2} \oplus Z_2$ and $q = 3 \pmod{4}$.
- 4) $k = 3$: $t^2 = q$ and m is even.
- 5) $k = 4$: $t^2 = 2q$ and $p = 2$ and m is odd.
- 6) $k = 6$: $t^2 = 3q$ and $p = 3$ and m is odd.

For supersingular curves, there is always so-called a distortion map, $\Psi : E(\mathbb{F}_q) \rightarrow E(\mathbb{F}_{q^k})$, which is easily computable. This allows us to choose $G = \langle P \rangle$, $G = \Psi(P)$ together with Weil/Tate pairing to produce a non-degenerate bilinear map $e : G \times G \rightarrow G$ such that $e(P, Q) = f(P, \Psi(Q))$. Distortion maps are all known for supersingular curves. Therefore, we have computable pairing associated to any supersingular curves.

Example 13.

If $q = 3 \pmod{4}$ and $E : y^2 = x^3 + ax$ for any $a \in \mathbb{F}_q^*$, then a distortion map is of the form $\Psi : E(\mathbb{F}_q) \rightarrow E(\mathbb{F}_{q^2})$, $\Psi(x, y) = (-x, iy)$, where i is a square root of -1 .

It is a research problem to find suitable non-supersingular (ordinary) curves for pairing-based cryptography [3], [19]. For this, one needs to find curves with large subgroups of size r for which embedding degree k of $E[r]$ is sufficiently small. It is known that the choice of these curves are very special due to the following theorem [2].

Theorem 14. [2] Let E be a randomly chosen elliptic curve over $\mathbb{F}_q$, where q is prime and $z/2 \geq q \geq z$. Let G be a subgroup of order r . Then the probability that $r \mid q^k - 1$ for some $k \geq (\log q)$ is less than $c(\log z) (\log \log z) / z$ for an efficiently computable constant c .

New special techniques are needed to construct such pairing-friendly curves. The only known method so far is Complex Multiplication method to construct suitable ordinary elliptic curves for pairing-based cryptography. This method is used to construct curves with endomorphism ring isomorphic to a given order in a quadratic imaginary field $Q(\sqrt{-D})$ with specified number of points, where D is discriminant of the characteristic polynomial [1].

Some of the classification of pairing-friendly ordinary curves constructed by using the Complex Multiplication [16] are given as follows:

- 1) Miyaji, Nakabayashi, and Takano (MNT) [15] give a complete characterization of ordinary elliptic curves of prime order with embedding degree $k = 3, 4, 6$.

- 2) Freeman [9] gives a construction for curves of prime order with $k = 10$.
- 3) Barreto and Naehrig [4] give a construction for curves of prime order with $k = 12$.

We would like to note that there is a general construction, originally due to Cocks and Pinch [8], for curves of arbitrary embedding degree k , but in this construction $\rho = \log q / \log r \approx 2$ for arbitrary k , which leads to inefficient implementation. It should be noticed that ρ should be as close as one for an efficient pairing-based cryptographic protocols.

There is no distortion map on ordinary curves. One overcomes this difficulty by going into so-called its twist E' over $\mathbb{F}_q$. For an efficient computation as above, this can be done as follows : Let E be an elliptic curve given by the equation

$$E : y^2 = x^3 + a_4x + a_6$$

over $\mathbb{F}_q$, where $q = p^m$ and $p > 3$. Let v be a quadratic non-residue in $\mathbb{F}_q$. Then, the twist of the curve is defined by the equation

$$E' : y^2 = x^3 + v^2a_4x + v^3a_6$$

over $\mathbb{F}_q$.

Even embedding degree $k = 2d$ for $E[r] \subset E(\mathbb{F}_q)$, we consider the twist $E'(\mathbb{F}_{q^d})$ of $E(\mathbb{F}_{q^d})$. It is easy to show that the map $\Psi : E'(\mathbb{F}_{q^d}) \rightarrow E(\mathbb{F}_{q^k})$ given by $\Psi(x, y) = (v^{-1}x, v^{-3/2}y)$ is well-defined and easily computable. As in the supersingular case we can use this map Ψ to produce computable bilinear map $e(P, Q') = f(P, \Psi(Q'))$, where $Q' \in E'(\mathbb{F}_{q^d})$ of order a multiple of r and for the choice of Weil or Tate pairing. So, if we have a suitable ordinary elliptic curve for pairing-based cryptography, this method gives us a computable bilinear map e to used for these.

V. CONCLUSIONS

In this paper, we give an introduction to pairing-based cryptography. New cryptographic protocols and applications whose security is based on pairings are still growing very fastly. To implement these protocols new pairing methods based on Tate pairing are also being proposed.

ACKNOWLEDGMENT

We would like to thank Professor Ersan Akyıldız for his valuable comments.

REFERENCES

- [1] A. Atkin and F. Morain, "Elliptic Curves and Primality Proving", *Math. Comp.* Vol. 61, no.203, pp. 29-68, 1993.
- [2] R. Balasubramanian and N. Koblitz, "The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm", *Journal of Cryptology*, 11(2), 141-145, 1998.
- [3] P. Duan, S. Cui and C. Chan, "Finding More Non-Supersingular Elliptic Curves for Pairing-Based Cryptosystems", *Proceedings of 2nd International Conference on Information Security (ICIS2005)*, Vol. 2, pp.157-163, 2005.
- [4] P.S.L.M. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order" in *SAC 2005*, ed. B. Preneel, S. Tavares, Springer LNCS 3897, pp. 319-331, 2006.
- [5] I.F. Blake, G. Seroussi and N.P. Smart, "Advances in Elliptic Curve Cryptography", *London Mathematical Society Lecture Note Series. 317*, Cambridge University, 2005.
- [6] D. Boneh, B. Lynn and H. Shacham, "Short Signature from the Weil Pairing", *Advances in Cryptology - ASIACRYPT01*, LNCS 2248, pp. 514-532, 2001.
- [7] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", *Advances in Cryptology CRYPTO01*, LNCS 2139, pp. 213-229, 2001.
- [8] C. Cocks and R.G.E. Pinch, "Identity-based cryptosystems based on the Weil pairing", *unpublished manuscript*, 2001.
- [9] D. Freeman, "Constructing pairing-friendly elliptic curves with embedding degree 10", In *Algorithmic Number Theory Symposium ANTS-VII*, volume 4076 of *Lecture Notes in Computer Science*, Springer, pp. 452-465, 2006.
- [10] G. Frey, M. Muller and H. Ruck, "The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems", *IEEE Transactions on Information Theory* 45(5), pp. 1717-1719, 1999.
- [11] S. Galbraith, K. Paterson and N. Smart, "Pairings for Cryptographers", available at <http://eprint.iacr.org/2006/165.ps.gz>, 2006
- [12] A. Joux, "A One Round Protocol for Tripartite Diffie-Hellman", *Proceedings of ANTS 4*, LNCS 1838, pp. 385-394, 2000.
- [13] A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", *The Annual ACM Symposium on Theory of Computing (STOC)*, ACM Press, pp. 808-819, 1991.
- [14] V.S. Miller, "The Weil Pairing, and Its Efficient Calculation", *Journal of Cryptology*, 17, pp. 235-261, 2004.
- [15] A. Miyaji, M. Nakabayashi and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction", *IEICE Transactions on Fundamentals E84-A(5)*, pp. 1234-1243, 2001.
- [16] F. Morain, "Building cyclic elliptic curves modulo large primes", in *EUROCRYPT 91*, ed. D. W. Davies, Springer LNCS 547, 328-336, 1991.
- [17] A. Shamir, "Identity based cryptosystems and signature schemes", *Advances in Cryptology CRYPTO 84*, LNCS 196, pp. 47-53, 1985.
- [18] J.H. Silverman, "The Arithmetic of Elliptic Curves", *Springer-Verlag*, 1986.
- [19] E. Verheul, "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems", *Journal of Cryptology*, 17, 277-296, 2004.

Arithmetic on Pairing-Friendly Fields

Sedat AKLEYLEK, Barış Bülent KIRLAR, Ömer SEVER, Zaliha YÜCE

Abstract—Pairing-friendly fields are introduced mainly for extension field operations used in pairing based cryptography. In this note, we give the implementation and comparison results of arithmetic operations on extension fields constructed by trinomials and cyclotomic polynomials with extension degree 2,3,4,5 and also pairing-friendly fields with extension degree 2,4.

Keywords —extension field arithmetic, cyclotomic polynomials, pairing-friendly fields.

I. INTRODUCTION

Bilinear pairings were known but has not been used widely in cryptography until the three-party key exchange in one round protocol was proposed by Joux in [9]. Then, identity-based encryption scheme in [5] and the short signature scheme in [4] were given. Afterwards, many protocols based on pairings has seen frequently.

For pairing-based cryptosystems efficient arithmetic on extension fields is a crucial issue for implementing efficient pairings. This arithmetic is primarily based on the field operations. In this context, pairing-friendly fields are defined by Koblitz and Menezes in [12]. In extension field arithmetic we are interested in multiplication, exponentiation, inversion and their computational costs. It is known that addition and subtraction are trivial and squaring is almost equivalent to multiplication.

Choosing elliptic curve with appropriate parameters is very important for an efficient and secure pairing implementation issues. Generally, $\mathbb{F}_p$ must be large enough, so that $E(\mathbb{F}_p)$ can prevent the success of elliptic curve discrete logarithm attacks, while $\mathbb{F}_{p^k}$ must be large enough to resist discrete logarithm attacks over finite fields. At the same time, p and k should be as small as possible to minimize time and space usage. In the literature, k is generally the form of $k = 2^i 3^j$, where $i \geq 0, j \geq 0$ and not both them are zero. MNT curve proposed in [16] for pairing-based cryptography with the embedding degree 3, 4, 6, while the embedding degree 3 is not in the class of pairing-friendly fields. Embedding degree smaller than or equal to 6 is enough for near future, embedding degree 10 and 12 curves which currently produce excessively large finite fields may be more desirable as time passes and index calculus improvements are discovered.

When measuring the efficiency of an extension field operation, one must count the number of base field operations.

Manuscript received November 10, 2008.

S. Akleyek, B. B. Kirlar, Ö. Sever, Z. Yüce are with the Institute of Applied Mathematics, METU, Ankara, Turkey, e-mail: {akleyek,kirlar}@metu.edu.tr, severomer@yahoo.com, zyuce@stm.com.tr

S. Akleyek is also with the Department of Computer Engineering, Ondokuz Mayıs University, Samsun, Turkey

B. B. Kirlar is also with the Department of Mathematics, Süleyman Demirel University, Isparta, Turkey

Z. Yüce is a software engineer in STM A.Ş.

* This research is partially supported by ASELSAN A.Ş.

Multiplication is the most used one among the base field operations and that is why we primarily focus on it in this note. As previous works; multiplication and squaring methods for pairing-friendly fields $\mathbb{F}_{p^k}$ with $k \in 2, 3, 4, 6$ has been reviewed in [7]. The formulas of Karatsuba multiplication in extension fields are given in [19]. In exponentiation Lucas method provides a faster way than the classical square-and-multiply method.

Our contribution is to show that cyclotomic polynomials and trinomials can also be used in the construction of extension fields as efficient as pairing-friendly fields.

Organization of this note is as follows. Section II summarizes the mathematical preliminaries. The definition of pairing-friendly fields and construction of extension fields by using trinomials and cyclotomic polynomials are given in Section III. We describe the methods and the implementation results for multiplication, inversion and exponentiation in Section IV. Timings are given in Section V. We conclude in Section VI.

II. PRELIMINARIES

It is well known that when any polynomial $f(x) \in \mathbb{F}_p[x]$ of order k is irreducible over the finite field $\mathbb{F}_p$, one can get a simple algebraic extension $\mathbb{F}_{p^k}$ of $\mathbb{F}_p$ with a root of $f(x)$ as a defining element of $\mathbb{F}_{p^k} : \mathbb{F}_{p^k} = \mathbb{F}_p(\alpha) = \mathbb{F}_p[x]/\langle f(x) \rangle = \{\sum c_i \alpha^i | c_i \in \mathbb{F}_p\}$. Multiplication in $\mathbb{F}_{p^k}$ is computed as a multiplication of polynomials with modulo $f(x)$ reduction. Construction of finite fields with suitable irreducible $f(x)$ is important for an efficient arithmetic. When one focuses on multiplication, there are various techniques in the literature (see [3], [11]) for multiplying two n -digit integers, but we only recall briefly Karatsuba technique since this was implemented in open source libraries. Karatsuba's method [10] proceeds by splitting the integers into k parts, and therefore it is natural to consider using it to implement multiplication in quadratic field extensions. For computing the product $c = ab \in \mathbb{F}_{p^2}$ with the polynomial $x^2 - \beta$ using the Karatsuba Method proceeds by precomputing $v_0 = a_0 b_0, v_1 = a_1 b_1$, and then

$$\begin{aligned} c_0 &= v_0 + \beta v_1 \\ c_1 &= (a_0 + a_1)(b_0 + b_1) - v_0 - v_1 \end{aligned}$$

We now give the definition of cyclotomic polynomials which are used to get the extension fields in the following sections.

Definition 1. The roots of the splitting field of $x^n - 1$ over a field K are called the n -th roots of unity over K . A generator of the cyclic group composing of all these roots is called a primitive n -th root of unity over K .

Definition 2. Let $\mathbb{F}_{p^k}$ be a field, $n \in \mathbb{Z}^+$ and $p \nmid n$. Then, the n -th cyclotomic polynomial $\Phi_n(x)$ is defined as

$$\prod_{\xi} (x - \xi)$$

where ξ ranges over the primitive n -th roots of unity.

We need the Frobenius action that plays a crucial role in the arithmetic of extension field.

Definition 3. Let $\mathbb{F}_{p^k}$ be a finite field. Then, the Frobenius map $\varphi_p : \mathbb{F}_{p^k} \rightarrow \mathbb{F}_{p^k}$ is given by the map $x \mapsto x^p$.

III. PAIRING-FRIENDLY FIELDS

Extension field arithmetic has an important role in pairing-based cryptosystems for an efficient implementation. The problem is how to choose or find suitable irreducible $f(x)$ with degree k for an efficient implementation. In this problem, $f(x)$ should have low-weight such as binomials ($x^k + \beta$, where $\beta \in \mathbb{F}_p$) and trinomials ($x^k + x^h + \delta$, where $k > h$ and $\delta \in \mathbb{F}_p$). In this respect, one must give a restriction on p that how to find such β and δ . Kobitz and Menezes introduced the notion of pairing-friendly fields in [12].

Definition 4. Let $k = 2^i 3^j$ with $i > 0$ and $j \geq 0$. If $p \equiv 1 \pmod{12}$, then $\mathbb{F}_{p^k}$ is called pairing-friendly field.

Theorem 5. [12] Let $\mathbb{F}_{p^k}$ be a pairing-friendly field and $\beta \in \mathbb{F}_p$ be neither a square nor a cube in $\mathbb{F}_p$. Then, $x^k - \beta$ in $\mathbb{F}_p[x]$ is irreducible over $\mathbb{F}_p$.

The advantage of constructing pairing-friendly fields is to easily find a small value of β which helps to reduce the cost of extension field arithmetic. With the help of this construction, one can perform a field multiplication in $\mathbb{F}_{p^k}$, where $k = 2^i 3^j$, with $3^i 5^j$ field multiplications in $\mathbb{F}_p$ by Karatsuba method. There are special examples for quadratic extension.

- 1) [18] Let $p \equiv 3 \pmod{4}$ and $k = 2$. Then, $x^2 + 1$ is irreducible over $\mathbb{F}_p[x]$ since -1 is a quadratic non-residue modulo p . Representation of elements is $a_0 + a_1 i$, where i is the imaginary square root of -1 and $a_0, a_1 \in \mathbb{F}_p$.
- 2) [13] Let $p \equiv 2 \pmod{3}$ and $k = 2$. Then, $x^2 + x + 1$ is irreducible over $\mathbb{F}_p[x]$ (See Lemma 6). Representation of elements is $a_0 \alpha + a_1 \alpha^2$, where $\alpha^3 = 1$ and $a_0, a_1 \in \mathbb{F}_p$.

Construction of extension fields is not limited with this definition for an efficient implementation for pairing-based cryptographic systems. In this section, we give other classes which uses cyclotomic polynomials for the embedding degrees 2, 4, 6, 10 instead of binomials and trinomials for the embedding degrees 3, 5 and show that the cost of the multiplication is the same as fields given in Definition 4. Moreover, for every cyclotomic polynomials, where $(k+1)$ is prime one can choose different prime numbers to use in construction of extension fields as efficient as pairing-friendly fields.

Lemma 6. 1) Let p be a prime such that $p \equiv 2 \pmod{3}$. Then, the third cyclotomic polynomial $\Phi_3(x) = (x^3 - 1)/(x - 1) = x^2 + x + 1$ is irreducible over $\mathbb{F}_p$.

- 2) Let p be a prime such that $p \equiv \mp 2 \pmod{5}$. Then, the fifth cyclotomic polynomial $\Phi_5(x) = (x^5 - 1)/(x - 1) = x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{F}_p$.
- 3) Let p be a prime such that $p \equiv 3 \pmod{7}$ or $p \equiv 5 \pmod{7}$. Then, the seventh cyclotomic polynomial $\Phi_7(x) = (x^7 - 1)/(x - 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{F}_p$.
- 4) Let p be a prime such that $p \equiv 2 \pmod{11}$ or $p \equiv 6 \pmod{11}$ or $p \equiv 7 \pmod{11}$ or $p \equiv 8 \pmod{11}$. Then, the eleventh cyclotomic polynomial $\Phi_{11}(x) = (x^{11} - 1)/(x - 1) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{F}_p$.

Proof:

- 1) Since $p - 1 \equiv 1 \pmod{3}$ and $\text{ord}(\mathbb{F}_p^*) = p - 1$, there is no element in $\mathbb{F}_p^*$ of order 3. Then, $\alpha^3 - 1 = (\alpha - 1)\Phi_3(\alpha) \neq 0$ for any $\alpha \neq 1$ in $\mathbb{F}_p^*$. As a result, $\Phi_3(x)$ has no roots in $\mathbb{F}_p$. The proofs of (2)-(4) are similar. ■

It should be noticed that k^{th} cyclotomic polynomial can be used when $(k+1)$ is a prime number. To perform a field multiplication in $\mathbb{F}_{p^k}$ one needs $k(k+1)/2$ field multiplications in $\mathbb{F}_p$. Trinomials with the extension degree 3 and 5 are given in the following lemma.

Lemma 7. 1) Let $k = 3$. Then, $f(x) = x^3 + x + 1$ is irreducible over $\mathbb{F}_p$ if $p \equiv 1 \pmod{4}$.
2) Let $k = 5$. Then, $f(x) = x^5 + x^2 + 1$ is irreducible over $\mathbb{F}_p$ if $p \equiv 1 \pmod{6}$.

Table I summarizes how to choose primes when one has irreducible binomial, trinomial or cyclotomic polynomials with small degree k . For every trinomials or cyclotomic polynomials one can use different primes to construct extension fields as efficient as pairing-friendly fields.

TABLE I
PRIME CLASSES FOR IRREDUCIBLE BINOMIAL, TRINOMIAL AND CYCLOTOMIC POLYNOMIALS

	Binomial	Trinomial	Cyclotomic
Quadratic	$p \equiv 1 \pmod{12}$	$p \equiv 2 \pmod{3}$	$p \equiv 2 \pmod{3}$
Cubic	$p \equiv 1 \pmod{12}$	$p \equiv 1 \pmod{4}$	-
Quartic	$p \equiv 1 \pmod{12}$	-	$p \equiv \mp 2 \pmod{5}$
Quintic	-	$p \equiv 1 \pmod{6}$	-
Sextic	$p \equiv 1 \pmod{12}$	-	$p \equiv 3 \pmod{7}$ $p \equiv 5 \pmod{7}$
Tenth	-	-	$p \equiv 2 \pmod{11}$ $p \equiv 6 \pmod{11}$ $p \equiv 7 \pmod{11}$ $p \equiv 8 \pmod{11}$

In the following section, we will show that the costs of multiplication, exponentiation and inversion using cyclotomic polynomials and trinomials are more or less identical.

IV. MULTIPLICATION, INVERSION AND EXPONENTIATION ON PAIRING-FRIENDLY FIELDS

A. Multiplication

Field multiplication is one of the most used arithmetic operation in the extension fields. In this subsection, we give

quadratic, direct quartic extensions by cyclotomic polynomials and cubic, quintic extensions by trinomials irreducible over $\mathbb{F}_p$ with their costs. Finally, we review the idea how to construct the tenth extension field with quadratic over quintic and quintic over quadratic. The cost for multiplying elements in $\mathbb{F}_{p^k}$ is based on the following operations on $\mathbb{F}_p$: multiplication (M), addition or subtraction (A) and multiplication by 2 (S).

1) *Quadratic*: Let $p \equiv 2 \pmod{3}$ and $F_{p^2} = \mathbb{F}_p[x]/\langle x^2 + x + 1 \rangle$, $x^3 = 1$. Let α be a root of $x^2 + x + 1$.
 $a = a_0\alpha + a_1\alpha^2$, where $a \in F_{p^2}$ and $a_0, a_1 \in \mathbb{F}_p$
 $b = b_0\alpha + b_1\alpha^2$, where $b \in F_{p^2}$ and $b_0, b_1 \in \mathbb{F}_p$

$$\begin{aligned} a \times b &= (a_0\alpha + a_1\alpha^2)(b_0\alpha + b_1\alpha^2) \\ &= (a_1b_1 - a_0b_1 - a_1b_0)\alpha \\ &+ (a_0b_0 - a_0b_1 - a_1b_0)\alpha^2 \\ &= c_0\alpha + c_1\alpha^2 \end{aligned}$$

where

$$\begin{aligned} c_0 &= a_1b_1 - a_0b_1 - a_1b_0 \\ c_1 &= a_0b_0 - a_0b_1 - a_1b_0 \end{aligned}$$

Set

$$\begin{aligned} v_0 &= a_0b_0 \\ v_1 &= a_1b_1 \\ v_2 &= (a_0 - a_1)(b_0 - b_1) \end{aligned}$$

Then,

$$\begin{aligned} c_0 &= -v_0 + v_2 \\ c_1 &= -v_1 + v_2 \end{aligned}$$

Cost : $3M + 4A$

Table III shows the implementation timings of multiplication in $\mathbb{F}_{p^2}$ with MIRACL based code, our code and NTL module. MIRACL zzn2_mul function is clearly fastest because it uses a combination of Lazy Reduction and Karatsuba's method.

2) *Cubic*: Let $p \equiv 1 \pmod{4}$ and $F_{p^3} = \mathbb{F}_p[x]/\langle x^3 + x + 1 \rangle$, $x^3 = -x - 1$. Let α be a root of $x^3 + x + 1$.
 $a = a_0 + a_1\alpha + a_2\alpha^2$, where $a \in \mathbb{F}_{p^3}$ and $a_0, a_1, a_2 \in \mathbb{F}_p$
 $b = b_0 + b_1\alpha + b_2\alpha^2$, where $b \in \mathbb{F}_{p^3}$ and $b_0, b_1, b_2 \in \mathbb{F}_p$

$$\begin{aligned} a \times b &= (a_0 + a_1 + a_2)(b_0 + b_1 + b_2) \\ &= a_0b_0 - a_1b_2 - a_2b_1 \\ &+ (a_1b_0 + a_0b_1 - a_1b_2 - a_2b_1 - a_2b_2)\alpha \\ &+ (a_2b_0 + a_1b_1 + a_0b_2 - a_2b_2)\alpha^2 \\ &= c_0 + c_1\alpha + c_2\alpha^2 \end{aligned}$$

where

$$\begin{aligned} c_0 &= a_0b_0 - a_1b_2 - a_2b_1 \\ c_1 &= a_1b_0 + a_0b_1 - a_1b_2 - a_2b_1 - a_2b_2 \\ c_2 &= a_2b_0 + a_1b_1 + a_0b_2 - a_2b_2 \end{aligned}$$

Set

$$\begin{aligned} v_0 &= a_0b_0, \quad v_3 = (a_0 + a_1)(b_0 + b_1), \\ v_1 &= a_1b_1, \quad v_4 = (a_0 + a_2)(b_0 + b_2), \\ v_2 &= a_2b_2, \quad v_5 = (a_1 + a_2)(b_1 + b_2). \end{aligned}$$

Then,

$$\begin{aligned} c_0 &= v_0 + v_1 + v_2 - v_5 \\ c_1 &= -v_0 + v_3 - v_5 \\ c_2 &= -v_0 - 2v_2 + v_4 \end{aligned}$$

Cost : $6M + 13A + 1S$

Table IV explains the implementation timings of multiplication in $\mathbb{F}_{p^3}$ with MIRACL prepared code, our code and NTL module. Our code has a redundancy and MIRACL method is faster in larger prime modulo although Karatsuba are used by all methods and computational cost is the same theoretically.

3) *Quartic*: Let $p \equiv \mp 2 \pmod{5}$ and $F_{p^4} = \mathbb{F}_p[x]/\langle x^4 + x^3 + x^2 + x + 1 \rangle$, $x^5 = 1$. Let α be a root of $x^4 + x^3 + x^2 + x + 1$.

$a = a_0\alpha + a_1\alpha^2 + a_2\alpha^3 + a_3\alpha^4$, where $a \in \mathbb{F}_{p^4}$ and $a_0, a_1, a_2, a_3 \in \mathbb{F}_p$
 $b = b_0\alpha + b_1\alpha^2 + b_2\alpha^3 + b_3\alpha^4$, where $b \in \mathbb{F}_{p^4}$ and $b_0, b_1, b_2, b_3 \in \mathbb{F}_p$

$$\begin{aligned} a \times b &= (a_0\alpha + a_1\alpha^2 + a_2\alpha^3 + a_3\alpha^4) \\ &\times (b_0\alpha + b_1\alpha^2 + b_2\alpha^3 + b_3\alpha^4) \\ &= c_0\alpha + c_1\alpha^2 + c_2\alpha^3 + c_3\alpha^4 \end{aligned}$$

Set

$$\begin{aligned} v_0 &= a_0b_0, \quad v_5 = (a_0 + a_2)(b_0 + b_2), \\ v_1 &= a_1b_1, \quad v_6 = (a_0 + a_3)(b_0 + b_3), \\ v_2 &= a_2b_2, \quad v_7 = (a_1 + a_2)(b_1 + b_2), \\ v_3 &= a_3b_3, \quad v_8 = (a_1 + a_3)(b_1 + b_3), \\ v_4 &= (a_0 + a_1)(b_0 + b_1), \quad v_9 = (a_2 + a_3)(b_2 + b_3). \end{aligned}$$

Then,

$$\begin{aligned} c_0 &= v_0 + 2v_2 - v_6 - v_7 + v_8 \\ c_1 &= 2v_0 + v_1 - v_6 - v_7 + v_9 \\ c_2 &= v_2 + 2v_3 + v_4 - v_6 - v_7 \\ c_3 &= 2v_1 + v_3 + v_5 - v_6 - v_7 \end{aligned}$$

Cost : $10M + 28A + 4S$

The implementation timings of multiplication in $\mathbb{F}_{p^4}$ with our code based on MIRACL and NTL module are demonstrated in Table V. Our code uses cyclotomic polynomial which results as a direct extension.

4) *Quintic*: Let $p \equiv 1 \pmod{6}$ and $F_{p^5} = \mathbb{F}_p[x]/\langle x^5 + x^2 + 1 \rangle$, $x^5 = -x^2 - 1$. Let α be a root of $x^5 + x^2 + 1$.
 $a = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4$, where $a \in \mathbb{F}_{p^5}$ and $a_0, a_1, a_2, a_3, a_4 \in \mathbb{F}_p$

$b = b_0 + b_1\alpha + b_2\alpha^2 + b_3\alpha^3 + b_4\alpha^4$, where $b \in \mathbb{F}_{p^5}$ and $b_0, b_1, b_2, b_3, b_4 \in \mathbb{F}_p$

$$\begin{aligned} a \times b &= (a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4) \\ &\times (b_0 + b_1\alpha + b_2\alpha^2 + b_3\alpha^3 + b_4\alpha^4) \\ &= c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 + c_4\alpha^4 \end{aligned}$$

Set

$$\begin{aligned} v_0 &= a_0b_0, & v_8 &= (a_0 + a_4)(b_0 + b_4), \\ v_1 &= a_1b_1, & v_9 &= (a_1 + a_2)(b_1 + b_2), \\ v_2 &= a_2b_2, & v_{10} &= (a_1 + a_3)(b_1 + b_3), \\ v_3 &= a_3b_3, & v_{11} &= (a_1 + a_4)(b_1 + b_4), \\ v_4 &= a_4b_4, & v_{12} &= (a_2 + a_3)(b_2 + b_3), \\ v_5 &= (a_0 + a_1)(b_0 + b_1), & v_{13} &= (a_2 + a_4)(b_2 + b_4), \\ v_6 &= (a_0 + a_2)(b_0 + b_2), & v_{14} &= (a_3 + a_4)(b_3 + b_4), \\ v_7 &= (a_0 + a_3)(b_0 + b_3), \end{aligned}$$

Then,

$$\begin{aligned} c_0 &= 2v_0 + v_2 + v_3 + 2v_4 - v_{11} - v_{12} \\ c_1 &= -v_0 - v_1 + v_2 - v_3 + v_4 + v_5 - v_{13} \\ c_2 &= -v_0 + 2v_1 + 2v_3 + 3v_4 + v_6 - v_{11} - v_{12} - v_{14} \\ c_3 &= -v_0 - v_1 - 2v_3 + 2v_4 + v_7 + v_9 - v_{13} \\ c_4 &= -v_0 - v_1 + v_2 + v_8 + v_{10} - v_{14} \end{aligned}$$

Cost : 15M+49A+7S

The implementation timings of multiplication in $\mathbb{F}_{p^5}$ with our code and NTL module are given in Table VI. Our method is used MIRACL's base field operations and runs faster than NTL in larger prime modulus but slower in smaller prime modulus.

5) *Tenth Extension:* We consider two possibilities for building a tenth extension : quadratic over quintic and quintic over quadratic.

- 1) We build $\mathbb{F}_{p^{10}}$ as $\mathbb{F}_{p^5}[y]/(y^2 - \gamma)$, where $\mathbb{F}_{p^5} = \mathbb{F}_p/(y^5 - \beta)$, β is a quintic non-residue in $\mathbb{F}_p$. An element $a \in \mathbb{F}_{p^{10}}$ is represented as $a_0 + a_1y$, where $a_0, a_1 \in \mathbb{F}_{p^5}$.
- 2) We construct $\mathbb{F}_{p^2} = \mathbb{F}_p[x]/(x^2 - \beta)$ and $\mathbb{F}_{p^{10}} = \mathbb{F}_{p^2}[y]/(y^5 - \gamma)$, where β is a quadratic non-residue in $\mathbb{F}_p$ and $\gamma = \sqrt[5]{\beta}$ is a quintic non-residue in $\mathbb{F}_{p^2}$. An element $a \in \mathbb{F}_{p^{10}}$ is represented as $a_0 + a_1y + a_2y^2 + a_3y^3 + a_4y^4$, where $a_0, a_1, a_2, a_3, a_4 \in \mathbb{F}_{p^2}$.

The implementation timings of multiplication in $\mathbb{F}_{p^{10}}$ with our codes and NTL module are shown in Table VII. We implemented two different towering. The results show that quadratic over quintic is faster than quintic over quadratic as expected, since establishing towering from bigger modulus to smaller modulus is faster than vice versa.

Summary of multiplicative costs for quadratic, cubic, quartic and quintic extensions is given in Table II. It is observed that there is no significant difference when one compares with pairing-friendly fields. However, by using cyclotomic polynomial instead of binomial in quadratic extension one can implement quadratic field multiplication with 1A+1S less than binomials.

TABLE II
MULTIPLICATIVE COSTS FOR QUADRATIC, CUBIC, QUARTIC AND QUINTIC EXTENSIONS

	Quadratic	Cubic	Quartic	Quintic
Multiplication	3	6	10	15
Addition	4	13	28	49
Shift	-	1	4	7

B. Inversion

Inversion in extension field with degree k corresponds to computing a multiplicative inverse of a polynomial modulo an irreducible polynomial $f(x)$ of degree k . There is an efficient algorithm in [11]. By using this algorithm and irreducible polynomials defined in Section 3, one can obtain the following examples.

- Example 8.** 1) Let $p \equiv 1 \pmod{12}$ and $x^2 - \beta$ be irreducible over $\mathbb{F}_p$ where β is quadratic non-residue in $\mathbb{F}_p$. Let $a \in \mathbb{F}_{p^2}$ be the form $a = a_0 + a_1\alpha$, where α is a root of $x^2 - \beta$. Then, $a^{-1} = (-a_0 + a_1\alpha)/(-a_0^2 + \beta a_1^2)$ in $\mathbb{F}_{p^2}$.
- 2) Let $p \equiv 1 \pmod{12}$ and $x^3 - \beta$ be irreducible over $\mathbb{F}_p$ where β is cubic non-residue in $\mathbb{F}_p$. Let $a \in \mathbb{F}_{p^3}$ be the form $a = a_0 + a_1\alpha + a_2\alpha^2$, where α is a root of $x^3 - \beta$. Then, $a^{-1} = a_2((a_0^2 - \beta a_1 a_2) + (-a_0 a_1 + \beta a_2^2)\alpha + (-a_0 a_2 + a_1^2)\alpha^2)/(-a_0 a_1 + \beta a_2^2)$ in $\mathbb{F}_{p^3}$.
- 3) [17] Let $p \equiv \mp 2 \pmod{5}$ and $x^4 + x^3 + x^2 + x + 1$ be irreducible over $\mathbb{F}_p$. Let $a \in \mathbb{F}_{p^4}$ be the form $a = a_0\alpha + a_1\alpha^2 + a_2\alpha^3 + a_3\alpha^4$, where α is a root of $x^4 + x^3 + x^2 + x + 1$. Then, the inverse of a in $\mathbb{F}_{p^4}$ can be defined by $a^{-1} = a_3\alpha + a_2\alpha^2 + a_1\alpha^3 + a_0\alpha^4$. This trick can be used point addition and doubling in Elliptic Curve Cryptosystems [6].
- 4) There is a method originally developed for using with binary extension fields applied to $\mathbb{F}_{p^k}$ [8]. In this method, main idea is to use Frobenius map. Let $\alpha \in \mathbb{F}_{p^k}$. Then, using this algorithm, we get $a^{-1} = a^{s-1}/(a^s)$, where $s = (p^k - 1)/(p - 1)$.

Table VIII gives inversion timings in $\mathbb{F}_{p^2}$ with MIRACL's method and NTL method. It is seen that MIRACL is strongly faster than NTL. Their inversion implementation method is based on the binomials.

C. Exponentiation

There is a relatively low cost implementation way of exponentiation in $\mathbb{F}_{p^2}$. If the order of subgroup divides $p+1$, Lucas sequences can be used in the exponentiation of even embedding degree. Let P and Q be in $\mathbb{F}_p$. Then, Lucas sequences $\{U_n\}$ and $\{V_n\}$ are two particular solutions of the general second order linear recurrence relation $T_n = PT_{n-1} - QT_{n-2}$ which corresponds to the polynomial equation $x^2 - Px + Q = 0$. Let α and β be the roots of this polynomial. Then, they are defined by

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad V_n = \alpha^n + \beta^n$$

where $U_0 = 0$, $U_1 = 1$ and $V_0 = 2$, $V_1 = P$ are the initial conditions. In the light of this sequences, raising any element of $\mathbb{F}_{p^2}$ to a power m is given by the following equation:

$$(a + ib)^m = V_m(2a)/2 + U_m(2a)ba,$$

where $i^2 = \delta$ for some quadratic non-residue $\delta \in \mathbb{F}_p$.

Table IX and Table X show Lucas exponentiation timing with our codes in $\mathbb{F}_{p^2}$ with MIRACL's base field operations and exponentiation timing of NTL module, respectively. Our implementation is faster since NTL does not use Lucas method for $\mathbb{F}_{p^2}$ does square-and-multiply for exponentiation. For bigger exponent k 's the difference increases since Lucas method has complexity with $\log(k)$.

We now give the following example related to the Frobenius action, where k is the extension degree and $\alpha \in \mathbb{F}_{p^k}$ is the root of the irreducible polynomial in $\mathbb{F}_p$.

Example 9. 1) Let $k = 2$, $x^2 + 1$ is irreducible over $\mathbb{F}_p$ and $a = a_0 + ia_1 \in \mathbb{F}_{p^2}$, where $a_0, a_1 \in \mathbb{F}_p$ and i quadratic non-residue. Then, $a^p = (a_0 + ia_1)^p = (a_0 - ia_1)$
2) Let $k = 2$, $p \equiv 2 \pmod{3}$ and $a = a_0\alpha + a_1\alpha^2 \in \mathbb{F}_{p^2}$ be an element of $\mathbb{F}_{p^2}$, where $a_0, a_1 \in \mathbb{F}_p$. Then, the third cyclotomic polynomial is irreducible over $\mathbb{F}_p$. $a^p = (a_0\alpha + a_1\alpha^2)^p = (a_1\alpha + a_0\alpha^2)$.
3) Let $k = 4$, $p \equiv \mp 2 \pmod{5}$ and $a = a_0\alpha + a_1\alpha^2 + a_2\alpha^3 + a_3\alpha^4 \in \mathbb{F}_{p^4}$, where $a_0, a_1, a_2, a_3 \in \mathbb{F}_p$. Then, the fifth cyclotomic polynomial is irreducible over $\mathbb{F}_p$. $a^p = (a_0\alpha + a_1\alpha^2 + a_2\alpha^3 + a_3\alpha^4)^p = a_2\alpha + a_0\alpha^2 + a_3\alpha^3 + a_1\alpha^4$.

V. TIMINGS

Tables given in APPENDIX show the timing comparison for extension field arithmetics implemented on MIRACL and GMP-NTL. Both libraries are installed as default installation in which MIRACL is used without its optimizations. For MIRACL we worked with default library ms32.lib. For GMP we run Cygwin as Linux simulator on the same computer, installed NTL based on GMP functions and used NTL's ZZ_pE module for field extension arithmetic.

The performance of arithmetic operations was measured on an Intel Core Duo 2*1,6 GHz (but uses only one core) with 2 GB RAM, running Windows XP SP2. We have coded in C for MIRACL and compiled in Visual C/C++ 6.0. We have used standard ZZ_pE class for GMP/NTL and compiled by GNU C++ Compiler.

We implemented Karatsuba multiplication for $k = 2, 3, 5$ and 10 in MIRACL. We implemented extension degree 10 in two different towerings : quadratic over quintic and quintic over quadratic. We used irreducible cyclotomic polynomial for quadratic, field and trinomials for others. Random primes were generated by MIRACL.

In GMP/NTL we used ready class ZZ_pE and its functions. Timings start by generating two random field elements and ends by multiplication of that elements. For exponentiation we implemented Lucas sequences for quadratic exponentiation in MIRACL but used NTL's prepared polynomial powering function. For inversion we used the prepared functions of MIRACL and NTL in quadratic extension.

VI. CONCLUSIONS

We have presented arithmetic operations; namely multiplication, exponentiation and inversion in the fields with extension degree 2,3,4,5 and 10. We have used cyclotomic and trinomial irreducible polynomials for representing the extension fields. This representation is of course different than the ones used for pairing-friendly fields. Our first observation is that cyclotomics and trinomials are also as efficient as ones used in pairing-friendly fields. Theoretically, for the multiplication on $\mathbb{F}_{p^k}$, we have shown that the number of arithmetic operations performed on $\mathbb{F}_p$ are comparable with ones corresponding to pairing-friendly fields.

ACKNOWLEDGMENT

We would like to thank Professor Ersan Akyıldız for his valuable comments.

REFERENCES

- [1] IEEE P1636.3TM/D1Draft Standard for Identity-based Public-key Cryptography Using Pairings
- [2] J.C.B. Bajard, L.Imbert, C.Negre and T. Plantard, "Efficient Multiplication $GF(p^k)$ for Elliptic Curve Cryptography", *Proceedings of the 16th IEEE Symposium on Computer Arithmetic (ARITH'03)*, pp. 182, 2003.
- [3] Daniel J. Bernstein. "Multidigit Multiplication for Mathematicians", Available from <http://cr.yp.to/arith.html#m3>, 2001.
- [4] D. Boneh, B. Lynn and H. Shacham, "Short Signature form the Weil Pairing", *Advances in Cryptology - ASIACRYPT01, LNCS 2248*, pp. 514-532, 2001.
- [5] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", *Advances in cryptology CRYPTO01, LNCS 2139*, pp. 213229, 2001.
- [6] M. Brown, D. Hankerson, J Lopez and A. Menezes, "Software Implementation of the NIST elliptic curves over prime fields", *In Proceedings of the 2001 conference on topics in cryptology: the cryptographers track at RSA, LNCS 2020*, pp. 250265, 2001.
- [7] A. Devegili, C. Eigeartaigh, M. Scott and R. Dahab, "Multiplication and Squaring on Pairing-Friendly Fields", *IACR ePrint Archive*, eprint.iacr.org/2006/471.pdf, 2006.
- [8] T. Itoh and S. Tsujii, "A Fast Algorithm for Computing Multiplicative Inverses in $GF(2^m)$ Using Normal Bases", *Information and Computation*, Vol.78, pp.171-177, 1988.
- [9] A. Joux, "A One Round Protocol for Tripartite Diffie-Hellman", *Proceedings of ANTS 4, LNCS 1838*, pp. 385-394, 2000.
- [10] A. Karatsuba and Y. Ofman, "Multiplication of Multidigit Numbers on Automata", *Soviet Physisc Doklary 7(7)*, pp. 595-596, 1963.
- [11] D. Knuth, "The Art of Computer Programming", Vol. 2, Third Edition, 1998.
- [12] N. Koblitz and A. Menezes, "Pairing-Based Cryptography at High Security Levels", *In Cryptography and Coding - IMA 2005, LNCS 3796* volume 3796, pp. 13-36, 2005.
- [13] A. Lenstra and E. Verheul, "The XTR Public Key System", *CRYPTO'00*, pp. 1-19, 2000.
- [14] B. Lynn, PhD. Thesis with the title "On The Implementaton Of Parng-Based Cryptosystems", June 2007.
- [15] A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", *The Annual ACM Symposium on Theory of Computing (STOC)*, ACM Press, pp. 8089, 1991.
- [16] A. Miyaji, M. Nakabayashi and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction", *IEICE Transactions on Fundamentals, E84-A(5)*, pp. 1234-1243, 2001.
- [17] Y. Park, S. Jeong and J. Lim "Fast Exponentiation in Subgroups of Finite Fields", *Electronics Letters*, Vol.38 No.13, pp. 629-630, 2002.
- [18] M. Scott, "Implementing Cryptographic Pairings", 2004.
- [19] A. Weimerskirch and C. Paar, "Generalizations of the Karatsuba Algorithm for Efficient Implementations", *IACR ePrint Archive*, eprint.iacr.org/2006/224.pdf, 2006.

APPENDIX

TABLE III
MULTIPLICATION IN $\mathbb{F}_{p^2}$ WITH MIRACL LIBRARY VS OUR
IMPLEMENTATION VS NTL

	160-bit	192-bit	256-bit	512-bit
Karatsuba (zsn2_mul)	0,003	0,004	0,005	0,011
Our implementation	0,020	0,032	0,041	0,085
NTL (ZZ_pE)	0,019	0,023	0,029	0,064

TABLE IV
MULTIPLICATION IN $\mathbb{F}_{p^3}$ WITH MIRACL LIBRARY VS OUR
IMPLEMENTATION VS NTL

	160-bit	192-bit	256-bit	512-bit
Karatsuba (zsn3_mul)	0,020	0,019	0,021	0,039
Our implementation	0,034	0,067	0,095	0,119
NTL (ZZ_pE)	0,027	0,030	0,039	0,081

TABLE V
MULTIPLICATION IN $\mathbb{F}_{p^4}$ WITH OUR IMPLEMENTATION VS NTL

	160-bit	192-bit	256-bit	512-bit
Our implementation	0,063	0,073	0,085	0,128
NTL (ZZ_pE)	0,040	0,049	0,059	0,119

TABLE VI
MULTIPLICATION IN $\mathbb{F}_{p^5}$ WITH OUR IMPLEMENTATION VS NTL

	160-bit	192-bit	256-bit	512-bit
Our implementation	0,069	0,074	0,085	0,128
NTL (ZZ_pE)	0,040	0,065	0,080	0,156

TABLE VII
MULTIPLICATION IN $\mathbb{F}_{p^{10}}$ WITH OUR IMPLEMENTATION (DIFFERENT
TOWERINGS) VS NTL

	160-bit	192-bit	256-bit	512-bit
Our implementation (quadratic over quintic)	0,309	0,319	0,346	0,494
Our implementation (quintic over quadratic)	0,411	0,420	0,443	0,576
NTL (ZZ_pE)	0,125	0,140	0,172	0,372

TABLE VIII
INVERSION IN $\mathbb{F}_{p^2}$ WITH MIRACL VS NTL

	160-bit	192-bit	256-bit	512-bit
MIRACL (zsn2_inv)	0,023	0,027	0,036	0,081
NTL (ZZ_pE)	0,073	0,080	0,092	0,170

TABLE IX
LUCAS EXPONENTIATION IN $\mathbb{F}_{p^2}$ WITH OUR IMPLEMENTATION FOR
DIFFERENT EXPONENT K VS. NTL

	160-bit	192-bit	256-bit	512-bit
$k = 10$	0,030	0,035	0,044	0,080
$k = 50$	0,033	0,057	0,061	0,134
$k = 200$	0,058	0,069	0,090	0,183
$k = 600$	0,047	0,082	0,107	0,216
$k = 1000$	0,053	0,094	0,115	0,233
$k = 2000$	0,060	0,097	0,124	0,258

TABLE X
EXPONENTIATION IN ZZ_pE NTL FOR DIFFERENT POWERS K

	160-bit	192-bit	256-bit	512-bit
$k = 10$	0,094	0,105	0,127	0,245
$k = 50$	0,153	0,174	0,212	0,422
$k = 200$	0,192	0,219	0,270	0,531
$k = 600$	0,253	0,288	0,351	0,707
$k = 1000$	0,290	0,333	0,412	0,836
$k = 2000$	0,317	0,361	0,443	0,890

Efficient Multiplication in Finite Fields of Characteristic 3 and 5 for Pairing Based Cryptography

Murat CENK, Ferruh ÖZBUDAK

Abstract—In [1], it is investigated the eta paring computation on general divisors over hyperelliptic curves $y^3 = x^p - x + d$ where p is a prime satisfying $p \equiv 1 \pmod{4}$. One of the used finite field in that paper is $\mathbb{F}_{5^n}$. In that paper, it is given a multiplication formula for $\mathbb{F}_{5^n}$ with at most 15 multiplications in $\mathbb{F}_n$. In our paper, firstly we give a brief survey of efficient multiplication in finite fields by giving an example of multiplication formula for $\mathbb{F}_{6m}$. Then we will apply the methods used for $\mathbb{F}_{6m}$ to $\mathbb{F}_{5n}$ in order to obtain explicit multiplication formula in $\mathbb{F}_{5n}$. We give a formula for multiplying elements of $\mathbb{F}_{5n}$ with 11 multiplications in $\mathbb{F}_n$ which is better than the formula given in [1].

Keywords — Finite field multiplication, pairing-based cryptography

I. INTRODUCTION

FINITE fields of characteristic three are useful for pairing-based cryptography. Therefore, special attention has been given to $\mathbb{F}_{3^m}$, recently [2], [3], [4], [5]. The elements of $\mathbb{F}_{3^m}$ can be represented by at most $(m-1)$ degree polynomials over $\mathbb{F}_3$. To multiply elements of $\mathbb{F}_{3^m}$ one can use Karatsuba method [6], [7] or Montgomery formulae [8], which are among the main algorithms used in every finite fields. On the other hand, for finite fields of fixed characteristics, there are other methods that give more efficient algorithms for polynomial multiplication than Karatsuba and Montgomery in some cases. Some of those methods are Chinese Remainder Theorem (CRT) method [9] and Discrete Fourier Transform (DFT) method. In [3], [4], using DFT method, the multiplication formula in [2] for $\mathbb{F}_{3^{6m}}$ is improved. Moreover, in [5], it is found that using a method based on CRT for polynomial multiplication over $\mathbb{F}_3$ and suitable reductions, it is obtained an efficient multiplication method for finite fields of characteristic 3. For $5 \leq \ell \leq 18$, it is shown the canonical multiplication formulae over $\mathbb{F}_{3^{6m}}$ for any $m \geq 1$ with the best multiplicative complexity improving the bounds in [8].

In the recent paper [1], it is investigated the eta paring computation on general divisors over hyperelliptic curves $y^3 = x^p - x + d$ where p is a prime satisfying $p \equiv 1 \pmod{4}$. One of the used finite field in that paper is $\mathbb{F}_{5^{5n}}$. Moreover, in that paper, it is also given a multiplication formula for $\mathbb{F}_{5^{5n}}$ with at most 15 multiplications in $\mathbb{F}_{5n}$.

Murat Cenk is with the Department of Mathematics and Computer Science, Çankaya University, Ankara, Turkey, E-mail:mcenk@cankaya.edu.tr

Ferruh Özbudak is with the Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey, E-mail:ozbudak@metu.edu.tr

In this paper, firstly we give a brief survey of efficient multiplication in finite fields by giving an example of multiplication formula for $\mathbb{F}_{3^{6m}}$. Then we will apply the methods used for $\mathbb{F}_{3^{6m}}$ to $\mathbb{F}_{5^{5n}}$ in order to obtain explicit multiplication formula in $\mathbb{F}_{5^{5n}}$. We give a formula for multiplying elements of $\mathbb{F}_{5^{5n}}$ with 11 multiplications in $\mathbb{F}_{5n}$ which is better than the formula given in [1].

The rest of the paper is organized as follows. In Section II, we give a brief survey of efficient multiplication in finite fields by giving an example of multiplication formula for $\mathbb{F}_{3^{6m}}$. An explicit formula for multiplication in $\mathbb{F}_{5^{5n}}$ which requires 11 multiplications in $\mathbb{F}_{5n}$ is presented in Section III. Finally, we give the conclusion.

II. EFFICIENT POLYNOMIAL MULTIPLICATION OVER $\mathbb{F}_q$

In this section we give a brief review of efficient polynomial multiplication over $\mathbb{F}_q$.

Let $\mathbb{F}_q$ be the field with q elements. Let $n \geq 1$ be an integer. A polynomial $A(x)$ of the form

$$A(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}, \quad a_{n-1} \neq 0$$

is called an n -term polynomial. $M_q(n)$ denotes the minimum number of multiplications needed in $\mathbb{F}_q$ in order to multiply two arbitrary n -term polynomials. We note that $M_q(n)$ is also called multiplicative complexity of n -term polynomials. Let $n \geq 1$ be an integer, $f(x)$ be an irreducible polynomial and $\ell \geq 1$ be an integer such that

$$\ell \deg(f(x)) < 2n - 1.$$

Let $A(x)$ and $B(x)$ be arbitrary n -term polynomials, $C(x) = A(x)B(x)$ and $\bar{A}(x), \bar{B}(x), \bar{C}(x)$ be the uniquely determined polynomials of degree strictly less than $\ell \deg(f(x))$ such that

$$\bar{A}(x) \equiv A(x) \pmod{f(x)^\ell},$$

$$\bar{B}(x) \equiv B(x) \pmod{f(x)^\ell},$$

$$\bar{C}(x) \equiv C(x) \pmod{f(x)^\ell}.$$

Notation 2.1: Let $M_{q,f,\ell}(n)$ denote the minimum number of multiplications needed in $\mathbb{F}_q$ in order to obtain $\bar{C}(x)$ from given n -term polynomials $A(x)$ and $B(x)$. Obtaining such $\bar{C}(x)$ from $A(x)$ and $B(x)$ is called multiplication of n -term polynomials modulo $f(x)^\ell$.

Let $1 \leq w \leq 2n - 2$ be an integer and $C(x) = c_0 + c_1x + \dots + c_{2n-2}x^{2n-2}$. Obtaining the last w coefficients

$c_{2n-2}, c_{2n-3}, \dots, c_{2n-1-w}$ of $C(x)$ is defined as the multiplication of n -term polynomials modulo $(x - \infty)^w$ [9], [10].

Notation 2.2: Let $M_{q,(x-\infty),w}(n)$ denote the minimum number of multiplications needed in $\mathbb{F}_q$ in order to obtain $c_{2n-2}, c_{2n-3}, \dots, c_{2n-1-w}$ from given n -term polynomials $A(x)$ and $B(x)$.

CRT method for finite field polynomial multiplication can be summarized as follows. For $1 \leq i \leq t$, let $m_i(x) = f_i(x)^{\ell_i}$ be the ℓ_i -th power ($\ell_i \geq 1$) of an irreducible polynomial $f_i(x)$ such that $\deg(m(x)) \geq 2n - 1$ where $m(x) = \prod_{i=1}^t m_i(x)$. Assume that $f_1(x), \dots, f_t(x)$ are distinct. Let $w \geq 1$ be an integer which corresponds to multiplication modulo $(x - \infty)^w$ (see [10] and [9, p. 34]). It follows from CRT algorithm that if

$$w + \sum_{i=1}^t \ell_i \deg(f_i(x)) \geq 2n - 1 \quad (\text{II.1})$$

then

$$M_q(n) \leq M_{q,(x-\infty),w}(n) + \sum_{i=1}^t M_{q,f,\ell}(n). \quad (\text{II.2})$$

The value of $M_{q,f,\ell}(n)$ can be bounded from above by $M_q(\deg(f^\ell)) \leq M_q(\ell \cdot \deg(f))$. For example in [10], $M_{q,f,\ell}(n) \leq M_q(\ell \cdot \deg(f))$ is used for binary fields. In [11], we improved the estimate of $M_{q,f,\ell}(n)$ for the binary field $\mathbb{F}_2$. The same techniques also work for any finite field $\mathbb{F}_q$, in particular for fields of small characteristic such as $\mathbb{F}_3$ and $\mathbb{F}_5$. Before giving the improvement, we give the following definition.

Definition 2.3: Let $R = \mathbb{F}_q[x]$ be the ring of polynomials over $\mathbb{F}_q$ in variable x , $\ell \geq 1$ be an integer and

$$A(Y) = a_0(x) + a_1(x)Y + \dots + a_{\ell-1}(x)Y^{\ell-1},$$

$$B(Y) = b_0(x) + b_1(x)Y + \dots + b_{\ell-1}(x)Y^{\ell-1}$$

be two ℓ -term polynomials in the polynomial ring $R[Y]$ over R . Let $c_0(x), \dots, c_{2\ell-2}(x) \in R$ be given by

$$c_0(x) + c_1(x)Y + \dots + c_{2\ell-2}(x)Y^{2\ell-2} = A(Y)B(Y).$$

Let $\lambda_q(\ell)$ denote the minimum number of multiplications needed in R in order to obtain $c_0(x), c_1(x), \dots, c_{\ell-1}(x)$.

The following theorem provides further improvements. The proof can be seen in [11] and [5].

Theorem 2.4: Let $f(x)$ be an irreducible polynomial and $\ell \geq 1$ be an integer such that $\ell \deg(f(x)) < 2n - 1$. We have

$$M_{q,f,\ell}(n) \leq \lambda_q(\ell) M_q(\deg(f)). \quad (\text{II.3})$$

Remark 2.5: Let $1 \leq w \leq 2n - 1$ be an integer. Recall that the notation $M_{q,(x-\infty),w}(n)$ is given in Notation 2.2. It is clear that $M_q(1) = 1$. Using similar methods as in Theorem 2.4 we also obtain that

$$M_{q,(x-\infty),w}(n) \leq \lambda_q(w) M_q(1) = \lambda_q(w).$$

Corollary 2.6: $M_{q,x,w}(n)$ corresponds to computing first w coefficients $c_0, c_1, \dots, c_w$ of $c(x)$ and $M_{q,x,w}(n) = M_{q,(x-\infty),w}(n) \leq \lambda_q(w)$.

Some effective upper bounds of $\lambda_q(\ell)$ is given in the following proposition which contributes to improvements on $M_{q,f,\ell}(n)$. The proof is in [5].

Proposition 2.7: $\lambda_q(3) \leq 5, \lambda_q(4) \leq 8, \lambda_q(5) \leq 11, \lambda_q(6) \leq 15, \lambda_q(7) \leq 19, \lambda_q(8) \leq 24$, and $\lambda_q(9) \leq 29$.

Once we obtain a formula for multiplying n -term polynomials over $\mathbb{F}_q$, it is also valid over $\mathbb{F}_{q^m}$ because of the following theorem. The proof can be found in [12].

Theorem 2.8: The formulae for multiplication of two arbitrary n -term polynomials over $\mathbb{F}_q$ are also valid for multiplication of two arbitrary n -term polynomials over $\mathbb{F}_{q^m}$, where m is any positive integer.

The notation $\mu_q(n)$ represents the bilinear complexity of multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. It corresponds to the minimum number of $\mathbb{F}_q$ multiplications in order to multiply two arbitrary elements of $\mathbb{F}_{q^n}$. As reduction modulo an irreducible polynomial in $\mathbb{F}_q[x]$ can be performed without multiplications in $\mathbb{F}_q$, we have

$$\mu_q(n) \leq M_q(n). \quad (\text{II.4})$$

However $\mu_q(n)$ and $M_q(n)$ are not necessarily equal in general. Using a polynomial basis $\{1, \xi, \xi^2, \dots, \xi^{n-1}, \dots, \xi^{2n-2}\}$ for $\mathbb{F}_{q^{2n-1}}$ over $\mathbb{F}_q$, it is easy to show that

$$M_q(n) \leq \mu_q(2n - 1).$$

Example 2.9: The finite fields of $\mathbb{F}_{3^{6m}}$, where m is prime are used in id-based cryptography for efficient computation of the Tate pairing. In [2], it is given a multiplication algorithm in $\mathbb{F}_{3^{6m}}$ with 18 multiplications in $\mathbb{F}_{3^m}$. In [3], [4], multiplication in $\mathbb{F}_{3^{6m}}$ is decreased to 15 multiplications in $\mathbb{F}_{3^m}$. On the other hand, when we use $(x - \infty)^2, f_{11}, f_{12}, f_{13}, f_{21}, f_{22}$ and f_{23} in the method describe in Section II, we obtain $M_3(6) \leq 15$. Then by (II.4), the formula for multiplying two 6-term polynomials over $\mathbb{F}_3$ can be used for the multiplication over $\mathbb{F}_{3^{6m}}$ with 15 multiplications in $\mathbb{F}_{3^m}$. Now we will show that multiplication in $\mathbb{F}_{3^{6 \cdot 97}}$ which is investigated in [4] can be done with 15 multiplications in $\mathbb{F}_{3^{97}}$. Let us construct,

$$\mathbb{F}_{3^{97}} \cong \mathbb{F}_3[x]/(x^{97} + x^{16} + 2),$$

$$\mathbb{F}_{3^{6 \cdot 97}} \cong \mathbb{F}_{3^{97}}[y]/(y^6 + y - 1).$$

Let $\alpha, \beta, \gamma \in \mathbb{F}_{3^{6 \cdot 97}}$ such that $\alpha = \sum_{i=0}^5 a_i y^i, \beta = \sum_{i=0}^5 b_i y^i$

and $\gamma = \alpha \cdot \beta = \sum_{i=0}^5 c_i y^i$. Then the coefficients of γ

can be found as follows: First compute the coefficients of $\left(\sum_{i=0}^5 a_i y^i\right) \left(\sum_{i=0}^5 b_i y^i\right)$ and then reduce it modulo $y^6 + y - 1$.

Therefore, using the method described in Section II we get

$$c_0 = -m_{15} - m_1 + m_{10} - m_6 - m_5 + m_7 - m_8 - m_9 - m_{12} - m_{11};$$

$$c_1 = m_{15} + m_2 - m_3 - m_4 + m_5 - m_7 - m_8 + m_{10} - m_{11} + m_{12} + m_{13} + m_{14};$$

$$c_2 = -m_3 + m_5 + m_4 - m_6 - m_1 - m_2 - m_8 + m_9 - m_{13};$$

$$c_3 = -m_3 - m_5 + m_7 - m_1 - m_8 - m_9 - m_{13} - m_{15};$$

$$c_4 = m_6 + m_{13} - m_{12} - m_{11} - m_8 - m_{10} - m_5 - m_7 + m_2 - m_3 - m_4;$$

$$c_5 = m_{14} - m_8 + m_9 - m_{10} - m_6 + m_{13} - m_1 + m_3 - m_{11} + m_{12};$$

where m_i 's are

$$m_1 = (a_0 + a_1 + a_2 + a_3 + a_4 + a_5)(b_0 + b_1 + b_2 + b_3 + b_4 + b_5);$$

$$m_2 = (a_0 + a_1)(b_0 + b_1); m_3 = a_0 b_0; m_4 = a_1 b_1;$$

$m_5 = (a_1 - a_3 - a_5 + a_2)(b_1 - b_3 - b_5 + b_2);$
 $m_6 = (a_0 - a_2 - a_4 + a_1 - a_5)(b_0 - b_2 - b_4 + b_1 - b_5);$
 $m_7 = (a_0 - a_2 + a_4 + a_1 - a_3 + a_5)(b_0 - b_2 + b_4 + b_1 - b_3 + b_5);$
 $m_8 = (a_0 - a_2 + a_4)(b_0 - b_2 + b_4);$ $m_9 = (a_1 - a_3 + a_5)(b_1 - b_3 + b_5);$
 $m_{10} = (a_0 - a_1 + a_2 - a_3 + a_4 - a_5)(b_0 - b_1 + b_2 - b_3 + b_4 - b_5);$
 $m_{11} = (a_0 + a_2 - a_4 - a_3)(b_0 + b_2 - b_4 - b_3);$
 $m_{12} = (a_0 - a_4 + a_3 + a_1 - a_5)(b_0 - b_4 + b_3 + b_1 - b_5);$
 $m_{13} = (a_0 + a_2 - a_4 + a_3)(b_0 + b_2 - b_4 + b_3);$
 $m_{14} = (a_1 - a_3 - a_5 - a_2)(b_1 - b_3 - b_5 - b_2);$ $m_{15} = a_5 b_5;$
 On the other hand $\mathbb{F}_{3^{6 \cdot 97}}$ is constructed in [3], [4] using tower field representation, i.e.

$$\begin{aligned}
 \mathbb{F}_{3^{97}} &\cong \mathbb{F}_3[x]/(x^{97} + x^{16} + 2), \\
 \mathbb{F}_{3^{2 \cdot 97}} &\cong \mathbb{F}_{3^{97}}[y]/(y^2 + 1), \\
 \mathbb{F}_{3^{6 \cdot 97}} &\cong \mathbb{F}_{3^{2 \cdot 97}}[z]/(z^3 - z - 1).
 \end{aligned}$$

Therefore, the formula in [3], [4] contains multiplication by $\mp s, \mp(s+1)$ and $\mp(s-1)$, where $s \in \mathbb{F}_{3^{2 \cdot 97}}$ is a root of $y^2 + 1$. For both our proposed formula and the formula in [4], the number of multiplications is 15. The number of additions for our proposed formula is 137. Note that there are multiplications of form $(s \mp 1)m_i$ in the formula in [4]. Here $s \notin \mathbb{F}_3$. If we disregard the multiplication by s in the formula [4] and if we consider the cost of multiplication of the form $(s \mp 1)m_i$ for the formula in [4] as 1 addition only then the number of additions for the formula in [4] is still 138. Moreover, in our formula the only nonzero coefficients are ∓ 1 and we don't need to introduce intermediate field extension like $\mathbb{F}_{3^{2 \cdot 97}}$ containing $s \notin \mathbb{F}_3$. Therefore it seems that our construction would be preferable to the construction in [3], [4].

III. EFFICIENT MULTIPLICATION FOR $\mathbb{F}_{5^{5n}}$

The finite field $\mathbb{F}_{5^{5n}}$ is used in [1]. Multiplication in $\mathbb{F}_{5^{5n}}$ in [1] is performed by using Karatsuba-Ofman algorithm with 15 multiplications in $\mathbb{F}_{5^n}$ as follows. Let $A = \sum_{i=0}^4 a_i \rho^i$, $B = \sum_{i=0}^4 a_i \rho^i \in \mathbb{F}_{5^{5n}}$ where $\{1, \rho, \rho^2, \rho^3, \rho^4\}$ is a basis for $\mathbb{F}_{5^{5n}}$ over $\mathbb{F}_{5^n}$. Then

$$\begin{aligned}
 AB &= (A_2 \rho^3 + A_1)(B_1 \rho^3 + B_2) = A_2 B_2 \rho^6 + \\
 &((A_2 + A_1)(B_2 + B_1) - A_2 B_1 - A_1 B_1) \rho^3 + A_1 B_1,
 \end{aligned}$$

where

$$A_2 = (a_4 \rho + a_3), \quad A_1 = (a_2 \rho^2 + a_1 \rho + a_0)$$

$$B_2 = (b_4 \rho + b_3), \quad B_1 = (b_2 \rho^2 + b_1 \rho + b_0).$$

Since the polynomials A_2 and B_2 have 2 terms, $A_2 B_2$ needs 3 multiplications in $\mathbb{F}_{5^n}$ due to Karatsuba method. Since $A_1 B_1$ and $(A_2 + A_1)(B_2 + B_1)$ are 3-term polynomials over $\mathbb{F}_{5^n}$, they need 6 multiplications in $\mathbb{F}_{5^n}$ by Karatsuba method. Therefore, $\mu_{5^n}(5) \leq 15$.

In fact, the multiplication can be further improved. For example, we can improve this bound to 14 multiplications in $\mathbb{F}_{5^n}$ by observing a common multiplication $a_2 b_2$ in both $A_1 B_1$ and $(A_2 + A_1)(B_2 + B_1)$.

Moreover, we can decrease this bound to 13 as follows. Since $A_1 B_1$ and $(A_2 + A_1)(B_2 + B_1)$ are three term polynomials over $\mathbb{F}_{5^n}$, we can multiply them with 5 multiplications

by using the interpolation algorithm. For example, we can multiply 3-term polynomials over $\mathbb{F}_{5^n}$ as follows:

$$(a_0 + a_1 x + a_2 x^2)(b_0 + b_1 x + b_2 x^2) = m_1 + (4m_2 + 2m_3 + 3m_4 + m_5)x + (4m_2 + m_3 + m_4 + 4m_5)x^2 + (4m_2 + 3m_3 + 2m_4 + m_5)x^3 + (4m_1 + 4m_2 + 4m_3 + 4m_4 + 4m_5)x^4$$

where

$$m_1 = a_0 b_0,$$

$$m_2 = (a_0 + a_1 + a_2)(b_0 + b_1 + b_2),$$

$$m_3 = (a_0 + 2a_1 + 4a_2)(b_0 + 2b_1 + 4b_2),$$

$$m_4 = (a_0 + 3a_1 + 4a_2)(b_0 + 3b_1 + 4b_2),$$

$$m_5 = (a_0 + 4a_1 + a_2)(b_0 + 4b_1 + b_2).$$

Therefore, we can write $\mu_{5^n}(5) \leq 13$.

Now, we will show that this bound can be further improved by using the method presented in Section II by obtaining $M_5(5) \leq 11$. Let $a(x) = \sum_{i=0}^4 a_i x^i$ and $b(x) = \sum_{i=0}^4 b_i x^i$ be two 5-term polynomials over $\mathbb{F}_5$. Let

$$c(x) = \left(\sum_{i=0}^4 a_i x^i \right) \left(\sum_{i=0}^4 b_i x^i \right) = \sum_{i=0}^8 c_i x^i \quad (\text{III.1})$$

be product the polynomial. When we use the modulus polynomials $x^2, (x-1), (x-2), (x-3), (x-4)$ and $x^2 + 3$ as evaluation points in (III.1), we obtain the following system of linear, equations:

$$\begin{aligned}
 x^2 &\Rightarrow \begin{cases} m_1 = c_0, \\ m_2 - m_1 - m_3 = c_1, \end{cases} \\
 x-1 &\Rightarrow m_4 = (c_0 + \dots + c_8), \\
 x-2 &\Rightarrow m_5 = (c_0 + 2c_1 + \dots + 2^8 c_8), \\
 x-3 &\Rightarrow m_6 = (c_0 + 3c_1 + \dots + 3^8 c_8), \\
 x-4 &\Rightarrow m_7 = (c_0 + 4c_1 + \dots + 4^8 c_8), \\
 x-\infty &\Rightarrow m_8 = c_8, \\
 x^2 + 3 &\Rightarrow \begin{cases} m_9 + 2m_{10} = c_0 + 2c_2 + 4c_4 + 3c_6 + c_8, \\ m_{11} - m_9 - m_{10} = c_1 + 2c_3 + 4c_5 + 3c_7, \end{cases}
 \end{aligned}$$

where

$$\begin{aligned}
 m_1 &= a_0 b_0, \quad m_2 = (a_0 + a_1)(b_0 + b_1), \quad m_3 = a_1 b_1, \\
 m_4 &= (a_0 + a_1 + a_2 + a_3 + a_4)(b_0 + b_1 + b_2 + b_3 + b_4), \\
 m_5 &= (a_0 + 2a_1 + 4a_2 + 3a_3 + a_4)(b_0 + 2b_1 + 4b_2 + 3b_3 + b_4), \\
 m_6 &= (a_0 + 3a_1 + 4a_2 + 2a_3 + a_4)(b_0 + 3b_1 + 4b_2 + 2b_3 + b_4), \\
 m_7 &= (a_0 + 4a_1 + a_2 + 4a_3 + a_4)(b_0 + 4b_1 + b_2 + 4b_3 + b_4), \\
 m_8 &= a_4 b_4, \quad m_9 = (a_0 + 2a_2 + 4a_4)(b_0 + 2b_2 + 4b_4) \\
 m_{10} &= (a_1 + 2a_3)(b_1 + 2b_3), \\
 m_{11} &= (a_1 + 2a_3 + a_0 + 2a_2 + 4a_4)(b_1 + 2b_3 + b_0 + 2b_2 + 4b_4).
 \end{aligned}$$

So we obtain the following system of linear equations

$$M = G \cdot C, \quad (\text{III.2})$$

where

$$M = \begin{bmatrix} m_1 \\ m_2 - m_1 - m_3 \\ m_4 \\ m_5 \\ m_6 \\ m_7 \\ m_8 \\ m_9 + 2m_{10} \\ m_{11} - m_9 - m_{10} \end{bmatrix}, \quad C = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \\ c_8 \end{bmatrix},$$

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 & 1 & 2 & 4 & 3 & 1 \\ 1 & 3 & 4 & 2 & 1 & 3 & 4 & 2 & 1 \\ 1 & 4 & 1 & 4 & 1 & 4 & 1 & 4 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 2 & 0 & 4 & 0 & 3 & 0 & 1 \\ 0 & 1 & 0 & 2 & 0 & 4 & 0 & 3 & 0 \end{bmatrix}.$$

The resulting coefficients c_i 's for $0 \leq i \leq 8$ are obtained by solving equation (III.2). Since matrix G is invertible we have $C = M \cdot G^{-1}$ where

$$G^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 3 & 4 & 4 & 3 & 2 & 4 & 0 \\ 0 & 2 & 3 & 2 & 3 & 2 & 0 & 0 & 4 \\ 4 & 0 & 4 & 4 & 4 & 4 & 4 & 0 & 0 \\ 0 & 4 & 4 & 2 & 3 & 1 & 0 & 0 & 0 \\ 3 & 0 & 1 & 2 & 2 & 1 & 3 & 1 & 0 \\ 0 & 3 & 1 & 1 & 4 & 4 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

By using $C = M \cdot G^{-1}$, we get the following explicit formula.

$$\begin{aligned} c_0 &= m_1, \\ c_1 &= m_2 - m_1 - m_3, \\ c_2 &= 2m_1 + 3m_4 + 4m_5 + 4m_6 + 3m_7 + 2m_8 + 4m_9 + 8m_{10}, \\ c_3 &= 2m_2 - 2m_1 - 2m_3 + 3m_4 + 2m_5 + 3m_6 + 2m_7 + 4m_{11} - \\ &\quad 4m_9 - 4m_{10}, \\ c_4 &= 4m_1 + 4m_4 + 4m_5 + 4m_6 + 4m_7 + 4m_8, \\ c_5 &= 4m_2 - 4m_1 - 4m_3 + 4m_4 + 2m_5 + 3m_6 + m_7, \\ c_6 &= 3m_1 + m_4 + 2m_5 + 2m_6 + m_7 + 3m_8 + m_9 + 2m_{10}, \\ c_7 &= 3m_2 - 3m_1 - 3m_3 + m_4 + m_5 + 4m_6 + 4m_7 + m_{11} - \\ &\quad m_9 - m_{10}, \\ c_8 &= m_8. \end{aligned}$$

IV. CONCLUSION

We explain an efficient method for polynomial multiplication over $\mathbb{F}_q$. We give an explicit formula for multiplication in $\mathbb{F}_{5^{5n}}$ which requires 11 multiplications in $\mathbb{F}_{5^n}$. To the best of our knowledge, given formula which is better than the formula given in [1] is the best known formula.

ACKNOWLEDGMENTS

This work was supported by TÜBİTAK under Grant No. TBAG-107T826.

REFERENCES

- [1] E. Lee, H. Lee and Y. Lee, Eta pairing computation on general divisors over hyperelliptic curves $y^2 = x^p - x + d$, *Journal of Symbolic Computation*, 43(6-7), pp. 452-474.
- [2] T. Kerins, W. P. Marnane, E. M. Popovici, and P. S. L. M. Barreto, "Efficient hardware for the Tate pairing calculation in characteristic three", in *Cryptographic Hardware and Embedded Systems, CHES2005, ser. Lecture Notes in Computer Science*, J. R. Rao and B. Sunar, Eds., vol. 3659. Springer-Verlag, 2005, pp. 412 - 426.

- [3] E. Gorla, C. Puttmann and J. Shokrollahi, "Explicit formulas for efficient multiplication in $\mathbb{F}_{6m}$ ", in *Selected Areas in Cryptography (SAC 2007)* (Also available at http://www.arxiv.org/PS_cache/arxiv/pdf/0708/0708.3014v1.pdf).
- [4] J. Shokrollahi, E. Gorla and C. Puttmann, "Efficient FPGA-Based Multipliers for $\mathbb{F}_{97}$ and $\mathbb{F}_{6 \cdot 97}$ ", in *Field Programmable Logic and Applications (FPL 2007)* (Also available at http://www.arxiv.org/PS_cache/arxiv/pdf/0708/0708.3022v1.pdf).
- [5] M. Cenk, F. Özbudak, "Efficient multiplication in $\mathbb{F}_{\ell m}$, $m \geq 1$ and $5 \leq \ell \leq 18$ ", *Africacrypt 2008 volume 5023 of Lecture Notes in Computer Science*, 406-414 Springer - Verlag.
- [6] A. Karatsuba and Y. Ofman, "Multiplication of multidigit numbers by automata", *Soviet Physics-Doklady*, (7):595-596, 1963.
- [7] A. Weimerskirch, C. Paar, "Generalizations of the Karatsuba Algorithm for Polynomial Multiplication", available: <http://eprint.iacr.org/2006/224>.
- [8] P. L. Montgomery, "Five, six, and seven-term Karatsuba-like formulae", *IEEE Transactions on Computers*, 54(3):362-369, March 2005.
- [9] S. Winograd, *Arithmetic Complexity of Computations*, SIAM, 1980.
- [10] H. Fan and M. Anwar Hasan, Comments on "Five, Six, and Seven-Term Karatsuba-Like Formulae", *IEEE Transactions on Computers*, vol. 56, no. 5, pp. 716-717, 2007.
- [11] M. Cenk and F. Özbudak, "Improved Polynomial Multiplication Formulae over $\mathbb{F}$ Using Chinese Remainder Theorem", to appear in *IEEE Transactions on Computers*, accepted for publication on 7 October 2008.
- [12] M. D. Wagh and S. D. Morgera, "A new structured design method for convolutions over finite fields, Part I", *IEEE Transactions on Information Theory*, 29(4):583-594, 1983.

An Analysis of the Generalized ID-Based ElGamal Signatures

Hatice KOYUNCU, Kamer KAYA, Ali Aydın SELÇUK

Abstract—There have been many ID-based signature schemes proposed in recent years, most of which are, in one way or another, variants of the ElGamal signature scheme. Kalkan et al. proposed the concept of “generalized ID-based ElGamal signatures” as a unifying framework for these schemes, which also produced many new variants. In this paper, we analyze the security of these signature schemes and show that some of the proposed variants are insecure.

Keywords :—ID-based cryptography, ElGamal signatures, bilinear pairings.

I. INTRODUCTION

In 1984, Shamir [11] introduced the concept of ID-based cryptography to simplify key management procedures in public key infrastructures. Following Joux’s [7] discovery on how to utilize bilinear pairings in public key cryptosystems, Boneh and Franklin [2] proposed the first practical ID-based encryption scheme in Crypto 2001. Since then, ID-based cryptography has become one of the most active research areas in cryptography and numerous ID-based encryption and signature schemes have been proposed that use bilinear pairings.

ID-based cryptography helps us to simplify the key management process in traditional public key infrastructures. In ID-based cryptography any public information such as e-mail address, name, etc., can be used as a public key. Since public keys are derived from publicly known information, their authenticity is established inherently and there is no need for certificates in ID-based cryptography. The private key for a given public key is generated by a trusted authority and is sent to the user over a secure channel.

Recently, there have been many proposals for ID-based signatures [1], [3], [5], [9], [10], [12] and most of these schemes, in one way or the other, have been based on the ElGamal signature algorithm [4]. Horster et al. [6] showed that many variations of the basic ElGamal signature are possible by modifying the signature equation. Following their work, Kalkan et al. [8] extended those variants to the ID-based setting and observed that most of the existing ID-based signature schemes [1], [3], [5], [9], [10], [12] are special instances of a more general concept which they called the generalized ID-based ElGamal signature.

In this work, we analyze the security of these ID-based ElGamal signature variants and show that some of the schemes proposed by Kalkan et al. are actually insecure. We first show

how an attacker, having observed a message-signature pair, can obtain the private key of the signer or forge signatures on new messages. Second, we propose certain modifications on some of these signatures to avoid the security flaws involved.

The rest of the paper is organized as follows: Background concepts including bilinear pairings and generalized ElGamal signatures are discussed in Section II. We describe Kalkan et al.’s generalized ID-Based ElGamal signatures in detail in Section III. Some security flaws and attacks for some of the variants in [8] are described in Section IV and modifications to fix these variants are proposed in Section V. Section VI concludes the paper.

II. BACKGROUND

In this section, we present the tools that are used in generalized ID-based ElGamal signatures. We briefly discuss bilinear pairings, the ElGamal signature scheme and its generalizations.

A. Bilinear Pairings

Let G_1 be a cyclic additive group of order q generated by P . Let G_2 be a cyclic multiplicative group of the same order. A cryptographic bilinear pairing is defined as $e : G_1 \times G_1 \rightarrow G_2$ with the following properties:

- 1) *Bilinearity*: $e(aR, bS) = e(R, S)^{ab}$ where $R, S \in G_1$ and $a, b \in \mathbb{Z}_q$. This can also be stated as $\forall R, S, T \in G_1$ $e(R + S, T) = e(R, T)e(S, T)$ and $e(R, S + T) = e(R, S)e(R, T)$
- 2) *Non-degeneracy*: The map e does not send all pairs in $G_1 \times G_1$ to the identity of G_2 . That is $e(P, P) \neq 1$.
- 3) *Computability*: There exists an efficient algorithm to compute $e(R, S)$ for any $R, S \in G_1$

B. ElGamal Signature Scheme

Let p be a large prime and g be a generator of $\mathbb{Z}_p^*$. The user chooses $\alpha \in \mathbb{Z}_{p-1}$ as his private key and then computes $\beta = g^\alpha \mod p$ as his public key. The parameters p, g , and β are public whereas the user keeps α secret. To sign a message, the user generates a random $k \in_R \mathbb{Z}_{p-1}$. Then he computes $r = g^k \mod p$ and $s = k^{-1}(m - r\alpha) \mod (p - 1)$. The (r, s) pair is the signature of message m . The equation

$$m \equiv \alpha r + ks \pmod{p-1} \quad (1)$$

is called the *signature equation*, and verification is done by checking the congruence $g^m \stackrel{?}{=} \beta^r r^s \mod p$. Security of ElGamal signature relies on the discrete logarithm problem (DLP) since solving α from β or s from r, m, β can be reduced to solving the DLP in $\mathbb{Z}_p^*$.

H. Koyuncu is with ASELSAN INC Ankara, 06172, Turkey, e-mail: hkoyuncu@aselsan.com.tr

K. Kaya and Ali Aydın Selçuk are with Bilkent University, Department of Computer Engineering, Ankara, 06800, Turkey, email: {kamer,selcuk}@cs.bilkent.edu.tr

C. The Meta-ElGamal Signature Scheme

Horster et al. [6] showed that many variations of the basic ElGamal signature are possible by modifying the signature equation. Instead of using ElGamal's original signature equation, one can use the general equation

$$\pm A \equiv \pm \alpha B \pm kC \pmod{q}$$

where A , B and C are functions of m , r and s , q is a divisor of $p-1$, and g is an element in $\mathbb{Z}_p^*$ of order q . The signature can be verified by checking the equation:

$$g^{\pm A} \stackrel{?}{=} \beta^{\pm B} r^{\pm C} \pmod{p} \quad (2)$$

We refer the reader to [6] and [8] for further details.

D. An ID-Based ElGamal Signature Scheme

Let the private key generator (PKG) be a trusted party responsible for verifying the users' identities and generating their private keys. An ID-based signature scheme consists of four algorithms: SETUP, EXTRACT, SIGN, and VERIFY. As an example, consider the following ID-based version of the original ElGamal signature scheme:

- **SETUP:** Let G_1 be a cyclic additive group of order q generated by P . Let G_2 be a cyclic multiplicative group of the same order and $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing. The PKG chooses $s \in_R \mathbb{Z}_q^*$ as the global secret key and computes $P_{pub} = sP$ as the global public key. The PKG publishes system parameters $\langle G_1, G_2, e, P, P_{pub}, H, H_1 \rangle$ where H and H_1 are secure hash functions.
- **EXTRACT:** PKG verifies the user's identity ID and computes $Q_{ID} = H_1(ID)$ and $S_{ID} = sQ_{ID}$ as user's public and private keys respectively.
- **SIGN:** To sign a message $m \in \mathbb{Z}_q$, a user with his private key S_{ID} , first chooses $k \in_R \mathbb{Z}_q$, then computes:

$$\begin{aligned} r &= H(kP) \\ U &= k^{-1}(mP - rS_{ID}) \end{aligned}$$

The signature for the message m is (kP, U)

- **VERIFY:** Given ID , a message m , and a signature (kP, U) , the signature is valid if the following equation holds:

$$e(U, kP)e(Q_{ID}, P_{pub})^r \stackrel{?}{=} e(P, P)^m \quad (3)$$

The above scheme is the ID-based version of the original ElGamal signature scheme. The conversion process, which can also be used for the generalized signature equation, is described below:

In the original ElGamal scheme, the signature equation is $m \equiv \alpha r + ks \pmod{p-1}$ where $r = g^k$ and the signature is (r, s) . The corresponding signing equation for the ID-based ElGamal signature is:

$$mP = rS_{ID} + kU$$

Here, the uppercase letters are used to denote elements of the elliptic curve group G_1 . S_{ID} is the private key of the user; so it is a natural replacement for α in the original scheme. U is

the part of the signature that replaces s . The message m cannot be used in the equation directly since it is not a member of elliptic curve group; therefore mP is used to replace m .

A natural choice for r in the ID-based scheme is to compute r as $r = kP$ since r equals g^k in the original scheme. However, r must be an integer in $\mathbb{Z}_p$ in the signature equation, hence, it can be computed as $r = H(kP)$. Since kP is needed for verification (3), the signature will be issued as (kP, U) instead of (r, U) .

III. GENERALIZED ID-BASED ELGAMAL SIGNATURES

Kalkan et al. [8] discussed how the ID-based signature scheme above can be generalized by using the generalized signing equation

$$A = BS_{ID} + kC, \quad (4)$$

where (A, B, C) is a permutation of the parameters (m, r, U) , instead of the basic equation $mP = rS_{ID} + kU$. Note that, not all the permutations generate useful variants considering U as a member of elliptic curve group, and $m, r \in \mathbb{Z}_p$. Hence, A and C should be members of the elliptic curve group, but not B . Also note that mP and rP can be used instead of m and r , respectively. So, by permuting the elements of (m, r, U) , Kalkan et al. obtained four ID-based ElGamal signature variants. The signing equation for these variants are:

$$mP = rS_{ID} + kU \quad (5)$$

$$U = rS_{ID} + kmP \quad (6)$$

$$U = mS_{ID} + krP \quad (7)$$

$$rP = mS_{ID} + kU \quad (8)$$

Note that, the two variants where U is a coefficient of S_{ID} do not produce useful signing equations.

In the variants where kP is not needed for verification, r can be computed as $e(P, P)^k$ and the signature for m will be (r, U) . For other variants, where kP is needed for verification, r will be computed as $r = H(kP)$ and the signature for m will be (kP, U) . Kalkan et al. also proposed computing r as $H(m, kP)$ instead of $H(kP)$ or $e(P, P)^k$. In that case, m does not need to occur in the signing equations.

As in the work of Horster et al. [6], more variants can be produced by using different permutations. Instead of choosing (A, B, C) as a permutation of (m, r, U) , one can also choose them as a permutation of $(mr, U, 1)$, $(mr, mU, 1)$ and $(mr, rU, 1)$. Signs of A , B , and C can be changed by multiplying them by ± 1 . To obtain more variants, a general function $f(m, r)$ can be used instead of just the product mr . The verification equations and other details for all signatures proposed in [8] are summarized in Table I. Group I lists the variants that are obtained by permuting (m, r, U) and $(1, r, U)$. Group II lists the variants that are obtained by permuting $(mr, U, 1)$. Group III lists the variants that are obtained by permuting $(mr, mU, 1)$. Group IV lists the variants that are obtained by permuting $(mr, rU, 1)$ and $(r, rU, 1)$. Group V shows the rU variants, and finally, group VI shows the variants those were not possible on the basic ElGamal signatures. We refer the reader to [8] for more information about the generalization of the ID-based ElGamal signature schemes.

No.	r	U	Signature	Verification
ID I.1	$r = H(kP)$	$U = k^{-1}(mP - rS_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^r = e(P, P)^m$
ID I.2	$r = H(kP)$	$U = k^{-1}(rP - mS_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^m = e(P, P)^r$
ID I.3	$r = e(P, P)^k$	$U = kmP - rS_{ID}$	(r, U)	$e(U, P)e(Q_{ID}, P_{pub})^r = r^m$
ID I.4	$r = e(P, P)^k$	$U = rkP - mS_{ID}$	(r, U)	$e(U, P)e(Q_{ID}, P_{pub})^m = r^r$
ID I.5	$r = H(m, kP)$	$U = k^{-1}(P - rS_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^r = e(P, P)$
ID I.6	$r = H(m, kP)$	$U = k^{-1}(rP - S_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub}) = e(P, P)^r$
ID I.7	$r = H(m, kP)$	$U = kP - rS_{ID}$	(kP, U)	$e(U, P)e(Q_{ID}, P_{pub})^r = e(P, kP)$
ID I.8	$r = H(m, kP)$	$U = rkP - S_{ID}$	(kP, U)	$e(U, P)e(Q_{ID}, P_{pub}) = e(P, kP)^r$
ID II.1	$r = H(kP)$	$U = k^{-1}(P - mrS_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^{mr} = e(P, P)$
ID II.2	$r = H(kP)$	$U = k^{-1}(-S_{ID} + mrP)$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub}) = e(P, P)^{mr}$
ID II.3	$r = e(P, P)^k$	$U = kP - mrS_{ID}$	(r, U)	$e(U, P)e(Q_{ID}, P_{pub})^{mr} = r$
ID II.4	$r = e(P, P)^k$	$U = mrkP - S_{ID}$	(r, U)	$e(U, P)e(Q_{ID}, P_{pub}) = r^{mr}$
ID III.1	$r = H(kP)$	$U = k^{-1}(m^{-1}P - rS_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^r = e(P, P)^{m^{-1}}$
ID III.2	$r = H(kP)$	$U = k^{-1}(rP - m^{-1}S_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^{m^{-1}} = e(P, P)^r$
ID III.3	$r = e(P, P)^k$	$U = m^{-1}kP - rS_{ID}$	(r, U)	$e(U, P)e(Q_{ID}, P_{pub})^r = r^{m^{-1}}$
ID III.4	$r = e(P, P)^k$	$U = rkP - m^{-1}S_{ID}$	(r, U)	$e(U, P)e(Q_{ID}, P_{pub})^{m^{-1}} = r^r$
ID IV.1	$r = H(kP)$	$U = k^{-1}(mP - r^{-1}S_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^{r^{-1}} = e(P, P)^m$
ID IV.2	$r = H(kP)$	$U = k^{-1}(r^{-1}P - mS_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^m = e(P, P)^{r^{-1}}$
ID IV.3	$r = e(P, P)^k$	$U = mkP - r^{-1}S_{ID}$	(r, U)	$e(U, P)e(Q_{ID}, P_{pub})^{r^{-1}} = r^m$
ID IV.4	$r = e(P, P)^k$	$U = r^{-1}kP - mS_{ID}$	(r, U)	$e(U, P)e(Q_{ID}, P_{pub})^m = r^{r^{-1}}$
ID IV.5	$r = H(m, kP)$	$U = k^{-1}(P - r^{-1}S_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub})^{r^{-1}} = e(P, P)$
ID IV.6	$r = H(m, kP)$	$U = k^{-1}(r^{-1}P - S_{ID})$	(kP, U)	$e(U, kP)e(Q_{ID}, P_{pub}) = e(P, P)^{r^{-1}}$
ID IV.7	$r = H(m, kP)$	$U = kP - r^{-1}S_{ID}$	(kP, U)	$e(U, P)e(Q_{ID}, P_{pub})^{r^{-1}} = e(P, kP)$
ID IV.8	$r = H(m, kP)$	$U = r^{-1}kP - S_{ID}$	(kP, U)	$e(U, P)e(Q_{ID}, P_{pub}) = e(P, kP)^{r^{-1}}$
ID V.1	$r = H(kP)$	$U = k^{-1}r^{-1}(mP - S_{ID})$	(kP, U)	$e(U, kP)^r e(Q_{ID}, P_{pub}) = e(P, P)^m$
ID V.2	$r = H(kP)$	$U = k^{-1}r^{-1}(P - mS_{ID})$	(kP, U)	$e(U, kP)^r e(Q_{ID}, P_{pub})^m = e(P, P)$
ID V.3	$r = H(m, kP)$	$U = k^{-1}r^{-1}(P - S_{ID})$	(kP, U)	$e(U, kP)^r e(Q_{ID}, P_{pub}) = e(P, P)$
ID VI.1	$r = H(kQ_{ID})$	$U = (r + km)S_{ID}$	(kQ_{ID}, U)	$e(U, P) = e((r + km)Q_{ID}, P_{pub})$
ID VI.2	$r = H(kQ_{ID})$	$U = (m + kr)S_{ID}$	(kQ_{ID}, U)	$e(U, P) = e((kr + m)Q_{ID}, P_{pub})$
ID VI.3	$r = H(kQ_{ID})$	$U = (rm + k)S_{ID}$	(kQ_{ID}, U)	$e(U, P) = e((rm + k)Q_{ID}, P_{pub})$
ID VI.4	$r = H(kQ_{ID})$	$U = (1 + kmr)S_{ID}$	(kQ_{ID}, U)	$e(U, P) = e((1 + mkr)Q_{ID}, P_{pub})$
ID VI.5	$r = H(kQ_{ID})$	$U = r^{-1}(m + k)S_{ID}$	(kQ_{ID}, U)	$e(U, P)^r = e((m + k)Q_{ID}, P_{pub})$
ID VI.6	$r = H(kQ_{ID})$	$U = r^{-1}(1 + km)S_{ID}$	(kQ_{ID}, U)	$e(U, P)^r = e((mk + 1)Q_{ID}, P_{pub})$
ID VI.7	$r = H(m, kQ_{ID})$	$U = (r + k)S_{ID}$	(kQ_{ID}, U)	$e(U, P) = e((r + k)Q_{ID}, P_{pub})$
ID VI.8	$r = H(m, kQ_{ID})$	$U = r^{-1}(1 + k)S_{ID}$	(kQ_{ID}, U)	$e(U, P)^r = e((1 + k)Q_{ID}, P_{pub})$

TABLE I
THE GENERALIZED ID-BASED ELGAMAL SIGNATURES AND THEIR VERIFICATION EQUATIONS.

IV. INSECURE VARIANTS

We found that some of the schemes in Table III are insecure. Their insecurity results mainly from two reasons:

- There are variants where all the terms in the signing equation are public except S_{ID} ; hence, the private key S_{ID} can be extracted from the message-signature pair. Variants ID I.7, ID I.8, ID IV.7, and ID IV.8 have this kind of weakness.
- In some variants, r can be removed from the signature equation, which means that either the signature does not depend on the message or k can be modified according to a new message m' . Hence, one can forge a valid signature on a different message without knowing S_{ID} . Variants ID V.3, ID VI.5, ID VI.6, and ID VI.8 have this weakness.

Below, we describe our attacks in detail:

A. Variant ID I.7

The signature σ on a message m is computed as

$$\begin{aligned} r &= H(m, kP) \\ U &= kP - rS_{ID} \\ \sigma &= (kP, U). \end{aligned}$$

Seeing a message-signature pair (m, σ) , an adversary can find S_{ID} by computing

$$\begin{aligned} r &= H(m, kP) \\ S_{ID} &= r^{-1}(kP - U). \end{aligned}$$

B. Variant ID I.8

The signature σ on a message m is computed as

$$\begin{aligned} r &= H(m, kP) \\ U &= rkP - S_{ID} \\ \sigma &= (kP, U). \end{aligned}$$

Seeing a message-signature pair (m, σ) , an adversary can find S_{ID} by computing

$$\begin{aligned} r &= H(m, kP) \\ S_{ID} &= rkP - U. \end{aligned}$$

C. Variant ID IV.7

The signature σ on a message m is computed as

$$\begin{aligned} r &= H(m, kP) \\ U &= kP - r^{-1}S_{ID} \\ \sigma &= (kP, U). \end{aligned}$$

Seeing a message-signature pair (m, σ) , an adversary can find S_{ID} by computing

$$\begin{aligned} r &= H(m, kP) \\ S_{ID} &= r(kP - U). \end{aligned}$$

D. Variant ID IV.8

The signature σ on a message m is computed as

$$\begin{aligned} r &= H(m, kP) \\ U &= r^{-1}kP - S_{ID} \\ \sigma &= (kP, U). \end{aligned}$$

Seeing a message-signature pair (m, σ) , an adversary can find S_{ID} by computing

$$\begin{aligned} r &= H(m, kP) \\ S_{ID} &= r^{-1}kP - U. \end{aligned}$$

E. Variant ID V.3

The signature σ on a message m is computed as

$$\begin{aligned} r &= H(m, kP) \\ U &= k^{-1}r^{-1}(P - S_{ID}) \\ \sigma &= (kP, U). \end{aligned}$$

Seeing a message-signature pair (m, σ) , an adversary can forge a signature $\sigma' = (k'P, U')$ on a new message m' by first choosing a random $t \in_R \mathbb{Z}_q$. Then he can compute a valid $k'P$ and U' as follows:

$$\begin{aligned} k'P &= tkP \\ r' &= H(m', k'P) \\ U' &= t^{-1}r'^{-1}rU. \end{aligned}$$

Note that $U' = k'^{-1}r'^{-1}(P - S_{ID})$ hence, $\sigma' = (k'P, U')$ is a valid signature.

F. Variant ID VI.5

The signature σ on a message m is computed as

$$\begin{aligned} r &= H(kQ_{ID}) \\ U &= r^{-1}(m + k)S_{ID} \\ \sigma &= (kQ_{ID}, U). \end{aligned}$$

Seeing a message-signature pair (m, σ) , an adversary can forge a signature $\sigma' = (k'Q_{ID}, U')$ on a new message m' as follows:

$$\begin{aligned} k'Q_{ID} &= (m - m')Q_{ID} + kQ_{ID} \\ r' &= H(k'Q_{ID}) \\ U' &= r'^{-1}rU. \end{aligned}$$

Note that $U' = r'^{-1}(m' + k')S_{ID}$ hence, $\sigma' = (k'Q_{ID}, U')$ is a valid signature.

G. Variant ID VI.6

The signature σ on a message m is computed as

$$\begin{aligned} r &= H(kQ_{ID}) \\ U &= r^{-1}(1 + km)S_{ID} \\ \sigma &= (kQ_{ID}, U). \end{aligned}$$

Seeing a message-signature pair (m, σ) , an adversary can forge a signature $\sigma' = (k'Q_{ID}, U')$ on a new message m' as follows:

$$\begin{aligned} k'Q_{ID} &= mm'^{-1}kQ_{ID} \\ r' &= H(k'Q_{ID}) \\ U' &= r'^{-1}rU. \end{aligned}$$

Note that $U' = r'^{-1}(1 + k'm')S_{ID}$ hence, $\sigma' = (k'Q_{ID}, U')$ is a valid signature.

H. Variant ID VI.8

The signature σ on a message m is computed as

$$\begin{aligned} r &= H(kQ_{ID}) \\ U &= r^{-1}(1 + k)S_{ID} \\ \sigma &= (kQ_{ID}, U). \end{aligned}$$

Seeing a message-signature pair (m, σ) , an adversary can forge a signature $\sigma' = (k'Q_{ID}, U')$ on a new message m' as follows:

$$\begin{aligned} r' &= H(k'Q_{ID}) \\ U' &= r'^{-1}rU. \end{aligned}$$

Note that $U' = r'^{-1}(1 + k)S_{ID}$ hence, $\sigma' = (k'Q_{ID}, U')$ is a valid signature.

V. FIXING THE VARIANTS

As mentioned in Section IV, the first type of attack can be mounted since all terms in the signing equation are public except S_{ID} . Hence, seeing a message-signature pair, one can obtain the S_{ID} . To avoid this flaw, instead of P , we used P_{pub} in the signing equation for the variants ID I.7, ID I.8, ID IV.7 and ID IV.8. Note that even P_{pub} is public, kP_{pub} is secret since k is only known by the signer. The modified equations for these variants are given in Table II.

The variant ID I.7v2 is the same as the ID-Based ElGamal signature scheme of Yi [12]. Yi proved that the scheme is secure if the Diffie-Hellman problem is hard. The attacks proposed in this paper do not apply to the modified variants ID I.8v2, ID IV.7v2, and ID IV.8v2.

For other insecure variants, ID V.3, ID VI.5, ID VI.6 and ID VI.8, the main problem is that r can be eliminated from the signature equation with a single multiplication operation. We can change the signature equations by multiplying r^{-1} with only one term in the signature equation. For example, for variant ID V.3, the signature equation

$$U = k^{-1}r^{-1}(P - S_{ID})$$

No.	r	U	Signature	Verification
ID I.7v2	$r = H(m, kP)$	$U = kP_{pub} - rS_{ID}$	(kP, U)	$e(U, P)e(Q_{ID}, P_{pub})^r = e(P_{pub}, kP)$
ID I.8v2	$r = H(m, kP)$	$U = rkP_{pub} - S_{ID}$	(kP, U)	$e(U, P)e(Q_{ID}, P_{pub}) = e(P_{pub}, kP)^r$
ID IV.7v2	$r = H(m, kP)$	$U = kP_{pub} - r^{-1}S_{ID}$	(kP, U)	$e(U, P)e(Q_{ID}, P_{pub})^{r^{-1}} = e(P_{pub}, kP)$
ID IV.8v2	$r = H(m, kP)$	$U = r^{-1}kP_{pub} - S_{ID}$	(kP, U)	$e(U, P)e(Q_{ID}, P_{pub}) = e(P_{pub}, kP)^{r^{-1}}$

TABLE II
THE MODIFIED SIGNATURE AND VERIFICATION EQUATIONS OF SOME INSECURE VARIANTS.

can be modified as

$$U = k^{-1}(r^{-1}P - S_{ID})$$

or

$$U = k^{-1}(P - r^{-1}S_{ID}).$$

Although this modification prevents the attack to be mounted, the new variants are same as the variants ID IV.6 and ID IV.5, respectively. The same modification also generates the existing variants in the table for the remaining insecure variants ID VI.5, ID VI.6, and ID VI.8.

VI. CONCLUSION

In this paper, we revisited the generalized ID-based ElGamal signature schemes of Kalkan et al. [8] and showed that some of the proposed variants are insecure. We exploited the security flaws by proposing simple yet effective attacks in which an adversary can either obtain the private key of the signer or forge a signature on a message he desires. We then proposed some modifications to patch these variants. As this work shows, security proofs are necessary for the variants obtained in the generalization process of the ID-based signature schemes. For future work, we will try to prove the security of the remaining and the modified variants by using formal tools such as random oracles and zero-knowledge techniques.

REFERENCES

- [1] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J. Quisquater. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In *Proc. of ASIACRYPT'05*, volume 3778 of *LNCS*, pages 515–532, 2005.
- [2] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In *Proc. of CRYPTO'01*, volume 2139 of *LNCS*, pages 213–229. Springer-Verlag, 2001.
- [3] J. Cha and J.H. Cheon. An identity-based signature from gap Diffie-Hellman group. In *Proc. of PKC 2003*, volume 2567 of *LNCS*, pages 18–30. Springer-Verlag, 2003.
- [4] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Information Theory*, 31(4):469–472, 1985.
- [5] F. Hess. Efficient identity based signature schemes based on pairings. In *Proc. of SAC'02*, volume 2595 of *LNCS*, pages 310–324. Springer-Verlag, 2003.
- [6] P. Horster, H. Petersen, and M. Michels. Meta-elgamal signature schemes. In *Proc. of ACM Conference on Computer and Communications Security*, pages 96–107, 1994.
- [7] A. Joux. A one round protocol for tripartite diffie-hellman. In *Proc. of ANTS-IV*, volume 1838 of *LNCS*, pages 385–394, 2000.
- [8] S. Kalkan, K. Kaya, and A. A. Selçuk. Generalized ID-based ElGamal signatures. In *Proc. of ISCIS 2007*, pages 1–6, 2007.
- [9] K. Paterson. ID-based signatures from pairings on elliptic curves. Cryptology ePrint Archive, Report. <http://eprint.iacr.org/2002/004>.
- [10] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. In *Proc. of SCIS'00*, 2003.

- [11] A. Shamir. Identity-based cryptosystems and signature schemes. In *Proc. of CRYPTO'84*, volume 196 of *LNCS*, pages 47–53. Springer-Verlag, 1984.
- [12] X. Yi. An identity based signature scheme from the Weil pairing. *IEEE Communication Letters*, 7(2):76–78, 2003.

Dijital Hak Yönetimi ve Hukuksal Düzenlemeler

Caner AŞÇIOĞLU, Rüya ŞAMLI

Özet- Gelişen teknolojiler ve bu teknolojilerin hayatımızı kolaylaştıran yönleri gün geçtikçe artmaktadır. Ancak yenilikler ve gelişmeler pek çok soruyu ve sorunu da beraberinde getirmektedir. İnternetteki medya paylaşımı ve satışı, iktisadî anlamda milyar dolarlar ölçeğine ulaşırken, hukukun bu alanda getirmiş olduğu birtakım kurallar, şirketlerin çıkarları ve insanların özgürlük anlayışıyla çatışır duruma gelmiştir. Bu yüzden hem şirketler hem de insanlar alternatif yollarla sistemdeki boşlukları kullanarak, sistemi kendi lehlerine çevirmeye çalışmaktadırlar.

Şirketlerin yüksek kar marjı ve bireylerin karşısındakine zarar verici düzeylere ulaşabilecek sanal dünyadaki özgürlük talepleri arasında sıkışan hukuk, çözümü insan haklarının temel özelliklerinde bulmuştur. Bu çalışmada elektronik ortamda yapılan bilgi paylaşımı sonucunda kişilerin ve kurumların haklarının korunması anlamına gelmekte olan Dijital Hak Yönetimi konusu incelenecektir.

Anahtar kelimeler-Dijital Hak Yönetimi, DRM, telif hakları

I. GİRİŞ

Dijital Hak Yönetimi (Digital Right Management - DRM), temel olarak dijital ortamlar kullanılarak paylaşılan medya üzerindeki hakların korunması, kısıtlanması olarak tanımlanabilir. Tanımı, DRM sistemleriyle ilgili çok sayıda çözümün bulunması sebebiyle standartlaştırılamamıştır.

DRM yazılımları elektronik ortamdaki dosyaların değiştirilmesini, tamamen kopyalanmasını, içeriğinin kopyalanmasını, yazıcıdan çıktı alınması sırasında değişikliğe uğratılmasını, çıktı alınmasını, hatta ekran görüntüsünün alınmasını bile engelleyebilirler [1].

DRM sistemleri tüketici haklarına ve haklı rekabete izin vermesi ancak aynı zamanda da kullanıcıların özel ve gizli bilgilerinin korunması açısından işlevlerin yapılabilmesi için gereken en az seviyede kullanıcı bilgisi talep etmelidir.

Caner AŞÇIOĞLU is with the Computer Engineering Department and Faculty of Engineering İstanbul University, İstanbul, 34320 Turkey. (e-mail : 2Hcanasci@gmail.com).

Rüya ŞAMLI is with the Computer Engineering Department and Faculty of Engineering İstanbul University, İstanbul, 34320 Turkey. (e-mail : 3Hrsamli@istanbul.edu.tr).

Ülkemizin yasalarında, 5846 sayılı Fikir ve Sanat Eserleri Kanunu [2] ile DRM'nin hak yönetimi ve teknolojik önlemler ile ilgili düzenlemeler yapılmıştır. Ancak yine de diğer pek çok ülkenin hukuku kadar geniş yasalar içermemektedir.

Örneğin yasalarımıza göre telif hakkı ödenmeyen bir ürün ticarî kaygı olmaksızın dağıtılırsa suç kapsamına girmemektedir.

II. DİJİTAL HAK YÖNETİMİ (DIGITAL RIGHT MANAGEMENT - DRM)

Elektronik ortamda bulunan medya artık çok daha kolay kopyalanabilir hale gelmiştir. Medya ürünleri geniş bantlı iletişim ağları ve özellikle de p2p (peer to peer) [3] yazılımlar sayesinde pek çok kişiye iletebilmektedir. Ancak bu teknolojik paylaşım arttıkça buna paralel olarak etkin bir izleme ve kısıtlama sistemi de kurulmaktadır. Bu izleme ve kısıtlama yöntemlerine genel olarak dijital hak yönetim sistemleri denmektedir.

DRM, pek çok farklı tekniğin bulunması ve uygulamalar arasında gerekli standardizasyonun sağlanamaması nedeniyle kesin bir şekilde tanımlanamamaktadır. Tanımlamadaki zorluğun sebebi kullanılan her tekniğin farklı fonksiyonlarının mevcut olması ve bu fonksiyonların farklı birer medya üzerinde kullanılabilmesine imkan sağlamasıdır.

DRM yapısal olarak iki temelden oluşur :

A. Fikrî Mülkiyet Tanımlanması

DRM sistemlerinin en önemli ve zorunlu koşulu, dijital veriler üzerindeki fikrî mülkiyet haklarının ve hak sahiplerinin tanımlanmasıdır. Tanımlama bilgileri, yerleştirme yöntemiyle uyumlu çalışan okuma araçlarıyla (yazılım, donanım) yapılmaktadır.

DRM tanımlama bilgileri asgarî olarak şu bilgileri içermelidir:

- Fikrî mülkiyet sahiplerinin tanımlanması,
- Eser üzerinde korunan hakların tanımlanması,
- Eserin yaratılma zamanının tanımlanması,
- Tanımlama işleminde kullanılan yöntemlerin tanımlanması

B. Kullanım Kısıtlamalarının Uygulanması

DRM'nin fonksiyonel tarafı olan kullanım kısıtlamaları aşağıdaki şekillerde olabilir :

- İçeriğin tümüne erişimi engellemek,

-İçeriğin belirli bir bölümüne erişimin engellenmesi,

- a) Zaman bakımından,
- b) Bütünlük bakımından,
- c) Sayı sınırlı erişim bakımından

-İçeriğin değiştirilmesini engellemek,
-İçeriğin kopyalanmasını engellemek

III. SANAL ORTAMDA DRM'NİN ÖNEMİ

Bant genişliğinin artması, mobil araçların ve servis sağlayıcıların çoğalması dijital ortamdaki hizmet ve arz-talep döngüsünü arttırmış ve bunun oluşturduğu piyasayı büyüttüştür.

Araştırmalara göre 2004 yılında dünyada geniş bant kullanıcı sayısı 110 milyonun üzerine çıkmıştır. Teknolojinin gelişme ve yayılma hızı gözönüne alındığında önümüzdeki yıllarda bu sayının ne kadar olacağını öngörmek zordur. 2004 ve 2007 yılına ait online eğlence sektörüne ait veriler aşağıdaki tabloda gösterilmiştir [4].

Tablo 1 : Dünyadaki online eğlence pazarı ile ilgili iktisadi veriler

	2004	2007	Artış Yüzde
online eğlence pazarı	10 milyar \$	26 milyar \$	% 160
video on demand	79 milyon \$	2,3 milyar \$	% 3000
online video oyunları	1,2 milyar \$	3,5 milyar \$	%200

Tüm bu istatistiksel bilgiler bile online veya mobil dünyadaki paylaşımın ne kadar yoğun ve hızlı arttığını göstermeye yetmektedir. Bu verilere bakıldığında bu büyük rakamların döndüğü elektronik ortamda paylaşım konusunda hakların ve rekabetin korunmaması dünyadaki kayıtdışı ekonominin en önemli parçalarından biri olacağı ve hak sahiplerinin eşi benzeri görülmemiş bir hak kaybına destek vermiş olacağı görülmektedir. Bu yüzden bu durumu engellemek için çeşitli çalışmalar yapılmaktadır.

IV. DRM SİSTEMLERİ

Uluslararası alanda, çeşitli DRM sistemleri bulunmaktadır. Bu bölümde Windows Media DRM başta olmak üzere bu sistemlerden bazıları incelenecektir.

A. Windows Media DRM (WMDRM)

WMDRM, bilgisayarlar, taşınabilir aygıtlar ve ağ aygıtlarında, kayıttan yürütülmek üzere içerikleri koruma ve güvenli şekilde dağıtmada kendini kanıtlamış bir platformdur.

WMDRM'de baştan sona kimlik doğrulaması için dijital imzaları temel alan standart şifreleme protokolleri kullanılır. Örneğin, lisans sunucuları WMDRM tabanlı istemcilerin kimliğini doğrulamak için WMDRM teknolojilerini kullanır. Bu istemciler

kendi kişisel bilgisayarlarında dijital sertifikalar kullanır. Dijital sertifikaların benzersiz ortak anahtarı ve sürüm numarası istemciyi tanımlar. Lisanslar yalnızca kimliği doğrulanan istemcilere verilir. Lisansla bulunan dijital ortam dosyası anahtarı da yalnızca anahtarın verildiği WMDRM tabanlı istemci yazılımı tarafından alınabilecek şekilde şifrelenir. Dijital imza ise, kullanım kurallarının ihlal edilmesini önleyen ek koruma sağlar.

WMDRM'in çalışması esnasında alıcı yazılımı lisans sunucusundan içerik anahtarını sağlar. Sunucu bu anahtarı alıcıya göndermeden önce global olarak önceden belirlenmiş 160-bitlik Eliptik Eğri Kriptografisi (ECC : Elliptic Curve Cryptography) [5] anahtarıyla şifreler. Sunucu ayrıca şifrelenmemiş bir ID içerik anahtarını da gönderir. Lisanslı medya içerik anahtarı ile deşifre edilir.

Dolandırıcılığa karşı, medya yürütme hakları rastgele üretilmiş bir sayının alıcı ve sunucu tarafından alıcı yazılımı, alıcı makinesi ve sunucu yazılımı olmak üzere üç adet, önceden belirlenmiş ECC anahtarıyla şifrelenmesi ile korunur. Ayrıca anahtar değişimi, DES block cipher, RC4 stream cipher ve SHA-1 hashing fonksiyonları kullanılır.

Temel WMDRM çalışması şu şekildedir :

Paketleme: Windows Media Rights Managements dijital ortam dosyasını paketler. Şifrelenip bir anahtarla kilitlenmiş olan dosya şifreli bir lisans içinde depolanır. Lisansın alınabileceği URL gibi diğer bilgiler dijital ortam dosyasına eklenir. Dosya Windows Media Ses biçiminde (.wma uzantılı) veya Windows Media video biçiminde (.wmv uzantılı) kaydedilir.

Dağıtım: Paketlenen dosya yüklenmek üzere bir web sitesine yerleştirilebilir, uzaktan çalıştırılmak üzere bir dijital ortam sunucusuna konabilir, tüketicilere CD içinde verilebilir veya e-posta ile gönderilebilir. WMDRM, tüketicilerin kopya korumalı dijital ortam dosyalarını üçüncü şahıslara göndermelerine de izin vermektedir.

Lisans Sunucusu Belirleme: İçerik sağlayıcısı, lisansla ilgili belirli hakları ve kuralları depolayan ve Windows Media Rights Manager lisans hizmetlerini yerine getiren bir lisans onay merkezi seçer. Onay merkezinin görevi, tüketicinin lisans isteğini doğrulamaktır. Dijital ortam dosyaları ve bunların lisansları ayrı olarak dağıtılır ve depolanır, böylece tüm sistemin yönetimi kolaylaşır.

Lisans Alma : Tüketicinin paketlenmiş bir dijital ortam dosyasını çalıştırabilmesi için önce bir lisans anahtarı olarak dosyanın kilidini açması gerekir. Tüketici paketlenmiş bir dijital ortam dosyasını almayı denediğinde, önceden dağıtılan bir lisansı aldığında veya dosyayı ilk kez yürüttüğünde lisans alma işlemi otomatik olarak başlar. WM Rights Manager tüketiciye, bilgi istenen veya ödeme yapılmasını talep eden bir kayıt sayfası gönderir ya da onay merkezinde otomatik olarak bir lisans alır.

Dijital Ortam Dosyasını Yürütme: Dijital ortam dosyasını yürütmek için, tüketicinin WMDRM'yi

destekleyen bir yürütücüye gereksinimi vardır. Tüketici, lisansla yeralan kurallara veya haklara uygun şekilde dosyayı çalıştırabilir. Lisanslar başlangıç saatleri ve tarihleri, süreler veya sınırlı sayıda işlem gibi farklı haklar içerebilir.

B. SOFTWRAP

Yazılım üreticilerinin uygulamalarını internet üzerinden güvenli bir şekilde dağıtmalarını ve satmalarını sağlayan dijital bir pazarlama ve dağıtım sistemidir [6].

C. Elicense :

Viatech tarafından sağlanmakta olan sistem, içerik sahiplerine yazılım, kitap, müzik, video gibi ürünleri yayınlama ve dağıtma imkanı sağlayan e-ticaret teknolojisi [7].

D. CineadRM :

Dolby Laboratories'in bir bölümü olup DVD görüntüleyicilerini koruma özelliği olan bir DRM teknolojisi geliştirmiştir [4].

E. OPERA :

Birden fazla DRM platformunu entegre ederek, standardize edilmiş ara yüzler uygulamakta ve böylece karşılıklı sorunsuz olarak gerçekleştirilmektedir [4].

V. ULUSLARARASI ÇERÇEVEDE VE TÜRKİYE'DE DRM'İN HUKUKSAL DURUMU

DRM ilgili var olan hukuksal düzenlemeler genel olarak fikrî mülkiyet hukuku, tüketicinin korunması, rekabetin korunması, mahremiyetin korunması, yargı içtihadları konularını içermektedir. Buna göre DRM ile ilgili hukuksal durum uluslararası arenada ve Türkiye'de şu şekilde incelenebilir :

A. Uluslararası Alanda Durum

a)Uluslararası Alanda Çalışmalar

i)DRM ile İlgili Organizasyonlar

- MPEG: Hareketli görüntü uzmanları grubu [8].
 - OASIS: Yapılandırılmış bilgi standartlarının geliştirilmesi organizasyonu [9].
 - OeB: Açık e-kitap forumu [10].
 - TV-ANYTIME: Her zaman tv forumu [11].
 - OMA: Açık mobil ittifakı [12].
 - DMP: Dijital medya projesi [13].
 - CORAL : Coral Konsorsiyumu, araç ya da hizmet sağlayıcı fark etmeksizin, bugünün dijital müzik ve videolarına kolay erişim sağlanması amacıyla karşılıklı işbirlik amaçlamaktadır [14].
 - EC HLG-DRM : AB komisyonunun kurduğu High Level Group'tur [15].
 - ODRL: Açık dijital haklar dili teşebbüsü [16].
- ##### ii)DRM ile İlgili Uluslararası Projeler

DRM ile ilgili gerçekleştirilmekte olan pek çok uluslararası proje vardır. Elektronik hak yönetimi sistemlerinin gelişiminde diğer projeler ve gruplara yardım etmeyi amaçlayan [17], COPEARMS, internet ortamında telif haklarını ihlal eden durumların ortadan kaldırılmasına yönelik çalışmalar hakkında Avrupa çapında fikir birliği oluşturulması ve farkındalığın geliştirilmesine çalışan [18] RIGHTSWATCH, daha çok karma network ve platformlar arasında medyanın yaratılması, dağıtımı ve tüketilmesi problemlerinin çözümü ile ilgilenen [19] TIRAMISU bunlardan bazılarıdır.

b)Uluslararası Düzenlemeler

DRM tanımını içeren ve sadece bu konuyu kapsayan bir uluslararası düzenleme bulunmamakla beraber, kısmen de olsa DRM'ye ilişkin konuları ve bileşenleri düzenleyen uluslararası bazı düzenlemeler bulunmaktadır. Bu düzenlemelerde DRM ile ilgili yer alan konular, DRM'nin teknik bileşenleri olarak kabul edilebilecek olan hak yönetimi bilgileri, teknolojik önlemlerle ilgili düzenlemeler ve elektronik ortamda eser arzında bulunan kişiler hakkında uygulanabilecek servis sağlayıcılara ilişkin sorumluluklardır. Avrupa Birliği'nin 2001/29 ve 2000/31 [20] sayılı direktifleri ile ABD Digital Millenium Copyright Act [21], uluslararası bir düzenleme olmamalarına rağmen uygulamayı göz önünde bulunduran detaylı yaklaşımları ile uluslararası kabulleri gösteren önemli kaynaklar olarak kabul edilmektedirler.

WCT (WIPO Copyright Treaty – Eser Sahibinin Hakları Sözleşmesi) [22] ve WPPT (WIPO Performers and Phonograms Treaty – İcralar ve Fonogramlar Sözleşmesi) [23], eser sahiplerinin hakları ve bağlantılı haklar alanlarında mevcut olan uluslararası kabullerin yeni teknolojik gelişmeler sonucu yetersiz kaldığının ve uluslararası alanda yeni standartların kabul edilmesinin gerekli görülmesi üzerine Dünya Fikrî Mülkiyet Teşkilatı – WIPO [24] tarafından hazırlanmıştır. Her iki sözleşme de daha önceden hazırlanmış olmalarına rağmen 2002 yılında yürürlüğe girebilmiştir.

WCT ve WPPT'de çoğaltma hakkı, dijital ortam göz önüne alınarak geniş olarak tanımlanmış, ayrıca eserin elektronik ortamda dijital formda bulundurulmasının çoğaltma olacağı kabul edilmiştir. Yine her iki sözleşmede eserin internet ortamında bulundurulması özel bir hak kategorisi olarak düzenlenmiştir. Bu husus sözleşmelerde (WCT.m.8, WPPT.m.10,14) açık olarak “... eserlerinin kablolu ya da kablosuz ortamlarda, toplum üyelerinin kendileri tarafından seçilen bir yer ve zamanda bu eserlerden kişisel olarak yararlanacak biçimde topluma iletilmesine izin verme hususunda inhisarî bir hak sahibidir.” şeklinde ifade edilmiştir. Sözleşmelerde yer alan bu inhisarî nitelikteki hak ile, kuşkuyla uzak, açık ve anlaşılması kolay bir şekilde, hak sahiplerinin, eserlerinin dijital formda dağıtılmasını yasaklama yetkisi olduğunu iddia etmesi sağlanmıştır. Eser Sahibinin Hakları Anlaşması'nın 11 ve 12'nci maddelerine, İcralar ve Fonogramlar

Anlaşması'nın 18 ve 19. maddelerine göre sözleşmeye taraf olan ülkeler, eser sahiplerinin, yorumcuların ve fonogram yapımcılarının haklarını korumak üzere kullandıkları teknolojik önlemlerin ihlalini engellemek için gerekli yasal düzenlemeleri yapmak zorundadırlar. Anlaşmalara taraf olan ülkeler ayrıca; yetkisiz olarak elektronik hak yönetimi bilgisini kaldıran veya zarar veren, elektronik hak yönetimi bilgisi kaldırılmış veya zarar verilmiş eserleri, icraları veya fonogramları dağıtan, dağıtılmasına yardımcı olan veya ileten kimselere karşı gerekli yaptırımları içeren yasal düzenlemeleri yapmak zorundadırlar.

WIPO Eser Sahibinin Hakları Anlaşması'nın 12. (2) maddesinde, "hak yönetimi bilgisi"nin tanımı yapılmıştır. Buna göre; "hak yönetimi bilgisi"; eseri, eser sahibini, eserde herhangi bir hakkı bulunan hak sahibini ve/veya eserin kullanımıyla ilgili genel hükümleri tanımlayan bilgi veya bu bilgiyi tanımlayan numaralar veya kodlardır. WIPO İcralar ve Fonogramlar Anlaşması'nın 19. (2) maddesinde de benzer şekilde "hak yönetimi bilgisi"nin tanımı yapılmıştır. Buna göre; "hak yönetimi bilgisi"; yorumcuyu, yorumcunun yorumunu, fonogram yapımcısını, fonogramı, yorumda veya fonogramda herhangi bir hakkı bulunan hak sahibini, yorumun veya fonogram kullanımıyla ilgili genel hükümleri tanımlayan bilgi veya bu bilgiyi tanımlayan numaralar veya kodlardır. WIPO Eser Sahibinin Hakları Anlaşması'nın 10. maddesi ile WIPO İcralar ve Fonogramlar Anlaşması'nın 16. maddesinde "Sınırlamalar ve Bağışlıklar" başlığı altındaki hükümlerle Bern Sözleşmesinin üç basamak testinin (three-step test) eser sahibinin çoğaltma hakkının sınırlamalarına ve istisnalarına uygulanacağı öngörülmektedir. Söz konusu maddelerle akit tarafların Bern Sözleşmesiyle uyum sağlarken üç aşama testini kısıtlamaların ve istisnaların sınırlandırmasında uygulayacakları belirtilmiştir. Yine aynı maddelerle akit taraflar üç aşama testini kullanmak şartıyla ulusal mevzuat ile "eserin olağan kullanımını engellemeyecek ve eser sahibinin meşru yararlarına zarar vermeyecek bazı özel durumlarda" ek sınırlamalar ya da bağışlıklar öngörebilecektir. Bern sözleşmesinde yer alan üç basamak testi aynı zamanda eser sahibinin haklarından çoğaltma hakkının istisnalarının uygulanmasında, eserden yararlanabilmenin sınırlarını çizmektedir, bu doğrultuda hak ihlali yaratmayan çoğaltmanın özel durumlarla sınırlı kalma, eserin normal kullanım ölçülerini aşmama ve hak sahibinin yasal karını engellememe özelliklerine sahip olması gerekir. WCT'nin 1/4 maddesiyle Türkiye'nin de 1951 yılından beri üye olduğu [25] Bern Sözleşmesi'nin [26] çoğaltma hakkı ve istisnalarıyla ilgili hükmüne atıf yapılmış, akit tarafların bu hükümle bağlı olacakları belirtilmiştir. Buna göre Bern Sözleşmesinde yer alan "çoğaltma hakkı" ve "istisnaları" eserlerin dijital şekillerinin yer aldığı dijital ortama tamamiyle uygulanacaktır. Bir eserin dijital olarak depolanması onun kopyalanması olarak kabul edilecektir.

B. Türkiye'de Durum

Hukukumuzdaki DRM ile ilgili temel düzenleme 5846 sayılı Fikir ve Sanat Eserleri Kanunu'dur. Her ne kadar halen WIPO Sözleşmelerine taraf olunmamışsa da 5846 sayılı kanunda 2001 yılında 4630 sayılı kanunla yapılan değişiklikle – kanun gerekçesinde de açıkça belirtildiği üzere – WIPO Sözleşmeleri'nin temel hükümleri hukuk sistemimize alınmıştır. Yapılan değişiklikle, çoğaltma hakkı oldukça geniş olarak belirlenmiş, hak sahiplerine umuma iletim hakkı tanınmış ve ayrıca hak yönetim bilgileri ile teknolojik yöntemler hakkında düzenlemeler yapılmıştır.

2008 yılbaşından itibaren Türk Telekom, kullanıcılarına yasal müzik paylaşımı imkanı sunmaya başlamıştır. Bu imkan belli bir zaman aralığında belli bir sayıda şarkı indirilmesini içermek gibi bir sınırlamaya sahip olmakla beraber yalnızca Türk Telekom müşterilerinin sahip olduğu bir imkan olması açısından ve şarkılarda telif hakkına sahip olan sanatçılara emeğinin ödenmesi açısından online müzik paylaşımında bir devrim olarak kabul edilebilir. TTNet'in bu hizmetinde, TTNET, MÜ-YAP (Müzik Yapımcıları Meslek Birliği), MSG (Musik Eser Sahipleri Grubu meslek Birliği), MESAM (Müzik Eseri Sahipleri Meslek Birliği) ve MÜYORBİR (Müzik Yorumcuları Meslek Birliği) işbirliği içerisinde. Yasal olarak indirilebilen müzik parçaları, DRM ile TTNET ADSL abonelerine özel olarak lisanslanmakta, böylece şarkıların izinsiz olarak paylaşımının önüne geçilmektedir [27] [28].

VI. SONUÇ

İnternette her türlü bilginin paylaşımı gün geçtikçe artmaktadır. Kişilerin kendilerine ait dosyalarını paylaşmaları için internet biçilmiş bir kaftan olmasına karşın lisanslı film, müzik gibi multimedia araçlarının emeği geçen ve lisansa sahip olan kişilere herhangi bir ödeme yapılmaksızın paylaşılması konusunda maalesef uygunsuz bir ortam olmaktadır. Bu uygunsuz durumu engelleyebilmek için bu dijital ortamdaki paylaşım, DRM ile çözülmeye çalışılmaktadır. Ancak çok da eski olmayan DRM sistemleri henüz standartlaştırılamamıştır bu yüzden de sorunlar içermektedir. Farklı ülkelerin, farklı grupların DRM içerisine aldığı ve kanunlaştırdığı noktalar farklıdır. Birinin suç olarak gördüğünü diğeri suç olarak görmeyebilir. Bu durumda herkesin kabul edeceği ve uygulayacağı kurallar oluşturmak zorlaşmaktadır. Bununla birlikte DRM ile ilgili yapılan çalışmalar ve projeler devam etmekte; farklı gruplar farklı DRM sistemleri üzerinde çalışmakta ve optimum çözüm için büyük kaynaklar ayrılmaktadır. Bu durum ümit vericidir. Sonuçlar alınmaya başlandıkça bu konuya gelecekte daha fazla kaynak ayrılacağı ve bu şekilde daha yaratıcı ve kullanışlı sonuçlara ulaşılacağı düşünülmektedir. Ancak gene de DRM'in herhangi bir

bilginin mutlak gizliliğini sağlamanın mümkün olmadığı açıktır. Bu gizliliği sağlamak için kanunlaşmanın yanında çeşitli algoritmalara, kriptografik yöntemlere başvuruluyor olsa bile bu kriptografik yöntemler ne kadar güçlü olursa olsun her zaman bir açık kapı bulunacaktır.

KAYNAKLAR

- [1] Mehmet Emin Küçük, Kerem Özen, “*Telif Hakları, Bilgi Güvenliği ve Teknolojik Koruma*”, ÜNAK’07, Muğla.
- [2] <http://www.mevzuat.adalet.gov.tr/html/957.html>
- [3] <http://tr.wikipedia.org/wiki/Peer-to-peer>
- [4] İstanbul Bilgi Üniversitesi, Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi, Sayısal Haklar Yönetimi, İstanbul 2006.
- [5] <http://www.nationmaster.com/encyclopedia/WMDRM>
- [6] <http://www.softwrap.com>
- [7] <http://www.elicense.com>
- [8] <http://www.chiariglione.org/mpeg>
- [9] <http://www.oasis-open.org/home/index.php>
- [10] <http://www.idpf.org>
- [11] <http://www.tv-anytime.org>
- [12] <http://www.openmobilealliance.org>
- [13] <http://www.chiariglione.org/project>
- [14] <http://www.coral-interop.org>
- [15] http://europa.eu.int/information_society/europe/2005/all_about/digital_rights_man/index_en.htm
- [16] <http://odr1.net>
- [17] <http://www.ifla.org/VI/2/p5/projsum.htm>
- [18] www.rightswatch.com
- [19] <http://www.tiramisu-project.org>
- [20] http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32001L0029&mode=l=guichett
- [21] The Digital Millennium Copyright Act of 1998 – U.S. Copyright Office Summary
- [22] <http://www.wipo.int/treaties/en/ip/wct>
- [23] http://www.wipo.int/treaties/en/ip/wppt/trtdocs_wo034.html
- [24] <http://www.wipo.int>
- [25] DPT Sekizinci 5 Yıllık Kalkınma Planı – Fikri Haklar Özel İhtisas Komisyonu Raporu
- [26] <http://www.wipo.int/treaties/en/ip/berne>
- [27] www.akbilbilgisayar.com.tr
- [28] <http://www.ttnetmuzik.com>

Bir Sanal Noter Uygulamasının Teknolojik ve Hukuki Gereksinimleri

Dursun AKÇEŞME, A.Çoşkun SÖNMEZ

Abstract— Nowadays, internet has become an inseparable part of our lives. Every daily activities are being modeled under the name of e-process and with in the acceptance of e-sign law, e-state projects took part of virtual environment. This progress has arised the question wheter the public notary services can be realised in virtual environment.

In this study how public notary services can be realized is examined. As a result of this study, it's decided that a big part of public notary services can be implemented in virtual environment with in the consideration of technological and judicial requirements.

Keywords— Digital Certificate, Digital Notarization, Digital Signature, Private Key, Public Key, Public Key Infrastructure.

I. GİRİŞ

1970'lerde entegre devrelerinin icadı ile başlayan elektronikleşme süreci çok kısa sürede hayatın her alanına girmiştir. Hiç şüphe yoktur ki bu sürecin en önemli gelişmesi "internet"tir. Elektronik postayla başlayan bu süreç, internet bankacılığı ve elektronik ticaret ile doruğa ulaşmıştır. Bilişim dünyasında tüm bu gelişmeler ile birlikte sanal dünyada güvenliğin sağlanması da gitgide zorlaşmıştır.

Müthiş bir ivmeyle gelişen internet teknolojisi ile günlük hayatta yapılan işlerin birçoğu e-işlem adı altında internet ortamında modellenmiştir. Tüm bu gelişmeler beklentileri arttırmış kamu kurumlarını tek bir çatı altında birleştiren e-devlet kavramının doğmasına neden olmuştur. E-devlet projelerinde mutlak güvenliğin sağlanması gerekmektedir. Bu sebeple e-devlet projelerinde veri bütünlüğü ve veri gizliliği sağlanmalı, bunların yanında kimlik doğrulaması yapılabilmesi ve yapılan işlemlerin inkâr edilmemesi sağlanmalıdır.

Yukarıdaki bilgiler ışığında; kamu kurumları, işletmeler ve bireyler ile sürekli etkileşim halinde olan noterlere de sanal ortamda ihtiyaç duyulmuştur.

Noterlerin vermiş olduğu hizmetlerin tümünün sanal ortama taşınması hukuki mevzuattan ve yapılacak işin niteliğinden dolayı mümkün değildir[1]. Fakat noterlerin bazı hizmetlerinin sanal ortama taşınması, mevcut teknolojik koşullar ve hukuki düzenlemeler ile mümkün olabilmektedir. Bildiri içeriğinde, noterlerin sanal ortamda hizmet verebilmesi için, teknolojik gereksinimi açısından Açık Anahtar Altyapısı üzerine kurulan sayısal imza ve hukuki geçerlilik bakımından da 23 Temmuz 2004'te kabul edilen 5070 Sayılı Elektronik İmza Kanunu esas alınmıştır.

II. NOTER KURUMU

Noterler kamuya hizmet veren çok önemli kurumlardır. Toplum nazarında güven makamı olarak bilinirler. Yaptıkları her işlemde güvenliği maksimize etmeye çalışırlar. Herhangi bir noter işleminde temel olarak dört koşul yerine getirilir. Bunlar; noter işlemine konu olan belgenin içeriğinin tahrif edilemeyeceğinin(veri bütünlüğü), belgenin gizliliğinin muhafaza edileceğinin(veri gizliliği), işlemi yapan kişinin nüfus cüzdanı, ehliyet, pasaport vb. ile kimlik tespiti yapılacağı(kimlik doğrulama ve onaylama), inkâr edilmemesi için işlemi yapan kişinin ıslak imzasının alınacağı(inkâr edememe) güvence altına alınmasıdır. Tüm bu koşullar noterlerin yapmış olduğu her işlemde yerine getirilir. Görülüyor ki, bir Sanal Noter Uygulamasının gerçekleştirilebilmesi için yukarıda verilen,

- Veri Bütünlüğü
- Veri Gizliliği
- Kimlik Doğrulama ve Onaylama
- İnkâr Edememe

koşullarının sağlanması gerekmektedir. Aksi halde, Sanal Noter Uygulamasından söz edilemez.

Teknolojik olarak, Açık Anahtar Altyapısı üzerine kurulan sayısal imza ile veri gizliliği dışında, veri bütünlüğü, inkâr edememe, kimlik doğrulama ve onaylama sağlanabilmektedir[2]. Veri gizliliği için aşağıda verilen modelde görüleceği gibi kriptolojik yöntemlerden yararlanılmaktadır.

Hukuki açıdan, 5070 Sayılı Elektronik İmza Kanunu, nitelikli elektronik sertifika kullanılarak yapılan işlemleri hukuki olarak geçerli kılmaktadır.

III. TEKNOLOJİK GEREKSİNİMLER

A. Açık Anahtar Altyapısı(AAA)

Sanal Noter teknolojik altyapısı, Açık Anahtar Altyapısı üzerine kurulu olan sayısal imza ile sağlanmaktadır. Açık Anahtar Altyapısı'nın temel görevi; elektronik ortamda haberleşen, işlem gören ve çalışan kişiler, kurumlar ve cihazlar arasında güvenilir bir haberleşme ortamı oluşturmaktır[2]. Bu altyapı içerisinde gizlilik, bütünlük, inkâr edememe, kimlik doğrulama ve onaylama işlevleri sağlanarak sanal ortam güvenli hale getirilir.

AAA kriptoloji bilimi üzerine kurulmuş bir yapıdır. Kriptoloji bilimi günümüzde anahtar tabanlı şifreleme üzerine yoğunlaşmıştır. Anahtar tabanlı şifreleme iki çeşittir. Bunlar simetrik ve asimetrik şifrelemedir.

Simetrik şifreleme ve asimetrik şifreleme yöntemleri algoritma bağımsız şifreleme yöntemleridir. Algoritma bağımlı şifreleme yöntemleri günümüzde tercih edilmemektedir. Bunun sebebi, algoritmanın deşifre olması durumunda tüm sistemin güvenliğini tehlikeye girmesidir.

En eski şifreleme yöntemlerinden olan Sezar Şifreleme algoritma bağımlı şifrelemeye en güzel örnektir. Sezar Şifreleme, her karakteri kendisinden sonra gelen üçüncü karakteri alarak şifreler, deşifre etmek için de şifrelenmiş verinin her karakterinin kendisinden önce gelen üçüncü karakteri alarak metni deşifre eder[2].

Matematiksel olarak;

$$E(M) = (M+3) \bmod 29 = C \quad D(C) = (C-3) \bmod 29 = M$$

E	=	Şifreleme işlemi	D	=	Deşifre İşlemi
M	=	Şifrelenecek Metin	C	=	Şifrelenmiş Metin
C	=	Şifrelenmiş Metin	M	=	Deşifre Edilmiş Metin

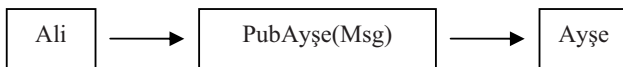
şeklinde ifade edilir. Fonksiyonda oluşan verinin 29 mod alınma sebebi alfabemizde 29 harf bulunmasıdır[2]. Bu şekilde bir şifreleme yapan sistemin algoritması mutlak suretle gizli kalmalıdır. Algoritmanın deşifresi tüm sistemi tehlikeye sokar.

Simetrik şifreleme yöntemlerinde metni şifreleme ve deşifre etmek için bir gizli anahtar kullanılır. Kullanılan bu anahtar şifreli haberleşmek isteyen her iki tarafta bilmelidir. Sistemin güvenliği gizli anahtarın büyüklüğü ile doğru orantılıdır. Simetrik şifreleme yönteminde, IBM tarafından geliştirilmiş olan DES(Data Encryption Standart) algoritması standart olarak kabul edilmektedir.

Asimetrik şifreleme yönteminde ise, veriyi şifrelemek ve deşifre etmek için farklı anahtarlar kullanılmaktadır. Bu iki anahtar üretilirken aralarında matematiksel bir bağ kurularak üretilir. Bu anahtarlar açık anahtar(public key) ve gizli anahtar(private key) olarak isimlendirilir. Bir anahtarın şifrelediği metni ancak ikizi olan diğer anahtar deşifre edebilir. Burada, açık anahtar herkes tarafından bilinen anahtardır. Gizli anahtar ise sadece sahibi tarafından bilinen ve gizli tutulması gereken anahtardır. Asimetrik şifrelemede, kullanılan algoritmanın bilinmesinin simetrik şifrelemede olduğu gibi hiçbir önemi yoktur.

AAA asimetrik şifreleme yöntemini kullanmaktadır. AAA da şifreli haberleşmek isteyen her bireyin açık ve gizli anahtarı vardır. Bu iki anahtarın nasıl kullanıldığını açıklayalım. Ali Ayşe ile AAA ile haberleşmek istemektedir. Her ikisi de birbirlerinin açık anahtarlarına erişebilmektedirler. Aşama aşama AAA'nın işlevlerini görelim.

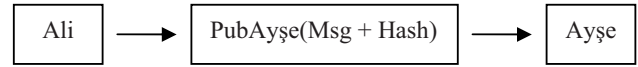
Ali Ayşe'ye gizliliği sağlanmış bir mesaj göndermek istediğinde; Ali göndereceği mesajı Ayşe'nin açık anahtarı ile şifreleyerek Ayşe'ye gönderir. Gönderim esnasında mesaja erişilse dahi şifrelenmiş olduğundan mesaj anlaşılamaz. Şifrelenmiş mesajı alan Ayşe kendi gizli anahtarı ile şifreli mesajı deşifre eder ve mesaja ulaşır. Bu örnekte anlaşıldığı üzere AAA ile gizlilik sağlanmış olur (Şekil 1).



Şekil 1. AAA Gizlilik İşlevi

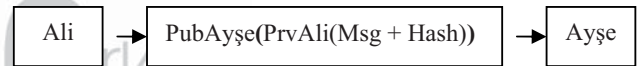
Ali Ayşe'ye gizliliği ve veri bütünlüğü sağlanmış mesaj göndermek istediğinde; Ali Ayşe'ye mesajı göndermeden önce hash algoritması (MD5, SHA-1, SHA-2 vb.) ile mesajın

özetini çıkartır. Bu algoritma mesajın uzunluğu ne olursa olsun sabit uzunlukta ve mesajı ifade eden eşsiz bir özetini çıkartır. Bu özeten mesajı elde etmek mümkün değildir. Mesajın özeti çıkartıldıktan sonra, mesaj ve mesajın özeti Ayşe'nin açık anahtarı ile şifrelenir. Ayşe'ye şifrelenmiş mesaj gönderilir. Şifrelenmiş mesajı alan Ayşe kendi gizli anahtarı ile şifreli mesajı deşifre eder ve mesaja ulaşır. Daha sonra hash algoritması ile mesajın özetini elde eder, kendi elde etmiş olduğu değer ile gelen mesaj özetini karşılaştırır. Her iki özet de aynı ise Ayşe mesajın yolda değişmediğini anlar. Bu örnekte AAA ile gizlilikle beraber veri bütünlüğü de sağlanmış olur(Şekil 2).



Şekil 2. AAA Veri Bütünlüğü İşlevi

Ali Ayşe'ye gizliliği ve bütünlüğü sağlanmış, kimlik doğrulama ve onaylama yapılabilen ve inkâr edilemeyen bir mesaj göndermek istediğinde; Ali Ayşe'ye mesajı göndermeden önce hash algoritması ile mesajın özetini çıkartır. Mesaj ve özetini kendi gizli anahtarı ile şifreler, daha sonra şifreli mesajı Ayşe'nin açık anahtarı ile şifreler. Son şifrelenmiş mesajı Ayşe'ye gönderir. Şifrelenmiş mesajı alan Ayşe önce kendi gizli anahtarı ile mesajı deşifre eder. Veri gizliliği bu aşamada sağlanmış olur. Daha sonra Ali'nin açık anahtarı ile şifrelenmiş ikinci mesajı deşifre eder. Eğer Ali'nin açık anahtarı bu şifreli mesajı deşifre ederse AAA ile kimlik doğrulama ve onaylama sağlanmış olur. Bununla beraber bu şifreli mesajı sadece Ali'nin gizli anahtarı oluşturabileceğinden AAA ile inkâr edememe sağlanmış olur. Sonraki aşamada da özet değeri ile hash algoritma sonucu karşılaştırılarak veri bütünlüğü de sağlanmış olur(Şekil 3).



Şekil 3. AAA Kimlik Doğrulama ve İnkâr Edememe İşlevi

B. Sayısal İmza

Sayısal İmza, Sanal Noter Uygulamasının en önemli bileşenidir. Başlangıçta belirtildiği üzere, noter kurumunda yapılan her işlemde yerine getirilen veri bütünlüğü, inkâr edememe, kimlik doğrulama ve onaylama sayısal imza ile yerine getirilir. Fakat sayısal imza haberleşmede gizliliği sağlamaz[2]. Bunun sebebi AAA'da haberleşmede gönderilecek mesaj şifrelenirken, sayısal imza yapısında sadece mesajın hash algoritmasından elde edilen özeti şifrelenir. Bu şifrelenmiş özet de sayısal imzayı oluşturur.

Sayısal İmza 5070 Sayılı Elektronik İmza Kanunu'ndaki tanımıyla; "başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi tanımlar" şeklindedir[3].

AAA'da haberleşmek isteyen her birey ve kurumun açık ve gizli anahtarı vardır. Sayısal imza'da AAA üzerine kurulmuş bir yapı olduğundan, sayısal imza ile haberleşmek isteyen her

bireyin açık anahtarını içeren elektronik sertifikası ve gizli anahtarını muhafaza eden token ya da akıllı kartı vardır. Elektronik sertifikalar sahibinin sanal kimlik kartlarıdır. Bu sanal kimlik kartlarının yönetimini sağlayan bir yapı daha vardır. Bu yapıda Elektronik Sertifika Hizmet Sağlayıcısıdır(ESHS).

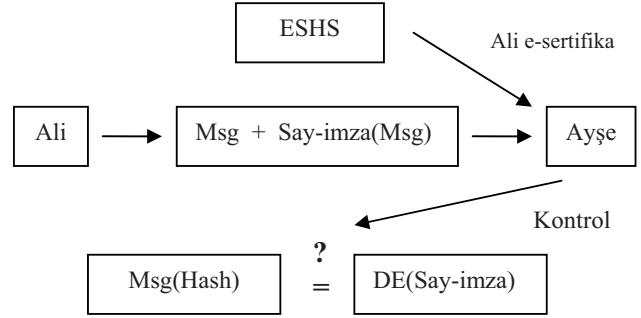
Ali Ayşe'yle sayısal imza kullanarak haberleşmek istediğinde ilk olarak hash algoritmasını kullanarak göndereceği mesaj özetini çıkartır. Ondan sonra içinde gizli anahtarı bulunan usb token ya da akıllı kartı ile mesajın özetini şifreler ve mesajla birlikte Ayşe'ye gönderir. Mesajı alan Ayşe ESHS'dan içinde Ali'nin açık anahtarı bulunan elektronik sertifikasını alır. Daha sonra buradaki açık anahtar ile sayısal imzayı deşifre eder. Mesajı da hash algoritmasından geçirerek mesajın özetine ulaşır. Deşifre ettiği sayısal imza ile özet aynı ise bu mesajı Ali'nin imzaladığını anlar(Şekil 4). Bu senaryo da elektronik sertifikalar, inkâr edilememeyi, kimlik doğrulama ve onaylamayı sağlamaktadır. Görülüyor ki ESHS'lardan alınan bilgi esas kabul edilmiştir. Bu kabul 5070 Sayılı Elektronik İmza Kanunu ile güvence altına alınmıştır.

C. Elektronik Sertifikalar

Elektronik sertifikalar, kişinin kimlik bilgisi ile kişinin açık anahtarını birbirine bağlayan elektronik kayıtlardır. Elektronik sertifikaların görevi kişinin kimliğini doğrulamak, inkâr edilememeyi sağlamaktır. 5070 Sayılı Kanun ile elektronik sertifikalar kayıtlı bir ESHS tarafından verilirse nitelikli elektronik sertifika(NES) olarak tanımlanırlar. Bu sertifikalar tektir, başka bir kişiye bağlı olamaz, yalnızca bağlı olduğu kimliği ifade eder.

Nitelikli elektronik sertifikalar Uluslararası Telekom Birliği standartlarına göre X.509 standardında tanımlanırlar[4]. Standart bir nitelikli elektronik sertifika örneği şekil 5'te görülmektedir.

Nitelikli elektronik sertifikaların bir ömrü vardır. Bu sürenin sonunda sertifika yenilenir veya iptal edilir. Hiçbir zaman hiçbir ESHS tarafından, süresiz nitelikli elektronik sertifika üretimi yapılamaz. Bu sertifikaların üst sınırı ülkemizde Telekomünikasyon Kurumu tarafından belirlenir. Bu sürenin sonunda yenilenmelidirler. Nitelikli elektronik sertifika sahibi, gizli anahtarını içeren donanımını kaybetmesi ya da benzer bir durumda nitelikli elektronik sertifikası iptal edilir. Sertifikalar geçersiz olsa bile, sertifikanın geçerli olduğu dönemlerde yapmış olduğu işlemlerde gelecekte ihtilaf oluşması ihtimaline karşı, sertifikayı üreten ESHS tarafından geçersiz olmasından sonra bile arşivlenirler.



Şekil 4. Sayısal İmza ile Haberleşme

Sertifika Seri No	59014325431
Sertifika Sahibinin Kimlik Bilgileri	Dursun Akçeşme
Sertifika Geçerlilik Başlangıç Tarihi	10 Şubat 2008 14.00
Sertifika Geçerlilik Bitiş Tarihi	10Eylül 2009 14.00
Sertifikanın Kullanım Amacı	Test Kullanımı
Kullanılacak Algoritma	Sha1RSA
Sertifika Sahibinin Açık anahtar Bilgisi	65 94 73 58 59 ef 8e 6f 1e 95 22 a7 c9 67 2e a5 d4 ee 2c 1c
Yayınlayan ESHS	XXXX Kurumu
ESHS Sayısal İmzası	4t 4a 31 e8 9y 3d fa 3e 0a b7 dd 70 71 c7 51 7c 45 83 4f 11

Şekil 5. Nitelikli Elektronik Sertifika

D. Elektronik Sertifika Hizmet Sağlayıcı(ESHS)

ESHS'lar bireylere veya kurumlara nitelikli elektronik sertifika veren ve vermiş oldukları sertifikaların yönetim işini üstlenen güven makamlarıdır. ESHS'lar temel olarak kayıt makamı, sertifika makamı ve kök sertifikadan oluşur. Kayıt makamı bireyin başvuru yaptığı, nitelikli elektronik sertifika taleplerinin alındığı ve ilgili kişinin kimlik doğrulamasının yapıldığı makamdır. Sertifika makamı ise eşsiz bir sertifika tanımlamasının yapıldığı ve tanımlanan sertifikayı kendi sayısal imzası ile imzalayarak yayınlayan makamdır. ESHS'ların temel görevleri;

- Nitelikli Sertifika Üretimi
- Zaman Damgası Hizmeti
- Nitelikli Elektronik Sertifikaları bir dizinde yayınlama (Örnek olarak LDAP dizini)
- SIL(CRL)(Sertifika İptal Listesi) yayınlama
- ÇİSDUP(OCSP)(Çevrim İçi Sertifika Durum Protokolü) hizmeti
- Sertifika Mali Sorumluluk Sigortası Yaptırma
- Kanunda belirtilen Sertifika ilkeleri(Sİ) ve Sertifika Uygulama Esaslarına göre hizmet verme

- Tüm bu hizmetlerini sürekli kılmak

Ülkemizde olduğu gibi bir ülkede nitelikli elektronik sertifika veren birden fazla kurum olabilir. Bu durumda sertifika makamlarının hepsi kök sertifika'ya bağlı olur. Her sertifika makamının elektronik sertifikasını da kök sertifika imzalar. Sertifika makamları kendi aralarında çapraz sertifikasyon yaparak iletişim kurarlar.

ESHS'ların hizmetlerinden en önemlilerinden biride iptal veya bir sebepten dolayı geçersiz kılınan sertifikaların yayımlandığı SIL listelerini belirli aralıklarla yayınlamaktır. ESHS, yayınladığı listeyi kendi sayısal imzasıyla imzalar. Sertifikanın geçerliliği kontrol edildiğinde, ESHS'ın yayınladığından emin olmak için sayısal imzalar mutlaka kök sertifikaya ulaşıncaya kadar doğrulanmalıdır. Geçersiz kılınan sertifikaları anlık öğrenmek için ise OCSP hizmetinden yararlanılır, anlık olarak sertifikanın durumu hakkında sayısal imza ile imzalanmış şekilde sertifikanın geçerliliği hakkında bilgi verir. SIL listesinde olduğu gibi bu işlemde de kök sertifikaya ulaşıncaya kadar doğrulama yapılmalıdır.

E. Sayısal İmza Donanımları

Sayısal imzayı oluşturabilmek için kişinin gizli anahtarının bir donanımda tutulması gereklidir. AAA tabanlı uygulamalarda, gizli anahtar bilgisi, bir kere yazılabilen ve donanımın içerisinden çıkartılamayan akıllı kartlar veya usb token'larda tutulurlar. Bu donanımların güvenlik seviyesi minimum EAL-4 uluslararası standardında olmalıdır.

Her iki donanım da PIN(şifre) bilgisi ile korunur. İşlem yapılmak istendiğinde sadece sahibinin bildiği PIN bilgisi girilerek işlem yapılır. Aksi halde işlem yapılması mümkün değildir. PIN bilgisi girildikten sonra gizli anahtar verisi karmaşık matematiksel fonksiyonlardan geçerek üretilir.

F. Bir Sanal Noter Uygulamasında Gizliliğin Sağlanması

Bir Sanal Noter Uygulamasında olması gereken veri bütünlüğü, kimlik doğrulama ve onaylama, inkâr edememe koşulları yukarıda ki bilgiler de görüldüğü gibi sayısal imza kullanılarak yerine getirilebilir. Gizlilik koşulu için kriptolojik yöntemlerden yararlanılır. Kriptolojik bir yöntem olan SSL(Secure Socket Layer) bu koşulu yerine getirir.

SSL çalışma prensibi; A kişisi B kişisine mesaj göndermek istediğinde sadece B kişinin sahibi olduğu gizli bir anahtarın eşi olan açık anahtarla mesajı şifreler, dolayısıyla sadece şifrelenmiş mesajı B kişinin sahibi olduğu gizli anahtar açabileceğinden mesaja erişile bile deşifre edilemez. Bu kriptolojik yöntem ile gizlilik sağlanmış olur. Sonuçta SSL ve sayısal imza kullanılarak, sanal ortamda bir noter işlemi için gerekli tüm koşullar yerine getirilmiş olur.

IV. SAYISAL İMZA İLE YAPILABİLECEK NOTERLİK İŞLEMLERİ

Daha öncede değinildiği gibi bir noterin tüm işlevlerini sanal ortama taşımak mümkün değildir. 5070 Sayılı Elektronik İmza Kanunu'nda yer alan "Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli Elektronik İmza ile gerçekleştirilemez.

"[3] ifadesine göre noterlerin yapmış olduğu işlemlerin bazıları sayısal imza kullanılarak yapılamaz.



Şekil 6. Sayısal İmza Donanımları

Fakat, yapılacak hukuki düzenlemeler(yönetmelik, tebliğ, genelge vb) ile, sayısal imza kullanılarak sanal ortamda aşağıdaki noter işlemleri hukuki normlara uygun, teknolojik olarak her türlü bilgi güvenliği sağlanmış olarak yapılabilir.

- Elektronik zaman damgası vurma
- Kendisine gönderilen elektronik belgelerdeki Elektronik İmza ve tarihi onaylamak
- Elektronik belgelerin saklanması ve istendiğinde belgelenmesi
- Özel Kanununda hükmü bulunmayan defterleri onaylamak
- Tebligat İşlemleri

A. Elektronik Zaman Damgası Vurma

Noterlik Kanunu'nun 60. Maddesi 4. bendi "Bu kanuna uygun olarak dışarıda yazılıp getirilen kâğıtların üzerindeki imza, mühür veya herhangi bir işareti veya tarihi onaylamak"[5] kanununa göre, noterler bir belge üzerinde herhangi bir işareti, tarihi, imzayı onaylayıp tarih atarak hukuki geçerliliğini sağlarlar. Sayısal imza kullanılarak imzalanmış bir elektronik belge notere ulaştığında kişinin elektronik sertifikasıyla kimlik doğrulama yapılabilir. Bu işlemde noter belgenin içeriği ile ilgilenmeyip sadece kimlik doğrulamasını yapmaktadır. Bu sonuç esas alınarak işlemin sanal ortamda modellenilebileceğini söyleyebiliriz, kurulacak bir otomasyon ile onaylama işlemi yapıp, sonuç olumlu ise noter kendi sayısal imzası ile elektronik belgeyi onaylar. Hali hazırda ülkemizde bu konuda hizmet veren bir kurum mevcuttur.

B. Kendisine Gönderilen Elektronik Belgelerdeki Elektronik İmza ve Tarihi Onaylamak

Noterlik Kanunu'nun 90. Maddesi "Hukukî işlemlerin altındaki imzanın onaylanması imzayı atan şahsa ait olduğunun bir şerhle belgelendirilmesi şeklinde yapılır"[5]. 91. Maddesi "Onaylama, imzanın noter huzurunda atılması veya kendisine ait olduğunun ilgili tarafından kabulü ile kabilirdir" şeklindedir[5]. Bu maddelere göre noter bir belgedeki imza ve tarihi kendi huzurunda ve kendisine ait olduğunun kabul edilmesi durumunda bir şerhle

belgelendirmektedir. Sayısal imza ile imzalanmış bir elektronik belgede kimlik doğrulama yapılabilirdiğinden noter sanal ortamda gerekli doğrulama mekanizması ile bu hizmeti verebilir.

C. Elektronik Belgelerin Saklanması ve İstendiğinde Belgelemesi

Noterler yapmış oldukları işlemleri 2000’li yıllardan itibaren kâğıt üzerinde tutmanın yanında elektronik olarak kayıt altına almaktadırlar. Noterlik Kanunu’nun 94. Maddesi “Noterler tarafından yapılan işlemlerin örnekleri, ancak ilgililerine, kanuni mümessil veya vekillerine yahut da mirasçılara verilir.”[5] şeklindedir. Bu kanuna göre birey ya da kurum kendisiyle ilgili bir belgeyi noterden elektronik olarak talep edebilir. Bu durumda sanal ortamda kişi sayısal imzası ile başvuruda bulunup, kimlik doğrulaması yapılarak kanunda öngörüldüğü gibi noter işlemi ile ilgili ise noter işlem örneklerini, noterin sayısal imzası ile imzalanmış olarak sanal ortamda alabilir.

D. Özel Kanununda Hükmü Bulunmayan Defterleri Onaylamak

Günümüzde ticari olsun olmasın hemen hemen tüm defterler elektronik ortamlarda tutulmaktadır. Fakat dijital olmayan bir kopyası, kanun gereği tahrifatı önlemek ve kayıt almak için belirli aralıklarla noterlere onaylatılır.

Noterlik Kanunu’nun 107. Maddesi “Özel kanununda hüküm bulunmayan hallerde defter onaylaması, defterin baş ve son sayfasına kaç sayfadan ibaret olduğu yazılmak ve her sayfası numaralanıp mühürlenmek suretiyle yapılır.” şeklindedir[5]. Bu kanuna göre; noterler sanal ortamda kurulacak bir otomasyon ile kendisine ulaştırılan özel kanunda hükmü bulunmayan defterleri, kendi sayısal imzası ile onaylayıp, kayıt altına alabilir.

E. Tebligat İşlemleri

Noterlerin en yoğun olarak yaptığı işlemlerden biri de kendisine gelen belgeleri ilgili kişiye tebliğ etmektir. Noterlik Kanunu’nun 106. Maddesi “Her türlü hukuki işlemlere ait ihtarname ve ihbarname:

- I. İstemde bulunan ve diğer tarafın ad ve soyadları ile açık adreslerini,
- II. İhtar ve ihbar konusunu,
- III. İstemde bulunanın imzasını,
- IV. Tebliğ şerhini, noterin imza ve mührünü ve tarihi (Yazı ve rakam ile),

kapsar. İhtarname ve ihbarnameler ilgili tarafından yazılıp tebliğ için notere getirebileceği gibi, notere de yazdırılabilir.”[5] şeklindedir. Bu işlem kurulacak bir otomasyon ile bireyin yâda kurumun internet üzerinden açık adres bilgilerini, ihtar ve ihbar konusunu elektronik belgeye girip sayısal imzası ile tebligat notere ulaştırılır. Gerekli kimlik doğrulaması yapıldıktan sonra tebligat ilgili kişiye klasik noter hizmetlerinde olduğu gibi ulaştırılır.

Fakat burada ihtar eden kişinin tebligat üzerinde ıslak imzası olmaması, hukuki normlara göre geçersiz gözükse de,

diğer yandan ıslak imzayla eş olan sayısal imzasının noter tarafından doğrulanmış olması hukuki geçerliliğini sağlamaktadır. Bu ve benzeri durumlar da oluşabilecek yorum farklılıklarından dolayı Sanal Noter Uygulaması için Noterlik Kanunu ve diğer ilişkili kanunlarda çeşitli düzenlemeler yapılmalıdır.

V. HUKUKİ GEREKSİNİMLER

Noter işlemlerinde teknolojik altyapı kullanılarak, normal bir noterin sağlamış olduğu tüm güvenlik sağlanmış olsa da hukuki mevzuat tam anlamıyla noterlik işlemleri yapmaya uygun değildir.

5070 Sayılı Elektronik İmza Kanunu kabul edilerek, sayısal imza ile ıslak imza belirli kısıtlamalar dışında eş kılınmıştır. Fakat kurumların yapmış olduğu işlemlere sayısal imzayı entegre edecek düzenlemeler yapılmamıştır. Oysaki kurumların birçoğunun noterlerde olduğu gibi (Noterlik Kanunu) kendi iş yapısına uygun kanunları vardır. Bu nedenle hukuki anlamdaki temel gereksinim, sayısal imzayı kurumların iş yapısına uyarlamaktır.

Sayısal imza ile yapılan sözleşmeler ve işlemler hukuki olarak, adi senet statüsündedir. Adi senet, “resmi bir makam veya memurun katılımı olmaksızın, bizzat hukuki ilişkilerin taraflarınca düzenlenen senetlerdir”[17]. Hukuk Usulü Muhakemeleri kanununda adi senetlerin ispat gücü; “Bir adi senet, senet altında imza tarafından ikrar edilirse kesin delil teşkil eder”[17] şeklinde tanımlanmıştır. Bu ifadelerle göre, sayısal imza ile işlem yapan taraflardan birinin noter olması, yapılan işlemin hukuki tanımıyla çelişmektedir. Çünkü artık taraflardan biri resmi bir makamdır. Bu durumda yapılan işlem adi senet statüsünde mi değerlendirilecektir? Burada üzerinde durulması gereken konu, sayısal imza ile yapılan işlemlerinin neden adi senet olarak tanımlandığıdır. Bunun sebebi, işlem taraflarından kaynaklanan güven zafiyeti mi, yoksa teknolojik altyapıya olan güven zafiyetidir? İşlem taraflarına olan güven zafiyeti var ise bu işlemi bir noter sayısal imza ile yapması veya koordine edip işleme sayısal imzasını koyması durumunda bu işlemi hukuki olarak hangi statüde değerlendirilecektir. Diğer yandan teknolojik altyapıya olan güven zafiyeti mi, işlemi hukuki olarak adi senet şeklinde tanımlamıştır. Sebep bu ise, sayısal imza ile yapılan işlemler, tarafların dışında üçüncü bir kurum olan ESHS tarafından teyit edilmektedir, bu sebeple adi senet tanımlamasının sayısal imza işlemleri ile ne kadar örtüştüğü değerlendirilmelidir.

Türkiye’de hizmet veren ESHS’ların Elektronik İmza Kanunu’na göre “Sertifika Mali Sorumluluk Sigortası” yaptırmaları gereklidir. Bu sigorta ESHS’nın, Elektronik İmza Kanunu’ndan doğan yükümlülüklerini yerine getirmemesi durumunda, nitelikli elektronik sertifika sahibi kişi veya kuruluşların ve üçüncü şahısların uğrayacağı zararlara ilişkin sorumluluğu, sözleşmede belirlenen zorunlu sigorta limitlerine kadar teminat altına alır[6]. Bu sigorta, sigortalıya karşı yapılan talepler sonucundaki yasal giderler için de teminat verir.

Sertifika Mali Sorumluluk Sigortası olay başına 10.000 (On bin YTL) ve Sözleşme süresince 1.000.000 (Bir Milyon YTL) teminat tutarlarını vermektedir[7]. Diğer sigorta işlemleri ile mukayese edildiğinde teminat tutarları oldukça düşüktür,

birey ve kurumlara güven vermemektedir. Sadece noter işlemleri için değil tüm işlemlerde bu teminat tutarları daha yukarı çekilmeli, toplumun sayısal imzayı kullanması teşvik edilmelidir.

Daha önce belirtildiği gibi, sayısal imza uygulamalarında işlemi yapan elektronik sertifikaların geçerli olup olmadığının doğrulanma süreci çok önemlidir. Doğrulama sürecinde SIL listeleri veya OCSP sorgusu kullanılabilir. OCSP anlık olarak elektronik sertifikanın geçerliliğini bize verdiği için, noter uygulamaların da mutlaka her işlem için OCSP kullanılmalıdır. OCSP sorgusundan dönen ESHS'nin sayısal imzasını koyduğu sonuca göre işlem yapılmamalı, dönen sonuçtaki sayısal imza kök sertifikanın doğrulanmasına kadar devam edilmelidir. Bu sebeple Noter uygulamaları için yapılacak yazılımlar mutlaka CWA 14167-1 standardında olmalı ve ek olarak OCSP sorgu şartı yönetmelik ve kanunlarla düzenlenmelidir.

Hukuki anlamda düzenleme gereken diğer bir konuda, sanal ortamda gerçekleştirilecek bir Sanal Noter Uygulamasının ne şekilde ücret tahsil edeceği. Noterlik Kanunu'na göre noterlik hizmetleri, peşin olarak noterde tahsil edilir. Bu durum da hukuki olarak düzenlenmelidir. Ücretlendirme için kontör sistemi ya da sanal poslar kullanılabilir.

VI. SONUÇLAR

Ülkemizin ilk sayısal imza uygulamalarından olan UYAP ile başlayan süreç, Sanayi Bakanlığı, Başbakanlık Dış Ticaret Müsteşarlığı ve Türk Patent Enstitüsü'nün uygulamaları ile devam etmiştir.

Bu projelerden bir sonraki adım Sanal Noter Uygulaması olmalıdır. Günümüzde bankacılık işlemlerini kâğıt üstünde yürütebiliriz demek, ne kadar imkânsız ise, artan iş yüküyle beraber gelecekte noter işlemlerini kâğıt üstünde yürütürüz demek o kadar imkânsızdır. Sanal ortamda e-ticaret hacmi arttıkça, e-sözleşme, e-fatura, e-devlet vb. uygulamalar arttıkça, Sanal Noter ihtiyacı daha da belirginleşecektir. Bu sebeple sanal ortamda noterin işlevlerini, gerekli güvenlik sağlanarak modellenmesi zorunluluk haline gelmiştir.

Yapılan çalışmada noterlerin, sanal ortamda bazı hizmetlerinin hiçbir kuşkuyla neden olmadan AAA teknolojisi üzerine kurulmuş sayısal imza ile gerçekleştirilebileceği aşikârdır.

5070 Sayılı Elektronik İmza Kanunu ile beraber kurum kanunlarında yapılacak hukuki düzenlemeler, Sanal Noter Uygulamasının hukuki dayanağını oluşturur. Bu koşullar altında Sanal Noter Uygulaması hayata geçirilebilir.

KAYNAKLAR

- [1] <http://turk.internet.com>, Kamu Yönetimi ve Hukuk Ekseninde E-noterlik, Kasım 2008.
- [2] Sağiroğlu, Ş., Alkan, M., Her Yönüyle Elektronik İmza (E-İmza), Grafiker Yayınları, ISBN:975-6355-23-9, Ankara, 2005
- [3] <http://mevzuat.basbakanlik.gov.tr>, 5070 Sayılı Elektronik İmza Kanunu, Kasım 2008.
- [4] Türkiye Bilişim Derneği, Nitelikli Sertifikasyon Altyapısı ve Yetkilendirme, Kasım 2008 Antalya.
- [5] <http://www.noterlerbirligi.org.tr/nkanunu.htm>, 1512 Nolu Noterlik Kanunu, Kasım 2008.
- [6] http://www.tk.gov.tr/eimza/eimza_mevzuat.htm, Zorunlu Sertifika Mali Sorumluluk Sigortası Genel Şartları, Kasım 2008.
- [7] http://www.tk.gov.tr/eimza/eimza_mevzuat.htm, Sertifika Mali Sorumluluk Sigortası Tarife ve Talimatı, Kasım 2008.
- [8] <http://www.k-binder.be>, Introduction to PKI - Public Key Infrastructure, Kasım 2008.
- [9] <http://www.comms.scitech.susx.ac.uk>, Understanding Public Key Infrastructure (PKI), Kasım 2008.
- [10] Keser Leyla, İstanbul Bilgi Üniversitesi, e-imza & e-Türkiye, Temmuz 2004.
- [11] <http://turk.internet.com>, Elektronik İmza Kanunu ve Dijital İmza, Mart 2008.
- [12] <http://www.pki.iam.metu.edu.tr>, Kriptografi Bölümü, Açık Anahtar Altyapısı Araştırma, Geliştirme ve Uygulamalar, Mart 2008.
- [13] Akçeşme Dursun, Sönmez Çoşkun, Bir Sanal Noterin Altyapısının Gerektirdikleri, Ağ ve Bilgi Güvenliği Sempozyumu, Mayıs 2008
- [14] Yavuz Alper, Digital Notary, Lisans Tezi, 2006
- [15] Demir İlke, ODTU Bilgisayar Topluluğu, e-bergi/Nisan 2007
- [16] [11] Çelikyılmaz Sertaç, Türkiye'de Kurumlar İçin e-Güven Altyapısı e-İmza, Aralık 2005.
- [17] <http://turk.internet.com>, e-imza ve Adi Senetler, Kasım 2008.
- [18] Beceni Yasin, Elektronik İmza ve Uygulamalar, Ocak 2006.

Uluslararası Ülke Güvenliğinde Hukuki ve Teknik Yaklaşım

Köksal ÖZENÇ, Mustafa ALKAN, Tayfun ACARER

Abstract- And the risks against the security of the information and data because of our today's developing technology increase too. The certain sources say that the market on the software programs for the internet security was about USD 4,4 bn as for the last of 1999 and also this figure amounts to USD 8,3 bn with an increase of % 23 on average per year. Furthermore while the overheads done for information security in the information and communication technologies which has great importance for EU were USD 465 million, this amount increased up to USD 2,74 bn in 2006. Because Euro 1,4 bn in the term of 2007/2013 has been assigned for the R&D projects in the field of information security technologies within the context of the 7th Framework Program which has a budget of Euro 5,3 bn. [1]

In deed while the market share of security software was USD 8,2 bn in 2006, it has been estimated that this share will be USD 9,1 bn in 2007 and the share for antivirus software USD 4,9 bn with the increasing of 54% in 2007. Therefore it has been understood that the financial burden to be realized for the information security is how much important taking into account this issue.

Keywords—Information security, Echelon, CETS, TEMPEST

I. GİRİŞ

Bilindiği üzere günümüzün gerek gelişen ve gerekse de birbirine yakınsayan teknolojileri sayesinde ses, data ve görüntü olmak üzere her türlü bilgi ve verilerin hızlı bir şekilde iletilmesi, alınması ve işlenmesi büyük ölçüde hayatımızı kolaylaştırmakla beraber bilgi ve iletişim teknolojilerinde “bilgi güvenliği” gibi oldukça önemli bir hususu da gündeme getirmektedir. Zira, bilgi ve iletişim teknolojilerinin toplum bazında yaygınlaştırılması, sadece etkin ve verimli kullanımına değil aynı zamanda söz konusu teknolojilerde kullanılan tüm cihaz, ekipman ve sistemlerde bilgi güvenliğinin de tam olarak sağlanmasına bağlıdır.

Bilgi toplumu hedefine ulaşılması ve elektronik imzaya dayalı elektronik devlet ve elektronik ticaret uygulamalarının yaygınlaşması, bilgi ve iletişim teknolojilerinde güvenli bir ortamın, açık ağlarda dolaşan bilginin güvenliğinin ve kişisel verilerin gizliliğinin sağlanması ile mümkün olmaktadır. Bu nedenle, taraflararası iletilerde bilginin gizliliği, bütünlüğü ve her istenilen anda erişilebilirliğinin sağlanması için teknik ve hukuki önlemlerin alınması büyük önem arz etmektedir.

Bilgi Teknolojileri ve İletişim Kurumu,
kozen@tk.gov.tr, malkan@tk.gov.tr, tacarer@tk.gov.tr

Çok çeşitli sayıda bilgi ve iletişim teknolojilerinin günümüzde hızla artan bir oranda kullanılır hale gelmesi ekonomik ve sosyal hayatta karşılaşılan pek çok işlemleri kolaylaştırdığı ölçüde bilgi güvenliğine karşı çeşitli boyutlarda risk ve tehditleri de beraberinde getirebilmektedir. Zira yabancı ülkelerde olduğu gibi ülkemizde de bilgisayar ve mobil iletişim teknolojisi cihaz ve sistemlerini kullanan kişiler çoğunlukla bilgi güvenliğine karşı oluşabilecek risk ve tehditlerin farkında değildir. Oluşan bu risk ve tehditler, kişilerin çoğunlukla maddi kayba uğramalarına ya da bilgilerin değiştirilmesi, silinmesi ya da izinsiz olarak erişilmesi gibi istenmeyen bazı durumlara neden olabilmektedir.

II. BİLGİ GÜVENLİĞİNİN EKONOMİK BOYUTU

1995 yılında sadece 20.000 olan web sitesi sayısının 2008 yılında 101 milyonu geçtiği dikkate alındığında internet ve multimedya ortamında kullanılan ses, data ve görüntü olmak üzere her türlü bilgi ve verinin güvenlik boyutunun ne kadar önemli olduğu ve buna bağlı olarak da güvenliğin sağlanması sorununun çözülmesinin de bir o kadar karmaşık ve zor olduğu ortaya çıkmaktadır. Ayrıca bilgi ve iletişim teknolojilerinin özelliği nedeniyle veri güvenliği hususunda uluslararası işbirliği de çok önemlidir. Zira günümüzün gelişen teknolojisi sayesinde bilişim suçları artık sınırları aşan bir boyut kazanmıştır. Örneğin, 2000 yılında ortaya çıkan Love Letter virüsünün tüm dünyada yaklaşık 7 milyar ABD Doları zarar verdiği tahmin edilmektedir.

Benzer şekilde 2001 yılında Code Red Worm virüsü ortaya çıktığından itibaren ilk 14 saat içinde 359.000 adet sisteme zarar verirken, 2003 yılında ortaya çıkan Sequel Slammer virüsü ise bundan çok daha hızlı bir şekilde yayılma göstererek sadece ilk 10 dakika içinde 75.000 adet sisteme zarar verdiği tahmin edilmektedir. FBI tarafından yapılan araştırmaya göre halen günümüze kadar yaklaşık 70.000 adet virüsün tesbit edildiği ve dünyada mevcut olan internet web server'lerinin yaklaşık %85'inin en az bir kez siber saldırıya maruz kaldığı dikkate alındığında konunun ekonomik boyutunun olduğu kadar uluslararası ilişkiler boyutunun da ne kadar önemli olduğu ortaya çıkmaktadır.

III. BİLGİ GÜVENLİĞİNDE AB'NİN HUKUKİ YAKLAŞIMI

Yukarıda belirtilen hususlar çerçevesinde istenmeyen bu durumların engellenebilmesini teminen AB, hukuki alanda aşağıda belirtildiği üzere bazı düzenlemeler yapmıştır. [2]

Avrupa Birliği'ndeki bilgi güvenliği alanındaki çalışmalar esas itibarıyla 1987 yılında başlamıştır. 1987 yılında yayınlanan Green Paper (Yeşil Rapor) ile AB, telekomünikasyon sektöründeki bilgi güvenliğinin önemine işaret etmiştir. Ayrıca AB, bilgi ve iletişim teknolojileri üzerinde bilgi güvenliğinin sağlanması ve mahremiyetin korunması konusunda gelişen teknolojik ve sosyal ihtiyaçları da dikkate alarak telekomünikasyon sektöründe serbestleşmenin Topluluk içinde 2000 yılına kadar tamamlanmasının hedeflendiği 1998 mevzuatı çerçevesinde 95/46/EC ve 97/66/EC sayılı AB Direktifleri düzenlenerek yürürlüğe konulmuştur.

Diğer taraftan AB, özellikle 1995'li yıllardan itibaren internet ve multimedya teknolojilerinin toplum tarafından çok büyük bir hızla kullanılır hale gelmesiyle birlikte özellikle internet teknolojilerinin beraberinde getirdiği bazı kolaylıklar ve imkanlara ilaveten küçük çocukların internet ortamındaki mızur yayımlardan korunması amacıyla "Küresel ağlar üzerinde zararlı ve yasadışı içerikle mücadeleyle internetin daha güvenli kullanımı" hususunda 99/276/EC sayılı bir Karar yayınlamıştır.

Ayrıca, 1998 tarihli mevzuat çerçevesinde telekomünikasyon sektöründe hedeflenen serbestleşmeyi tamamlayan AB, bu kez teknolojiye ve buna bağlı olarak da telekomünikasyon sektöründe

- * ses ve veri
- * telekomünikasyon ve radyo-TV yayını
- * sabit ve mobil

hizmetler olmak üzere üç farklı alanda gerçekleştirilen ve toplum hayatını ve dolayısı ile de telekomünikasyon alanındaki düzenlemeleri derinden etkileyen yakınsama konusunu dikkate alarak 2002 tarihinde yeni bir düzenleyici çerçeve mevzuatını hazırlayarak yürürlüğe koymuştur.

Yukarıda belirtilen hususlar çerçevesinde telekomünikasyon, radyo-TV yayını, sabit ve mobil hizmetler, ses ve veri hizmetleri, internet ve multimedya hizmetlerindeki bu yakınsama nedeniyle artık AB, 1998 tarihli çerçeve mevzuatında yer alan ve teknolojiye bağlı olan diğer bir deyişle belirli bir teknolojiyi çağrıştıran "telekomünikasyon", radyo-TV yayıncılığı", "uydu hizmetleri", "sabit ses hizmetleri", "mobil hizmetler", "veri hizmetleri" gibi tanım ve ifadeler yerine tüm bunları tek bir başlık altında kapsayacak şekilde ve teknoloji nôtür bir ifade olan dolayısı ile de teknolojilerin her alanında yakınsamayı ifade eden "elektronik haberleşme şebekeleri ve hizmetleri" şeklinde farklı bir tanımla gündeme getirmiştir.

Bu kapsamda, 2002 yılında kabul edilen ve 2003 yılında AB üyesi ülkelerde yürürlüğe giren yeni çerçeve düzenleyici paket kapsamında 1998 tarihli mevzuatta yer alan telekomünikasyon sektöründeki kişisel verilerin işlenmesi ve mahremiyetin korunması konusundaki 97/66/EC sayılı AB Direktifi'nin yerine geçen elektronik haberleşme sektöründe mahremiyetin korunması ve kişisel verilerin işlenmesi hususundaki 2002/58/EC sayılı Direktifi yürürlüğe

koymuştur. AB mevzuat uyum çalışmaları çerçevesinde sözkonusu Direktifin uyumlaştırılması amacıyla Kurum tarafından 06.02.2004 tarihinde Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik çıkartılmıştır.

Yukarıda belirtilen hususların yanı sıra, AB yukarıda sayılan direktifleri tamamlayıcı nitelikte olmak üzere aşağıda belirtilen bazı kararlar almıştır.

- Bilgi güvenliğinin sağlanmasına ilişkin 31 Mart 1992 tarih ve 92/242/EC sayılı Konsey Kararı,
- Şebeke ve bilgi güvenliği kültürüne doğru Avrupa'nın yaklaşımına ilişkin 18 Şubat 2003 tarih ve 2003/48/EC sayılı Konsey Kararı,
- Şebeke ve bilgi güvenliğinin iyileştirilmesi ve uygulamanın yayılması ile ilgili e-Avrupa Eylem Planı'nın izlenmesine ilişkin 17 Kasım 2003 tarih ve 2256/2003/EC sayılı Konsey Kararı,

Ayrıca, yukarıda belirtildiği üzere kişisel verilerin ve mahremiyetin korunmasına yönelik olarak bir çok farklı alanda düzenleme yapma ihtiyacı hisseden AB, sözkonusu düzenlemelerden özellikle genel anlamda ve sektör spesifik alanda olmak üzere iki ayrı yapı halinde kurumsallaşmaya doğru da bir adım atmıştır. Bu çerçevede kişisel verilerin ve mahremiyetin korunmasına yönelik olarak 95/46/EC sayılı Direktifte belirtilen hususlara kurumsal bir yapı kazandırmak amacıyla "Topluluk kurumları tarafından kişisel verilerin işlenmesi, kişilerin korunması ve bilgilerin serbest dolaşımı"na ilişkin olarak onayladığı 2001/45/EC sayılı Tüzük ile AB içinde ilk kez "Veri Koruma Görevlisi" ve "Avrupa Veri Koruma Denetmeni" gibi bazı görev ve fonksiyonlara işlerlik kazandırılmıştır.

Benzer şekilde sektör spesifik bir alanda, sadece telekomünikasyon sektörüne özgü olmak üzere ve bu kapsamda düzenleme amacıyla yürürlüğe konulan 2002 tarihli yeni düzenleyici çerçeve mevzuatı kapsamında kabul edilen elektronik haberleşme şebeke ve hizmetleri konusundaki 2002/58/EC sayılı Direktif ve 99/276/EC sayılı Karar'a ilişkin hükümleri de kapsayacak şekilde AB tarafından "Avrupa Şebeke ve Bilgi Güvenliği Kurumu"nun (ENISA-European Network and Information Security Agency) kurulması amacıyla 2004/460/EC sayılı Tüzük yayımlanmıştır.

Yukarıda belirtilen hususlara ilaveten AB, özellikle tüm dünyada 1990'lı yıllardan itibaren gelişen ve yaygınlaşan elektronik ticaret ve elektronik imza uygulamalarına özgü çıkartmış olduğu 2000/31/EC ve 99/93/EC sayılı Direktifler'de de kişisel verilerin ve mahremiyetin korunmasını sağlamak üzere kriptografi ve elektronik imza teknolojileri çerçevesinde uygulanan standartlara ilişkin olarak bazı hükümler getirmiştir.

Son olarak da AB tarafından elektronik haberleşme şebekeleri kullanılarak gerçekleştirilen tüm haberleşmenin (telefon, faks, VoIP, e-posta vs.) kim tarafından ne zaman ve kimle yapıldığına dair ve haberleşmenin içeriği de dahil olmak üzere ileride meydana gelebilecek herhangi bir yasal soruşturma ya da incelemede kullanılabilmesini teminen gerekli olabilecek tüm bilgilerin 6 aydan az olmamak ve 2 yıldan fazla olmamak şartıyla depolanması yönünde telekomünikasyon sektöründeki mobil işletmecilere, sabit işletmecilere, MVNO ve ISP gibi diğer tüm sektör aktörlerine bir görev verilmiştir. Bu çerçevede 13.4.2006 tarihli AB Resmi Gazetesi'nde yayınlanan 2006/24/EC sayılı Direktif gereğince bu husus yasal bir zorunluluk haline getirilmiştir.

IV. AVRUPA BİRLİĞİ'NDE GÜVENLİK POLİTİKASI

Bilgi toplumu hizmetlerinin gelişmesiyle bilgi güvenliği, iş dünyasının vatandaşın ve kamu sektörünün yaptığı her işlemde vazgeçilmez bir unsur olmuştur. Bu nedenle, AB bünyesinde ortak tutum, fikir ve anlayış birliğinin kurulması ve iç pazarın sağlıklı çalışması amacıyla, AB içinde güvenlik kültürü oluşturulması hedeflenmiştir. Bu kapsamda, 92/242/EC sayılı Konsey Kararı ile 2002 yılı e-Avrupa Eylem Planı ve 2256/2003/EC ve 2003/48/EC Sayılı Konsey Kararları ile 2005 yılı e-Avrupa Eylem Planları oluşturulmuştur. Bu eylem planlarında;

- Elektronik ortamda depolanan, işlenen ve iletilen bilginin kazara veya kasıtlı tehditlere karşı uygun şekilde korunması,
- Konu ile ilgili uluslararası standartların kabul edilmesi,
- Konu ile ilgili üye devletlerde gerekli düzenlemelerin yapılmasının gerekliliği,
- Bilgi sistemlerinin güvenliği için kullanıcı ve servis sağlayıcılara düşen görevlerin tanımlanması,
- Her kesimden kullanıcının bilgilendirilmesi ve bilinçlendirilmesi için bilgi ve veri güvenliği ile mahremiyetin korunması eğitimlerine önem verilmesi, gerektiği vurgulanmıştır.

V. ULUSLARARASI BİLGİ GÜVENLİĞİNE İLİŞKİN BAZI ÖRNEKLER

A. İngiltere

İngiltere, biyometrik güvenlik önlemlerini de içeren kimlik kartlarının vatandaşlara dağıtılması için bir proje başlatmıştır. Zira kimlik bilgilerinin çalınarak kopyalanması sonucu çok sayıda insan maddi ve manevi zarara uğramış bulunmaktadır. İngiltere'de kimlik bilgilerinin çalınmasına karşı mücadele vermek üzere sivil toplum kuruluşu sıfatıyla kurulmuş olan Cifas'a göre örneğin sadece 2004 yılında 119.000 kişinin kimlik bilgileri kullanılarak maddi çıkar sağlanmıştır. Cifas, İngiltere'de 240 üyesi ile beraber başta telekomünikasyon şirketleri olmak üzere bankacılık sektörü ve çeşitli ticari firmalardaki kişisel bilgilerin başka amaçlarla kullanılmasını önlemek ve kullanıldığı takdirde bunu yetkili makamlara ihbar etmek üzere kar amacı gütmeyen çalışma yapan çok sayıdaki sivil toplum kuruluşundan birisidir. [3]

B. Kanada'da Çocuk Pornosunun Önlenmesine Yönelik Bir Sistem: CETS

Bilindiği üzere günümüzde internet kullanımının her geçen gün artması, beraberinde çocukların internet kullanılarak istismar edilmesi ve bu çerçevede çocuk pornosunun çok büyük bir boyuta ulaşmış olması toplumda büyük bir rahatsızlığa neden olmaktadır. Bu rahatsızlıktan hareketle Kanada polisi, 2003 yılında bir çocuk pornosunun kullanıldığı bir web sitesinin izlenmesi ve tespit edilebilmesini teminen Microsoft firmasından yardım talep edilmiştir. Söz konusu talep üzerine Microsoft tarafından hazırlanan ve adına CETS (Child Exploitation Tracking System) denilen özel bir yazılım sayesinde tüm internet siteleri önceden belirlenmiş olan kelime ve/veya kelime grupları ve belirli resimler taranarak çocuk pornosunun kullanıldığı sitelerin tespit edilmesi sağlanmıştır. Söz konusu projenin maliyeti yaklaşık 2,5 milyon ABD Doları olup, internete erişim yapan çocukların yaklaşık % 20'sinin pornografik saldırıya maruz kaldığı tahmin edilmektedir. [4]

C. Carnivore

Carnivore, ABD'de FBI tarafından 2000'li yılların başında geliştirilen özel bir elektronik izleme sistemine verilen isimdir. Bu sistem FBI tarafından daha önceden kullanılan Omnivore adlı sistemin geliştirilmiş versiyonudur. Carnivore sistemi, adli mercilerin izni ile internet üzerinden gerçekleştirilebilecek suçları ve suçluları önleme ve izleme amacıyla ya internet servis sağlayıcısına bağlanır. Bu sayede takibe alınan kişinin e-posta mesajları, ICQ mesajlaşmaları ve hangi web sayfasında ne kadar süre gezindiği ve ne yaptığı gibi her türlü işlem dahil olmak üzere internet vasıtasıyla gerçekleştirmiş olduğu her türlü işlem takibe alınır. Carnivore sisteminin FBI tarafından kullanılması sayesinde 25600 suçlu yakalanmıştır.

11 Eylül 2001'de ABD'de yaşanan terörist saldırı sonucu iki adet gökdelenin çökmesi sonucu ABD Temsilciler Meclisi tarafından 24 Ekim 2001 tarihinde kabul edilen ABD Vatandaşlık Kanunu ile internetteki her türlü verilerin FBI tarafından izlenmesi ve kayıt altına alınması hüküm altına alınmıştır.

Ancak her şeye rağmen Carnivore sisteminin kullanılmasının, 2001 yılında FBI tarafından terk edildiği 2005 yılında ilan edilmiştir. Bunun yerine daha da geliştirilmiş olan ve kod adı "DragonWare Suite" olan ve üç ayrı amaca yönelik olarak hazırlanmış olan "Carnivore", "Packeteer" ve "CoolMiner"dan oluşan bir sistem hizmete alınmıştır. FBI bu ve buna benzer sistemleri daha ziyade suçluları, casusları, kaçakçıları ve teröristleri takip etmek amacıyla yoğun bir şekilde kullanmıştır. Söz konusu sistemin toplam maliyetinin 6-15 milyon ABD Doları olduğu ifade edilmektedir. [5]

D. Echelon

Echelon sistemi küresel bir haberleşme müdahale (COMINT - Communications Interception) sistemi olup,

tüm dünyadaki askeri ve sivil her türlü haberleşme izlenmekte ve kaydedilmektedir. Sistemin yönetimi, tamamen ABD'nin Ulusal Güvenlik Kurumu (NSA - National Security Agency) olup, sistemin varlığı 1999 yılına kadar sürekli olarak inkar ediliyordu. Ancak 16 Mart 1999'da Avustralya'daki Ulusal Askeri Muhabere Merkezi (DSD - Defense Signals Directorate) Müdürü Martin Bradley'in bir muhabir olan Ross Coulthart'a yazdığı mektupta ortaya çıktı. Bunun üzerine Avustralya hükümeti, Mayıs 1999'da yapılan bir açıklama ile Echelon sisteminin bir parçası olduklarını kabul etti.

Sistem çok güçlü bir yazılım ve donanım altyapısına sahipti. Zira 1992 yılında NSA'den emekli olan ve buranın müdürlüğünü yapmış olan Amiral William Studeman'ın yaptığı açıklamaya göre Echelon sistemi, saatte 2 milyondan fazla telefon, telex, e-posta ve faks mesajını izleyebiliyor ve kaydedebiliyordu ki bu rakam bir yılda 17,5 milyar mesaja karşılık gelmektedir. 1992 yılındaki teknolojik imkanlar sayesinde 2 milyon olan bu rakamın, günümüzde çok daha fazla bir değere ulaştığı düşünülebilir.

Echelon sayesinde yapılan tüm izleme ve kayıtlar doğrudan NSA ve CIA'ya yönlendirilmektedir. 11 Temmuz 2001 tarihinde Echelon sisteminin mevcut olup olmadığı konusunda AB Parlamentosu tarafından çok kapsamlı bir şekilde hazırlanan ve yayınlanan rapor, Echelon sisteminin mevcut olduğunu kanıtlamıştır. Ayrıca sözkonusu raporda Echelon sistemine benzer başka sistemlerin Rusya, Çin ve Fransa gibi bazı ülkelerde de kurulu olabileceği ifade edilmektedir.[6]

VI. TEMPEST (TRANSIENT ELECTROMAGNETIC PULSE SURVEILLANCE STANDARD)

Bakır kablo ve monitör gibi ilave bazı donanımlardan oluşan tüm bilgisayar sistemleri, Hollanda'lı bilim adamına hitaben adını Van Eck'ten alan alıcılar tarafından alınabilen ve kaydedilebilen elektromanyetik yayınları yaymaktadır. Tempest teknolojisi, bu yayınların kullanılarak ve ortamdaki parazitlerden arındırılarak ve güçlendirilerek ilgili cihaz tarafından yaklaşık 500 m kadar uzaktan alınmasını engellemeye yönelik olarak oluşturulmuş bir teknolojidir.

Bilgisayarın klavyesinden, ekranından, modem kablosu gibi çeşitli yerlerden elektromanyetik sinyaller klavyede basılan tuşlara, ekrandaki görüntüye ve modemle bilgisayar arasında geçen bilgileri içermektedir. Yeterli donanıma sahip herhangi biri bu yayınları bir veya iki kilometreye varabilen bir mesafeden kaydedebilir ve ekranınızda ne görüldüğünü, klavyede ne girildiği veya modemden ne geçtiği bu yayınlar işlenerek tekrar oluşturabilir. [7]

Tempest'de ekranlama, filtreleme veya yayılan dalgalara gürültü ekleyerek sinyali anlaşılmaz kılmak gibi uygulanabilecek bazı elektromanyetik güvenlik yöntemleri mevcuttur. Bu tip yöntemlerde ya doğrudan kullanılan elektronik malzemeler ekranlanır ve giriş/çıkışları filtrelenir veya ekranlı olması gerekmeyen aletler ekranlı odalarda (Faraday kafesi) kullanılır. Ekranlanacak odalar tamamen

iletken bir maddeyle kaplanarak elektromanyetik yayınları durdurucu Faraday kafesi oluşturulur. Odaların havalandırma girişlerine dalga kırıcı yansıtıcılar konur. Elektrik şebekesine olan bağlantılar açıkverici işaretlerin bulunabileceği frekansları kesen filtreler aracılığıyla yapılır. Bu tip odalar genellikle ses yalıtımına da tabi tutulur.

VII. İSTEK DIŞI HABERLEŞME

Ülkemizin AB mevzuatına uyumlaştırma sürecinde, istek dışı haberleşme konusuna önem verilerek bu konuda bir an önce yasal düzenleme çalışmalarına başlanması, bu konudaki sorumluluk ve yaptırımların belirlenmesi gerekmektedir. Yapılacak yasal düzenleme ile, abonenin önceden rızası olmadan istek dışı haberleşme yapılmasının önlenmesi, gerçek ve tüzel kişilerin kendi müşterilerine çıkan yeni bir ürün veya hizmet hakkında bilgi vermek amacıyla mesaj gönderebilmesi, ancak mesajın içeriğinde mesajı gönderenin açık bir şekilde belirtildiği ve alıcının mesajı tekrar almak istememesi durumunda ücretsiz ve kolay bir yolla reddedilme imkanının tanınması, mesajın içeriğinin ahlaka ve kamu düzenine aykırı olmaması, mesaj gönderen kişilerin sahte isim ve şaşırtıcı konu başlığı kullanmalarının önlenmesi, kişinin rızası olmamasına rağmen mesajın zorla gönderilmemesi, ahlaka ve kamu düzenine aykırı olması durumunda cezai müeyyidelerin konulması, pornografik içerikli mesajların gönderilmesinin yasaklanması sağlanmalıdır. Bunun yanı sıra, diğer AB üyesi ülkelerde olduğu gibi kapsam içi yöntemin uygulanması gerekmektedir.

VII. SONUÇ VE DEĞERLENDİRMELER

Güvenlik açısından göz önüne alınması gereken husus, güvenlik alanlarının çok iyi tespit edilerek bilginin özelliğine en uygun önlemlerin alınmasıdır. Ancak ünlü hacker Kevin Mitnick'in "Kırılmayacak site, sızılmayacak ağ yoktur" sözünden de anlaşılacağı üzere tam olarak bilgi güvenliğinden söz etmek mümkün olamamaktadır. Ancak, bu konuda atılacak en önemli adımın etkin ve verimli bir güvenlik kültürünün oluşturulması, bilgi güvenliğinin temel unsuru olan kişisel verilerin korunması ile ilgili düzenlemelerin yapılması ve küresel bir ağ haline gelen bilgi ve iletişim teknolojilerinde uluslararası işbirliğine önem verilmesinin şart olduğu değerlendirilmektedir.

A. Hükümetin;

Tüm kesimden kullanıcının katılımını sağlayacak bir "Eylem Planı"nı başlatması, bilgi sistemlerinin güvenliği için ulusal politika geliştirmesi ve diğer ülkelerle işbirliği yapması, eğitimler, broşürler, internet siteleri hazırlaması ve danışma birimleri kurması, konu ile ilgili uluslararası standartları Türk Standardı haline getirmesi ve kullanımını sağlaması, tüm kurumların, özel kuruluşların ve sivil toplum kuruluşlarının işbirliği içinde bulunmasını sağlaması, ülke güvenliğini sağlayacak yasal düzenlemelerin bir an önce

yürürlüğe girmesini sağlaması, bilgi teknolojilerinin gelişimi için araştırma-geliştirmenin devletçe desteklenmesi, bilgi güvenliği ve kişisel mahremiyete yönelik ihlalleri asgari düzeye indirecek cezai önlemlerin alınmasını sağlaması, bilişim suçları ile ilgili birimler kurması, diğer ülkelerde olduğu gibi bilgi güvenliği konusunda kişileri yönlendirebilecek ve olaylara müdahale edebilecek CERT gibi kurumlar kurması, gereklidir. Ayrıca bu konuda uluslararası işbirliğinin önemli olması nedeniyle diğer ülkelerle işbirliği kurma yoluna gitmesi gereklidir.

B. Kurum ve kuruluşlarının;

Kurumun yapısına uygun “Kurumsal Güvenlik Politikası” geliştirmesi, bilgi güvenliği konusunda oluşturulan standartların kullanımına özen göstermesi gereklidir.

C. Kullanıcıların;

Bilgi sistem ve ağlarındaki diğer kullanıcılara karşı sorumlu olduklarının bilincinde olması, güncel antivirüs yazılımı ve lisanslı yazılımlar kullanması, İnternette kişisel verilerini nasıl koruyacaklarını bilmesi, bilgisayar ve e-postaları için parola kullanması ve bunları sık sık güncellemesi, güvenmedikleri sitelere girmemesi ve tanımadıkları kişilerden gelen e-postaları açmaması gereklidir.

D. Düzenleyici otoritelerin

Güvenlik kültürü oluşturulmasında her kurum, kuruluş ve bireye sorumluluk düşmesi nedeniyle Telekomünikasyon Kurumu (TK) tarafından “Kurumsal Bilgi Güvenliği Politikası” oluşturulması, Kurum çalışanlarının elektronik ortamda tutulan ve aktarılan bilginin güvenliğini sağlama hususunda uyması gereken kural ve politikaların belirlenmesi gerekmektedir.

İSS'lere bilgi güvenliği ihlallerini önleme yetkisi ve yükümlülüğü verilmelidir. İSS'lerin aboneleri ile yaptıkları sözleşmede kendi abonelerinin bilgi güvenliği ihlali yapamayacakları hüküm altına alınmalı ve kendi abonesinin ihlalinden İSS sorumlu tutulabilmelidir. Ayrıca abonelerinin hazırlamış oldukları İnternet sitelerinde özellikle ticari sitelerde gizlilik politikalarının ne olduğu kişisel bilgilerin niçin istendiği, bilgilerin hangi amaçla kullanılacağı ve bilgilerin güvenliğinin nasıl sağlanacağına ilişkin bilgilerin sunulması sağlanmalıdır. Bununla birlikte siteler, “çerez” (cookie) gönderilip gönderilmediği konusunda kullanıcıyı bilgilendirmeli ve kullanıcıya bunu reddetme imkanı tanınmalıdır.

TK önderliğinde tüm sektör aktörlerinin katılımı ile oluşturulacak ve “Elektronik Haberleşme Sektöründe Kişisel Verilerin ve Mahremiyetinin Korunması Komisyonu” olarak adlandırılacak bir komisyon sayesinde abone ve kullanıcılar dahil olmak üzere tüm sektör aktörlerinin yapacağı toplantılarda karşılıklı bilgi alış veriş ve istişarelerde bulunarak kişisel verilerin ve mahremiyetin korunmasına yönelik olarak ilgili mevzuatın varsa eksikliklerinin tespiti, usul ve esasların belirlenmesi, mevzuatın nasıl daha iyi ve sağlıklı olarak işletilebileceğinin

değerlendirilmesi gereklidir. Kurumun diğer ülkelerdeki düzenleyici kurumlarla ikili işbirliği geliştirerek, onların telekomünikasyon alanında kişisel verilerin ve mahremiyetin korunması konusunda yaptıkları tecrübelerden faydalanması, edindiği izlenim ve tecrübeleri sektöre aktarması oldukça büyük önem arz etmektedir.

Bilgi toplumunun oluşturulması ve yaygınlaştırılmasında en büyük engel olarak görülen istek dışı haberleşmenin artması toplumun hemen hemen tüm kesiminin (internet kullanıcıları, kamu sektörü, İSS'ler, hizmet sağlayıcılar) ortak kararlılığı, yapılacak işbirliği ve dayanışmayla oluşturulacak mücadelede başarı sağlayabilecektir. Bu itibarla Kurum diğer ilgili kurum ve kuruluşların işbirliği ile istek dışı haberleşmeyi önleme konusunda görüş, öneri ve politikaların oluşturulacağı forumlar düzenlemelidir. Ayrıca kamu kurum ve kuruluşlarında ülke güvenliğine yönelik olarak Bilgi Güvenliği Yönetim Sistemi'nin (ISO/IEC 27001, COBIT vs.) kurulması ve bu çerçevede imkanlar ölçüsünde tüm bireylerin ve kamu çalışanlarının bilgi güvenliği konusunda bilgilendirilmesi ve bilinçlendirilmesi çalışmalarının bir an önce başlatılması ve bu bağlamda eğitim çalışmalarının yapılması son derece önemlidir.

Sadece bilgi ve iletişim teknolojileri boyutunda değil, günümüz kullanıcılarında olduğu kadar üretici ve işletmeciler gibi daha bir çok sektör aktörlerinin hepsinde ortak duyulan bir endişe sözkonusudur. “Güvenlik”. Zaten konu ile ilgili olarak çeşitli platformlarda halen çalışmaları yürütülmekte olan tüm standardizasyon faaliyetlerinin temel hedefi sistem ve cihazlar arasında uyumlu çalışabilmeyi sağlamak olduğu kadar, güvenlik unsuru da birinci derecede rol oynamaktadır. Ülke güvenliği kavramı içinde kişisel ve kurumsal bilgi güvenliği gibi temel hususlar yer almakla birlikte, bunların altında iletişim ağı güvenliği, işletim sistemi güvenliği, veri tabanı güvenliği, internet erişim güvenliği, terminal cihazı ve sistem güvenliği gibi oldukça önemli hususlar bulunmaktadır. Özetle, burada sayılanların hepsinin “**Toplam Sistem Güvenliği**” adı altında toplanması mümkündür.

Yukarıda belirtilen hususlar, geniş bantlı teknolojilerin toplum bazına yaygınlaştıkça ülke güvenliği ve veri güvenliği olgusunun beraberinde getireceği muhtemel risklerin ve siber saldırıların da doğru orantılı olarak artacağına işaret etmektedir. Dolayısı ile, konu sadece bilgisayar suçlarına yönelik olarak ülkelerde görevli bir Kuruma işlerlik kazandırılmasını değil aynı zamanda yargı organları, sanayi, tüketici kuruluşları, üniversiteler ve veri koruma kurumları arasında işbirliğinin artırılmasını ve geliştirilmesini gerektirmektedir. Bununla beraber, bilgi ve iletişim teknolojilerinde veri güvenliğinin belki de en önemli kısmını oluşturan telekomünikasyon işletmecileri

ile erişim sağlayıcılarının gelişen teknoloji çerçevesinde tesbit edilecek olan asgari seviyedeki güvenlik kriterlerine uymaları da büyük önem arz etmektedir. Bu bağlamda “siber-suç polisi” ve “siber-suç savcısı” gibi yeni tanım ve meslek dallarının ya da diğer bir deyişle bilgi ve iletişim teknolojileri alanında veri güvenliği konusunda hukuki ve teknik ihtisas gerektiren yeni branşların gündeme gelmesi bir teknolojik zorunluluk olarak ortaya çıkmaktadır.

Bu çerçevede; bilgi ve iletişim teknolojileri alanında bilgi güvenliği ve mahremiyetin korunmasına yönelik olarak AB’de halen çok çeşitli platformlarda mevcut çalışmalar, dikkate alınır ise, konu sadece Ülkemizin AB’ne uyumu açısından değil; aynı zamanda günümüz teknolojisinin gereklerine ve ihtiyaçlarına mümkün olan en kısa sürede uyum sağlayabilme ve hatta gerçekleştirilebilir ise; Ülkemizde başta bilgi ve iletişim teknolojilerinde veri güvenliği olmak üzere, diğer teknolojik alanlarda da **Devlet-Sektör-Üniversite işbirliğinin geliştirilebilmesi** için, sözkonusu çalışmaların mümkün olan en kısa sürede başlatılmasının, Ülkemiz menfaatleri açısından doğru bir yaklaşım olacağı değerlendirilmektedir. Zira burada önemli olan husus, bir çok gelişmiş ülkede yazılım ve donanım ürünleri dahil olmak üzere bilişim sektörünün **“Stratejik Sektör”** olarak ilan edildiği olgusunun gerektirdiği ölçüde Ülkemizde topyekün bir işbirliğinin ve eyleminin gerektiridir.

Bu çerçevede ülkemizde başta Telekomünikasyon Kurumu olmak üzere, Ulaştırma Bakanlığı gibi ilgili tüm kamu kurum ve kuruluşlarının ve diğer sektör aktörlerinin de iştirakinin sağlandığı **“Bilgi Güvenliği Ulusal Koordinasyon Kurulu”**nun kurulması son derece önem arz etmektedir. Kurulun temel amacı, telekomünikasyon sektöründeki abone ve kullanıcılar dahil olmak üzere tüm sektör aktörlerinin ve ilgili kamu kurum ve kuruluşlarının iştirak edeceği toplantıların düzenlenmesi ve bu çerçevede ilgili tüm taraflar arasında bilgi, tecrübe ve doküman paylaşımının yapılmasıdır. Ayrıca **“Bilgi Güvenliği Ulusal Koordinasyon Kurulu”** tarafından yürütülecek çalışmaların kapsamı ise, ilgili taraflarla karşılıklı bilgi alış veriş ve istişarelerde bulunarak bilgi güvenliğinin teminine yönelik olarak ülkemizde ihtiyaç analizinin yapılması, hazırlanacak rapor ışığında alınabilecek hukuki ve teknik tedbirlerin tespit edilmesi ve bu kapsamda yapılabilecek önerilerin değerlendirilerek ülkemiz açısından bir raporun hazırlanması olarak belirlenmelidir.

KAYNAKLAR

- [1] European Innovation, May 2007, pp8
- [2] http://ec.europa.eu/information_society/index_en.htm
- [3] www.eurocomms.co.uk, Identity Crisis, Lynd Morley, pp7
- [4] http://ncecc.ca/cets_e.htm
- [5] www.foxnews.com
- [6] <http://en.wikipedia.org/wiki/echelon>
- [7] System Security, Srdjan Capkun, pp6

İGS Tabanlı Yeni Bir Video–Sırörtme Yöntemi

Özdemir ÇETİN, Ahmet T. ÖZCERİT

Özet — Bu çalışmada, algılanabilirliği düşürebilmek için farklı bir yaklaşıma sahip yeni bir İGS (İnsan Görme Sistemi) tabanlı veri gömme yöntemi önerilmiştir. Önerdiğimiz yöntem iki işlem adımına sahiptir. İlk işlem olarak örtü video dosyası içerisindeki veri gömmeye uygun piksellerin bulunması gerçekleştirildikten sonra ikinci işlem olarak; gizli veri, belirlenen uygun piksellere yeni bir kodlama tekniği ile gömülür. Bu çalışmada, yüksek haberleşme güvenliği sağlayabilmek için sırlı videodaki gizli verinin algılanabilirliğini en düşük seviyede tutma amaçlanmıştır.

Anahtar Kelimeler— Sırörtme, Veri Gizleme, Sayısal Video, Histogram, Dalgaboyu

I. GİRİŞ

İnternet için “zifiri karanlıkta mayın tarlasında ilerlemeye çalışmak” benzetmesini yapmak herhalde yanlış bir tanım olmaz. Sınırları belli olmayan bu devasa dünyada güvenliği sağlamak kolay değil neredeyse imkânsızdır. Sayısal teknolojinin hızlı bir şekilde gelişmesi bilgi hırsızlığını kolaylaştırmış, İnternetin güvenlik zafiyeti de bilgi hırsızlığına iyi bir ortam oluşturmuştur. Ortaya çıkan bu güvenlik zafiyeti, gizli haberleşme tekniklerinin de gelişmesine neden olmuştur. Bu çalışmada, önemli bilgilerin saldırganlardan korunarak haberleşmenin gerçekleştirilebilmesi için yeni bir sırörtme tekniği geliştirilmiştir.

Sayısal medyanın gelişen teknolojiye paralel hızla büyümesi sayısal damgalama, sırörtme gibi veri gizleme yöntemlerinin ortaya çıkmasına neden olmuştur. Sayısal damgalama (watermarking) ve sırörtme (steganography) tekniklerinde kullanılan yöntemler birbirlerine benzerlik gösterse de kullanım amaçları itibarıyla farklılıklara sahiptirler. Bir sayısal medyanın (sinema filmi, müzik parçası vb.) illegal yollarla paylaşılmasını önlemek için sayısal damgalama tercih edilirken bireyler veya kurumlar aralarında gizli haberleşme (askeri istihbarat vb.) yapmak için ise sırörtmeyi kullanırlar.

İki yöntem arasındaki en büyük fark; sayısal damgalama herkes tarafından bilinen bir medya dosyasının korunmasında kullanılırken, sırörtme herkes tarafından bilinmeyen bir medya dosyası ile gizli haberleşme yapmak için kullanılır. Bu yüzden de her iki yöntemin karşılaştığı saldırılar farklılıklar gösterir. Çünkü sırörtmede kullanılan örtü dosyası bilinmeyen herhangi bir dosya olacaktır ve saldırıya maruz kalması çok düşük

bir ihtimaldir. Her iki yöntemde de en önemli nokta, gizli verinin algılanabilirliğinin neredeyse imkânsız olmasının gerçekleştirilebilmesidir.

Gizli haberleşme teknikleri ilk olarak resim dosyaları üzerinde uygulanmış fakat yüksek gizli veri kapasitesi ihtiyacı ve resimlerin sınırlı kapasiteleri, yapılan araştırmaları videolar üzerinde yoğunlaştırmıştır [1]. Video dosyalarına gizli veri gömmek için; genelde resim ve ses içerisine veri gizleme yöntemleri beraber kullanılır. Video içerisine veri gizlemek için dönüşüm–boyutu yöntemleri (Discrete Cosine Transform–DCT, Discrete Wavelength Transform–DWT) kullanılır.

Videoonun veri gizleme için kullanılmasının en büyük yararlarından biri de çok büyük miktarda gizli veri kapasitesi sağlamasıdır. Örneğin 30 fps ve 10 saniye süreli bir video dosyası 300 hareketsiz resimden oluşmaktadır. Böylece bir resim dosyası içerisine gizlenecek gizli veri kapasitesi, bu örnek video dosyası için 300 kat daha fazla olacaktır.

Video dosyaları üzerinde yapılan ilk veri gizleme çalışmaları ham videolar üzerine odaklanmıştır. Bu çalışmalar video içerisine veri gömme yöntemlerinin temelini oluşturmuştur. Günümüzde gerek ilerleyen sıkıştırma teknikleri ve gerekse büyük kapasiteye sahip videoların İnternet üzerinden iletimleri sırasında yaşanan bant genişliği sorunları, çalışmaların sıkıştırılmış videolar üzerine kaymasına neden olmuştur.

Ham video kullanılarak yapılmış ilk veri gizleme çalışmasına örnek olarak Hartung ve Girod’un çalışmasını gösterebiliriz [3]. Bu çalışmada araştırmacılar, yayılı–izge haberleşmesinden esinlenmişlerdir. Hartung bir başka çalışmada resim içerisine veri gömme tekniklerini doğrudan ham videoya uygulamıştır [4]. Gizli verinin geri elde edilmesi aşamasında alıcı tarafında ilgileşim metodu uygulanır. Elde edilen deney sonuçlarına göre gizli veri kapasitesi 50 bit/sn’dir. Hartung ham video için önerdiği bu çalışmasını ayrıca sıkıştırılmış videoya da uygulamıştır. Intra–çerçeve (I-frames), forward predicted çerçeve (P-frames) ve bi-directional predicted çerçevelerinin (B-frames) her birisine diğer yöntemindeki işleyişin aynısını uygulamıştır. Videoda her bir sıkıştırılmış çerçeve için 8×8 DCT katsayılarını kullanarak gizli veriyi çerçevelere eklemiştir. Deneylerden elde edilen sonuçlara göre, standart sinyal işleme saldırılarına karşı daha dayanıklı sonuçlar vermiştir.

Bir başka çalışmada ise Swanson, çoklu–ölçek damgalama yöntemini önermiştir [5,6]. Bu yöntemde, her bir çerçeveye zamansal dalgacık dönüşümü uygulanarak zamansal alçak geçiren ve yüksek geçiren çerçeveler elde

Özdemir Çetin and Ahmet T. Özcerit are with the Department of Computer Systems, Sakarya University, Sakarya, 54188, Turkey (e-mail: {ocetin, aozcerit}@sakarya.edu.tr)

edilir. Bu çalışmada damganın geri elde edilmesi için orijinal video bilgisine ihtiyaç duyulur.

Bu makalede, önceki çalışmalardan farklı olarak örtü videosu içindeki veri gömmeye uygun pikseller İGS'ne duyarlı yeni bir yaklaşımla belirlenmiştir. Ayrıca yapılan çalışmada veri gömme (iletişim amaçlı) ve damga ekleme (güvenlik amaçlı) problemleri birbirlerinden ayrılarak sadece veri gömme üzerinde durulmuştur [7]. Gizli haberleşme süresince taşıyıcı videosunun dışarıdan gelebilecek saldırılara maruz kalmaması için gizli veri algılanabilirliğinin en düşük seviyelerde tutulması çalışmanın asıl amacıdır.

II. SAYISAL VIDEO, HİSTOGRAM VE DALGABOYU KAVRAMLARI

Bir sayısal video, hareketsiz resimlerin İGS tarafından akıcı olarak algılanabilmesi için ardışık olarak saniyede en az 25 kez oynatılması ile oluşmaktadır. Bu çalışmada sunulan yöntem, sıkıştırılmamış (AVI) videolar için geliştirilmiştir. Deneysel çalışmalar süresince kullanılan 'vipmen.avi' videosunun çerçeve yapısı Şekil 1'de görülmektedir.



Şekil-1. Örnek bir video çerçevesi.

Şekil-1'de verilen vipmen videosunun örnek çerçevesinin 120×160 boyutlarında olduğu görülmektedir. Bu bilgiye dayanarak deneysel çalışmalar esnasında kullanılacak olan 'vipmen.avi' videosunun bellekte kapladığı alan aşağıdaki gibi hesaplanabilir;

Video boyutu × Çerçeve sayısı × Renk yoğunluğu
(bayt) × Video süresi (2)

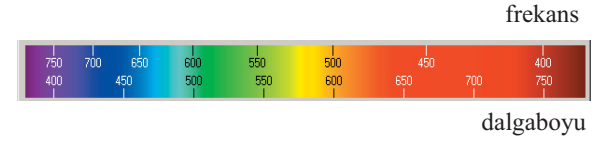
$120 \times 160 \times 30 \times 3 \times 9,43 = 16,300,742$ bayt

Elde edilen sonuca göre vipmen videosu bellekte 16,300,742 bayt yer tutar.

Çalışmamızda kullanılan yöntemlerde bahsedilen terimleri sırası ile kısaca açıklayalım.

Histogram: Bir sinyalin sahip olduğu frekans bileşenleri hakkında bilgi veren bir göstereydir. Sayısal resimlerde veya videolarda histogram grafikleri resmin renk bileşenleri hakkında bilgi verir. 8-bit renk yoğunluğundaki bir video çerçevesinin histogramı, 0-255 arası renk yoğunluğuna ait kaç tane piksel olduğu konusunda bilgi verir.

Dalgaboyu: Bir dalga örüntüsünün tekrarlanan kısımlarının arasındaki mesafe olarak tanımlanabilir ve frekans ile ters orantılıdır. Görülebilir ışığın sahip olduğu dalgaboyu dalgalar ise İGS tarafından algılanamamaktadır (morötesi, kızılötesi vb.) [8].



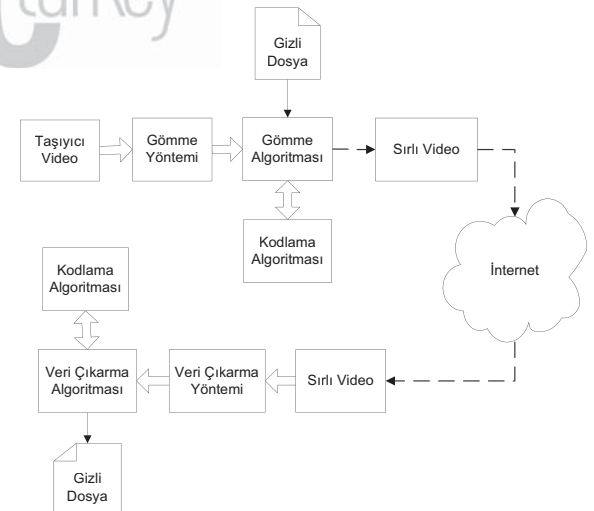
Şekil-2. Görülebilir Işık Dalgaboyu tayfi.

Elektromanyetik tayfta görülebilir alanın dalgaboyu değerleri Şekil-2'de de görüldüğü gibi her bir renk için farklıdır ve alt sınırı 350nm ile mor, üst sınırı da 780nm ile kırmızı temsil eder.

III. ÖNERİLEN VERİ GÖMME ALGORİTMALARI

Bu çalışmada İGS tabanlı yeni bir veri gömme yöntemi geliştirilmiştir [15]. Taşıyıcı video içerisinde veri gömme yapılabilecek bölgelerin belirlenmesinde daha önceki yapılmış çalışmalardan farklı olarak histogramlar ve ışık dalgaboyu yaklaşımları kullanılmıştır. Histogramlar yöntemi, video içerisindeki hareket veya renk yoğunluklarının fazla veya az olduğu durumların belirlenmesinde kullanılan etkili bir yöntemdir. Ayrıca bu yöntem video bölümlendirme çalışmalarında da sıklıkla kullanılmaktadır [9]. Gizleme yapılabilecek uygun piksellerin bulunmasında algılanabilirliği daha da düşürmek nerdeyse imkânsız hale getirmek için ışık dalgaboyu yaklaşımı da histogramlar yöntemi ile birlikte kullanılır.

Şekil-3'de yapılan çalışmayı gösteren genel bir blok diyagram görülmektedir. Gizli veri, gömme yöntemi seçiminden sonra örtü dosyası içerisine gömme ve kodlama algoritmaları vasıtası ile gömülür. Ardından haberleşme kanalına gönderilen şifreli video alıcıya gönderilir. Alıcı tarafta öncelikle işlem türü olarak çıkarma yöntemi seçilir. Çıkarma yönteminin seçiminden sonra gönderici tarafta kullanılan gömme algoritmasına göre çıkarma algoritması belirlenerek gizli veri geri elde edilir.



Şekil-3. Geliştirilen sıfırtme yöntemlerin genel blok diyagramları.

A. Histogramlar Yaklaşımı

Histogramlar yaklaşımında; ardışık gelen her bir video çerçevesinden elde edilen histogram değerleri yorumlanır. İçerisine veri gizlenecek videonun çerçeveleri elde edildikten sonra her bir video çerçevesinin histogram değerleri bulunur. Yapılan çalışmada, ardışık video çerçeveleri arasındaki histogram farkları her bir renk bileşeni (R, G, B) için ayrı ayrı elde edildikten sonra bu bileşenlerin ortalaması alınarak tek bir değer elde edilir. Elde edilen bu değer eşik değeri olarak adlandırılan sayısal bir değer ile karşılaştırılır. Eşik değeri, ardışık çerçeveler arasında bir değişim veya benzerlik algılamasında kullanılan, maksimum alabileceği değer video çerçevesinin boyutu ile ifade edilen piksel sayısıdır. Ardışık çerçevelerin histogram değerleri eşik değeri ile karşılaştırılarak veri gizlenebilecek video çerçeveleri ve pikselleri belirlenir. Eşik değerinin üzerinde kalan bileşenler seçilirse, ardışık video çerçevelerinin renk bakımından karışık bir yapıya sahip olduğu anlaşılır ki bu yöntem farklı histogramlar yöntemi, eşik değerinin altında kalan bileşenlerin seçilmesi durumunda ise ardışık video çerçevelerinin renk bakımından tekdüze olduğu anlaşılır ki bu yöntem de benzer histogramlar yöntemi olarak adlandırılır.

Farklı histogramlar yöntemi ile hedeflenen; video çerçeveleri arasındaki uzamsal algılanabilirliğin önlenmesinin yanında literatürde titreşim sorunu olarak da bilinen zamansal algılanabilirlik sorununa da bir çözüm getirmektir. Bu yöntemde; ardışık video çerçeveleri arasındaki İGS'nin algılayamadığı renk veya hareket geçişleri belirlenerek veri gömmeye kullanılmaları sağlanır.

Benzer histogramlar yönteminde, video içerisindeki ardışık çerçevelerin renk ve hareket bakımından değişmeyen bölgelerine veri gizlemenin yapılması önerilmektedir. Örneğin renk veya hareket bakımından değişmeyen arka plana sahip bir video veri gizleme için ideal alanlardır.

B. Dalgaboyu Yaklaşımı

Dalgaboyu yönteminde İGS'nin zaafından faydalanılarak veri gömme işlemi gerçekleştirilir. Enerji tayfındaki İGS'nin algıladığı renk dalgaboyu aralığı, yani görülebilir ışık alanı bilgisinden faydalanarak veri gizlenecek piksellerin belirlenmesi bu yöntemin temelini oluşturmaktadır.

İçerisine veri gömülmek istenen örtü videosunun çerçevelerinde görülebilir ışık aralığının sınır dalgaboyu değerlerine (380nm–750nm) yakın renklere sahip pikseller belirlenir. Başka bir ifadeyle, morötesi ve kızılötesi dalgaboyu değerlerine yakın renklere sahip pikseller belirlenir. Bu sınırlara yakın dalgaboyu değerlerine sahip renkler kullanılarak veri gizleme işlemi gerçekleştirilir. Burada faydalanılan durum İGS'nin morötesi ve kızılötesi ışık dalgalarını algılayamamasıdır.

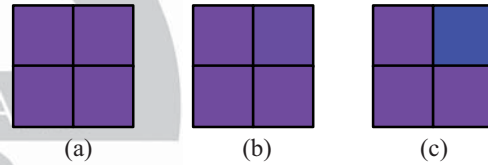
Bu yöntemde, her bir video çerçevesindeki piksellerin ait olduğu renk dalgaboyu değeri bulunur. Bunun için öncelikle mor ve kırmızı renkleri veren RGB renk karışımlarının bir tablosu oluşturulur. Bu tabloyu oluşturmak için herhangi bir resim işleme programından faydalanılabilir. Ayrıca İnternette kolayca bulunabilen

renk kodlarının listelerinden de faydalanmak mümkündür. Bu çalışmada faydalanılan renklerin listesi ve dalgaboyu değerleri Tablo 1'de verilmiştir.

TABLO 1. DALGABOYU DEĞERLERİNİN TANIMLANMASI.

Dalgaboyu Değeri	R renk yoğunluğu	G renk yoğunluğu	B renk yoğunluğu
Mor renk: 380~400	97~130	0~30	97~175
Kırmızı renk: 730~750	161~200	0~30	0~50

Yukarıdaki tabloya göre, örneğin 100,0,105 RGB değerine sahip bir pikselin kabul edilebilir ışık dalgaboyu aralığında olduğu söylenebilir. Böylelikle, veri gizleme algoritması kullanılarak görülebilir ışığın sınır değerlerine (380nm veya 750nm) yakın dalgaboyuna sahip pikseller veri gömme için belirlenir. Belirlenen her bir pikselin veri gömüldükten sonra da ilk dalgaboyu değerine yakın bir değerde kalıp kalmadığı kontrol edilir. Piksel kabul edilebilir bir ışık dalgaboyu değerinde kalıyorsa, bir başka ifadeyle gömme işlemi sonucunda pikselin sahip olduğu ilk dalgaboyu değerinde çok büyük bir değişim olmuyor ise, bu piksele veri gömme yapılabilir. Şekil-4.a'da örnek resimdeki 400nm dalgaboyu değerine sahip mor renkli piksel, veri gömüldükten sonra 400nm ile 410nm aralığında bir dalgaboyu değerinde kalıyorsa bu piksele veri gömme yapılabilir (Şekil 4.b). Fakat piksel veri gömme gerçekleştirildikten sonra 420nm değerine sahip oluyorsa bu piksel veri gömme için uygun değildir (Şekil 4.c). İlk piksel değeri ile sonraki piksel değeri arasında İGS'nin algılayabileceği derecede bir fark söz konusudur.



Şekil 4. (a) 4 pikseli de 400nm dalgaboyu olan örnek bir blok. (b) 2 numaralı pikseli 405nm dalgaboyu olan örnek bir blok. (c) 2 numaralı pikseli 420nm dalgaboyu olan örnek bir blok.

Standart bir video çerçevesinin 352x288 boyutlarında olduğunu düşünürsek piksel sayısı 101376 olarak hesaplanabilir. Yaklaşık olarak 100 bin piksel içerisinde Şekil 4.a'da gösterilen orijinal pikselin Şekil 4.b'deki gibi değişmesinin İGS tarafından algılanması çok zor olacaktır. Fakat Şekil 4.c'deki gibi bir değişikliğin İGS tarafından algılanma ihtimali daha yüksektir.

Dalga boyu yönteminde esas olan, gizli verinin içerisine yerleştirildiği pikselin dalga boyu aralığının sahip olduğu orijinal dalga boyu aralığından çıkmaması kısıtıdır ve bu sayede video çerçevelerini oluşturan her bir piksele birbirinden bağımsız olarak veri gömme işlemi gerçekleştirilebilir.

Dalgaboyu yönteminin benzer ve farklı histogramlar yöntemleri ile birlikte kullanılması sayesinde gizli verinin algılanabilirliği daha da düşürülerek haberleşme güvenliği en üst seviyeye çıkarılabilir. Fakat bu durumun gizli veri kapasitesini önemli ölçüde düşüreceği unutulmamalıdır.

IV. ÖNERİLEN VERİ GÖMME KODLAMA TEKNİĞİ

Görüntüde en az bozulma ve en yüksek veri gizleme, sırtörme yöntemlerinde aranan en temel kıstaslardandır. İstenilen bu kıstasları sağlamak amacıyla RGB ağırlıklı kodlama tekniği geliştirilmiştir [10].

RGB: (89,143,240) olarak üç ana renk dağılımına sahip olan bir pikselin R=89, G=143, B=240 ağırlıklarına sahip olduğu söylenebilir. RGB ağırlıklarına sahip bu pikselin içerisine “s” harfinin ASCII karşılığı olan “115” sayısının gömülme işlemi şu şekilde olacaktır; öncelikle RGB değerinin son rakamları sıfırlanır. Buna göre elimizde R=80, G=140, B=240 değerleri olur. Bir sonraki aşamada “s” karakterinin ASCII karşılığı her basamak değeri 10 sayısından çıkarılır (10-1=9, 10-1=9, 10-5=5). Elde edilen rakamlar her bir RGB değerlerinin son basamaklarına yerleştirilir. Son durumda ise elimizde R=89, G=149, B=245 olan bir RGB değeri bulunur. Gizli verinin elde edilmesi aşamasında ise; pikselin sahip olduğu RGB değerinin son rakamları alınır (9, 9, 5). Bu rakamlar 10 sayısından (10-9=1, 10-9=1, 10-5=5) çıkarılarak tekrar “s” harfinin ASCII kodları elde edilmiş olur.

V. DENEYSEL SONUÇLAR

Çalışmanın bu bölümünde önerilen sırtörme tekniklerinin kapasite, algılanabilirlik ve gömme süreleri gibi parametrelere bağlı başarımları değerlendirilecektir. Çalışmanın sıkıştırılmamış formattaki videolar için geliştirilmiş olmasından dolayı, deneysel çalışmalar süresince literatürde sıklıkla kullanılan ‘vipmen’ videosu kullanılmıştır. Vipmen videosunun çerçeve sayısı 283, çerçeve boyutları ise 160x120 dir.

Deney sonuçlarının değerlendirilmesi aşamasında, sırlı videoların istatistiksel kalitelerini ölçmek için Tepe Sinyal Gürültü Oranı (Peak Signal to Noise Ratio-PSNR) ölçeği kullanılmıştır. PSNR, orijinal görüntü ile sırlı görüntü arasındaki benzerlik oranını hesaplar. Hesaplama sonucunda PSNR tek bir değer üretir. Bu değerin yüksek olması benzerliklerinin de yüksek olduğu anlamına gelmektedir. Aslında PSNR değeri, İGS ile birebir uyuşan bir sonuç vermemektedir. Çünkü insanların renkleri ve tonları algılama davranışı tamamen birbirinden farklıdır. Bu durum göz önüne alınarak bir başka görsel kalite değerlendirme kıstası olan görsel denek ölçüm yöntemi de geliştirilen tekniklerin başarımlarını değerlendirilmesinde kullanılmıştır.

İki görüntü arasındaki PSNR değerini hesaplamak için öncelikle Ortalama Kare Hatası (Mean Squared Error-MSE) değeri hesaplanmalıdır [11]. MSE değerinin hesaplanması için Denklem-3 kullanılabilir.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \|I(i, j) - K(i, j)\|^2$$

veya

$$MSE = \frac{\sum_{M,N} [I(i, j) - K(i, j)]^2}{M \times N}$$

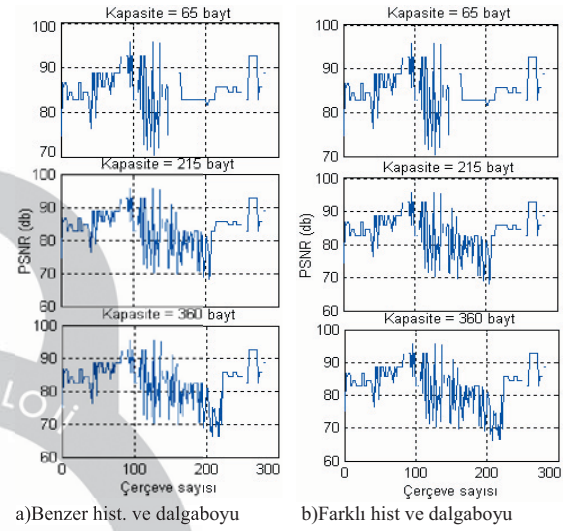
(3)

Burada I ve K birbirleriyle kıyaslanan görüntülerdir. I orijinal görüntüyü K ise yeniden elde edilmiş görüntüyü ifade eder. Görüntü boyutları ise $m \times n$ dir. MSE değerinin hesaplanmasının ardından Denklem-4’e göre PSNR hesaplanır [12,13].

$$PSNR = 10 \log_{10} \left(\frac{MAX^2}{MSE} \right)$$

(4)

Denklem 4’deki MAX, görüntüye ait bir pikselin kaç bit ile ifade edildiğini gösterir. Örneğin 8 – bit renk yoğunluğundaki bir görüntü için MAX = 255 olacaktır.



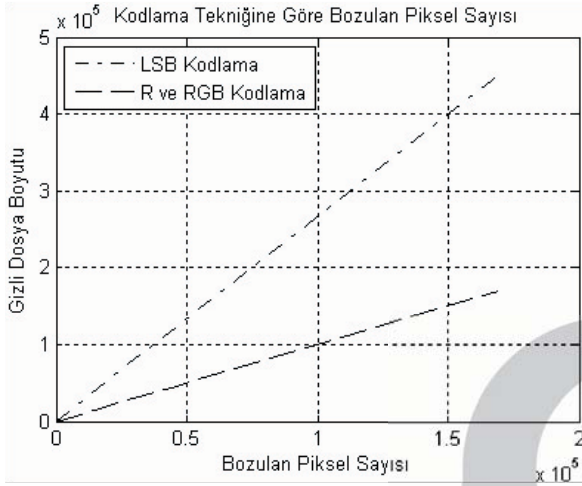
Şekil 5. Önerilen yöntemlerden elde edilen PSNR değerleri.

Bu makalede geliştirilen yöntemlerden elde edilmiş sonuçlar Şekil 5’de verilmiştir. Kayıplı resim/video sıkıştırma işlemlerinden sonra elde edilen görüntüler için kabul gören PSNR değerleri 30db ile 50db arasındadır [12, 13, 14]. Çalışmada, geliştirilen yöntemlerin PSNR değerlerinin yaklaşık olarak 65db ile 95db arasında olduğu görülmektedir ki bu da tatminkar sınırlar içerisinde kabul edilebilir.

Çalışma süresince geliştirilen gizleme yöntemlerine uyarlanan RGB ve R ağırlıklı kodlama tekniklerinden [10] elde edilen başarımlar değerleri Tablo 2’de, grafiksel olarak ise Şekil 6’da gösterilmiştir. Elde edilen sonuçlar ışığında literatürdeki ilk veri gizleme çalışmalarında kullanılan LSB kodlama tekniğinin geliştirilen yeni tekniklere göre çok zayıf olduğu söylenebilir. Deneysel çalışma süresince aynı taşıyıcı video içerisine farklı boyutlarda gizli veri gömme işlemi gerçekleştirilmiştir. Deneysel verilere göre RGB ve R ağırlıklı kodlama tekniklerinin sırlı video içerisinde meydana getirdikleri bozulan piksel sayısı LSB kodlama tekniğine göre yaklaşık 2,5 kat daha azdır.

TABLO 2. GÖMME İŞLEMİ SONUNDA KODLAMA TEKNİKLERİNE GÖRE
GÖRÜNTÜDE BOZULAN PİKSEL SAYISI.

Örtü Video Boyutu (bayt)	Gizli Veri Boyutu (bayt)	Bozulan Pİksel Sayısı		
		LSB	RGB	R
15,220,624	73	195	73	73
	1800	4800	1800	1800
	27648	73728	27648	27648
	54784	146091	54784	54784
	103424	275798	103424	103424
	168960	450560	168960	168960



Şekil 6. Kodlama yöntemlerine göre taşıyıcı video içerisinde bozulan piksel sayısı.

Tablo 2'ye bakıldığında bozulan piksel sayısına göre RGB ve R kodlama tekniklerinden elde edilen sonuçların aynı olduğu görülmektedir. Fakat bu durum piksel seviyesinde incelendiğinde, R kodlama tekniğinde pikseldeki bozulmanın RGB kodlamaya göre daha az olduğu görülür. Çünkü RGB kodlamada; R, G ve B renk bileşenlerine uygulanan kodlama yöntemi aynıdır. Bu renk bileşenlerindeki değişimler 0-9 değerleri arasında olacaktır. Fakat R kodlamada ise R renk bileşeni G ve B renk bileşenlerinden farklı olarak sadece 0-2 değerleri arasında bozulmaya maruz kalacaktır. Bu durum video içerisinde bozulan piksel sayısını azaltmamakta fakat algılanabilirliği azaltmaktadır.

VI. SONUÇLAR

Bu makalede sunulan araştırmanın amacı, İnternet gibi güvenli olmayan ortamlarda güvenli haberleşme sağlayabilmek için haberleşme bilgilerinin korunmasını kapsayan yeni birtakım veri gizleme tekniklerini ortaya koymak ve gerçekleştirmektir.

Sırtörme işleminde birinci ve en önemli gereksinim algılanamazlıktır. Resim, video gibi görsel içerikli taşıyıcı dosyalarda algılanabilirlik kıstası İGS'ne bağlıdır. Bu durumda geliştirilmesi gereken yeni yöntemin İGS özelliklerine, sınırlarına hassas olması gerekmektedir. Araştırmada gizli verinin video çerçevelerinin veri gömmeye uygun pikselleri içerisine yerleştirilmesinde daha önceki yapılmış benzer çalışmalarda uygulanmayan histogram ve görülebilir ışık dalgaboyu yöntemleri kullanılmıştır. Video dosyalarında İGS'nin duyarlı olduğu en önemli nokta, renk geçişleri ve video içerisindeki

hareketliliklerdir. Bu düşünce ile taşıyıcı videoların histogram değerleri hesaplanarak renk geçiş noktaları, hareketliliğin bulunduğu çerçeveler belirlenmiştir. Algılanabilirliği daha da düşürmek için görülebilir ışık dalgaboyu yöntemi histogramlar yöntemi ile birleştirilmiştir. Burada ana fikir; taşıyıcı video içerisindeki görülebilir ışığın sınırlarına yakın olan dalgaboyu değerlerine sahip piksellerin bulunarak veri gömmek için kullanılmasını sağlamaktır. Veri gizlemek için kullanılacak olan piksellerin dalgaboyu değerleri kızılötesi (750nm) veya morötesi (380nm) dalgaboyu değerlerine ne kadar yakın olursa, algılama işlemi de o kadar imkânsız olacaktır.

Ayrıca araştırmamızda; gizli veri kapasitesini literatürdeki En Düşük Değerlikli Bit (LSB) kodlama tekniğine göre önemli ölçüde artıran, resim sırtörme için geliştirilmiş RGB ve R ağırlıklı kodlama teknikleri video sırtörtmeye uygulanmıştır. Bu kodlama tekniği ile video görüntüsünde en az bozulma hedeflenerek gizli veri kapasitesi artırılmaya çalışılmıştır.

KAYNAKLAR

- [1] A. Koz, A. Alatan, "Oblivious Video Watermarking Using Temporal Sensitivity of HVS", Proceedings of the 2005 International Conference on Image Processing (ICIP 2005), Genoa, Italy, September 11-14, 2005, IEEE.
- [2] A. Mangarac, Stego FAQ, <http://zone-h.org> Zone-H, 2006.
- [3] F. Hartung, B. Girod, "Digital watermarking of raw and compressed video," in Proc. SPIE 2952: Digital Compression Technologies and Systems for Video Communication, Berlin, Germany, Oct. 1996, pp. 205-213.
- [4] F. Hartung, B. Girod, "Digital watermarking of uncompressed and compressed video", Trans. Of Signal Processing – Special Issue on Copyright protection and Access Control for Multimedia Services, 66(3):283-301, 1998.
- [5] M. D. Swanson, B. Zhu, A.T. Tewfik, "Multiresolution scene-based video watermarking using perceptual models", IEEE J. Select. Areas Commun., vol. 16, pp. 540-550, 1998.
- [6] M. D. Swanson, B. Zhu, A.T. Tewfik, "Data Hiding for Video-in-Video", Proc. ICIP'97, Santa Barbara, CA, 2:676-679, 1997.
- [7] M. K. Mihçak, "Watermarking Via Optimization Algorithms For Quantizing Randomized Image Characteristics", Microsoft Research, Cryptography and Anti-Piracy Group WA, USA.
- [8] O. Cetin, A.T. Özçerit, M. Cakiroglu, "A New Data Embedding Method into Motion Pictures" The 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing, June 26-29, 2006, Las Vegas, USA.
- [9] I. Koprinska, S. Carrato, "Temporal Video Segmentation: A Survey", Signal Processing Image Communication, Elsevier Science, 2001.
- [10] F. Akar, H. S. Varol, "A New RGB Weighted Encoding Technique for Efficient Information Hiding in Images" Journal of Naval Science and Engineering Number 2 Volume 2 July 2004.
- [11] K.S. Jonathan, F. Hartung, B. Girod, "Digital Watermarking Of Text, Image, And Video Documents Comput. & Graphics", Vol. 22, No. 6, pp. 687-695, Elsevier Science, 1999.
- [12] A.N. Netravali, B.G. Haskell, "Digital Pictures: Representation, Compression, and Standards (2nd Ed)", Plenum Press, New York, NY 1995.
- [13] M. Rabbani, P.W. Jones, "Digital Image Compression Techniques", Vol TT7, SPIE Optical Engineering Press, Bellvue, Washington 1991.
- [14] http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio#searchInput#searchInput (Erişim Tarihi: Haziran 2008).
- [15] O. Cetin, "A Data Embedding Algorithm Design for Video Applications Using a New Steganography Approach (Thesis or Dissertation style)", Ph.D. dissertation, Dept. Elect. Eng., Sakarya Uni., Sakarya, Turkey, 2008.

Verileri Nota Kullanarak Şifreleme ve Ses Dosyası İçerisine Gizleme

Muhammet Hamdi YAVUZ, Oğuz ERGİN

Özet—Gizli tutulması gereken verilerin dışarıya açık sistemlerle aktarılması veriyi ilgilendiren kişiler için büyük bir sorun teşkil etmektedir. Bu çalışmada veri şifrelemeye ve veri içerisine veri saklamaya farklı bir yaklaşım getirilmiştir. Önce AES şifreleme algoritmasıyla şifrelenen veriler daha sonra müzik notalarına dönüştürülmekte, dönüştürülen bu notalar AES'nin S-kutusu'nu (S-box) güncellerken aynı zamanda bir ses dosyasındaki müziğin notalarına dönüştürülmeleri için gerekli olan veriler aynı ses dosyası içerisine seçilen bir anahtar yardımıyla gizlenmektedir. Sonuçta ortaya şüphelenilmeyen fakat gizli verileri taşıyan bir şarkı çıkmaktadır.

Anahtar Kelimeler—aes, güvenlik, kriptografi, müzik, nota, steganografi.

I. GİRİŞ

GÜNÜMÜZ dünyasında gizli tutulması gereken bilgilerin dışarıdan erişilebilir sistemler vasıtasıyla, bilginin kaynağından başka bir yere aktarılması, bilginin sahipleri için şüphesiz ciddi sorunlar oluşturmakta ve bilginin gizli kalmamasının etkileyeceği kitleler için çok önemli bir tehdit unsuru olmaktadır.

Gizli tutulan veriler internet gibi herkese açık olan bir ağdan gönderildiği zaman üçüncü şahıslar tarafından erişilebilir. Bu tehlikeye karşı birçok şifreleme algoritması geliştirilmiş ve hala dünyanın dört bir yanında kullanılmaktadır. Veriler şifrelendiğinde hala veri sıfatındadırlar, sadece başka bir türe dönüşmüş olarak nitelendirilebilirler. Veriyi ne şekilde eski haline dönüştürebileceklerini bilen kişiler tarafından eski haline dönüştürülebilirler. Şifrelenmiş verilerdeki en büyük sıkıntılardan birisi üçüncü şahıslar tarafından ele geçirildiklerinde ortada şifrelenmiş bir veri olduğunun görülmesidir. Yeterince zaman harcayan birisi şifrelenmiş gizli bilgilere, veriyi özgün haline dönüştürerek erişebilir. Bu durumu göz önünde bulunduran ve gizli veri aktarımı yapmak isteyen bazı insanlar steganografi (veri içerisine veri gizleme) yoluna başvururlar. Burada aktarılan bilgiyi eline geçirmiş olan kişinin şifrelenmiş bir veri olduğunu görmemesi ve eline geçirdiği verilerden şüphelenmemesi şifrelemeye göre avantaj sağlamaktadır [1]. Pooyan ve Delforouzi çalışmalarında, bu

şüpheleri azaltmak için taşıyıcı ses dosyasındaki en anlamsız bitleri saptamak suretiyle verileri bu anlamsız bitlere saklamanın daha iyi olacağını belirtmişlerdir [2]. Gopalan ise yapmış olduğu çalışmada her örnekteki bir biti gizli verisindeki bitler ile değiştirmiştir [3]. Söz konusu gizli bilgi kişiye özel olduğunda, ele geçmesi durumunda çok kötü sonuçlar doğurmayacağı zaman şifreleme veya steganografi yollarına başvurmak çoğu zaman yeterli olacaktır ancak bu gizli bilginin bir askeri bilgi veya devlet sırrı olduğu ve bir ülkenin kaderini belirleyebileceği düşünüldüğünde bu yöntemler tek başlarına hiçbir zaman yeterli olmayacak ve sürekli yeni teknikler geliştirilmeye devam edilecektir. Bu çalışmada, gizli veri aktarımını daha güvenli hale getirebilmek için bazı bilinen teknikleri içeren yeni bir yöntem ortaya çıkarılmıştır.

Yapılan yeni yaklaşımın ilk aşamasında AES şifreleme yöntemi kullanılmaktadır. Rijndael algoritması ile 128 bitlik veri parçaları 128, 192 veya 256 bitlik şifreleme anahtarları ile şifrelenmektedir [4]. İkinci aşamaya geçildiğinde şifrelenen veriler, önceden belirlenmiş olan bir tabloya göre müzik notalarına çevrilmekte ve ortaya, icra edildiğinde kulağa hoş gelmesi tesadüfi olan bir nota dizisi çıkmaktadır. Gizli verinin bir ses dosyası içerisine gizlenerek taşınması amaçlanmıştır. Bu ses dosyası herhangi bir şarkı olabilmektedir. Son durumda elde bulunan nota dizisinin anlamsız bir dizi nota olma ihtimali çok yüksek olacaktır. Bu nota dizisi ile öncelikle birinci aşamada AES şifrelemesi için kullanılan S-kutusu (S-box) [4] güncellenir ve bir sonraki aşamaya geçilir. Üçüncü aşamaya geçilir. Üçüncü aşamada ise bu notalar, taşıyıcı ses dosyasındaki müziğin notalarına dönüştürülür. Bu aşamada esas olan notayı dönüştürürken eldeki nota ve hedef nota arasındaki üçüncü notanın saptanmasıdır. Asıl taşınacak olan veri bu üçüncü nota dizisidir. Üçüncü nota dizisi saptanarak önceden hazırlanan tablodaki karşılığı olan onaltılık değerine dönüştürülmektedir. Dördüncü ve son aşamada ise son durumda elde edilen veriler taşıyıcı ses dosyasının içerisine gizlenmektedir.

Bütün bu işlemleri bir boru hattı tasarlayarak yaptırmak zaman tasarrufu sağlayacaktır. Örneğin ikinci aşamanın sonunda elde edilen nota dizisi S-kutusu'nu güncellerken aynı anda üçüncü aşamanın başlaması tasarımın verimli çalışması için çok uygun olacaktır.

Dördüncü aşamanın sonunda artık gizli bilgi, güvenle aktarılmak için hazır hale gelmiş bulunmaktadır. Eğer aktarılan ses dosyası üçüncü şahıslar tarafından ele geçirilirse öncelikle bu dosyanın gizli bir bilgi taşıdığına dair

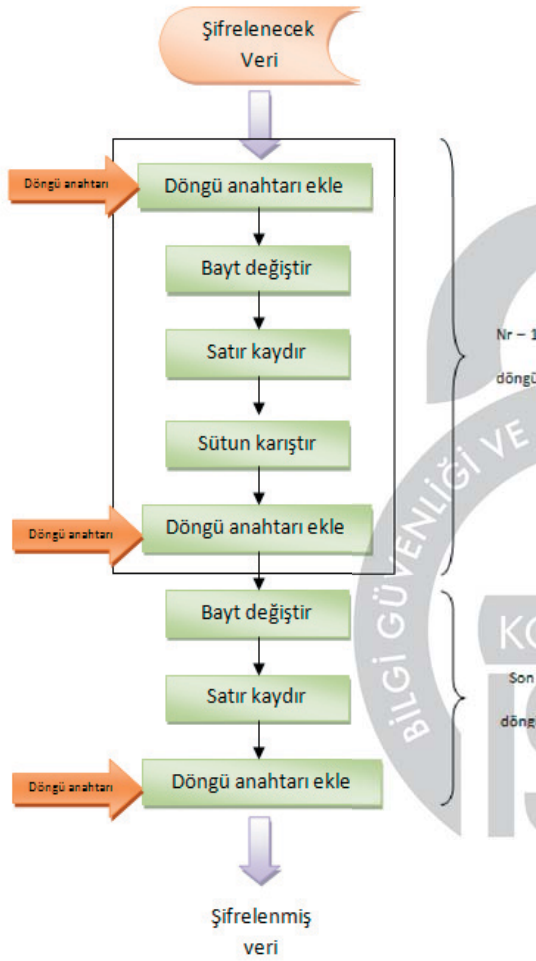
Muhammet Hamdi Yavuz, Gazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Kimya Mühendisliği Bölümü, Ankara'da lisans eğitimine devam etmektedir. e-posta: muhammethamdiyavuz@gmail.com

Oğuz Ergin, TOBB Ekonomi ve Teknoloji Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü. Tel: (312) 292 4059, Faks: (312) 292 4180, e-posta: oergin@etu.edu.tr

şüphelenmeleri daha sonra çalan müziği notaya dökebilecek kadar iyi seviyede müzik bilgilerinin olması, daha sonra bütün tasarımı çözmeleri (nota dönüştürmede kullanılan tablolar ve yöntemler dahil) ve en sonunda karşılırlarına çıkan S-kutusu güncellenen bir AES algoritmasını tersine çevirmeleri gerekmektedir.

II. AES ALGORİTMASI

DES şifreleme algoritmasının iyi bir algoritma olduğunun



Şekil 1. AES şifreleme algoritmasının işleyişi (Nr döngü sayısını ifade etmektedir)

kabul edilmesine rağmen düşük döngü (round) sayısı, düşük şifre parça boyutu sebebiyle ve dönemin meşhur EFF paralel bilgisayarı *Deep Crack*'e yapılan test saldırılarının sonucunda DES algoritması yerini AES algoritmasına bırakmıştır [5].

AES algoritması, 128, 192 veya 256 bitlik şifreleme anahtarları ile 128 bitlik veri parçalarını şifreleyen bir algoritmadır. Her veri parçası, "state" adı verilen 4×4' lük bayt dizilerinden oluşmaktadır. Algoritmanın temel işlemleri bu diziler üzerine uygulanmaktadır [6]. AES algoritması,

"Bayt Değiştirme (Sub Bytes)", "Satır Kaydırma (Shift Rows)", "Sütun karıştırma (Mix Columns)" ve "Döngü Anahtarı Ekleme (Add Round Key)" adları verilen dört temel dönüşümden oluşmaktadır. Döngü sayısı, anahtar boyutuna bağlı olarak 10, 12 veya 14 olabilmektedir. Şekil. 1'de AES şifreleme algoritmasının işleyişi gösterilmiştir.

Başlangıçta döngü anahtarı eklendikten sonra, yukarıda ifade edilen dört temel dönüşümü içeren döngü fonksiyonu uygulanır. Son döngüde sütun karıştırma dönüşümü uygulanmaz. Bayt değiştirme dönüşümü, S-kutusu dönüşüm tablosunu kullanarak, 4×4'lük bayt dizilerinin her birini bağımsız olarak, doğrusal olmayan bir şekilde dönüştürme işlemidir. Satır kaydırma dönüşümü, 4×4' lük bayt dizilerinin satırlarını dairesel olarak kaydırma işlemidir. Sütun karıştırma işleminde her bir sütun dört terimli birer polinom olarak düşünülerek sabit bir polinomla çarpılır ve sütunlar dönüştürülmüş olur. Döngü anahtarı ekleme işleminde ise; anahtar genişletme işlemi sonucunda üretilen döngü anahtarlarının, her bir tekrarda diziyeye özel veya (XOR) işlemi ile katılması söz konusudur.

AES şifreleme algoritması ile şifrelenmiş bir veriyi çözmek için AES şifreleme algoritmasında uygulanan dönüşümlerin tersi uygulanmaktadır [4][5][6].

III. ŞİFRELENEN VERİNİN NOTAYA ÇEVİRİLMESİ

Tasarımın ikinci aşamasında, ilk aşamada AES şifreleme algoritması ile şifrelenen verilerin müzik notalarına çevrilmesi esastır. Bu işlemin yapılabilmesi için önce notaların kullanılacak özellikleri tanımlanmıştır.

A. Notalar ve Kullanılacak Özellikleri

Batı müziğinde arızalı sesler (diyez ve bemol) dahil kullanılan 12 ses bulunmaktadır. Bunlar; *do*, *do diyez* (*re bemol*), *re*, *re diyez* (*mi bemol*), *mi*, *fa*, *fa diyez* (*sol bemol*), *sol*, *sol diyez* (*la bemol*), *la*, *la diyez* (*si bemol*), ve *si*'dir. Yukarıda yazılı her ardışık sesin arası yarım ses olarak tanımlanır. Örneğin; *re* sesi yarım ses inceltildiğinde *re diyez* sesi elde edilir. Şekil. 2'de notaların müzik yazımındaki gösterimleri sunulmuştur.



Şekil 2. Notaların müzik yazımındaki gösterimi.

Müzikteki seslerin her birinin birer frekans değeri vardır. Bir frekans değeriyle, o değerin iki katı veya yarısı arasına bir oktav denir. Örneğin dördüncü oktavda *la* sesinin frekansı 440 Hz'dir. Buradan yola çıkarak herhangi bir oktavdaki nota değerinin frekansı aşağıdaki formülle hesaplanabilir.

$$f = 2^{n/12} \times 440 \text{ Hz} \quad (1)$$

Yukarıdaki formülde "*f*" frekansı, "*n*" ise frekansı hesaplanmak istenen nota ile dördüncü oktavdaki *la* (La4) arasındaki yarım seslerin sayısıdır. Eğer frekansı hesaplanmak

istenilen nota $La4'$ ün üzerindeyse ($La4'$ ten inceyse) n pozitif, altındaysa ($La4'$ ten kalınsa) n negatiftir. Bu çalışmada kullanılan notalar ikinci oktavdaki do 'dan ($Do2$) yedinci oktavdaki re diyez'e ($Re\#7$) kadar olan notalardır.

Müzik yazımında her bir notanın birer uzunluk değeri vardır. Bunlar aşağıdaki gibi sıralanabilir:

- Tam (Birlik) Nota
- 1/2'lik (Yarımlık) Nota
- 1/4'lük (Bir Dörtlük) Nota
- 1/8'lik (Sekizlik) Nota
- 1/16'lık (Onaltılık) Nota
- 1/32'lik (Otuzikilik) Nota
- 1/64'lük (Altmışdörtlük) Nota

Birlik nota müzikte en uzun değer olup dört vuruştan ibarettir. Yarımlık nota birliğin yarısı değerindedir. Aynı şekilde sekizlik, bir dörtlüğün, otuzikilik onaltılığın, altmışdörtlük otuzikiliğin yarısıdır. Yani birlik nota, iki tane ikilik, dört tane dörtlük, sekiz tane sekizlik, onaltı tane onaltılık, otuziki tane otuzikilik veya altmışdört tane altmışdörtlük değerindedir [7].

Bu çalışmada notaların yalnızca yukarıda bahsedilen özellikleri kullanılmıştır. Yani bu tasarımda esas olan notanın hangi nota olduğu ve notanın değerinin ne olduğudur.

B. Verinin Tanımlanması ve Notaya Dönüştürülmesi

Yukarıda bahsedilen özelliklerin sayısı düşünülecek olursa nota değerleri (birlik, yarımlık, bir dörtlük, sekizlik, onaltılık, otuzikilik, altmışdörtlük) 7 tanedir. Çalışmanın bu aşamasında yalnızca yarımlık, bir dörtlük, sekizlik ve onaltılık nota değerleri kullanılacaktır. O halde bu dört değer ikilik tabanda düşünüldüğünde nota değerleri iki bitle ifade edilebilir. Bu iki bitin nota değeri karşılıkları Tablo 1'de sunulmuştur.

TABLO 1
İKİLİK TABANDAKİ DEĞERLERİN NOTA DEĞERİ KARŞILIKLARI

İkilik değer	00	01	10	11
Nota değeri	Yarımlık	Bir dörtlük	Sekizlik	Onaltılık

Birinci aşamadan gelen veriler bir baytlık paketler halinde işlenecektir. Bahsedilen sekiz bitin ilk iki biti notanın değerini, sonraki altı bit ise notanın ne olduğunu ifade etmektedir. Sonraki altı bitin ikilik tabandaki karşılıklarına göre hangi nota olduğunun nasıl belirleneceği ise Tablo 2'de sunulmuştur.

Örneğin ilk aşamadaki AES şifreleme algoritmasından gelen sekiz bitlik bir çıktı 10101101 olduğu takdirde bu verinin Tablo 1 ve Tablo 2'den yararlanılarak ilk iki bitin sekizlik nota değerine, sonraki altı bitin ise $LA5'$ e denk geldiği açıkça görülebilir. O halde, 10101101 değeri, sekizlik ve beşinci oktavdaki la notasıdır.

C. S-kutusu'nun Güncellenmesi

Birinci aşamada AES şifreleme algoritmasından gelen veriler notaya çevrilirken aynı zamanda AES algoritmasının temel yapıtaşı olan S-kutusunun güncellenmesi

düşünülmüştür. Bunun için her notada farklı olan frekans değerleri kullanılacaktır. Bu sebeple ilk aşamadan gelen sekiz bitlik verinin ilk iki biti ilk aşamada düşünülmemektedir. Sonraki altı bit bir notayı ifade ettiğinden Denklem 1 kullanılarak frekans kolayca hesaplanabilir. Ancak öncelikle söz konusu denklemde kullanmak üzere bir " n " değeri hesaplanmalıdır. " n " değerinin ikilik tabandaki karşılığı aşağıdaki denklem yardımıyla kolaylıkla hesaplanabilmektedir.

$$n = (V - 100001)/10 \quad (2)$$

Yukarıdaki denklemde " V " 6 bitlik notayı ifade etmektedir.

TABLO 2
İKİLİK TABANDAKİ DEĞERLERİN NOTA KARŞILIKLARI

İkilik Değer	Nota	İkilik Değer	Nota
000000	DO2	100000	SOL#4
000001	DO#2	100001	LA4
000010	RE2	100010	LA#4
000011	RE#2	100011	Sİ4
000100	Mİ2	100100	DO5
000101	FA2	100101	DO#5
000110	FA#2	100110	RE5
000111	SOL2	100111	RE#5
001000	SOL#2	101000	Mİ5
001001	LA2	101001	FA5
001010	LA#2	101010	FA#5
001011	Sİ2	101011	SOL5
001100	DO3	101100	SOL#5
001101	DO#3	101101	LA5
001110	RE3	101110	LA#5
001111	RE#3	101111	Sİ5
010000	Mİ3	110000	DO6
010001	FA3	110001	DO#6
010010	FA#3	110010	RE6
010011	SOL3	110011	RE#6
010100	SOL#3	110100	Mİ6
010101	LA3	110101	FA6
010110	LA#3	110110	FA#6
010111	Sİ3	110111	SOL6
011000	DO4	111000	SOL#6
011001	DO#4	111001	LA6
011010	RE4	111010	LA#6
011011	RE#4	111011	Sİ6
011100	Mİ4	111100	DO7
011101	FA4	111101	DO#7
011110	FA#4	111110	RE7
011111	SOL4	111111	RE#7

Bulunan n değeri Denklem 1' de yerine yazılarak, işlem yapılan notanın frekans değeri hesaplanır. Frekans değerinin

tam kısmı alınarak bu değerin başına iki bitlik nota değeri eklenir ve S-kutusu'nun ilk bayt'ı güncellenir. Veri akışı devam ettikçe sürekli güncellenen bir S-kutusuyla işlem yapmaya devam edilir.

IV. NOTAYA DÖNÜŞTÜRÜLEN VERİNİN TAŞIYICI SES DOSYASINDAKİ MÜZİĞİN NOTALARINA DÖNÜŞTÜRÜLMESİ

Üçüncü bölümde anlatılan işlemler sonucunda şifrelenmiş verilerden büyük olasılıkla anlamsız bir nota dizisi elde edilmiş olacaktır. Tasarımın temel amacı, bu notaları taşıyıcı ses dosyasındaki müziğin notalarına çevirmek, daha doğrusu çevirmek için gerekli olan veriyi bu ses dosyasına gizlemektir. Söz konusu anlamsız nota dizisinin frekansları Denklem 1 yardımıyla hesaplanmıştır.

Öncelikle taşıyıcı ses dosyasındaki müziğin önceden kararlaştırılmış notaları belirlenir. Örneğin müziğin içerisinde sadece piyano notaları esas alınarak bütün bu işlemler gerçekleştirilebilir. Notaların yine sadece ikinci bölümün B başlığında bahsedildiği özellikleri kullanılacaktır. Diğer tüm müzikal özellikler ve taşıyıcı müzikteki farklı notalar ihmal edilecektir.

Elde bulunan anlamsız notalar ile taşıyıcı dosyadan alınan anlamlı notalar sırasıyla ve birebir *özel veya* işlemine tabi tutulur. *Özel veya* işleminin yapısı gereği, anlamsız nota ve anlamlı nota arasında *özel veya* işlemi yapıldığında anlamsız notayı anlamlı hale çevirecek veri elde edilmiş olacaktır.

Örneğin üçüncü bölümde anlatılan işlemler sonucu *onaltılık ve üçüncü oktavdan si* notası elde edilmiş ise bu notanın ikilik

tabanda karşılığı *11010111*'dir. Taşıyıcı müziğin sıradaki notası ise *sekizlik ve dördüncü oktavdan sol* notası olsun. Bu notanın ikilik tabanda karşılığı ise *10011111*'dir. Bu iki sayı *özel veya* işlemine tabi tutulursa;

$$\{11010111\} \oplus \{10011111\} = 01001000$$

elde edilir.

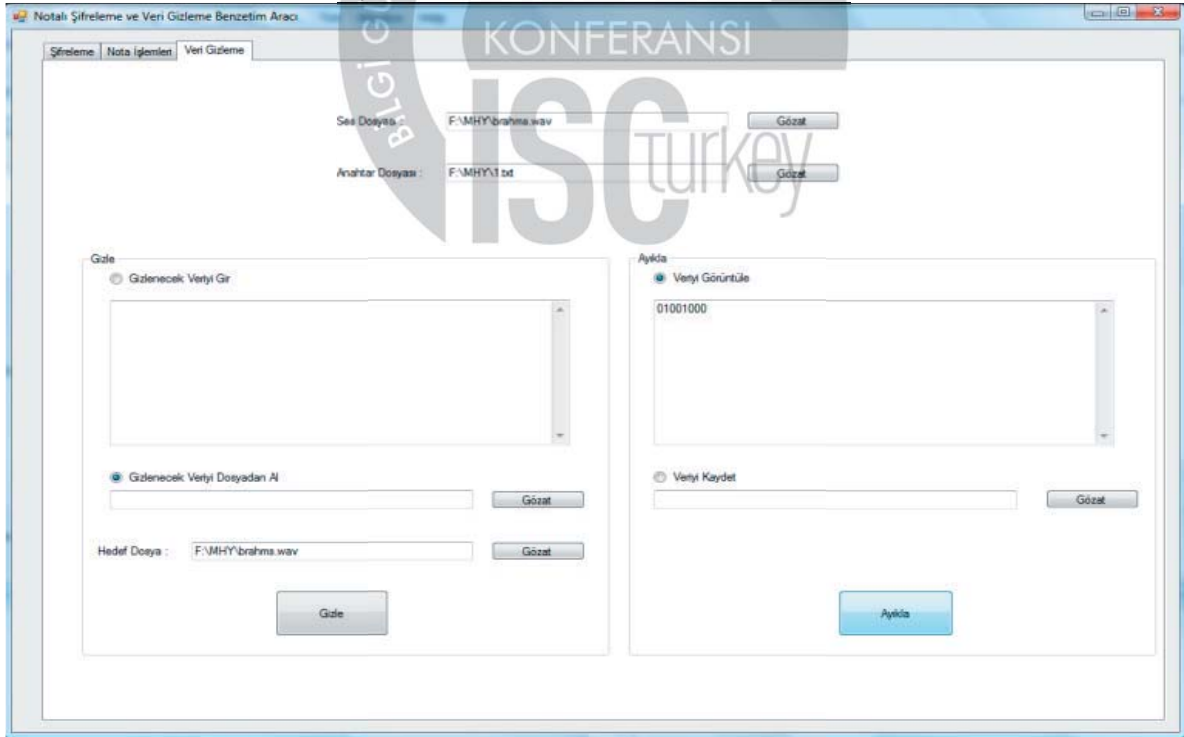
Anlamsız nota dizisindeki her bir notaya bu işlem uygulandığında elde edilen veriler, anlamsız nota dizisini anlamlı nota dizisine çeviren verilerdir ve bu veriler taşıyıcı ses dosyasının içine gizlenecek olan verilerdir.

V. ELDE EDİLEN VERİLERİN TAŞIYICI SES DOSYASINA GİZLENMESİ

Bu çalışmadaki tasarımın son aşaması dördüncü bölümde elde edilen verilerin taşıyıcı ses dosyası içerisine gizlenmesidir.

Gizleme işlemi gizlenmek istenen verinin bitlerinin, taşıyıcı ses dosyasının bazı bitleri üzerine yazılmasından ibarettir. Verinin hangi bitlerin üzerine yazılacağı önceden belirlenmiş bir anahtar yardımıyla tespit edilmektedir.

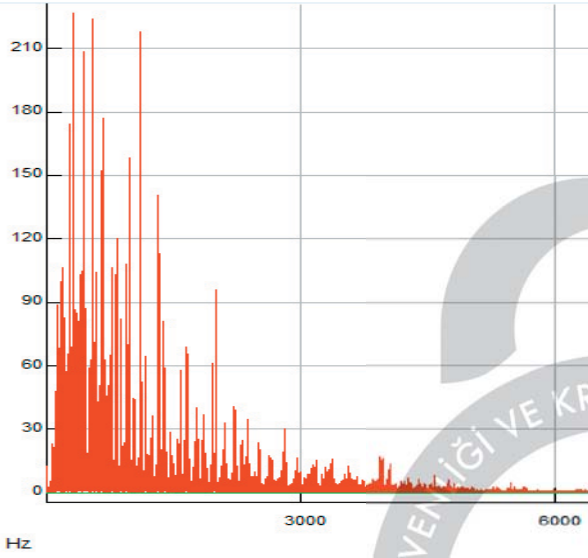
Gizlenecek veri taşıyıcı dosyaya sekiz bitlik paketler halinde yazılmaktadır. Her paketin sonunda anahtarın boyutu kadar bit atlanarak daha sonraki sekiz bit yazılmaya başlanır. Şekil 3'te bu çalışmada önerilen yöntemin denenmesi amacıyla C# ile tasarlanıp kullanılan benzetim aracından (daha önceden içerisine 01001000 verisi saklanmış olan dosyanın içinden veri ayıklanırken) veri ayıklama ekran görüntüsü sunulmuştur.



Şekil 3. Benzetim Aracı Ekran Görüntüsü.

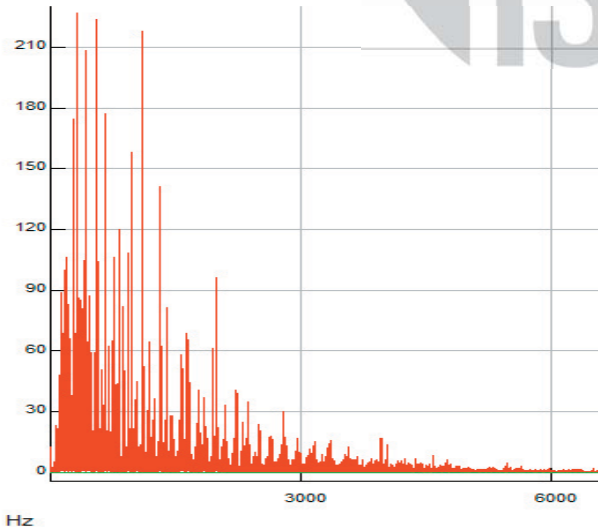
VI. GİZLENEN VERİLERE ULAŞMA İŞLEMİ

Ses dosyasına sayısal işleme yapılmadığı sürece seste kayıplar her zaman mevcut olacaktır. Örneğin bilgisayarınıza önceki bir kayıttan çalmak suretiyle ses kaydettiğinizi düşünürseniz iki kayıttaki veriler birbirini tamamiyla tutmayacaktır. Bu sebeple gizlenmiş olan veriler sonucu yapılan denemelerde, seslerdeki farklılıkların dikkat çekmediği tespit edilmiştir. Şekil 4'te taşıyıcı ses dosyasının ilk halinin ve Şekil 5'te taşıyıcı dosyanın veri gizlendikten sonraki halinin izge (spektrum) çözümü sunulmuştur.



Şekil 4. Taşıyıcı ses dosyasının ilk halinin izge çözümü.

Yapılan izge çözümü, oldukça fazla veri değiştirildiğinde bile taşıyıcı dosyanın ilk haliyle veri gizlendikten sonraki hali arasında çok büyük farklılıklar olmadığını göstermektedir.



Şekil 5. Taşıyıcı ses dosyasına veri gizlendikten sonraki izge çözümü.

Yukarıda bahsedilen algoritma ile şifrelenip ses dosyası içerisine gizlenen verilerin ayıklanıp işlenmesi işlemi aslında anlatılan yöntemten tamamen tersine çevrilmesinden ibarettir.

Öncelikle taşıyıcı ses dosyasında bulunan müzik notalara dokülür. Bu işlem, iki şekilde mümkün olabilmektedir. Birincisi tamamen insan kulağına bağlı olarak notaları saptama işlemidir. İkincisi ise söz konusu dosyanın sayısal olarak işlenerek notaların saptanmasıdır.

Veriler ses dosyasına gizlenirken kullanılan anahtar çözümde de kullanılarak ses dosyasının hangi bitlerine verilerin saklandığı anlaşılır ve böylece kullanılacak olan veriler ses dosyasından ayıklanır.

İlk etapta bulunan anlamlı notaların tasarımı ilgilendiren elemanları (ikinci oktav do'dan yedinci oktav re diyeze kadar yarımlik, bir dördlük, sekizlik ve onaltılık olanlar) üçüncü bölümde anlatıldığı gibi 8 bitlik verilere çevrilir.

Ulaşılan bu anlamlı nota verileri, taşıyıcı ses dosyasından ayıklanan veriler ile özel veya işlemine tabi tutulur ve artık AES ile şifrelenmiş anlamsız nota olarak tanımlanan verilere ulaşılmış olunur.

Bu anlamsız notaların frekans değerleri üçüncü bölümde anlatıldığı gibi hesaplanır. Böylece AES'nin S-kutusu için yapılan güncellemeler ortaya çıkmış olacaktır.

Son veriden önce S-kutusu'na yapılan güncellemelerin tamamı dikkate alınır. Son veriden başlamak suretiyle, S-kutusu her adımda güncellenerek (şifreleme yapılırken yapılan güncellemeler sırayla geri alınarak) AES çözüm algoritması uygulanır ve gizlenen verilere ulaşılır.

VII. SONUÇ

Bu çalışmada gizlenmek istenen veriler, bazı işlemlerden geçerek, dinlendiğinde hiç şüphe uyandırmayan şarkılar içerisine gizlenmiştir. Diğer çalışmalardan farklı olarak, bu çalışmada veriler önce AES şifreleme algoritması ile şifrelenmiş, daha sonra AES'den çıkan veriler notalara dönüştürülmüş ve en sonunda ortaya çıkan anlamsız nota dizilerinin taşıyıcı ses dosyasındaki müziğe göre anlamlı kılınmasını sağlayan veriler herhangi bir anahtar kullanılarak taşıyıcı ses dosyasına gizlenmiştir. Gizleme işlemi yer değiştirme esasıyla yapıldığı için taşıyıcı dosyada herhangi bir boyut değişimi söz konusu olmamaktadır.

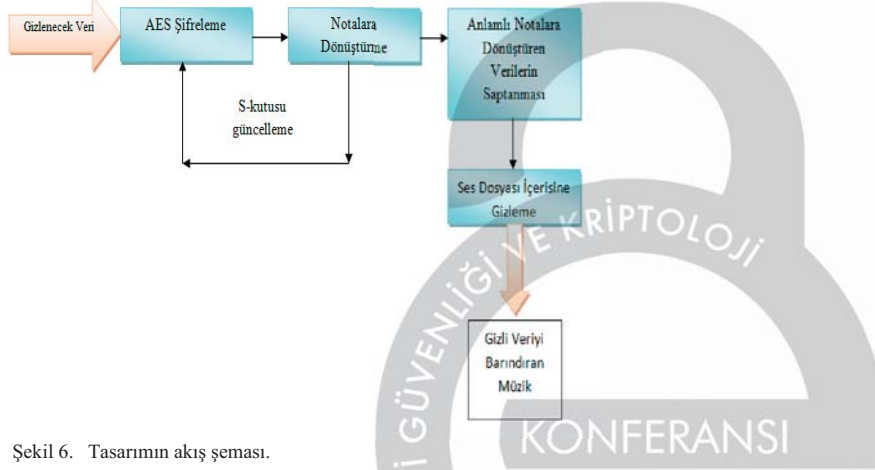
İçerisine farklı miktarlarda veri gizlenen üç taşıyıcı ses dosyası ile laboratuarda 12 kişi ile yapılan denemelerde; yalnızca 32 bit veri taşıyan dosya için ortalama fikir puanı (MOS) 5, taşıyabileceği veri miktarının %50'sini taşıyan dosya için MOS değeri 4.67, %100'ünü taşıyan dosya için MOS değeri ise 4.25 olarak ölçülmüştür. Yukarıdaki ölçümlerde kullanılan ses dosyası wav uzantılı olup, 60 saniyelik bir klasik müzik eseri içermektedir. Dinleyicilere önce veri taşımayan dosyalar dinletilerek 5 üzerinden puanlama yapmaları istenmiştir. Farklı tür müziklerle yapılan çalışmalarda daha farklı MOS değerleri elde edilmiştir. Örneğin *Rock* müzikte dinleyicilerin verdiği puanlar artarken *Klasik Türk Müziği*'nde ise dinleyiciler hissedilen gürültünün arttığına dair yorumlar yapmışlardır.

Ses dosyasına ne kadar az veri gizlenirse, taşıyıcı dosya o

kadar güvenli olacaktır [8].

Bu işlemler gerçekleşirken, anlamsız nota dizisi AES'nin S-kutusu'nu güncellemiştir. Bu, işlemlerin çözümünü biraz daha karmaşık hale getirmesine rağmen işlemlerin hepsinin tersinir olması, yöntemi bilen ve yeterli veriye sahip bir alıcının, gizli veriye ulaşabilmesini sağlamaktadır.

Son halde elde edilen şarkıdan gizlenen veriyi ayıklayabilmek için, öncelikle o şarkının gizli bir veri taşıdığının bilinmesi, daha sonra çok iyi bir dikte¹ kabiliyetine sahip olunması ve hangi aralıklarla veri gizlendiğini, hangi notaların ve o notaların hangi özelliklerinin temel alındığının bilinmesi gereklidir. Bunlara ek olarak notalarla hangi işlemin yapıldığının, AES'nin S-kutusunun nasıl güncellendiğinin bilinmesi ve anahtarlar bilinmediği için çok fazla zaman harcanması gerekmektedir. Bu tasarım tek başına AES kullanmanın veya tek başına veri içerisine veri gizlemenin bile yeterli görüldüğü durumlarda fazladan güvenlik sağlayacaktır.



Şekil 6. Tasarımın akış şeması.

Örneksel (analog) yollarla bu ses dosyasındaki müziğin aktarımı söz konusu olursa veri kaybı olması kaçınılmazdır. Bahsedilen yöntemin sonucunda elde edilen, içerisinde gizli veri bulunduran ses dosyası ancak sayısal yollarla taşındığında gizli verilerin tamamı korunacaktır.

Sürekli gelişen uydu teknolojisiyle bu tasarımı kullanmak mantıklı olacaktır. Örneğin askeri alanda gizli bir konum bilgisinin iletilmesi gerektiği düşünülürse, bu tasarım kullanılarak bir ses dosyası hazırlanabilir ve bu müzik uydudan yayın yapan bir televizyon kanalında örneğin bir reklamın arkasında çalabilir. Sayısal iletişimde veri bozulmayacağı için mesajı alacak olan kişi bu reklamın sesini yine sayısal ortamda kaydederek gerekli işlemleri yapıp gizli konum verisine ulaşabilir. Silahlı Kuvvetler bünyesinde yetişmiş ve çok iyi dikte¹ kabiliyetine sahip müzisyenler olduğu düşünülürse, taşıyıcı ses dosyasındaki müziğin notalarının başka bir yolla iletimine de gerek kalmayacaktır ve gizli verinin ayıklanması bir takım çalışması haline gelecektir.

Bu çalışmadaki tasarımın akış şeması Şekil 6'da sunulmuştur.

¹ Dikte, duyulan sesleri kağıda dökmektir. Örneğin çalınan bir şarkının notalarını yazabilmek o şarkıyı dikte etmektir.

KAYNAKLAR

- [1] D. Artz, "Digital Steganography", *IEEE Internet Computing*, vol. 5, is. 3, pp.75-80, 2001.
- [2] M. Pooyan, A. Delforouzi, "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform ", *Signal Processing and Information Technology, 2007 IEEE International Symposium*, pp. 600-603, 2007.
- [3] K. Gopalan "Audio Steganography Using Bit Modification", *Multimedia and Expo, 2003. ICME '03. Proceedings. 2003 International Conference*, vol.1, pp. 629-632, 2003.
- [4] Advanced Encryption Standard, Federal Information Processing Standards Publication 197, November, 2001.
- [5] D. Forte, "The future of the advanced encryption standard", *Network Security*, vol. 1999, is. 6, pp. 10-13, 1999.
- [6] S. M. Yoo, D. Kotturi, D. W. Pan, J. Blizzard, "An AES crypto chip using a high-speed parallel pipelined architecture", *Microprocessors and Microsystems*, vol. 29, is. 7, pp. 317-326, 2005.
- [7] N. Cangal, Armoni, Arkadaş Yayınları, Ankara, 1999.
- [8] R. J. Anderson, F. A. P. Petitcolas, "On the limits of steganography", *Selected Areas in Communication*, vol. 16, is. 4, pp. 474-481, 1998.

Bir Steganografi Sisteminin FPGA Üzerinde Gerçeklenmesi

Betül ELÇİ, Berna ÖRS, Volkan DALMIŞLI

Özet— Bu çalışmada, öncelikle steganografinin içeriği ve uygulama alanları incelenmiştir. İlk olarak bir kölenin saçının kazınarak, bilginin dövme şeklinde kölenin kafa derisine işlenmesi ve kölenin saçı yeteri kadar uzadığında bilginin tekrar elde edilmesi ile başlayan, veri gizleme bilimi olarak adlandırılan steganografi, günümüzde teknolojik gelişmelerle çok ileri boyutlara ulaşmıştır. Veriyi gizlerken ve veriyi tekrar elde ederken kullanılan yöntemler her geçen gün gelişme göstermektedir. Böylece verinin en güvenli şekilde iletimi sağlanmaya çalışılmaktadır.

Bu çalışmada incelenen üç steganografi yöntemi uygulanmıştır. Bu yöntemleri gerçeklerken VHDL donanım tanımlama dili kullanılmıştır. Steganografi sisteminin FPGA üzerinde tasarımı ve gerçekleştirilmesi sağlanmıştır. Gerçeklenen üç yöntemin sonuçları kıyaslanarak avantajları ve dezavantajları yorumlanmıştır.

Anahtar Kelimeler—Steganografi, FPGA, VHDL

I. GİRİŞ

Bu çalışmada, steganografi sisteminin FPGA üzerinde tasarımı ve gerçekleştirilmesi sağlanmıştır. Eski Yunancada gizlenmiş yazı anlamına gelen steganografi, bilginin görünürlüğünü gizleme bilimine verilen isimdir [1]. Günümüzde karşılaşılan en büyük yanlış anlama steganografinin şifreleme ile karıştırılmasıdır. Veriyi gizleme sanatı olarak bilinen bu bilimin şifrelemeye göre en büyük üstünlüğü bilgiyi gören bir kimsenin gördüğü şeyin içinde önemli bir bilgi olduğunu fark edemiyor olmasıdır, böylece içinde bir bilgi aramaz oysa bir şifreli mesaj, çözmesi zor olsa bile, gizemi dolayısıyla ilgi çeker. Çünkü bir bilginin gizlendiği bellidir [3]. Günümüzde steganografi bilimi sayesinde ses, video, resim dosyalarına, disketlere ve haberleşme kanallarına istenilen veri gizlenebilmektedir [1].

Çalışmada steganografinin resim alanındaki uygulamaları donanımsal olarak gerçekleştirilmiştir.

Steganografide resmin içine veri gizlerken en çok kullanılan yöntem resmi oluşturan piksellerin en anlamsız bitlerinin kullanıldığı uygulamalardır. Bunun nedeni en düşük anlamlı bitte yapılan değişiklikler insan gözünün fark edememesidir. Yani en anlamsız bitlere saklanan veriyi içeren resimle, esas resim yan yana konulduğunda gözle görülür hiçbir fark yoktur.

B. Elçi İstanbul Teknik Üniversitesi öğrencisidir.

B. Örs İstanbul Teknik Üniversitesi, Elektrik-Elektronik Fakültesi, Elektronik ve Haberleşme Mühendisliği Bölümü, 34469 Maslak, İstanbul'da Yardımcı Doçent Dr. olarak görev yapmaktadır. Tel: 0212 285 36 03, Fax: 0212 285 35 65, url: www2.itu.edu.tr/~orssi.

V. Dalmışlı İstanbul Teknik Üniversitesi öğrencisidir.

Bu durumdan yola çıkılarak steganografide resmin içine veri gizlenirken çeşitli yöntemler geliştirilmiştir [1].

Bu çalışmada bu yöntemlerden üç tanesi kullanılmıştır. Bunlardan birincisinde bir resmi oluşturan tüm piksellerin son bitleri değiştirilmiş ve bu değişimin bir fark yaratmadığı anlaşılmış, ikincisinde ilk pikselden başlanarak veri gizlenmiş daha sonra da aynı şekilde çözümlenmesi yapılmıştır. Son yöntemde ise verinin hangi piksellere gizleneceğini belirten bir steganografik anahtar kullanılarak veri gizlenmiş ve tekrar elde edilmiştir.

II. STEGANOĞRAFI

Steganografi veriyi gizlemenin ve zararsız taşıyıcılarla veriyi taşınan sanatıdır [1]. Kelime anlamı olarak kökleri ve γραφειν'e ait olmakta ve Yunan alfabesinden gelmekte olup kaplanmış yazı anlamına gelmektedir. Yunanca steganos sözcüğü gizli, saklı ve grafi sözcüğü çizim ya da yazım demektir. Bu sanat var olan veriyi gizlemede birçok gizli haberleşme tekniği kullanılmaktadır. Steganografi eski bir el sanatı olmasına rağmen günümüzde bilgisayar teknolojisiyle yeni bir içerik kazanmıştır. Bilgisayar tabanlı steganografi teknikleriyle veriyi yeni gizleme teknikleri geliştirilmiştir.

Bilgiler metin formunda, sayısal 1 ve 0 olarak ya da başka çeşitlerde iletme geçerken verinin kime ait olduğunu belirten bir çeşit parmak izi bırakırlar. Steganografi bir çeşit kriptografi yöntemi gibi düşünülebilir. Her ikisi de haberleşme sırasında kaydedilmiş veriye bilgi ekleyerek çalışırlar. Kriptografi teknikleri bilgiyi belirli algoritmalarla dayanarak şifreleyip güvenli bir örtü yaratmayı amaçlar. Steganografi ise kriptografiden farklı olarak veriyi örtük olarak gizlemeyi sağlar. kriptografide şifreli metin olarak adlandırdığımız örtülü yapı dikkat çekebilirken steganografide kendini gizlediğinden dikkat çekmemeyi sağlar. Bu da verinin güvenli bir şekilde taşınması açısından önemli ve yararlı bir durum oluşturmaktadır [7].

III. STEGANOĞRAFI UYGULAMASI

Günümüzde resim alanında yapılan steganografi uygulamalarında çeşitli algoritmalar ve yöntemler kullanılmaktadır. Bunlardan en yaygın olanı resmi oluşturan piksellerin en düşük anlamlı bitinde yapılan değişiklikleri kapsar. Bu çalışmam kapsamında bu yöntemlerden üç tanesi yer almaktadır.

A. Uygulamada Kullanılan Yöntemler

Çalışmada resmi oluşturulan piksellerin son bitinde yapılan değişikliklerle üç yöntem gerçekleştirilmiştir. Gerçeklenme aşamasından sonra elde edilen resimlerle esas resimlerle kıyaslandığında gerçekten gözle görülür bir fark olmadığı ortaya çıkmıştır. Çalışma esnasında en yüksek verim alınabilmesi için resimler için kayıpsız bir sıkıştırma algoritması olan bitmap formatı seçilmiştir.

1) En Düşük Anlamli Bitlerin Tümüünün Değiştirilmesi

Yöntemi

Bu yöntemle steganografinin kapsamında anlatılanları gerçekleyerek gerçekten kullanılan ve değişen resimler arasında fark olmadığını görülmesi sağlanmıştır. Öncelikle resimler piksellerden oluştuğu ve matris halinde bu pikseller dizildiği için bir metin dosyasına aktarım işlemi yapılması gerekiyordu. Bunun için wnbrowse editörü ile Şekil 1'deki resmin hex formatında görülmesi sağlanmıştır.



Şekil 1 F15 Uçak Resmi [4]

Oluşan 205×138'lik resim içinde sadece hex formatında pikseller içeren bir yapı oluşmuştur. Şekil 2'de bu matrisin sadece ilk 10 x 10'luk kısmı alınmıştır.

Burada 8 bitlik yapılardan yani baytlardan oluşmuş bir matris görülmektedir. Bu matriste her satır ve sütun 10 bayttan oluşmaktadır.

8 bitlik bu yapıya resimde piksel adı verilmektedir. Resmin boyutu değiştiğinde matris boyutu da dolayısıyla resmi oluşturan piksel sayısı da değişmektedir [2].

42	4D	76	30	05	00	00	00	00	00
00	00	9A	01	00	00	14	01	00	00
00	00	00	00	00	00	C4	0E	00	00
00	00	00	00	00	00	C0	86	48	C4
86	49	C1	84	46	C2	85	49	C1	85
47	C1	86	4B	C1	84	46	C4	84	46
C1	86	46	C3	86	45	C0	86	48	C2
89	44	C4	87	43	C3	86	45	C3	85
49	C4	87	45	C2	88	47	C5	8A	49
C2	86	4A	C4	84	46	C2	87	47	C0
82	45	BF	81	46	BD	85	47	C2	87

Şekil 2 Orijinal resmin ilk 10×10'luk kısmının heksadesimal formatında Görünümü

Steganografideki en yaygın yöntem olan en düşük anlamli bitin değiştirilerek uygulanmasını burada matriste gerçekleştirilmesi sağlanmıştır. Yöntemde belirtilen yapıya göre bir resmi oluşturan piksellerin her birinin son bitlerini değiştirilirse yani 0 ise 1, 1 ise 0 yapılırsa yeni oluşan resimle

eskisi kıyaslanırsa arada gözle görülür bir farkın olmayacağıdır [7].

Şekil 2'deki kaynak resmin ilk 10×10'luk kısmının piksellerine bakacak olursak her pikselin son biti 1 ise 0, 0 ise 1 yapılarak yöntem gerçekleştirilmiştir. Bunun için her hex yapısı ikilik düzende düşünülmüştür. Bu işlemin resimdeki her piksele uygulanması sağlanmıştır ve Şekil 3'deki matris elde edilmiştir.

43	4C	77	31	04	01	01	01	01	01
01	01	9B	00	01	01	15	00	01	01
01	01	01	01	01	01	C5	0F	01	01
01	01	01	01	01	01	C1	87	49	C5
87	48	C0	85	47	C3	84	48	C0	84
46	C0	87	4A	C0	85	47	C5	85	47
C0	87	47	C2	87	44	C1	87	49	C3
88	45	C5	86	42	C2	87	44	C2	84
48	C5	86	44	C3	89	46	C4	8B	48
C3	87	4B	C5	85	47	C3	86	46	C1
83	44	BE	80	47	BC	84	46	C3	86

Şekil 3 Son Bitleri Değiştirilmiş Resmin İlk 10×10'luk Kısmının Görünümü

Sadece son bit değiştirilmesi için kombinezonasal bir devre tasarımı yapılmıştır. Bundan sonra gereken işlem 205×138 formatındaki piksellerden resim elde etmektir. Ancak bu şekilde bitleri değiştirilmeden önceki resimle farkının olup olmadığını karşılaştırabilmektedir [2].

Bu aşamada tasarlanan devrenin benzetimi devreye Şekil 1'deki resmin piksel değerleri giriş olarak verilerek yapılmıştır. Sonuçta tüm piksellerin son bitleri değiştirilmiş haliyle elde edilen resim Şekil 4'deki gibidir.



Şekil 4 F15 Uçak Resmi

Bu iki resimde burada da görüldüğü gibi gözle görülür hiçbir fark yoktur.

2) Bir Veriyi En Düşük Anlamli Bitlere Gömme ve Elde Etme Yöntemi

Bir resmi oluşturan tüm piksellerin son bitlerinin değişimi resimde fark edilir bir ayrım yaratmadığından ilerleyen steganografik çalışmalarda bu en düşük anlamli bitlerle veri gömmeye başlanmıştır. Bu konuda çeşitli algoritmalar geliştirilmiştir [3]. Bu çalışmada resmin içine veri gizlenmiş ve daha sonra bu resim iletilmiştir. Resmi alan kullanıcı resmin içine gömüldüğü gibi veriyi çıkartmış ve böylece haberleşme sağlanmıştır. Bu yöntemde veriyi gömme işlemi Algoritma 1'de gösterildiği gibidir.

Bu yöntemde önceki yöntem gibi resmin wnbrowse editörü gibi bir araç ile hex formatında gösterimi sağlanır ve bir metin

dosyasına kaydedilir. Elde edilen bu esas resim *cover* olarak ifade edilir. Esas resmin baytlar c_i olarak ifade edilmektedir. Steganografik tanım olarak steganografik anahtar ifadesi s_i olarak belirtilmiştir. Resmin içine gömülme istenen verinin bitlerini ifade etmek için m_i kullanılmıştır. Bu algoritmaya göre veri gizlenirken resmi oluşturan ilk baytın son bitinde değişiklik yapılarak veri gömülmeye başlanır. Yani veriyi gömme işlemi ilk baytın en düşük anlamlı bitinden başlanarak sırayla hangi baytın en düşük anlamlı bitine kadar gidiyorsa yapılır. Bu çalışmada, veri gizlenirken alfabedeki harflerin ikilik düzende karşılıkları şeklinde bir dönüşüm kullanılması gerekmektedir. Bunu sağlamak için ascii karakter kodlamasından yararlanılmıştır [2]. Karşı taraf veriyi elde ettiğinde ikilik düzenin karşılığını alfabede bulunan 29 harfin karşılığı olarak elde etmesi içinse Matlab programında yazılan kod parçası kullanılmıştır. Örnek bir uygulama olarak olarak *itu* sözcüğünü gizlemeye çalıştığımızda ilk olarak yapılan işlem *itu* kelimesinin ascii karakter kodlamasında karşılığını bulmak olacaktır.

Algoritma 1

Giriş: $c = (c_1 c_2 \dots c_n)_8$, $m = (m_1 m_2 \dots m_l)_2$

Çıkış: $s = (s_1 s_2 \dots s_n)_8$

for $i = 1, \dots, l$

$s_i \leftarrow c_i$

$s_{i8} \leftarrow m_i$

for $i = l + 1, \dots, n$

$s_i \leftarrow c_i$

itu kelimesinin ascii karakter kodlamasındaki karşılığı bulunur. Buna göre $i = 69$, $t = 74$, $u = 75$ şeklinde belirlenir. Burada 69, 74 ve 75 şeklinde gördüğümüz sayılar hex formatında yapılarıdır. Veriyi resmin son bitlerine gizlemek için ikilik düzendeki ifadesine ihtiyacımız var. Bu nedenle *itu* sözcüğünün ikilik düzendeki karşılıkları $i = 0110\ 1001$, $t = 0111\ 0100$, $u = 0111\ 0101$ şeklinde belirlenir. Bundan sonraki işlemi bu bitleri verinin gizleneceği resme ilk baytın son bitlerinden başlayarak sırayla gömmektir. Alfabede bulunan üç harfi gizlemek için her bir harfin 8 bitlik karşılığı olduğundan 24 bite ihtiyaç vardır. Bu da resmimizin ilk baytından başlanarak sırayla 24 baytın son bitlerine veriyi gizlemek anlamına gelmektedir. F15 uçak resminin ilk 10×10 'luk kısmındaki ilk bayt, 42 idi. Yani 0100 0010 şeklinde ikilik düzende ifadesi vardır. Gizlemek istediğimiz "*itu*" sözcüğünün ise ilk karakteri $i = 0110\ 1001$ şeklinde ifade edilmişti. Demek ki ilk baytın son bitine yani 42 in son bitine i karakterinin ilk biti gömülmelidir. $42 = 0100\ 0010$ olduğundan son bit 0'dır. $i = 0110\ 1001$ olduğundan ilk bit 0'dır. Demek ki kaynak resmin ilk baytında bir değişiklik olmayacaktır. Yine 0 olarak kalacaktır. Bu şekilde bu durum sırayla devam edecektir. Daha sonraki aşama i karakterinin ikinci biti olan 1'i ana resmin ikinci baytının son bitine gömmek olacaktır. Gömmek istenilen 24 bit resmin ilk baytından başlanarak 24 baytın en düşük anlamlı bitlerine yerleştirilecektir.

Burada algoritmada da belirtildiği gibi resmin bitlerini kontrol eden bir yapı yoktur. Yani i karakterinin ilk biti 0, aynı zamanda resmin ilk baytının da son biti 0 diyen bir kontrol mekanizmasına gerek yoktur. Saklamak istediğimiz bilgi ne ise onu oluşturan bitleri teker teker piksellerin son bitlerine yazdırmak yeterlidir [2].

Veriyi gömme işlemi bittikten sonra tekrar Matlab programı kullanarak bu matrisi bitmap formatında resme dönüştürürüz. Yeni oluşan resimle eskisi kıyaslandığında gözle görülür bir fark olmamaktadır.

Bu içinde veri gömülü resim iletilmek istenen kişiye iletildiğinde o kişinin bu bilgiye ulaşması için tekrar o bilgiyi elde etmesi gerekir. Bunun için kullanılan algoritma aşağıdaki gibidir.

Algoritma 2

Giriş: $s = (s_1 s_2 \dots s_n)_8$

Çıkış: $m = (m_1 m_2 \dots m_l)_2$

for $i = 1, \dots, l$

$m_i \leftarrow s_{i8}$

İçine veri gizlenmiş olan resim iletilmek istenen kişinin eline geçtiğinde veriyi gönderenden gerekli bilgileri önceden aldığından, veriye ulaşmak için Algoritma 2'nin kullanılması yeterlidir. Bu gerekli bilgi verinin alfabetik olarak ya da bit sayısı olarak uzunluğunu içermektedir.

Veri uzunluğunu bilen kullanıcı, verinin içerdiği bit sayısı kadar matrisi oluşturan baytlardan baştan başlayarak alır. Aldığı bu baytların son bitlerini bir metin dosyasına çıkartır ve ascii karakter kodlamasına göre her baytın karşılığını alfabedeki harfler olarak elde etmelidir [2]. Bunun için de Matlab programında her harfin ascii karakter kodlamasını içeren bir kod parçası kullanarak bunun elde edilmesi sağlanır.

Günümüzde steganografinin çok fazla gelişme imkânı bulmasıyla buna karşı geliştirilen atak türlerinde de gelişme olmuştur. Bu nedenle böyle bir veri örneğin internet ortamında dolaşırken çok da fazla güvenli olmaz. Çünkü resmin içinde veri var mı diye bakan analiz yapmak isteyen kişi ilk baytın son bitlerinden başlayarak bir çözümleme yapmaya çalışabilir. Bu da verinin güvenliğini önemli ölçüde tehdit eden bir yapı oluşturur. Bu nedenle steganografinin resim alanındaki birçok çalışmada bu yöntem kullanılsa da saldırı ve analiz tekniklerinin de geliştirilmesiyle veriyi gömme - çıkarma alanında yeni algoritmalar geliştirilmiştir [2,3].



Şekil 5 Veri gömülmeden önce



Şekil 6 Veri gömüldükten sonra

Görüldüğü gibi *itu* sözcüğü gömülmeden önce Şekil 6'daki resimle, gömüldükten sonraki halini yani Şekil 7'deki resmi yan yana koyduğumuzda gözle görülemeyecek kadar değişim olduğundan fark edilememektedir.

3) Rastgele Aralık Yöntemi

Bir önceki yöntemin zayıf yanı iletilmek istenilen verinin başkaları tarafından ele geçirilme durumunun olmasıydı. Bu ihtimali azaltmak için geliştirilen algoritmalarından birisi "Rastgele Aralık Yöntemi" dir. Bu yöntemin bir önceki yöntemden farkı gizlenecek verinin bitlerinin ilk bayttan başlanarak sırayla en düşük anlamlı bitlere yüklenmeyecek olmasındandır. Rastgele Aralık Yöntemi'nde hangi piksellere verinin gizleyeceği belirli denklemlere bağlıdır [2]. Bu yöntemde kullanılan algoritma aşağıdaki gibidir.

Algoritma 3

Giriş: $c = (c_1 c_2 \dots c_n)_8$, $m = (m_1 m_2 \dots m_l)_2$

Çıkış: $s = (s_1 s_2 \dots s_n)_8$

for $i = 1, \dots, n$

$s_i \leftarrow c_i$

Rastgele $1 \leq k_i \leq n$ olmak üzere l adet k değeri belirlenir.

$j_1 = k_1$

for $i = 1, \dots, l$

$j_i = j_{i-1} + k_i \mod n$

for $i = j_1, \dots, j_l$

$s_{i_8} \leftarrow m_i$

Bu yöntemin en önemli özelliği veri gizlenirken bir steganografik anahtarın kullanılmasıdır. Steganografik anahtar verinin rastgele olarak hangi piksellerin en düşük anlamlı bitlerine gizleneceğini belirtir. Burada önemli olan hem veriyi gönderen hem veriyi alan kişi için steganografik anahtardır. İki taraf da aynı steganografik anahtar olmadan veri iletimini sağlayamazlar [2].

Çalışma sırasında steganografik anahtar belirleme de çeşitli yöntemler araştırılmıştır. Bu yöntem dahilinde Matlab programı ile rastgele sayılar üretilmiştir. Bu sayıların steganografik anahtar olmasına karar verilmiştir. Matlab programı kullanılarak bu anahtarı üretilme sebebi bunun

gerçekten diğer algoritmalarından daha hızlı ve kolay bir yol olmasıdır.

Rastgele aralık yöntemine dayalı olarak steganografik anahtarın uzunluğu gizlenmek istenen verinin uzunluğu ile aynı olmalıdır. Bu yöntemde veriyi gömme işlemine bir önceki yöntemdeki gibi başlanır [2].

Burada gizlenmek istenen verinin bitleri yine resmin piksellerinin en son bitlerine gömülecektir. Yalnız bu yöntemde ilk bayttan başlanarak sırayla gömme işlemi yapmak yerine hangi baytlara verinin gizleneceğini gösteren bir steganografik anahtarın kullanıldığı denklem yer almaktadır [2]. Burada saklamak istediğimiz bilgi toplam 24 bitten oluşmaktadır. Bu da oluşturmamız gereken anahtarın 24 bit uzunluğunda olması gerektiğini belirtir. Bu steganografik anahtar belirlendikten sonra yöntemde dayalı olarak veriyi resmin hangi baytlarına saklanıldığını belirtildiği denklem 4 kullanılır.

$$j_1 = k_1 \quad (4)$$

$$j_i = j_{i-1} + k_i \mod n$$

Bu denklemde j_i rastgele belirlenmiş steganografik anahtarı buna bağlı olarak 4 denklemini kullanarak resmin hangi baytlarına verinin gizleneceğini belirten bir indistir [2].

Örneğin Matlab programını kullanarak *itu* sözcüğün *i* harfini gizlemek için 8 tane rastgele sayı yani 4 denklemindeki k değerlerini belirlensin. Bu sayılar 1, 3, 12, 56, 9, 10, 18, 22 şeklinde belirlendi. Buradan anlaşıldığı gibi k değerleri sırasıyla rastgele belirlenen 8 değerden oluşmaktadır. Belirlenen bu k değerlerinden yararlanarak verinin gizleneceği j değerleri 4 denkleminde göre belirlenir.

$$k_1=1 \rightarrow j_1=1$$

$$k_2=3 \rightarrow j_2=j_1 + k_2=4$$

$$k_3=12 \rightarrow j_3=j_2 + k_3=16$$

$$k_4=56 \rightarrow j_4=j_3 + k_4=72$$

$$k_5=9 \rightarrow j_5=j_4 + k_5=81$$

$$k_6=10 \rightarrow j_6=j_5 + k_6=91$$

$$k_7=18 \rightarrow j_7=j_6 + k_7=109$$

$$k_8=22 \rightarrow j_8=j_7 + k_8=131$$

Belirlenen k dolayısıyla j değerleri resmin bayt numaralarını göstermiş oldu. Buradan çıkarılması gereken sonuç *i* harfini gizleme işleminin, resmin 1, 4, 16, 72, 81, 91, 109 ve 131 numaralı baytlarında gerçekleşmesi gerektiğidir. Numarası belirtilmiş baytların en düşük anlamlı bitlerine sırasıyla 0110 1001 bitleri gömülür. Aynı işlemler diğer karakterler için de steganografik anahtar ve verilen denklem yardımıyla hangi baytlara gömme işleminin yapılacağı belirlenerek uygulanır. Gömme işlemi rastgele aralık yöntemine göre gerçekleştirilmiştir. İçine veri gömülen resim iletilmek istenen yere ulaştığında bu veriyi tekrar elde etmek için de bu yöntem dahilinde bir algoritma vardır.

Burada unutulmamalıdır ki hem veriyi gönderen hem veriyi alan kişilerde aynı steganografik anahtar bulunmaktadır [2].

Steganografik anahtarın her iki tarafta da olduğu kabul edilen bu yöntem gereği veriyi resimden çıkartma algoritması aşağıdaki gibidir.

Algoritma 4

Giriş: $s = (s_1 s_2 \dots s_n)_8$, $k_1, k_2, \dots, k_l$

Çıkış: $m = (m_1 m_2 \dots m_l)_2$

$j_1 = k_1$

for $i = 1, \dots, l$

$j_i = j_{i-1} + k_i \bmod n$

for $i = j_1, \dots, j_l$

$m_i \leftarrow s_{i8}$

Algoritma 4’de ifade edildiği gibi gömülmüş veriyi tekrar elde ederken öncelikle hangi baytlara verinin gizlenmiş olduğunun bulunması gerekir. Bu nedenle elinde steganografik anahtar değerleri olan kişi denklem 4 gereği j_i değerlerini yani hangi baytlara veri gizlendiğini belirler.



Şekil 7 Veri gizlenmeden önce



Şekil 8 Veri gizlendikten sonra

Daha sonra belirlenen baytların en düşük anlamlı bitleri yan yana getirilerek gizlenmiş olan veri elde edilmiş olur [2]. Burada yapılması gereken son işlem elde ettiğimiz veriyi alfabe düzenine geçirmektir. Bunun için de bir önceki yöntem de olduğu gibi Matlab programı yardımıyla gerekli dönüşüm yapılır ve alfabetik karşılıklar elde edilir. Şekil 7 ve Şekil 8’de görüldüğü gibi algoritma gerçekleştirildikten sonra resmin içine veri gömüldüğünde gözle görülür bir fark olmamıştır.

IV. SONUÇ

İlk yöntem gerçekleştirildiğinde resmi oluşturan baytların en düşük anlamlı biti değiştirildiğinde ve yeni yapı tekrar resim

haline getirildiğinde resimde gözle görülür bir fark olmadığı görülmüştür. Resmi oluşturan piksellerin en anlamsız bitine bir veri gömülüp tekrar elde etme işlemi yapıldı. Yani bir yerden bir yere verinin resim aracılığıyla güvenli bir şekilde taşınabileceği ve verinin tekrar gömüldüğü gibi çıkarılabileceği gösterildi ve FPGA üzerinde gerçekleştirildi.

Yapılan araştırmalar sonucunda steganografi teknikleri ve bu alanda kullanılan algoritmalar geliştikçe stegoanaliz tekniklerinin de zamanla geliştiği görülmüştür. Bu nedenle bu algoritmanın aslında zayıf bir yanın olduğu belirtilmelidir. Bu zayıf yan veri gömülme işlemi sırasında ilk baytın en düşük anlamlı bitinden başlanarak sırayla verinin gömülme işleminin uygulanmasındandır. Bu nedenle steganografi alanında kullanılan başka yöntemler de araştırılmış ve gerçekleştirilebilir. Rastgele aralık yöntemi seçilmiştir. Bu yöntemde veri gizlenirken güvenliği sağlamak adına steganografik bir anahtar kullanılır. Kullanılan bu anahtar sayesinde algoritmaya bağlı olarak verinin hangi baytların en anlamsız bitine gizleneceği belirlenir. Bu sayede elinde steganografik anahtar olmayan birinin veriyi ele geçirmesi çok güçtür.

Yukarıda anlatılan her üç steganografi yöntemi VHDL tanımlama dili kullanılarak tasarlandı ve FPGA üzerinde gerçekleştirildi. Benzetimleri yapılarak sonuçların beklendiği gibi olduğu görüldü.

V. KAYNAKLAR

- [1] Johnson, N. F., Duric Z. ve Jajodia S., 2001. Information Hiding : Steganography and Watermarking - Attacks and Countermeasures, Boston.
- [2] Katzenbeisser, S. ve Petitcolas, Fabien A. P., 2000. Information Hiding Techniques for Steganography and Digital Watermarking, London.
- [3] Marvel, L. M., *Information Hiding: Steganography and Watermarking*, 2005, Optical and Digital Techniques for Information Security
- [4] Petitcolas, Fabien A. P., 2008. The Image Downgrading Problem, http://petitcolas.net/fabien/steganography/image_downgrading/index.html.

Doğruluk Oranı İyileştirilmiş $(2, n)$ Olasılıklı Görsel Sır Paylaşma Şeması

Vasif V. NABİYEY, Mustafa ULUTAŞ, Güzin ULUTAŞ

Özet— Görsel Sır Paylaşma (GSP), gizli bir görüntünün görüntü benzeri paylara kodlanmasıdır. GSP yöntemlerinde, gizli görüntüdeki bir pikselin paylarda m pikselle kodlanıyor olması *büyüme oranı* problemini beraberinde getirmiştir. Bu problemin giderilmesi için, m değerini 1 olarak belirleyen ve Olasılıklı Görsel Sır Paylaşma (OGSP) olarak adlandırılan yeni bir yöntem önerilmiştir. Geleneksel GSP ve OGSP yöntemlerinde gizli görüntünün ortaya çıkarılması için insan görme sistemi yeterli olmaktadır. 2007 yılında Wang, insan görme sistemini kullanmayan ve yalnızca mantıksal işlemlere dayanan yeni bir $(2, n)$ OGSP yöntemi önermiştir. Yöntem siyah pikselleri 1, beyaz pikselleri ise $\frac{1}{2}$ olasılıkla doğru olarak koruyabilmektedir. Bu yayında, Wang'ın yönteminde kullanılan rasgele B matrislerinin içeriklerinin belirlenmesinde kullanılacak olan yeni bir yöntem önerilmiştir. Bu sayede yapılandırılan resimdeki beyaz piksellerin doğruluk oranı yükselmiştir. Test sonuçlarında, yapılandırılan görüntünün sahip olabileceği maksimum PSNR değeri, Wang'ın önerdiği yöntemle elde edilen değerden daha yüksek çıkmıştır. Böylelikle Wang'ın yönteminin, GSP şemalarının değerlendirilmesinde önemli bir parametre olan, doğruluk oranı iyileştirilmiştir.

Anahtar Kelimeler —GSP, OGSP, PSNR.

I. GİRİŞ

Sır Paylaşma (SP) şeması olarak adlandırılan yöntem ilk olarak Blakley ve Shamir tarafından 1979 yılında önerilmiştir [1, 2]. (k, n) eşik şeması olarak da adlandırılan bu yöntem, verinin güvenliğini n tane parçaya bölerek sağlar. Her bir parça “pay” olarak adlandırılır. Oluşturulan n tane pay n tane kişiye dağıtılır. Sırı paylaşan her bir kişinin elinde yalnız bir pay vardır. Gizli veri, ancak bu paylardan en az k tanesi bir araya getirildiğinde ortaya çıkacaktır. k adetten az payın bir araya getirilmesi, gizli veri hakkında hiçbir bilgi açığa çıkarmaz.

SP yöntemini temel alan ve daha yeni bir yöntem olan “Görsel Sır Paylaşımı” (GSP) Naor ve Shamir tarafından 1994 yılında önerilmiştir [3]. Bu şema için paylaşılan sır gizli bir görüntüdür (el yazısı notları, yazıcı çıktıları, resimler gibi). Bu yeni sır paylaşım tekniğinin en önemli özelliği, başka bir hesaplama ihtiyacı duymaksızın insan görme sistemini, gizli veriyi ortaya çıkarmada kullanmasıdır. Geleneksel şifreleme tekniklerinin, şifre çözme için gerektirdiği kompleks hesaplamalar bu yeni alanda yer almamaktadır. (k, n) GSP şeması için,

sır sahibi olan kişi, gizli görüntüden görsel şifreleme tekniklerini kullanarak n tane anlamsız pay oluşturur ve sıırı paylaşacağı guruptaki alıcıların her birine bir adet pay gönderir. Paylar; aslında anlam ifade etmeyen görüntü benzeri görüntülerdir. Gizli görüntünün ortaya çıkarılabilmesi için en az k adet kişinin kendi paylarını slayt üzerine basmaları ve bu slaytları tam olarak üst üste getirmeleri gerekmektedir. Gizli veri, görsel şifreleme teknikleri kullanılarak paylara dağıtıldığı için, kötü amaçlı kişiler herhangi tek bir paydan gizli görüntüyü elde edemeyecektir.

Naor ve Shamir tarafından önerilen bu şemayı geliştirmek amacı ile çeşitli yaklaşımlar önerilmiştir. Bazı çalışmalar, paylaşılacak olan görüntünün yalnızca siyah beyaz resim olmak yerine, gri seviye veya renkli resim olabileceğini göstermiştir [4-6]. Paylaşılacak olan sır sayısının artırılması ise ilgi çeken diğer bir konudur [7-9]. Görsel şifrelemenin doğası gereği oluşan kontrast problemlerinin giderilmesi ise çözülmeye çalışılan problemlerden biridir [10]. Tanımı gereği görsel şifrelemede, sır olarak paylaşılacak olan görüntüdeki bir piksel, paylarda birden çok alt piksel ile temsil edilmektedir. Böyle bir kodlama tekniği ise görüntü boyutlarının belirli bir oranda genişlemesine neden olmaktadır. Genişleme faktörü olarak adlandırılan bu büyüme oranı, bellekte saklama açısından ihtiyaç duyulan kapasitenin artması ile sonuçlanmaktadır. Yapılan birçok çalışma ile bu oranın küçültülmesi amaçlanmıştır.

(k, n) GSP şemalarının başarımını test etmekte kullanılan dört parametre mevcuttur. Bu parametrelerden ilki *güvenliktir*. k adetten az payın bir araya getirilmesi sır hakkında hiçbir bilgi ortaya çıkarmamalıdır. İkinci parametre *doğruluştur*. En az k adet payın bir araya gelmesi ile ortaya çıkarılan sıırın, orijinaline olan benzerliğidir. Diğer bir kriter ise *hesaplama karmaşıklığıdır*: payları üretmede gereken işlem sayısı ile ölçülür. Son kriter ise gizli görüntüdeki bir pikselin paylarda kaç piksel ile kodlandığına bağlı olarak değişen *büyüme oranıdır*.

Büyüme oranı kriterini iyileştirmeye çalışan bazı çalışmalar “olasılıklı görsel sır paylaşma” (OGSP) şemalarını önermişlerdir [11-14]. Bu çalışmalarda, sır olarak paylaşılacak olan görüntüdeki her bir piksel paylarda tek piksel kullanılarak kodlanır. Böylelikle payların boyutu orijinal görüntünün boyutu ile aynı kalır. Orijinal görüntüdeki piksellerin, yeniden yapılandırılan görüntüde aynı olarak elde edilebilmesi belirli bir olasılık

dahilindedir. Gizli görüntüdeki pikseller, yeniden yapılandırılma işleminden sonra bire bir aynı kalmaz. Fakat bölgesel olarak bakıldığında resmin, orijinal görüntüsünü koruduğu gözlemlenebilir. Her ne kadar OGSP teknikleri, hesaplama karmaşıklığını ve büyüme oranını azaltsa da, doğrulukta kayıplara sebep olmaktadır.

2007 yılında Wang, mantıksal işlemlere dayalı yeni bir $(2, n)$ OGSP şeması ileri sürmüştür [14]. Bu şema XOR ve AND işlemlerini kullanarak siyah beyaz resimleri rastlantısal bir teknikle kodlar. Geleneksel OGSP' den farklı olarak, yeniden yapılandırma işlemi için insanın görme sistemi yeterli değildir. Elde etmiş olduğu sonuçların karşıtlık açısından geleneksel tekniklerden daha iyi olduğunu deneysel sonuçlarla göstermiştir.

Bu makalede, Wang tarafından önerilen tekniğin kontrast değerini iyileştirerek, yeniden yapılandırılan resimlerin doğruluk değerinin yükseltilmesi sağlanmıştır. Önerilen tekniğin Wang'ın çalışmasından üstün olduğu, yeniden yapılandırılan resimlerin PSNR değerlerinin test edilmesi ile gösterilmiştir.

Yayının geri kalanı şu şekilde düzenlenmiştir. İkinci kısımda GSP ve OGSP şemalarının ayrıntılarından bahsedilmiştir. Üçüncü kısımda ise Wang'ın önermiş olduğu $(2, n)$ şeması açıklanarak önermiş olduğumuz yöntem, ayrıntıları ile verilmiştir. Son olarak önerilen teknik ile elde edilen test görüntüleri verilmiş ve sonuçlar yorumlanmıştır.

II. GSP VE OGSP YÖNTEMLERİ

A. Görsel Sır Paylaşma (GSP)

(k, n) GSP şemasında orijinal görüntünün siyah ve beyaz piksellerden oluştuğu varsayılmıştır. Orijinal görüntüdeki her bir piksel, paylarda m adet alt piksel olarak kodlanır. GSP şeması $n \times m$ büyüklüğündeki mantıksal S matrisi ($S = [s_{ij}]$) tarafından tanımlanır. Sütun sayısını gösteren m değeri, gizli görüntüdeki tek bir pikselin paylarda kaç pikselle temsil edeceğini gösterir. Eğer i . paydaki j . alt piksel siyah ise $s_{ij} = 1$, aksi takdirde $s_{ij} = 0$ 'dır. $i_1, i_2, \dots, i_k$ ile gösterilen paylar, alt pikselleri uygun bir şekilde örtüşecek şekilde üst üste getirildiklerinde sır ortaya çıkacaktır. S matrisindeki satırlara OR mantıksal işleminin uygulanması sonucu oluşan vektörün Hamming ağırlığı, ilgili pikselin insan görme sistemi tarafından nasıl algılanacağını göstermektedir. Siyah ve beyazı ayırt etmek için sabit bir eşik değeri olsun ve d ($1 \leq d \leq m$) ile gösterilsin. Resmin görünebilirliği açısından, α ile gösterilen kontrastın sıfırdan büyük olması gerekir. İlgili piksel için belirlenen S matrisinin satırlarının OR'lanması sonucu oluşan $1 \times m$ lik vektör V ile gösterilsin. Bu durumda eğer $H(V) \geq d$ ise, yeniden yapılandırılan piksel insan görme sistemi tarafından siyah, eğer $H(V) \leq d - \alpha m$ ise beyaz olarak algılanacaktır.

Tanım 1. (k, n) GSP şeması, B_0 ve B_1 ile gösterilen $n \times m$ büyüklüğündeki mantıksal matrislerden oluşan iki küme ile temsil edilebilir. Beyaz bir piksel paylaşılacağı zaman kişi

B_0 mantıksal matrisinin satırlarından birini rastgele olarak seçer ve ilgili paya yerleştirir. Siyah bir piksel paylaşılacağına ise B_1 matrisinden seçilen rastgele bir satır ilgili payı kodlama da kullanılacaktır. B_0 veya B_1 matris kümelerinden rasgele seçilen bir matris, n tane paydaki m adet alt pikselin gri seviyesini belirlemeye yardımcı olacaktır. Naor ve Shamir'in tanımı gereği, bir GSP şeması ancak aşağıdaki koşulları sağladığı takdirde geçerli olacaktır.

1. B_0 veya B_1 kümelerinden seçilen herhangi bir matrisin, n tane satırının herhangi k tanesinin OR'lanması sonucu oluşan vektörün (V), seçildiği kümeye bağlı olarak; B_0 'dan seçilen bir matris için $H(V) \leq d - \alpha m$ veya B_1 'den seçilen bir matris için $H(V) \geq d$ olmalıdır.

2. $\{1, 2, \dots, n\}$ 'nin herhangi alt kümeleri $\{i_1, i_2, \dots, i_q\}$ ($q(k)$ için, B_0 ve B_1 matrislerinin içermiş olduğu matrislerin sıklığı eşit olmalıdır.

İlk parametre kontrast olarak adlandırılırken, ikinci parametre şemanın güvenliğini garanti eder. İkinci koşul sayesinde, k adetten az sayıda payın üst üste getirilmesi ile sıranın elde edilemeyeceği garanti edilir.

(k, n) GSP şemalarının nasıl kurulabileceğini göstermek amacıyla, $(2, 2)$ durumu bir örnek ile açıklanacaktır. B_0 ve B_1 matrisleri aşağıdaki şekilde tanımlanabilir.

$$B_0 = \begin{cases} \text{kolonların permütasyonu ile} & \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} \\ \text{elde edilen tüm matrisler} & \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix} \end{cases}$$

$$B_1 = \begin{cases} \text{kolonların permütasyonu ile} & \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \\ \text{elde edilen tüm matrisler} & \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \end{cases}$$

B_0 ve B_1 kümelerini oluşturan matrislerin satırlarının görünme olasılıkları birbirlerine eşittir. Bu da belirli bir görüntünün belirli bir renge ait olduğu bilgisinin gizli görüntüyü ele geçirmeye çalışan saldırganlar tarafından çıkarılmasına engel olacaktır. Permütasyon işleminin gerçekleştirileceği matrislerden de anlaşılacağı üzere, B_0 kümesini oluşturan herhangi bir matrisin satırlarının OR'lanması sonucu oluşan vektörün Hamming uzaklığı 2 iken (beyaz pikseli temsil eder), B_1 kümesindeki bir matris için hesaplanan Hamming uzaklığı 4 olacaktır. Aradaki fark, insan gözünün siyah ve beyaz arasında ayırım yapmasını sağlayacak karşıtlığı oluşturmaktadır.

Kodlama işlemi esnasında, gizli görüntüdeki beyaz pikselin kodlanması için B_0 kümesinden rasgele bir matris seçilecektir (R_0). Birinci payda karşı düşen alt piksel grubunun içeriği R_0 'ın birinci satırı tarafından belirlenirken, ikinci payın karşı düşen piksel grubu ikinci satır tarafından belirlenecektir. Benzer şekilde siyah pikselin kodlanması için kullanılacak olan matris ise B_1 kümesindeki matrisler arasından seçilecektir. Görüntüdeki tüm siyah ve beyaz pikseller için bahsedilen kodlama gerçekleştirildiğinde, sırrı paylaşacak olan kişilere dağıtılacak olan paylar oluşturulmuş olmaktadır. Açıklanan kodlama işlemine ilişkin bir örnek Tablo 1'de verilmektedir.

Tablo 1. (2,2) şeması için siyah ve beyaz piksellerin kodlanması.

B	Pay 1	Pay 2	Sonuç	S	Pay 1	Pay 2	Sonuç
□	■	■	■	■	■	■	■
□	■	■	■	■	■	■	■
□	■	■	■	■	■	■	■
□	■	■	■	■	■	■	■
□	■	■	■	■	■	■	■
□	■	■	■	■	■	■	■
□	■	■	■	■	■	■	■
□	■	■	■	■	■	■	■

Gizli görüntüdeki her bir pikselin, paylarda kaç alt piksel ile temsil edileceği GSP şemalarının oluşturulmasındaki parametrelerden biridir. Verilen örnekte bu değer 2 olarak seçilebileceği halde resmin en boy oranında bozulmaya neden olmaması için her iki doğrultuda da 2 olacak şekilde, yani 4 olarak belirlenmiştir. Şemanın karışıklığını belirten α değeri, kodlanmış beyaz piksel ile siyah pikselin Hamming uzaklıkları arasındaki farktır. α değerinin büyük olması, tekrar yapılandırılan resmin karışıklığını, bir başka deyişle görünebilirliğini iyileştirecektir. Verilen bu örnekte α değeri ikidir.

B. Olasılıklı Görsel Sır Paylaşma (OGSP)

2004 yılında Yang tarafından olasılıklı görsel sır paylaşma olarak adlandırılan yeni bir yöntem önerilmiştir. Yeni yöntemin ürettiği payların büyüklüğü, geleneksel yöntemlerden farklı olarak, paylaşılacak olan gizli görüntü ile aynı kalmaktadır. Üretilen payların boyutlarının, gizli görüntü ile aynı kalması, bellekte saklama kapasitesi açısından önemli ölçüde kazançları da beraberinde getirmektedir. Yeni şema beyaz piksellerin siyah ve beyaz bölgede görünme sıklığını, insan gözünün siyah ve beyazı ayırt etmesini sağlayacak şekilde kullanmaktadır. Yang, yayınında vermiş olduğu tanım bağıntıları ile $(2, 2)$, $(2, n)$, (k, k) ve (k, n) şemalarının nasıl oluşturulabileceğini göstermiştir.

Olasılıklı yöntemi geleneksel yöntemden ayıran en önemli fark, kodlanacak olan görüntüdeki pikseli birden çok alt pikselle paylarda temsil etmek yerine tek bir piksel ile kodlamasıdır. Orijinal görüntünün yeniden yapılandırılması için gereken yalnızca gerekli $((k, n)$ lik bir şema için en az k adet payın üst üste getirilmesidir. Bu da geleneksel yöntemdeki OR'lanma işlemine karşı düşmektedir. Geleneksel yöntem beyaz pikseli temsil etmek için $x_0 y_0 S$ (x_0 adet beyaz, y_0 adet siyah), siyah pikseli temsil etmek için ise $x_1 y_1 S$ kullanır. Bir pikselin kaç alt pikselle temsil edildiği m ile gösterilecek olursa, $x_0 + y_0 = x_1 + y_1 = m$ olacaktır. OGSP şemalarında ise m değeri 1'e eşit olacaktır. Geleneksel yöntemde kullanılan, $n \times m$ büyüklüğündeki B_0 ve B_1 matrislerinin yerini, $n \times 1$ büyüklüğündeki B_0 ve B_1 matrisleri alacaktır. Beyaz piksellerin kodlanması esnasında, B_0 kümesinden rasgele bir matris seçildikten sonra, rasgele seçilen satırlardaki değerler paylara dağıtılacaktır. Siyah piksellerin kodlanması esnasında kullanılacak olan matris B_1 matrisleri arasından seçilecektir. Yeniden yapılandırılma esnasında oluşacak görüntüyü, üst üste getirilen payların, pik-

sel düzeyinde oluşturdukları Hamming ağırlıkları belirleyecektir. Siyah ve beyaz bölgelerdeki beyaz sıklığı, yeniden yapılandırılan resmin, insan gözü tarafından ayırt edilebilmesini sağlayacaktır. p_0 , yeniden yapılandırılan resmin beyaz bölgesinde beyaz pikselin görünme olasılığını temsil eder. p_1 ise, siyah bölgede beyaz görünme olasılığını verecektir. Beyaz ve siyahın ayırt edilmesini belirleyecek parametrelerden biri olan değişmez eşik olasılığı p_{th} ile gösterilsin.

(k, n) OGSP şeması ancak aşağıdaki üç durumu sağlıyorsa geçerlidir:

1. B_0 ve B_1 kümelerindeki her bir matrisin herhangi k satırının oluşturduğu sütun vektörü V ile gösterilsin. $L(V)$ ise ilgili vektörün satırlarının OR'lanması sonucu elde edilen değer olsun. B_0 kümesinden elde edilen $L(V)$ değerleri λ kümesi, B_1 den elde edilen değerler ise γ kümesini oluştursun.

2. λ ve γ kümeleri, $(p_0 \geq p_{th})$ ve $(p_1 \leq p_{th} - \alpha)$ koşullarını sağlayacaktır.

3. $\{1, 2, \dots, n\}$ 'nin herhangi alt kümelerinde $\{i_1, i_2, \dots, i_q\}$ ($q(k), p_0$ ve p_1 değerleri eşit olacaktır).

Böyle bir şemanın nasıl yapılandırılacağını gösterebilmek amacıyla, $(2, 2)$ OGSP şemasının [14]'de verilen tanım bağıntısı kullanılacaktır. μ_{ij} , Hamming ağırlığı i olan bütün $n \times 1$ lik kolon matrislerini temsil eder. j indisi ise, matrisin B_0 veya B_1 'e ait olduğunu gösterecektir, $j \in \{0, 1\}$. Örneğin $n=3$ iken, $\mu_{2,0}$ kümesine ait matrisler aşağıdaki şekildedir.

$$\mu_{2,0} = \left\{ \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \right\}$$

Tanım 2. $B_0 = \{\mu_{0,0}, \mu_{2,0}\}$ ve $B_1 = \{\mu_{1,1}\}$. B_0 ve B_1 , $(2, 2)$ OGSP'nin oluşturulması için gerekli 2×1 lik matrislerin kümesidir. Bu durumda B_0 ve B_1 ait matrisler aşağıdaki şekilde verilebilir.

$$B_0 = \{\mu_{0,0}, \mu_{2,0}\} = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\} \quad B_1 = \{\mu_{1,1}\} = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$$

$$\lambda = \left\{ L \left(\begin{bmatrix} 0 \\ 0 \end{bmatrix} \right), L \left(\begin{bmatrix} 1 \\ 1 \end{bmatrix} \right) \right\} = \{0, 1\}$$

$$\gamma = \left\{ L \left(\begin{bmatrix} 1 \\ 0 \end{bmatrix} \right), L \left(\begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) \right\} = \{1, 1\}$$

λ ve γ 'da pikselin beyaz olma olasılığı olan p_0 ve p_1 sırayla 0.5 ve 0'dır. Bu nedenle bu şemaya ait eşik olasılığı olan $p_{th} = 0.5$ ve karışıklık $\alpha = 0.5$ 'dir.

III. (2, N) OLASILIKLI GÖRSEL SIR PAYLAŞMA YÖNTEMİ

Bu bölümde öncelikle Wang tarafından önerilen $(2, n)$ OGSP şemasının tanımı verilecek daha sonra ise yayın kapsamında önerilen yöntemden bahsedilecektir.

A. Wang'ın (2, n) OGSP şeması

Wang tarafından önerilen bu şema XOR ve AND gibi mantıksal işlemlerin kullanımına dayanır [14]. Gizli görüntünün ortaya çıkarılması sırasında insan görme sistemi yerine, özel bir yazılım gerektirmeden görüntüleme yazılımlarının olanakları kullanılabilir. Önerilen yöntem, orijinal görüntüdeki siyah pikselleri kesin doğrulukla yeniden yapılandırabilirken, beyaz pikselleri doğru olarak yapılandırma olasılığı 0.5'dir. Önerilen şemanın payları oluşturmak için gerçekleştirdiği adımlar aşağıdaki şekilde verilebilir.

Girişler: n ile ifade edilen bir tamsayı değeri ($n \geq 2$) ve A ile gösterilen gizli görüntü.

Adım 1: $B_1, B_2, \dots, B_{n+1}$ ile gösterilen $(n+1)$ adet matris üret.

Adım 2: $C_1, C_2, \dots, C_n$ ile gösterilen n adet ara matrisi $C_i = B_i \& A, i = 1, 2, \dots, n$ denklemini kullanarak hesapla.

Adım 3. $A_1, A_2, \dots, A_n$ ile gösterilen n adet payı $A_i = C_i \oplus B_{n+1}, i = 1, 2, \dots, n$ denklemini kullanarak hesapla.

Gizli görüntünün (A') oluşturulması için gerçekleştirilecek olan yapılandırma işlemi Denklem 1'de verilmektedir.

$$A' = A_i \oplus A_j, i, j \in \{1, 2, \dots, n\} \text{ ve } i \neq j \quad (1)$$

$A_i(s, t)$ basitçe A_i olarak gösterilsin. Yukarıda bahsedilen yapılandırma adımları göz önüne alındığında A ile gösterilen gizli görüntüdeki herhangi bir siyah pikselin i ile gösterilen paya kodlanması esnasında $C_i = B_i \& 0 = 0$ olacaktır. Buradan da i ile gösterilen paydaki piksel değeri $A_i = B_{n+1} \oplus 0 = B_{n+1}$ olacaktır. Böylece gizli görüntünün yeniden yapılandırılması esnasında $A' = A_i \oplus A_j = B_{n+1} \oplus B_{n+1} = 0$ olacaktır. Buradan da kodlanan siyah piksellerin yeniden yapılandırma esnasında kesin doğrulukla oluşturulacağını göstermektedir.

A' 'daki beyaz (1) piksel için $C_i = B_i \& 1 = B_i$ ve $A_i = B_{n+1} \oplus B_i$ olacaktır. Böylece gizli görüntünün yeniden yapılandırılması için i ve j ile gösterilen payların bir araya getirilmesi sonucu (2) deki ifade elde edilecektir.

$$A' = B_{n+1} \oplus B_i \oplus B_{n+1} \oplus B_j = B_i \oplus B_j \quad (2)$$

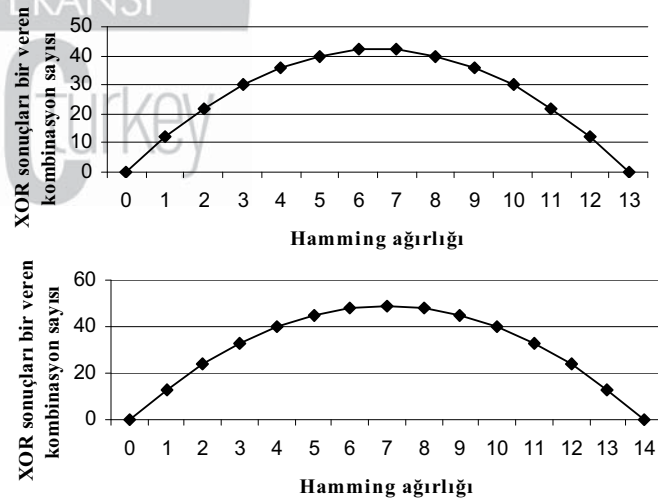
Yukarıdaki ifadeden de görüleceği gibi, beyaz bir pikselin doğru olarak kodlanma olasılığı $\frac{1}{2}$ 'dir. Bu olasılık aynı zamanda XOR fonksiyonunun sonucunda 1 görülme olasılığını temsil etmektedir.

Wang tarafından önerilen (2, n) OGSP şeması, gizli görüntü A ile yeniden yapılandırılan görüntü A' arasında 0 bitlerini aynı tutmayı başarırken, 1 bitlerini doğru kodlayabilme olasılığı $\frac{1}{2}$ 'dir. Bu nedenle de bu şemaya ilişkin α değeri ile gösterilen kontrast değeri $\frac{1}{2}$ 'dir. Olasılıksal bir yöntem olan bu şemanın kontrast değerinin ölçümünde (3) bağıntısı kullanılmıştır.

$$\alpha = \frac{p_0 - p_1}{1 + p_1} \quad (3)$$

B. Önerilen (2, n) OGSP şeması

2007 yılında Wang tarafından önerilen yöntemde, orijinal gizli görüntüdeki beyaz piksellerin yeniden doğru bir şekilde yapılandırma olasılığı XOR fonksiyonuna giriş olarak verilen iki rasgele matrisin (B_i veya B_j) karşılıklı piksellerin değerlerine bağlıdır. (2, n) GSP şeması için oluşturulması gereken rasgele B matrisi sayısı $n+1$ dir. Son matris hariç (B_{n+1}) geri kalan matrisler, beyaz piksellerin doğru bir şekilde yeniden yapılandırılmasında rol oynayacaktır. Makalede önerilen yöntemde, tüm bu matrisler birbirlerinden bağımsız olarak rasgele anlamda üretilmektedir. N tane matrisin herhangi ikisinin karşılıklı elemanlarının XOR sonucunun 1 verme olasılığı $\frac{1}{2}$ 'dir. Yeniden yapılandırma sonucunda oluşan görüntünün doğruluk oranını yükseltebilmek, algoritmanın beyaz pikselleri yeniden üretmedeki başarı oranını yükselterek gerçekleştirecektir. Bu nedenle B matrisleri birbirlerinden bağımsız olarak üretilmek yerine, n adet matrisin karşılık düşen piksellerine yerleştirilecek değerler seçilirken, XOR sonucunun farklılık durumunda 1 verdiği göz önüne alınmalıdır. n boyutlu bir diziden seçilen ikili kombinasyonların XOR sonuçlarının 1 verme olasılığını yükseltmek, yöntemin başarısını yükseltmekle eşdeğerdir. $n=13$ ve $n=14$ elemanlı bir vektörün sahip olabileceği farklı Hamming ağırlıklarına bağlı olarak, iki elemanlı kombinasyonların XOR sonuçlarının 1 verdiği durumların sayısına ait grafik Şekil 1'de verilmiştir. Alınan ikili kombinasyonların en çok sayıda bir verdiği durum, simetri nedeni ile n değerinin çift veya tek olmasına göre değişmektedir. Toplam pay sayısını gösteren n değerinin çift olduğu durumlarda tek bir maksimum değer varken, tek olduğu durumlarda iki maksimum değer vardır.



Şekil 1. Sırasıyla $n=13$ ve $n=14$ için farklı hamming ağırlıklı vektörlerin, kendi elemanlarının ikili kombinasyonlarının XOR sonuçlarının değerlendirilmesi.

B matrislerindeki karşılıklı pikselleri n boyutlu vektörler oluşturmaktadır. Matrislerin Wang tarafından önerildiği şekilde ayrı ayrı oluşturulması yerine, karşılıklı elemanlarının oluşturduğu vektörlerin sınırlı bir rasgelelik kullanılarak seçilmesi yeniden yapılandırılan resmin doğruluğunu artıracaktır. B mat-

rislerini oluşturmak için önerilen yöntem Şekil 2’de verilmektedir. Orijinal görüntünün $N \times M$ boyutlarında olduğu varsayılmıştır.

Gösterimde B matrislerinin karşılıklı elemanlarına yerleştirilecek olan değerleri içeren vektör v ile gösterilmektedir. V vektörünün içeriği E ile gösterilen vektör uzayından seçilen rasgele bir vektörün içeriği olacaktır. E uzayının oluşturulması esnasında toplam pay sayısının çift veya tek olması durumu göz önüne alınmaktadır. Çift olması durumunda değer atamada kullanılacak vektörler kümesi elemanlarının Hamming ağırlıkları, toplam pay sayısının yarısına eşittir. $\mu_{n/2}$ ifadesi, Hamming ağırlığı $n/2$ olan $1 \times n$ boyutundaki vektörleri temsil etmektedir. Bu durumda tek sayı olan bir n değer için, E kümesi $\mu_{[n/2]}, \mu_{[n/2]+1}$ değerlerinden oluşacaktır. Uygun bir şekilde oluşturulan E kümesinden rasgele seçilen bir vektör değerini taşıyan v vektörünün içeriği, B matrislerinin o an işlem görmekte olan karşılıklı piksellerinin içeriğini oluşturacaktır. B matrislerinin, j ve k ile gösterilen koordinatlarındaki piksel değerleri v vektörünün içeriğine uygun olarak doldurulur. Böylelikle gizli görüntünün yeniden yapılandırılması aşamasında n pay içerisinden seçilecek rasgele iki payın 1 üretme olasılığı yükseltilmiş olacaktır.

```

if  $n \circ 2 == 0$ 
     $E = \{ \mu_{n/2} \}$ 
     $K = C_{n/2}^n$ 
     $v = \{ v^i \mid v^i \in E, i \in \{1, 2, \dots, K\} \}$ 
     $v^i = \{ v_j^i \mid j \in \{1, 2, \dots, n\} \}$ 
if  $n \circ 2 == 1$ 
     $E = \{ \mu_{[n/2]}, \mu_{[n/2]+1} \}$ 
     $K = C_{[n/2]}^n + C_{[n/2]+1}^n$ 
     $v = \{ v_i \mid v_i \in E, i \in \{1, 2, \dots, K\} \}$ 
     $v^i = \{ v_j^i \mid j \in \{1, 2, \dots, n\} \}$ 
 $B = \{ B^i \mid i \in \{1, 2, \dots, n\} \}$ 
 $B^i = \{ B_{jk}^i \mid j \in \{1, 2, \dots, N\}, k \in \{1, 2, \dots, M\} \}$ 
 $B_{jk}^i = v_m^i, i \in \{1, 2, \dots, n\}, m = (rand \times (K-1)) + 1$ 

```

Şekil 2. B matrislerini oluşturmak için önerilen yöntem.

E kümesi aslında OGSP yönteminin $(2, n)$ şemalar için siyah pikselleri kodlamada kullanmış olduğu küme bağıntısı ile eş değerdir. Bu nedenle, aslında önerilen yöntem sonucunda oluşan B matrislerinin içeriği, tümüyle siyah piksellerden oluştuğu varsayılan gizli bir görüntü üzerinde $(2, n)$ OGSP yöntemi kullanılarak üretilen paylarla eşdeğerdir.

IV. SONUÇLAR

Önerilen yöntemin, Wang’ın yönteminden üstünlüğünü gösterebilmek amacı ile yapılan testlerde Şekil 3’de verilen 256×256 boyutlarındaki renksiz “Lena” görüntüsü Floyd-

Steinberg yöntemi ile yalnız siyah ve beyaz piksellerden oluşan görüntüye dönüştürülerek kullanılmıştır. Her iki yöntem de Matlab 7.0 ortamında programlanmıştır. Testler, Intel® Core 2 Duo 1.66 GHz işlemcili ve 1 GB RAM’i olan taşınabilir bir bilgisayar üzerinde gerçekleştirilmiştir. İşletim sistemi olarak Windows XP Professional kullanılmıştır.



Şekil 3. 256×256 büyüklüğündeki test görüntüsü

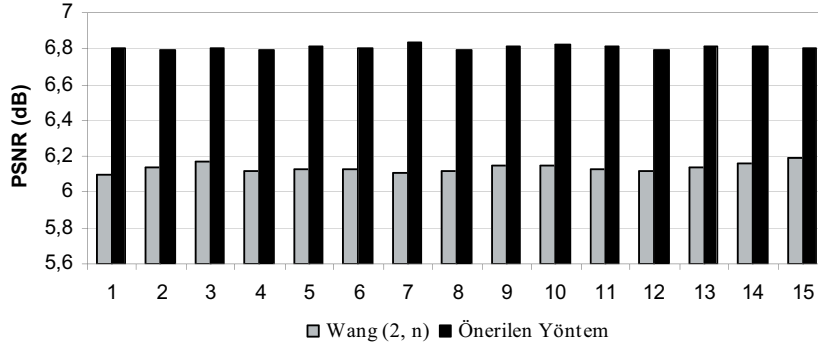
Değerlendirme için her iki yöntem tarafından yeniden yapılandırılan resimlerin doğruluk oranı dikkate alınmıştır. Doğruluk oranını belirleyebilmek için PSNR değerleri hesaplanmıştır. Sabit bir n değeri için, yeniden yapılandırma aşamasında oluşabilecek C_n^2 farklı durum göz önüne alınmıştır. Kombinasyonların XOR’lanması sonucu elde edilen görüntülerin, orijinal görüntüden farkı doğruluk oranı hakkında yorum yapılabilmesini sağlamıştır. PSNR değerlerinin hesaplanması için kullanılan ifade Denklem 4’de verilmiştir.

$$PSNR = 10 \log_{10} \frac{Maks^2}{MSE} dB \quad (4)$$

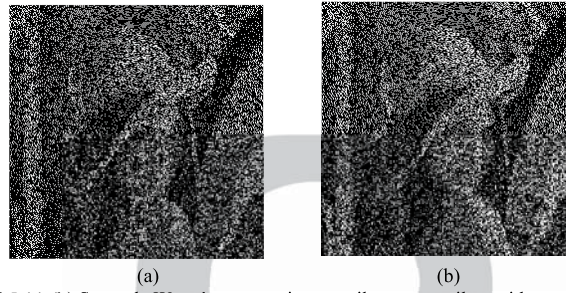
$$MSE = \frac{1}{N \times M} \sum_{i=1}^N \sum_{j=1}^M (x_{ij} - a_{ij})^2$$

$Maks$, görüntüdeki piksellerin sahip olabileceği parlaklık değeri aralığının üst sınırını gösterir. Makalede işlenen görüntünün siyah beyaz olması sebebi ile bu değer 1 olarak alınmıştır. Verilen ifadede, PSNR değeri, $N \times M$ boyutlarındaki X ile gösterilen gizli görüntünün, A ile gösterilen orijinal görüntüden ne kadar farklı olduğunun bir ölçütüdür. Daha yüksek PSNR’ye sahip yeniden yapılandırma sonucu oluşan görüntü orijinale daha çok benzemektedir. x_{ij} ve a_{ij} , sırasıyla test ve orijinal görüntünün (i, j) koordinatlarındaki piksel değerlerini göstermektedir.

Şekil 4’de $n=6$ değeri için önerilen yöntemle oluşturulan 6 farklı payın aralarında oluşturabilecek olduğu 15 farklı kombinasyonun, üretecek olduğu yeniden yapılanmış resimlere ilişkin PSNR değerleri verilmektedir. Şekilden de görüldüğü gibi, Wang tarafından önerilen yöntemin yeniden yapılandığı görüntülerin PSNR değerleri 6.1dB düzeyinde olmasına karşılık önerilen yöntemle 6.8 dB düzeyine yükselmiştir. Gösterilen serilerde maksimum değer oluşumu sağlayan pay kombinasyonlarının ürettiği sonuç görüntüler Şekil 5.a ve Şekil 5.b’de gösterilmektedir.



Şekil 4. PSNR değerleri ile yöntemlerin karşılaştırma sonuçları.



Şekil 5.(a) (b) Sırasıyla Wang'ın yöntemi ve önerilen yöntem ile yeniden yapılandırılan görüntüler.

V.DEĞERLENDİRME

Yapılan çalışmada 2007 yılında Wang tarafından önerilmiş olan tekniğin üretmiş olduğu yeniden yapılandırılan görüntünün PSNR değerinin iyileştirilmesi amaçlanmıştır. Bu kapsamda yöntem tarafından kullanılan rastgele matrislerin üretimi için yeni bir yöntem önerilmiştir. Sonuçlar kısmında da vurgulandığı gibi, her iki yöntemin yeniden yapılandırıldığı resimler arasında sayısal ve görsel bir farklılık mevcuttur. İlerleyen çalışmalarda, ilgili yöntemin (k, n) şemasına genelleştirilmesi amaçlanmıştır.

KAYNAKLAR

- [1] G. R. Blakley, "Safeguarding Cryptographic Keys," *Proceedings of the National Computer Conference, American Federation of Information Processing Societies Proceedings, New York, USA*, pp. 313-317, June 1979.
- [2] A. Shamir, "How to Share a Secret," *Communications of ACM*, vol. 22, no. 11, pp. 612-613, 1979.
- [3] M. Naor, A. Shamir, "Visual Cryptography," *Advances in Cryptology - Eurocrypt'94, LNCS*, vol. 950, pp. 1-12, 1995.
- [4] Hou, Y.-C., "Visual cryptography for color images", *Pattern Recognition*, vol. 36, pp. 1619-1629, 2003.
- [5] Lin, C.-C., Tsai, W.-H., "Visual cryptography for gray-level images by dithering techniques", *Pattern Recognition Letters*, vol. 24, no. 1-3, pp. 349-358, 2003.
- [6] Shyu, S. J., "Efficient visual secret sharing scheme for color images", *Pattern Recognition*, vol. 39, no. 5, pp. 866-880, 2006.
- [7] Wu, C. C., Chen, L. H., "A study on visual cryptography", *Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan*, 1998.
- [8] Wu, H.-C., Chang, C.-C., "Sharing visual multi-secrets using circle shares", *Computer Standards & Interfaces*, vol. 28, no.1, pp. 123-135, 2005.
- [9] Shyu, S. J., Huang, S.-Y., Lee, Y.-K., Wang, R.-Z., "Sharing multiple secrets in visual cryptography", *Pattern Recognition*, vol. 40, no. 12, pp. 3633-3651, 2007.
- [10] Cimato, S., De Prisco, R., De Santis, A., "Colored visual cryptography without color darkening", *Theoretical Computer Science*, vol. 374, no. 1-3, pp. 261-276, 2007.
- [11] R. Ito, H. Kuwakado and H. Tanaka, "Image Size Invariant Visual Cryptography," *IEICE Transaction on Fundamentals*, no. 10, pp. 2172-2177, 1999.
- [12] C.N. Yang, New visual secret sharing schemes using probabilistic method, *Pattern Recognition Letters*, vol. 25, no. 4, pp. 481-494, 2004.
- [13] S. Cimato, R. De Prisco, and A. De Santis, "Probabilistic Visual Cryptography Schemes," *The Computer Journal*, vol. 49, no. 1, pp. 97-107, 2006.
- [14] D. Wang, L. Zhang, N. Ma, and X. Li, "Two Secret Sharing Schemes Based on Boolean Operations," *Pattern Recognition*, vol. 40, pp. 2776-2785, 2007.

Policy Negotiation System based on Privacy Preference

In Joo JANG, Wenbo SHI, Hyeong Seon YOO

Abstract— In this paper, we consider a problem of monopolistic information management technologies. Most service providers have an access to any information. Even though the information is really a personal data, service providers can access to it merely with the user's first subscription.

In order to limit the disclosure and avoid the misuse of personal data, this paper discusses an architectural proposal for a policy negotiation system. This proposed architecture mediates among the three actors: the users, the service providers and the law. The central unit of the proposed architecture is a policy negotiation engine. A negotiation engine undertakes the enforcement of user's privacy preference, by matching the service provider's disclosure policy and user's privacy policy. Several additional components assigned with supporting functional tasks complement the architecture, while the formal definition of personal data type and services type.

This architecture provides *more* powerful right to each user. Finally, this paper discusses the formalization how users can express their privacy preferences and how regulations can be expressed in this system.

Keywords — Privacy, Information management

I. INTRODUCTION

All Every software application domain should provide and ensure security issues. Especially, as countries around the world transition from paper-based to electronic information record infrastructures, compliance with these data protection laws will require sophisticated information management technologies [1,2,3,4]. Technical and policy challenges concerning the widespread adoption of electronic information records systems have been discussed, for example, in [1] and [2].

In addition to, there are different aspects between the users and the service providers. Most users want to disclosure only least privacy data, while the service providers request at most personal information. Under this environment, if most right of information management comes up to the service providers, it

provides the unfair position to the users. It is the problem of monopolistic information management technologies. As a solution of this problem, we introduce the policy negotiation system for privacy protection in this paper.

Security issues usually are derived from laws such as data protection acts or general security rules stemming from the domain itself. However, the laws and rules are given as plain texts and lack a common formalism. This may make it impossible to predict unambiguous privacy regulation and privacy guidelines [5,6,7,8]. Knowledge is not only a form of property governed by intellectual property law, but also an individual attribute, and as part of the personality, it may be governed by privacy law [5].

During the last years ontology has been used as formalism to describe laws and rules on common bases [9,10,11,12,16,17,18,19]. As sets of concepts in a specific domain, ontologies have proven to be a useful tool in the areas of the semantic web and personalized information management. By using ontologies, we can provide a common description for any type of policy, rule, and law, independently from the specifics of the system implementation.

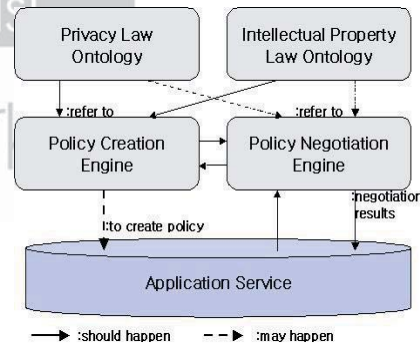


Fig. 1 Policy based privacy management system architecture

A policy negotiation system (PNS) is suggested to satisfy the requirement. In this architecture, each user provides ones own privacy policy by using a policy creation interface, as in Fig.1. The privacy policy could be represented as the set of privacy concept.

This interface also makes the specific privacy policy ontology for the each user. Each individual stores the encrypted privacy policy in his/her potable storages or in his/her computer. And then they can use it as new authentication certification. The policy negotiation engine performs collaborative process with the certain service's data disclosure policy. The concept is

Manuscript received November 10, 2008. This work was supported in part by the Brain Korea 21 project in 2006.

In Joo Jang is with Computer Engineering Department, INHA University, Incheon, Korea, (corresponding author to provide phone: 82-032-860-7381; fax: 82-032-874-1435; e-mail: ijjang@inha.ac.kr).

Wenbo Shi is with Computer Engineering Department, INHA University, Incheon, Korea, (e-mail: swb319@hotmail.com).

Hyeong Seon Yoo is with Computer Engineering Department, INHA University, Incheon, Korea, (e-mail: hsyoo@inha.ac.kr).

shown in figure 1. Each engine refers to law ontologies for reflecting current legislation.

When the privacy policy makes agreement with the data disclosure policy, policy negotiation engine sends the encrypted results to application services. The result is used as a consensual privacy policy and also can be used as a kind of certification for legal user.

II. RELATED WORKS

A. Web service policies in OWL-DL

Kolovski et al. proposed a mapping of WS-Policy to the description logic fragment species of the Web Ontology Language (OWL-DL) [11,12,13] and claimed that OWL reasoners could be used as policy processing tools. They describe how standard OWL-DL reasoners can be used to check policy conformance and perform several policy analysis tasks. Since OWL-DL is much more expressive than WS-Policy, it provides a framework for exploring richer policy languages.

B. Hippocratic databases [14]

R. Agrawal et al. defined a set of standards in terms of data access and protection that would comprise the Hippocratic Database (HDB). Here it is advocated that future databases should include responsibility for the privacy of the data that they manage. In addition to the existing capabilities of databases today, such as the ability to manage persistent data and the ability to access a large amount of data efficiently, data repositories in future would also need to ensure that they adhere to a certain set of standards in terms of data access and protection. These privacy principles, also borrowing from the OECD guidelines (see <http://www.oecd.org>), include diverse terms such as; broadly purpose specification, consent, limited collection, limited use, limited disclosure, limited retention, accuracy, safety, openness and compliance. A privacy constraint validates checks whether the privacy policy of the enterprise is acceptable to the user, before actually receiving any data from the user. While recording the data, the purpose for which the user is sharing it is also recorded. In HDB, when a user submits the query to the system, she also submits the intended purpose for requesting the data. The system validates the identity of the user and then checks whether the user is allowed to access the requested data for a given purpose. The HDB system returns only those data records whose purpose attribute includes the query's purpose attribute.

C. XACML framework

XACML is an initiative to provide a standard for access control and authorization systems, which is generic, distributed, and powerful [13,15]. In contrast, most of the current systems implement access control and authorization in a proprietary manner.

XACML provides an XML based access control policy language together with an access control decision request/response language. Applications and systems can use these to fulfill their access control needs. The XACML

specification just deals with the framework and leaves the exact implementation details of the access control engine for the actual implementation. Besides the objective to create a portable and standard way of describing access control entities and their attributes, XACML aims at providing a mechanism that offers much finer granular access control than simply denying or granting access

III. POLICY NEGOTIATION SYSTEM ARCHITECTURE

The complete PNS solution is comprised of three stages – policy creation stage, policy negotiation stage and application service retrieval as in Fig.2.

A. Policy creation stage

In the policy creation stage (step 1a, 1b in Fig.2), there are two parts of the policy – the data disclosure policy and the privacy policy.

The user creates his/her own privacy policy by using the policy creation engine. The privacy policy would be represented as the set of privacy concepts to express their privacy preference.

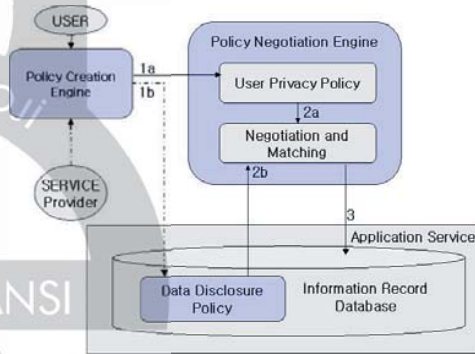


Fig. 2 Policy negotiation system architecture

The policy creation engine provides the keyword-Set to users and service providers. The users select some or more keywords to express their privacy preference.

1) Definition 3.1 : Keyword-Set (KeyS)

A Keyword, denoted by k_i , is a tuple $\langle \text{keyword}_i, C_i \rangle$

Keyword-Set(KeyS) describes the set of all possible keywords used describe concept C_i .

$\forall k_i \in \text{KeyS}$

$k_i = \langle \text{keyword}_1, \dots, \text{keyword}_n, C_i \rangle$

2) Definition 3.2 : Privacy Concept (PCS)

A Privacy Concept, denoted by PCS_i , is a tuple $\langle k_i, k_j, op \rangle$. A privacy concept contains a set of that together result in a privacy breach.

$\forall PCS_i \in \text{PCS}$

$PCS_i = \langle k_i, k_j, op \rangle$

op : operation (ex. $\wedge, \vee, <, =, >$)

3) Example 1 :

A user doesn't want to expose to others his social security number, birth date, and address on the ID-card. Also, he wants to keep his employee-ID and his telephone number as a privacy information.

In this case, we could express the user's privacy concept as follows.

$$k_1 = \langle \text{socialID}, \text{BirthDay}, \text{Addr}, C_1 \rangle,$$

C_1 : a certificate of residence

$$K_2 = \langle \text{employeeID}, \text{Telephone}, C_2 \rangle,$$

C_2 : a certificate of employee

$$PCS_1 = \langle k_1, k_2, V \rangle$$

Privacy is a very subjective notion. Some users may create a specific concept; say age, as private, whereas others may not. Because of it, the encrypted PCS would be used as an authentication for the disclosure of his/her personal information, also according to the category of information feature, the purpose of the request, and the intended recipient. We'll develop it in depth for future work.

The policy governs the access privileges for each role according to the category of information feature, the purpose of request, and the intended recipient of results.

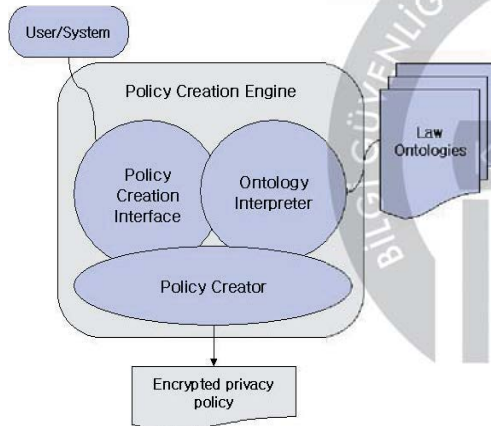


Fig. 3 Policy Creation Engine

The policy creation engine has three main components such as a policy creation interface, an ontology interpreter, and a policy creator. First the policy creation interface supports users easily define their privacy policy without the expertise. The ontology interpreter imports the privacy law ontology and the intellectual property law ontology. Policy creator provides encrypted privacy policy after integrates the rules from ontologies.

B. Policy negotiation stage

In the policy negotiation stage (step 2a, 2b in Fig.2), the user is notified of the system organization's policies concerning data use and disclosure, advised of any disagreement with ones

own privacy and security preferences. This fully automated process is completed before the user provides any personal data to the organization. The user first uses the policy creation engine to express his personal policy concerning the use and disclosure of his personal data. This information is specified in a preference language [14] and matched with the system organization's privacy and security policies to identify any conflicts. The user is advised of these conflicts and given an opportunity to resolve them or terminate the process.

Lastly, the user should modify the policy regarding whether his data may be disclosed to third parties or used for a different purpose than for which it was collected. This changing information are recorded as a result of policy negotiation in the application service database and factored in at the time of service processing. A successful policy negotiation confirms agreement between the privacy policy and the data disclosure policy concerning the processing of the personal data.

The policy negotiation engine has mainly four components such as a policy reader, a policy analyzer, negotiation processor, and result creator, as in Fig.4.

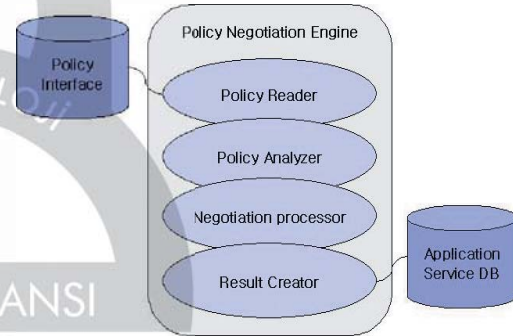


Fig. 4 Policy Negotiation Engine

The reader imports the privacy policy and the data disclosure policy. The analyzer matches for each item of the policies. If there are some disagreements, the negotiation processor provides a disagreement-report and sends it to user and service provider. After the processor get a reply from user and service provider, the result creator makes an agreement result. The result could be a policy agreement between the policies.

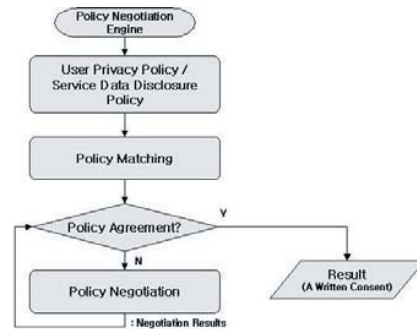


Fig. 5 Negotiation Flow

The figure 5 shows the policy negotiation flow. The negotiation engine performs this fully automated process before the user provides any personal data to the organization. A successful policy negotiation confirms agreement between the privacy policy and the data disclosure policy concerning the processing of the personal data. This agreement could be used a personal certification to access a certain service

C. Application service stage

In the application service retrieval stage (step 3 in Fig.2), the application system controls accesses based upon the user's role, purpose, and intended recipient.

During service, the service system use the result of negotiation as a user's information, a kind of user's certification and a agreement between service provider and user. This system already installed the result of policy negotiation between the privacy policy and the data disclosure policy. This PNS can be integrated into existing environments through a database interface.

D. Active enforcement scenario

Alice wants to access several e-services such as e-market, e-learning, and online service of a hospital. In this case, Alice can access to the services with her own privacy policy by using the system based on the PNS architecture.

1) Policy creation In this stage, Alice can make her own privacy policy by using the policy creation engine. This engine makes privacy policy ontology for Alice according to the privacy law and the intellectual property law. She can store it in her portable memory or in her computer. Therefore the privacy policy can also be used a kind of authentication certification.

The application service providers already make their data disclosure policy by using the policy creation engine or their service-programming engine.

2) Policy negotiation As Alice registers to use services, the policy negotiation engine requests the Alice's privacy policy and the data disclosure policy of the each service. And then, the result is installed in the application service database. If the result is not adoptable, that means Alice's privacy policy does not agreement with the data disclosure policy. At that time, the policy negotiation engine provides a message to Alice to make an agreement.

3) Application services The each application service installs the result of policy negotiation in its database. The each service provider realizes the results as a legal user-list. The service checks the installed data whenever Alice accesses the each service. The encrypted negotiation-result is used as a certification for the user.

IV. CONCLUSION

Considering the problem of monopolistic information management, we proposed new information management system - PNS. In this system architecture, before access to services, the policy negotiation is performed. By using the policy negotiation, PNS provides powerful right for users to handle their confidential data. Service systems can access the personal data if only if they get the policy agreement. This

agreement is a result of the negotiation between the privacy policy and the data disclosure policy. That means the service provider cannot monotonically control the privacy data without user's strong agreement. It will be a new model of the e-service system architecture.

The PNS can fulfill efficient management, sharing, and processing of sensitive data in compliance with the principles of the data protection laws.

In addition to, the encrypted privacy policy will be used as a new way for authentication certification.

V. REFERENCES

- [1] B. Humphreys, "Electronic health record meets digital library", *Journal of the American Medical Information Association*, Vol. 7, no 5, 2000, pp. 444-452.
- [2] I. Iakovidis, "Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe", *International Journal of Medical Information*, vol. 52, no. 1, 1998, pp. 105-115.
- [3] D. Gritzalis, C. Lambrinoudakis, "A security architecture for interconnecting health information systems", *International Journal of Medical Information*, Vol 73, no 3, 2004, pp.305-309.
- [4] R.E.Scott, P. Jennett, et al., "Access and authorization in a Global e-Health Policy context", *International Journal of Medical Information*, Vol. 73, no. 3, 2004, pp259-266.
- [5] A. Dulipovici, R. Baskerville, "Conflicts between privacy and property: The discourse in personal and organizational knowledge", *J. Strategic Information System* Vol.16, 2007, pp.187-213.
- [6] M. Pulkkinen, A. Naumenko, et al., "Managing information security in a business network of machinery maintenance services business - Enterprise architecture as a coordination tool", *The Journal of Systems and Software*, Vol. 80, 2007, pp. 1607-1620.
- [7] Editorial, "Some issues in privacy data management", *Data & Knowledge Engineering* Vol. 63, pp.591-596, 2007.
- [8] Ji-Won Byun, et al., "Purpose Based Access Control of Complex Data for Privacy Protection", *Proc. of 10th ACM Symposium on Access Control Models and Technologies*, Stockholm (Sweden), June 1-3, 2005,
- [9] D.F.Ferraiolo, D.R. Kuhn, et al., "Role-Based Access Control", *Artech House*, 2003.
- [10] R.Agrawal, C. Johnson, "Securing electronic health records without impeding the flow of information", *International Journal of Medical Information*, vol. 76, 2007, pp. 471-479.
- [11] Jun Choe, Sun K. Yoo, "Web-based secure access from multiple patient repositories", *International Journal of Medical Information*, 2007.
- [12] S. Berlik et al., "An Ontology-Based Approach for Managing and Maintaining Privacy in Information Systems", *LNCS 4275*, 2006, pp982 - 994.
- [13] D. Geneiatakis, C. Lambrinoudakis, "An ontology description for SIP security flaws", *Computer Communications*, Vol. 30, 2007, pp. 1367-1374.
- [14] R. Agrawal, et al., "Hippocratic Databases", *the 28th VLDB Conference*, 2002.
- [15] M.Verma, "XML Security: Control information access with XACML," [Online] Available: <http://www-128.ibm.com/developerworks/library/x-xacml/>, 2005
- [16] A. Katifori, C. Halatsis, "Ontology Visualization Methods-A Survey", *ACM Computing Surveys*, Vol.39, no. 4, 2007.
- [17] M. Thinyane, L. Dalvit, H. Slay, et al., "An ontology-based, multi-modal platform for the inclusion of marginalized rural communities into the knowledge society", *ACM Int. Conf. Proceeding series*, Vol.226, 2007, pp.143-151.
- [18] InJoo Jang, et al. " Collaborative Privacy Management System," International Conf. On Information Security and Assurance No.2, 2008, pp52-56.
- [19] Yolanda B.F, et. al., "A flexible semantic inference methodology to reason about user preferences in knowledge-based recommended systems," *Knowledge-Based Systems*, 21, 2008, pp305-320.

Partially Opened Data and Its Security

Hidema TANAKA

Abstract—We discuss a method of disclosing data which includes secret information. In general, such method is called sanitizable signature and context extraction signature and many schemes are proposed. In the previous schemes, we can make an opened data (covered data) after signed the data which includes secret information. And maker of covered data and signer are another person. We assume that the person who knows the secret information is only signer and maker of covered data and signer are the same person. We analyze security requirements for such purpose and develop a proposal method. We show a security analysis of our proposal protocol and its applications. We also show that our proposal protocol is a method that can be used for not only the data concerning to national security and digital forensics but also the secure network construction.

Keywords —Digital forensics, ElGamal encryption method, secure protocol, Partially opened data, Content Extraction Signature

I. INTRODUCTION

A. Background

WE have demands for disclosing information partially while concealing the confidential information. For example, though all information can be opened at X-day, it is necessary to open it partially for one's innocence at the court before the day. Figure 1 shows the methods of disclosing printed data which includes secret information. There are two types of solution, TYPE-1 and TYPE-2. TYPE-1 is a method of painting out the secret information. This is a popular solution and they are founded in several place such as confidential documents of government which are allowed to be open under some condition, some indictment documents, X-Files and so on. TYPE-2 is a method of cutting off a secret information. It is well adopted to audio and video data than printed data. It is a technique for keeping the secret by removing an inconvenient part from the original data. In this paper, we discuss how such a method is applied to digital data. The necessity of this technology grows up greatly with an increase in the use of digital data. For instance, the Sarbanes - Oxley act [21] is enforced as for an economic activity, and management and disclosing digital data are the important problems for corporations. Moreover, it is necessary to treat as evidence of the criminal case. In the politics of Japan, assembly member Nagata's fake email in 2006 is famous [15]. He tried to open the main text without the informations of sender and he printed email and eliminated such information, then submitted as the evidence with his declare that all information is opened later. Fortunately his fake was solved by another matter, however, the case where digital data is treated as a legal evidence will increase.

H. Tanaka is with the National Institute of Information and Communications Technology, Japan, 4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan.

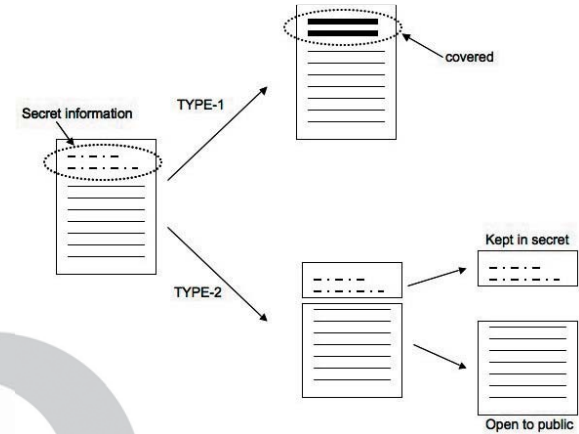


Fig. 1. Method of disclosing printed data including secret information

B. Previous works

If the data which includes secret information has already been signed, some methods have already been proposed [2], [10] and so on. They are applications of hash functions and aggregate signature scheme with pairing techniques [4]. The validity of the data (ciphertext) is guaranteed by the signature. So they do not consider the attack and injustice act of malicious signer by using unopened data which does not have been signed yet. The proposers assume the signer of the data and the maker of covered data (sanitized data) are another person. Therefore the maker can know the confidential information. We assume that the person who knows the secret information is only the signer, it is not suitable method for our purpose. Of course their methods can be improved to achieve our requirement, the weakness against attack using collision search of hash functions remains. An outline of previous proposal scheme is that it calculates the hash value at every the subblock of data, and calculates the signature of it. Then the signed subblock of data concatenated to another subblock of data and repeated above procedure. From such mechanism and procedure, they are categorized into TYPE-1 in Figure 1. From such a mechanism, estimating the secret information, we can determine the secret information using hash value and signature, so the essential security of the method depends on the difficulty of collision search of the hash function. The influence on the weakness of some concrete applications when the assumption of computational difficulty of collision search of hash function collapses is shown in [16] and [20]. The previous methods are not required to open the secret information later. In addition, it is needed for the maker of covered data to have anonymity and the method needs to prevent injustice act by them. These points are not

corresponding to our purpose. Especially, because we assume maker of covered data to be the same person with the signer, the discussion of anonymity of maker of covered data is omitted in this paper.

C. Our purpose

First of all, we assume that the secret information should be open to public later and the person who knows the secret is only the signer before the day. The signer and the maker of covered data are the same person. Therefore, we develop the method which can be applied to the data which has not been signed yet. We assume that the secret information is concerning to national security and digital forensics such as legal evidences. So the security and consistency of data are higher level than previous proposal schemes are required. Since the signer and the maker of covered data are the same person, the injustice act and attack of signer is needed to be prevented. Similarly, the signer should show that any injustice act is not done before X-day. The differences of purpose and condition between previous methods and our method are summarized as Table 1. In Section 2 we discuss the security requirements for our purpose. In the section, we summarize the property of security and analyze their purpose in details. In Section 3, we show our proposal method. It is based on ElGamal encryption method. Our proposal method is categorized into TYPE-2. In Section 4, we show a security analysis of our proposal method according to the security requirements in Section 2. In Section 5, we propose another application of our method. We assume that the secret data is concerning to high secret important data such as national security. However, when the small size data is used, some applications are considered.

II. SECURITY REQUIREMENTS

Suppose that Alice has a digital data M which contains secret information. After X-day, she can open all of M , however, she wants to open a part of M which contains no secret information before the day. Let M' be a part of M which can be open to Public. We call M' "partially opened data". Authority who does not know M , authenticates that M' is a part of M and guarantees that M can not be changed after M' is open. We assume that Authority is a trusted person and we can believe that he does not do any injustice acts. Table 2 shows the variables and their roles in the protocol.

Then we faces the following security requirements.

[R1] *It is impossible to calculate M using open data in the protocol.*

First of all, it is necessary to prevent to re-calculation of the secret part of M using partially opened data M' . In addition, the protocol opens some data for verification and authentication which are generated from M and Alice's secret information. As the results, the attacker can use many open information (For examples, see Table 4). This is the fundamental requirement for the protocol. Therefore if the term when M is kept secret long, it is necessary to choose

the parameters of cryptographic primitives considering the evolution of computer and cryptanalysis techniques. This is a requirement concerning Alice's secrecy.

[R2] *It is possible to verify that M' is a part of M without opening M .*

It is necessary to verify that the partially opened data M' is a part of M . We assumed that M is kept secret, the verification are done without opening M . Blind signature scheme [3] and partially signature scheme [10] seems to have same purpose. Both of them can verify the ciphertext without opening plaintext to verifier. However they can not decrypt a part of ciphertext. And they can not prove the relation between partially opened data and its ciphertext. For the methods using hash functions, the calculation of hash value of a part of data is done at the same time as the data creation. Therefore it is not secure to apply such method to the data which was made in the past. It is because the change in the content by attack using collision search of hash function. The attacks of X.509 certificates [20] and pdf files [16] are well known as the advanced attack using collision search of hash function. Such attack method can be applied to previous methods for unsigned data. To solve these problem, we show a proposal protocol in Section 3. We should show that the partially opened data can not be generated by another data. Or when forgery data M is open, It is necessary for us to find out the injustice act. This is a requirement concerning authentication of data M and M' .

[R3] *It is impossible to change M after M' is opened.*

To hold this requirement, it is necessary to show that it is secure against following two types of attack; one is an injustice attack of Alice and another is forgery attack of malicious people who can get open data. This is a requirement concerning consistency of data M and M' . Though these attack techniques are essentially the same, Alice has advantageous condition because she can prepare forgery data beforehand. Thus it is necessary for us to find out her injustice. Detailed security analysis for our proposal protocol is shown in Section 4.

[R4] *It is possible to verify that Alice did no injustice act before X-day.*

When Alice opens the all of data M , it is necessary to be proven that she did no injustice act for M and M' . This is a requirement concerning integrity of data M and M' . It is considered that this requirement is held if the R1, R2 and R3 are held.

III. PROPOSAL SCHEME

A. Protocol flow

Our proposal scheme is as follows. Table 3 shows variables used in the protocol. The protocol is based on ElGamal encryption method [7]. Figure 2 shows the diagram of the protocol.

<Proposal protocol for secure partially opened data>

Step 1 Alice sends the size of data M to Authority.

TABLE I
DIFFERENCE OF PURPOSE AND CONDITION

	maker of covered data	secret information	category in Figure 1
Previous method	another person of signer	not required to be open	TYPE-1
Our method	same person of signer	required to open after X-day	TYPE-2

TABLE II
VARIABLES AND THEIR ROLES

Alice	A holder of data M . She wants to open a part of M .
Authority	Trusted party such as organizations of government or court.
M	Secret data of Alice.
M'	Partially opened data. Disclosable part of M .
X-day	The day when Alice can open all of M .
Public	People who want to know M . Before X-day, they want to get information as much as possible.

TABLE III
VARIABLES

G	A multi-plicate cyclic group of order q	K	A public key of Alice, $K = g^{k_s}$
q	A prime number	M	A secret data of Alice, $M \in G$
g	A generator of G	M'	Partially opened data of Alice, $M \in G$
r	A random number chosen from $\{0, \dots, q-1\}$	$ X $	The size of X
k_s	A secret key of Alice chosen from $\{0, \dots, q-1\}$		

Step 2 According the size, Authority chooses G , g and q whose size is larger than M . Then he open to public G , q and g . Authority chooses a random number r from $\{0, \dots, q-1\}$ then he sends g^r to Alice.

Step 3 Alice converts her data into elements of G . Next she chooses a secret key k_s from $\{0, \dots, q-1\}$ and calculate her public key $K = g^{k_s}$ and K^{-1} which is an inverse of K . She calculates $M \cdot g^{Kr}$, g^M and $g^{g^{K^{-1}+1}}$ and then sends them to Authority. Note that public key K is kept secret before X-day.

Step 4 Authority calculates $\alpha = (g^M)^{g^r} \times (g)^{M \cdot g^{Kr}}$ and $\beta = (g^{g^{K^{-1}+1}})^{M \cdot g^{Kr}}$. If $\alpha = \beta$, he can fix the message M without opening it. He guarantees g^M .

Step 5 Alice makes a partial open data M' from M . Then she opens M' and $g^{M-M'}$ to Public.

Step 6 Public can know M' and verify $g^{M'} \times g^{M-M'} = g^M$.

Step 7 After X-day, Alice opens M and k_s and Authority opens r .

B. Characteristic of our protocol

Our proposal protocol is an application of ElGamal encryption method. Therefore the security of protocol depends on the security of ElGamal. The main feature of this protocol is that the validity of M' is guaranteed by ciphertext $M \cdot g^{Kr}$, g^M and $g^{M-M'}$. To keep secret M and K , we uses the data $g^{g^{K^{-1}+1}}$. By using it, Authority and Public can verify M' . The detailed security analysis is shown in Section 4.

There is difficulty in implementation. Our proposal protocol uses many times of multi-plicate calculation. We assume M is the data concerning to the very important data such as national security or digital forensics, so it is not a disadvantageous problem the necessity of a large computing time. However in the case of huge size of M , it becomes impossible to calculate. For such a case, it is necessary to reduce M beforehand. Let $M = (m_1 || m_2 || m_3)$ be a huge size data and we assume that Alice want to open a part of m_2

which includes secret information. Alice makes a shrunken data $\tilde{M} = (hash(m_1) || m_2 || hash(m_3))$ and opens $hash(M)$ (where $hash(\cdot)$ denotes a secure hash function). Then Alice starts the protocol with $\tilde{M}$. Alice also open m_1 and m_2 .

IV. SECURITY ANALYSIS

We analyze the security of our proposal protocol according to the security requirements shown in section 2. Table 4 shows the variables which appear in the protocol. From the purpose of the protocol, all variables are opened after X-day. Adding the analysis for security requirements, we analyze the security against malicious Public in "[RX] Attack of malicious Public".

[R1] It is impossible to calculate M using open data in the protocol.

In Step 3 and Step 4, the attacker can get some information which generated from M , that is $M \cdot g^{Kr}$, g^M and pair of $(M', g^{M-M'})$. The attack scenarios are follows (in the following (given information)→target).

[Case1] $(g, g^M) \rightarrow M$

[Case2] $(g, g^r, M \cdot g^{Kr}) \rightarrow M$

[Case3] $(g, M', g^M, g^{M-M'}) \rightarrow M$

It is easy to see that the attack condition of [Case1] and [Case3] are equivalent to the discrete logarithm problem. Therefore the attacker can not get no information on M in the cases. In the same way, it is easy to see that the condition of [Case2] is equivalent to the attack of ElGamal encryption method. Therefore the security of M depends on the security of ElGamal encryption method. As a result, it can be concluded that requirement [R1] has been achieved.

It is well known that ElGamal encryption method is unconditionally malleable and therefore it is not secure against chosen ciphertext attack. So the attacker can easily construct a valid ciphertext $2M \cdot g^{Kr}$ and g^{2M} for the data $2M$. However,

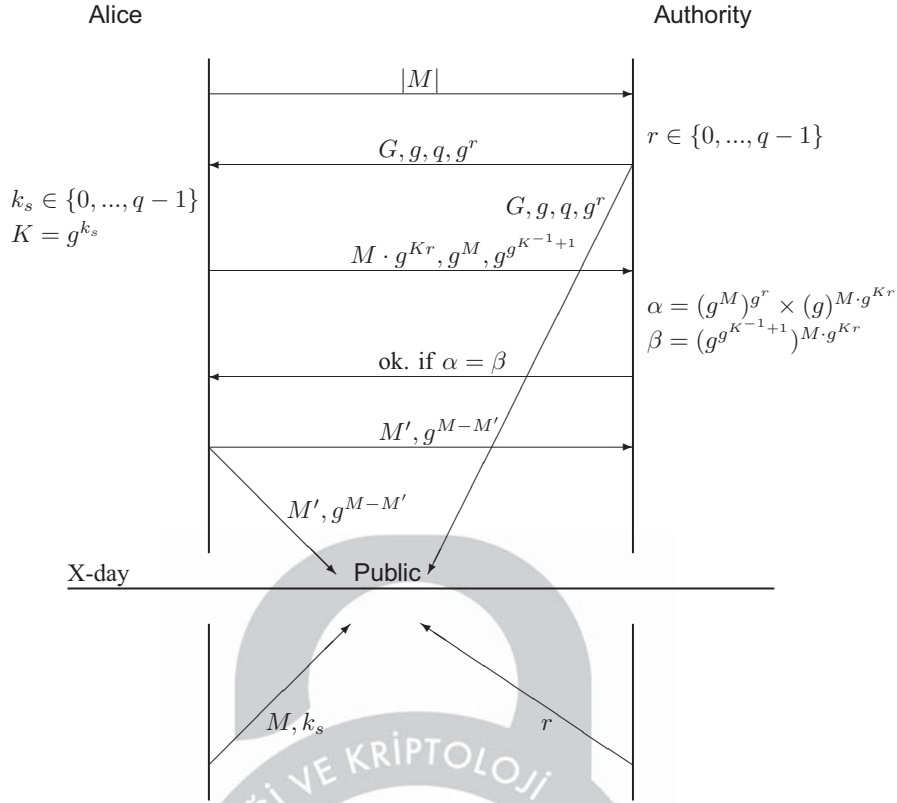


Fig. 2. Diagram of proposal protocol

TABLE IV
VARIABLES IN PROTOCOL

Public information	G, q, g	setup of protocol
	g^r	opened by Authority
	$M \cdot g^{K_r}, g^M, g^{g^{K^{-1}+1}}, g^{M-M'}$	contains secret information M and secret key K
	M'	Alice's open information
Secret Information	M, k_s, K	Alice's secret information
	r	Authority's secret information

in Step 5, Alice opens $(M', g^{M-M'})$ then we can find out that such attack is done. In this attack scenario, there are no benefit for Alice and Authority and such attack is easy to find.

[R2] It is possible to verify that M' is a part of M without opening M .

To analyze this security requirement, it is necessary to show that g^M is generated from M without opening M . In Step 4, Authority and Public can check $\alpha = (g^M)^{g^r} \times (g)^{M \cdot g^{K_r}}$ and $\beta = (g^{g^{K^{-1}+1}})^{M \cdot g^{K_r}}$. We should check that α and β can be calculated from M and K uniquely. Therefore the attack scenario is summarized as follows. Note that the size of $\hat{M}$ equals to M .

$$[\text{Case4}] (g, M, \hat{M} (\neq M), g^r, K) \rightarrow (g^M)^{g^r} \times (g)^{M \cdot g^{K_r}} = (g^{\hat{M}})^{g^r} \times (g)^{M \cdot g^{K_r}}$$

As mentioned above, we can easily make $\hat{M}$ which holds $M \cdot g^{K_r} = \hat{M} \cdot g^{K_r}$. However, for malicious Public who does not

know M , it is impossible to find $\hat{M}$ which can hold $g^M = g^{\hat{M}}$ at the same time because this problem is based on the discrete logarithm problem. And for malicious Alice who knows M , it is impossible to find out $\hat{M}$ whose size is equals to q . On the other hand, if $|\hat{M}| > |M|$, malicious Alice can make $\hat{M}$ as $M+nq$ where $n = 1, 2, \dots$ because of $g^q = 1$. But in this case, the size of $\hat{M}$ becomes larger than the size of q , Authority and Public can easily find out the malicious Alice's injustice after X-day. Considering the purpose of this protocol, we can conclude that there are no benefit for Alice in such attack.

Under the assumption that we can verify that g^M is generated from M without opening M by the method in Step 4, we analyze the requirement by the following attack scenario.

$$[\text{Case5}] (g, M', g^M, g^{M-M'}) \rightarrow \hat{M} \text{ which holds } g^{\hat{M}} \times g^{M'} = g^M$$

A malicious Alice can find out such $\hat{M}$ but there are no benefit for Alice because M has been already fixed. As the result, we

can verify that M' is a part of M without opening M by the method in Step 5 and Step 6.

[R3] *It is impossible to change M after M' is opened.*

From the analysis of security requirement [R2], under the assumption of using same key K , it is obvious that it is impossible to rewrite M after M' is opened.

There is another attack scenario.

[Case6] (M_1, K_1, M_2, K_2) where $M_1 \neq M_2$ and $K_1 \neq K_2 \rightarrow M_1 \cdot g^{K_1 r} = M_2 \cdot g^{K_2 r}$, $g^{M_1} = g^{M_2}$ and $g^{g^{K_1^{-1}+1}} = g^{g^{K_2^{-1}+1}}$

Under the condition of $|M_1| = |M_2|$, from the result of analysis of [R2], it is impossible to do the attack according to this scenario. Under the condition of $|K_1| \neq |K_2|$, we can find pair of (K_1, K_2) which holds $g^{K_1^{-1}+1} = g^{K_2^{-1}+1}$. So the attacker can execute the above scenario for $|M_1| \neq |M_2|$. Therefore if malicious Alice prepared such pairs of (M_1, K_1) and (M_2, K_2) , she can success the attack in this scenario. Of course, after X-day, the unnatural setting of size of G is found in this scheme. Therefore Public will have a doubt in the validity of M and Alice. However, the countermeasure against this attack is easy by using hash functions or time stamp protocol. For example, in Step 3, Alice opens the hash value of M with the time stamp protocol. In that case, the validity of M depends on the security of hash function and time stamp protocol. We assume that our proposal protocol is used for long term validity of partial opened data M' . In this case, the security requirement of hash function becomes high performance. Such discussion is found in [9].

[R4] *It is possible to verify that Alice did no injustice act before X-day.*

In Step 7, Alice opens M and her secret key k_s and Authority opens his random number r . So Public can calculate $K = g^{k_s}$ and decrypt $M \cdot g^{K r}$. In Step 3, Alice opens $g^{g^{K^{-1}+1}}$. Public can not verify that it is generated by k_s without knowing its value. This is an open problem of our protocol. However, as mentioned above, some attack and injustice activity are discovered as an unnatural setting of G .

[RX] *Attack of malicious Public*

We analyze the attack of malicious Public who want to ruin Alice's confidence. In this section, we assume an active attack to the protocol.

Man-in-the-middle-attack : In place of Alice, malicious Public opens another M' or M . In Step 3 and Step 5, malicious Public can changes Alice's data. So, if there are no authentication protocol between Alice and Authority, the attack successes. Before Step 1, Alice and Authority must make a secure channel by using PKI and so on.

Forgery attack : At X-day, malicious Public opens forgery data $\hat{M}$. As mentioned above, if $|M| = |\hat{M}|$, it is impossible to do such attack. If $|M| \neq |\hat{M}|$, the attack is discovered by another Public and Authority.

Basically, the attack which Alice can not execute, can not be done by malicious Public. Therefore the protocol which holds

security requirements shown in Section 2, is secure against malicious Public.

We confirmed the security of our proposal protocol for the requirements shown in Section 2. As a results, we conclude that our protocol holds the security requirements.

V. APPLICATIONS

A. Incident analysis

CERT and IRT analyze the incident which caused by malicious software (Malware), illegal access, DoS attack and so on . They collect data concerning attacks or incidents from user who are in trouble. Such data has often includes privacy information which should be kept secret. On the other hand, CERT and IRT need to confirm the report of attacks is the true. The difference exists in information that the user can show and information that CERT and IRT need. Today they solve this problem by making NDA each other. Because it is such a situation, the information from general user is difficult to collect. Additionally, if it can, there will be a possibility that information from general user contains lies and mistakes. By using proposal protocol, CERT and IRT get more information from general users. As mentioned above, user's privacy is protected and CERT and IRT know the details of attacks and incidents. And CERT and IRT can check the information is true or false. It is expected that our proposal can be applied effectively to such use.

B. Encryption Email

Some email servers such as in the corporation, the encryption email to the address that has not been permitted is prohibited. Though it is because of prevention of information leakage, it limits the activity of staff. Such a problem can be solved by submitting the partially opened data which is generated by our protocol. Our protocol can verify the ciphertext and partially opened data, so if the information is leaked by encryption email, we can find the malicious user.

C. Traceable network and incident detection

It is well known that the attack to the network using encrypted IP packet. Since the router, the server, and the administrator can not analyze the content, encrypted IP packet is an effective attack method. As the countermeasure against such problem, our proposed protocol can be used. For example, the router issues ID to the sender. The sender writes ID in his IP packet, then he encrypts it. (Of course, plaintext IP packet should be written ID, too.) Next he make partially opened data which open only ID and sends encrypted IP packet, ID, g^M and g^{M-ID} . The router checks ID and stores ID, g^M and g^{M-ID} . In the same way as the case of Section 5.2, the administrator can find the packet which makes incident or troubles and the sender. In this system, the router, the server and client PCs need to do the large number of calculation for huge number of IP packets. It is a problem of implementation of our protocol and it is hard to solve at once.

VI. CONCLUSION

In this paper, we propose a protocol which generates partially opened data. The security requirements are shown in Section 2 and proposal protocol is shown in Section 3.

In Section 4, we analyze the security of our proposal protocol. Note that we did not discuss whether forgery data $\hat{M}$ was possible to have semantic meaning which is effective for attack. Suppose text data M , it is very hard to find some meaning in $\hat{M} = M + nq$. Therefore we conclude that the successful attack in Section 4 has no sense for real data. In addition, even if most successful attack, since the evidence was left Alice gets disadvantageous. As a result, we conclude that our proposal protocol is secure enough for semantic data.

In Section 5, we show an application of our protocol whose purpose is other than national security and digital forensics. For the usage for national security and digital forensics, necessity of huge computational cost does not become a fatal problem. For the general usage, it becomes important problem to be solved.

Analysis of security concerning $g^{g^{-K}+1}$ and improvement of protocol is our next research topics. It is a disadvantageous not to be able to verify $g^{g^{-K}+1}$ until X-day. Our proposal protocol uses transmission of a huge amount of data and it has some redundant steps. The optimization of the data transfer is our next theme.

REFERENCES

- [1] H. Kopka and P. W. Daly, *A Guide to L^AT_EX*, 3rd ed., Harlow, England: Addison-Wesley, 1999.
- [2] G. Ateniese, D. Chou, B. Medeiros, G. Tsudik, "Sanitizable Signatures", ESORICS 2005, LNCS 3679, pp.159-177, Springer, 2005.
- [3] M. Bellare and P. Rogaway, "The Exact Security of Digital Signatures - How to Sign with RSA and Rabin", Proc. of EUROCRYPT 1996, LNCS 1070, pp.399-416, Springer, 1996.
- [4] D. Boneh, C. Gentry, B. Lynn, H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps", EUROCRYPT 2003, LNCS 2656, pp.416-432, Springer, 2003.
- [5] R. Cramer and V. Shoup, "Signature Schemes Based on the Strong RSA Assumption" Proceedings of the 6th ACM conference on Computer and communications security, pp.46-51, 1999.
- [6] D. Chaum, "Blind signature for untraceable payments", Advances in Cryptology: Proceedings of Crypto 82, pp.199-203, Plenum, New York, 1983.
- [7] T. El Gamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", Advances in Cryptology, Proceedings of CRYPTO '84, LNCS 196, pp.10-18, Springer, 1984.
- [8] S. Goldwasser, S. Micali and R. L. Rivest, "A digital signature scheme secure against adaptive chosen message attacks", SIAM Journal on Computing, pp.236-238, 1988.
- [9] Y. Hirai, T. Kurokawa, S. Matsuo, H. Tanaka and A. Yamamura, "Classification of Hash Functions Suitable for Real-Life Systems" IEICE Transactions 91-A(1): pp.64-73 (2008)
- [10] T. Izu, N. Kanaya, M. Takenaka, T. Yoshioka, "PIATS: A Partially Sanitizable Signature Scheme", ICICS 2005, LNCS 3783, pp.72-83, Springer, 2005.
- [11] H. Kuwakado, M. Morii, "Restrictively Sanitizable Signature Scheme", SCIS 2006, 4A1-3, pp.274, 2006.
- [12] K. Miyazaki, G. Hanaoka, H. Imai, "Digitally Signed Document Sanitizing Scheme from Bilinear Maps", SCIS 2005, 3E3-5, pp.1471-1476, 2005.
- [13] K. Miyazaki, M. Iwamura, T. Matsumoto, R. Sasaki, H. Yoshiura, S. Tezuka, H. Imai, "Digitally Signed Document Sanitizing Scheme with Disclosure Condition Control", IEICE Transactions on Fundamentals, Vol E88-A, pp.239-246, No. 1, 2005.
- [14] K. Miyazaki, S. Susaki, M. Iwamura, T. Matsumoto, R. Sasaki, H. Yoshiura, "Digital Documents Sanitizing Problem", IEICE Technical Report, ISEC 2003-20, pp.61-67, 2003.
- [15] H. Nakata, "Nagata now admits e-mail was fake, faces Diet discipline", The Japan Times Online, 3rd Mar, 2006, <http://search.japantimes.co.jp/cgi-bin/nn20060303a1.html>
- [16] M. Gebhardt, G. Illies and W. Schindler, "A Note on Practical Value of Single Hash Collisions for Special File", Proc. of NIST 1st Cryptographic Hash Workshop, 2005.
- [17] S. Lu, R. Ostrovsky, A. Sahai, H. Shacham and B. Waters, "Sequential Aggregate Signatures and Multisignatures without Random Oracles", Cryptology ePrint Archive, Report 2006/141, 2006.
- [18] C. P. Schnorr, "Efficient Identification and Signatures for Smart Cards", Advances in Cryptology - CRYPTO '89, LNCS 435, pp.239-252, 1990.
- [19] R. Steinfeld, L. Bull, Y. Zheng, "Content Extraction Signatures", ICICS 2001, LNCS 2288, pp.285-304, Springer, 2001.
- [20] M. Stevens, A. Lenstra and B. Weger, "Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities", Proc. of EUROCRYPT 2007, LNCS 4515, pp.1-22, Spring, 2007.
- [21] P. Sarbanes and M. G. Oxley, "Public Company Accounting Reform and Investor Protection Act of 2002", PL 107-204, 2002.
- [22] M. Suzuki, T. Ishiki, K. Tanaka, "Sanitizable Signature with Secret Information", SCIS 2006, 4A1-2, pp.273, 2006.
- [23] B. Waters, "Efficient identity based encryption without random oracles", Proc. of EUROCRYPT 2005, LNCS 3494, pp.114-127, Spring, 2005.

Project TWOVAULT – Secure and Selectively Deniable Data Storage

Markku-Juhani O. SAARINEN, Member IEEE

Abstract—We introduce TWOVAULT, a cryptographic data storage mechanism with novel features that has been designed primarily for securing removable memory devices and Solid State Disks. The design is organization-centric and therefore suitable for large corporations and governmental organizations that wish to control the access and flow of sensitive information.

In TWOVAULT, data confidentiality and integrity protection are achieved with *Envaulting*, a standards-based cryptographic mechanism for securing stored data with keyless access control. Envaulted removable devices can be remotely disabled if the device is stolen or lost. Furthermore TWOVAULT makes attempts to access envaulted data traceable by its owners.

In Envaulting, cryptographically diffused data is split into two parts of unequal size. The larger portion is stored in a container (e.g. a USB Flash Drive), while the smaller portion, together with keying information, is stored in a separate fragment database, the FragmentVault Server. After establishing a secure connection with FragmentVault, the user sees files stored in the data container as part of the regular file system, making the system transparent and easy to use.

Encrypted blocks in the data containers are indexed by a FragmentVault server using a mechanism that gives it a high degree of deniability; TWOVAULT is a deniable steganographic filesystem. The total amount of information stored on a device remains unknown to an adversary even if portions of it has to be revealed due to legal or extralegal pressure.

The Content-Addressed Storage (CAS) mechanism of TWOVAULT often eliminates block duplicate writes on the container (removable storage device), speeding up common operations, increasing capacity and device lifetime. The indexing system also allows “undo” operations; recovery of earlier snapshot views the filesystem.

A fully operational prototype of TWOVAULT has been implemented for the Linux operating system.

Keywords— Data storage, protocol, analysis

I. INTRODUCTION

We shall first introduce the concepts and motivational observations behind TWOVAULT.

One of the motivating observations in the design of TWOVAULT is the widely predicted and already occurring transition from spinning magnetic disks to solid state storage. Filesystems have traditionally been designed to optimize the storage of files onto continuous blocks on disks to enable fast retrieval. One of the main differentiating characteristics of Flash and Solid State Drive (hereafter simply SSD) storage solutions is near-zero latency and seek time. Usage of defragmentation tools on SSDs makes little sense as blocks on these drives can be accessed in random order. We note that NAND flash memory does not behave exactly like RAM; the underlying technology often necessitates that information is

erased one allocation block at a time, thus making byte-level random access slow.

Another major difference between traditional disk systems and SSD systems is that the latter may only offer a limited number number of erase/write cycles. Some vendors only guarantee 10000 writes before errors may occur. We address this problem by randomizing the use of a disk across the entire physical drive space. TWOVAULT has near-optimal wear-leveling characteristics, thus increasing drive lifetime.

A. Envaulting

The essential feature of the Envaulting concept is that some *a priori* knowledge of complete plaintext contents is required to decrypt a block of data – even if the secret key is known. The entropy of a message is split into two halves of unequal size; the larger portion can be stored or transmitted on high-capacity medium, and the much smaller portion on low-bandwidth secure channel. Both portions are required to reconstruct the original message and can be used to verify its integrity.

In the TWOVAULT instantiation of Envaulting the high-capacity medium is a SSD and the low-bandwidth secure channel is an online connection to a “FragmentVault” Server. Other instantiations might use a fast internet connection or shared disk space as the insecure channel and a quantum link or a smart card as the secure low-bandwidth channel.

There are many ways to perform Envaulting, but in the present work we use a cryptographic hash function and a tweakable block cipher mode of operation as the Envaulting construction (see Figure 1). The Envaulting operation is discussed in detail in Section II-B.

The theoretical background of Envaulting can be traced to Claude Shannon’s 1948 work on information theory; in some ways the low-capacity channel acts as an Error Correcting Code that allows decoding of the data in the high-capacity medium (see Section 12 in [1]). However, due to use of a cryptographic diffusion layer, no partial information about plaintext is leaked unless both portions, together with a third element, a symmetric cryptographic key, are fully available.

B. Resistance to Key Disclosure

Most traditional encryption systems encrypt the entire protected volume with a single key that is derived from a passphrase or password in some way. Dictionary attacks against the passphrase cannot be mounted against envaulted volumes.

Recent research has found many (if not most) disk encryption systems vulnerable to so-called *cold-boot* attacks

M.-J. O. Saarinen can be reached at ENVAULT CORPORATION, Teknobulevardi 3–5, 01530 Vantaa, Finland. E-Mail: mjos@envaultcorp.com

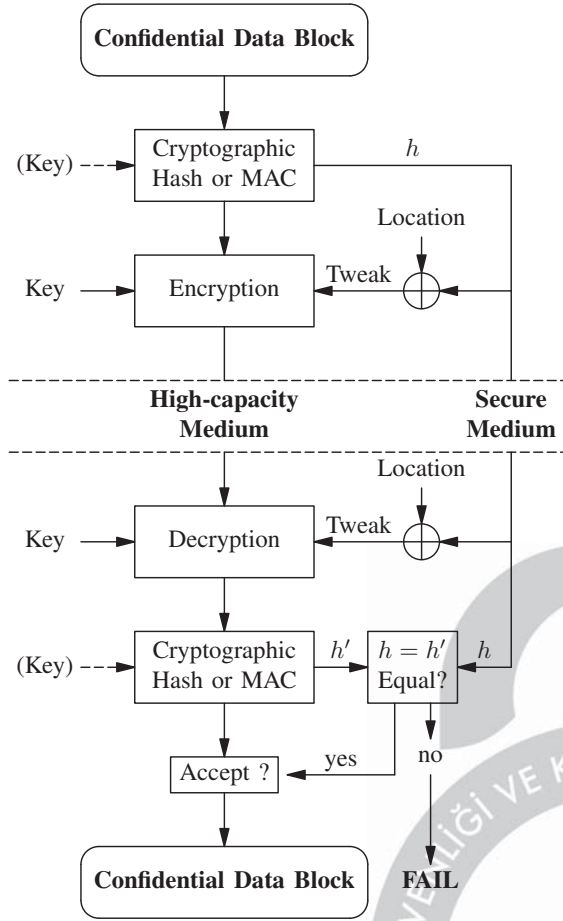


Fig. 1. Envaulting and devaulting using a hash function. Use of a hash function as a tweak guarantees that the ciphertext is fully diffused. Decryption of a block is not possible without the hash value h , even if the secret encryption key is known to the adversary.

[2]. Cold-boot attacks are based on the observation that the contents of system memory degrade slower than previously thought, allowing attackers to remove physical memory and copy passwords and encryption keys from system memory.

Even a full snapshot disclosure of encryption keys and Fragment Vault contents does not allow decryption of modifications performed after the snapshot has been made. Envaulted storage therefore has *forward secrecy* properties, as applicable to static storage.

C. Content-Addressed Storage and Version Control

TWOVAULT implements a CAS (Content-Addressed Storage) scheme. If two bulk data blocks (of size that is equal to allocation unit, typically 4096 bytes) contain exactly the same data, they are stored on the medium only once. This is achieved using a collision-resistant hash function (see Chapter 9 of [3]).

We utilize a simple queuing mechanism for block allocation which guarantees that blocks are not immediately reused. Therefore previous snapshot views of the entire filesystem can be recovered by simply altering the virtual block indexing system.

D. Selective Deniability

TWOVAULT introduces information hiding with an implementation of an highly efficient steganographic storage system based on ideas of Anderson, Shamir, Needham and others [4], [5]. This feature can be used to hide not only the plaintext contents, but the very existence and amount of information stored on a disk. Multiple hidden filesystem containers can exist on a single removable media. Even if an adversary obtains access to one such container, it does not reveal any information about *additional* information stored on the device. Proving that the storage device holder has not provided access to all information contained in the storage device can be shown to be impossible.

E. Organizational Remote Control

With TWOVAULT, each read and write operation must be individually authenticated. In our implementation, an authenticated SSL/TLS connection to a trusted server is required to store and retrieve deniability, confidentiality and integrity information. Each individual block read and write operation can be logged on a trusted secure server. This allows access to memory devices to be centrally controlled, and dictionary attacks can be proactively prevented. A lost, stolen, or decommissioned memory device can be simply remotely disabled. Any attempt to access it, with or without the authentication keys, can be detected and even traced.

II. IMPLEMENTATION

TWOVAULT utilizes a client-server model where bulk data is stored on a SSD memory device by the TWOVAULT client, and indexing, authentication, and integrity validation information on a remote server, FragmentVault. The communication link between a TWOVAULT client and FragmentVault is secured using the SSLv3 or TLS protocol [6].

In the prototype Linux version of TWOVAULT, the client side is implemented as a user-level process that listens to incoming Network Block Device (NBD) connections on a local socket. This allows installation without modifications to current stock Linux Kernel. This is illustrated in Figure 2.

A. Binary Protocol

We currently use a very light-weight binary protocol over SSL/TLS. The OpenSSL library [7] is used to implement AES, RIPEMD-160 and TLS/SSL. The “https” port 443 is used by default as typical firewall configurations allow outgoing traffic through this port. FragmentVault is authenticated using a trusted site X.509 certificate. The TWOVAULT client may use any authentication mechanism allowed by the local OpenSSL installation, including password authentication, (smart card) certificate authentication, and various two-factor authentication schemes.

The binary protocol is not used to transmit data blocks stored on the bulk memory device, but rather their message digests (hashes) and indexing information. Even if the communication link is somehow breached, there is no actual confidential data leakage. Figure 3 illustrates the messages in the current binary protocol.

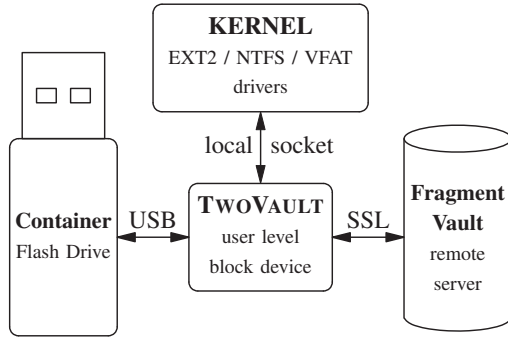


Fig. 2. Kernel file systems communicate with TwoVAULT via a local NBD socket. TwoVAULT encrypts and stores data on a bulk data device (here a USB flash drive) while communicating with FragmentVault.

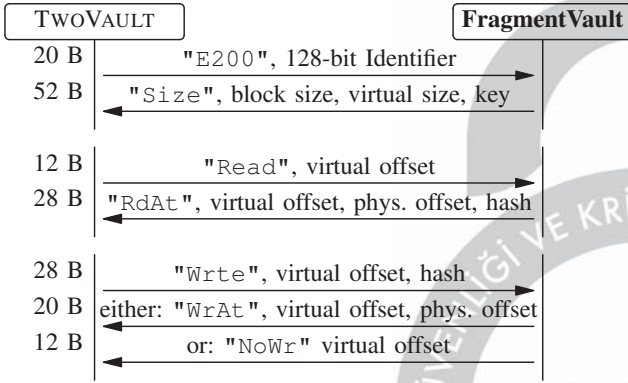


Fig. 3. Illustration of the current version of the binary protocol, which is encapsulated inside an authenticated TLS connection. All sizes and offsets are 64-bits in size, hashes are 128 bits, key is 256 bits and big-endian (network) byte order is used for numbers.

B. Confidentiality and Integrity Mechanism

TwoVAULT confidentiality protection (encryption) is based on the standardized Advanced Encryption Standard (AES) algorithm in the XTS mode of operation, as specified in FIPS 197 and IEEE P1619 standards [8], [9]. The XTS mode tweak is specified as the XOR of the cryptographic hash of the plaintext block and physical block index.

RIPE-MD160 [10] hash function is used due to reported problems with security of MD5 and SHA hashes. After NIST completes its SHA-3 selection process, we plan to migrate to the chosen SHA-3 algorithm [11].

We use the following symbols and variables in the description of the Envaulting encryption mode used in TwoVAULT:

- $\oplus$ Bitwise XOR operation.
- $\otimes$ Multiplication in the finite field $GF(2^{128})$ defined by the polynomial $x^{128} + x^7 + x^2 + x + 1$.
- H Collision-resistant hash function RIPEMD-160.
- E_k AES Encryption with key k .
- D_k AES Decryption with key k .
- K Secret key. Split into two halves: $K = K_1 \mid K_2$.
- i Physical block index.

j Index within the block. For 4096-byte blocks, $0 \leq j \leq 255$.

α Generator in $GF(2^{128})$ i.e. x .

P_j 128-bit plaintext block.

C_j 128-bit ciphertext block.

Encryption and decryption is always performed on full filesystem allocation unit blocks, typically 4096 bytes in size. To encrypt a block, the following steps are required.

1. Compute the cryptographic hash of the message.
 $h = H(P_0 \mid P_1 \mid \dots \mid P_{n-1})$
2. Find its physical index on device as discussed in Section II-C. Encryption and write operations can be avoided if the data contents are already stored on the device.
 $i = \text{find_write_loc}(h)$;
3. Compute the tweak mask T .
 $T = E_{K_2}(h \oplus i)$.
4. Encrypt each 128-bit block $i = 0, 1, \dots, n-1$.
 $C_i = E_{K_1}(P_i \oplus (T \otimes \alpha^i)) \oplus (T \otimes \alpha^i)$

The finite field multiplication is very fast; only one shift and conditional XOR by a 128-bit mask value is required for computation of $T \otimes \alpha^i$ if $T \otimes \alpha^{i-1}$ is known. XTS encryption is illustrated in Figure 4.

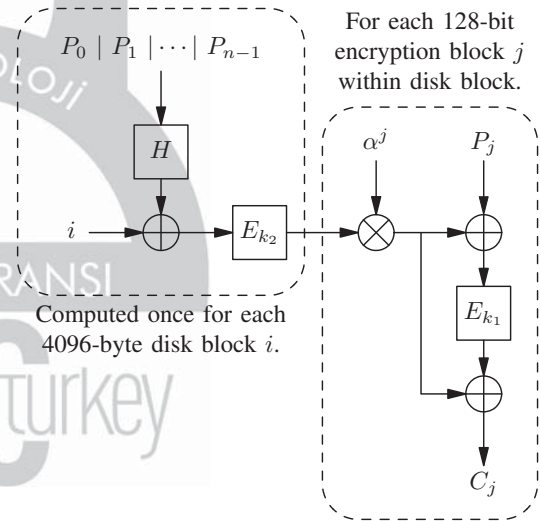


Fig. 4. The IEEE 1619 XTS mode is "tweaked" with the hash of the plaintext.

For decryption operation to work, the h value must be available – it is obtained from the FragmentVault and also used to verify the integrity of the plaintext. Encryption and decryption processes are the same, except for the last step 4:

4. Decrypt each 128-bit block $i = 0, 1, \dots, n-1$.

$$P_i = D_{K_1}(C_i \oplus (T \otimes \alpha^i)) \oplus (T \otimes \alpha^i)$$

Integrity is verified by computing the hash of the resulting decrypted plaintext and comparing that to the h value used in decryption.

Using a standardized cipher and a mode of operation that has been specifically standardized for protection of data on storage devices, rather than a proprietary system, allows data to be recovered even in distant future when the software tools and platform that were used to store data are no longer easily available. The P1619 standard has a XML-based mechanism

for storing secret keys and tweaks. TWOVAULT can be made to support this mechanism for permanent storage.

Another feature of the XTS mode of operation when compared to more classical modes of operation is its inherent parallelism. Encryption using the CBC mode requires the ciphertext of the previous block in order to encrypt the next one, thus breaking parallelism. We envision standardized hardware components that use AES in XTS mode of operation. For discussion about the security of XTS mode of operation, see section IV-A.

C. Indexing of Blocks by FragmentVault

Data blocks are indexed by a map based on the hash of the data content of the block. Each unique block is only stored once; if a block of data with given contents already exists on disk, it is unnecessary to write another copy of it. It is sufficient to simply update tables that map virtual block indexes to physical block indexes.

Indexing is based on RIPEMD-160 [10] truncated to 128 bits due to storage considerations. By birthday paradox, collisions are not likely to occur before $2^{64} \approx 1.845 \cdot 10^{19}$ blocks have been written on disk. This, together with 64-bit sector addressing, allows the current solution to be comfortably expanded up to exabyte range. [3]

The mapping of virtual block positions to physical block positions is performed via two tables, `hmap` and `pmap`. The array `hmap` is a table of hashes (type `md_t`) corresponding to each virtual block. The `pmap` table maps physical indexes and maintains information that is used for hash searches and allocation of physical disk blocks. Figure 5 illustrates how these data structures are used.

The `pmap` structure is internally defined as:

```
typedef struct {
    md_t md; // hash of a block
    uint64_t pcnt; // block usage count
    uint64_t scnt; // for hash search
    uint64_t ploc; // location on disk
} pmap_t;
```

We will now briefly describe the hash table algorithms used. All of these algorithms have $O(1)$ speed, therefore being faster than e.g. $O(\log n)$ binary search algorithms. No sorting is required.

1) *Block allocation / deallocation*: A ring queue `rngq` of n elements is used for physical block allocation and deallocation. The ring queue is initialized with the indices of all blocks contained in the particular volume; they can be in random order. Also, n doesn't have to correspond to physical disk size in blocks. The deniability (information hiding) feature of TWOVAULT (see [4]) relies on this property. Two index variables, `rqtop` and `rqend` maintain the top and bottom of the queue, in wrap-around fashion. New blocks are obtained from the top of the queue with

```
new_block = rngq[rqtop++];
if (rqtop >= n) // wraparound
    rqtop = 0;
```

Unused ones can be freed by inserting them at the queue end:

```
rngq[rqend++] = old_block;
```

```
if (rqend >= n) // wraparound
    rqend = 0;
```

We chose a queue mechanism rather than a stack mechanism to facilitate the “undo” feature; recently overwritten blocks are not immediately reused. Undo is achieved by simply reversing changes caused by write operations in the FragmentVault by using a write log. This also acts as a wear-leveling mechanism.

2) *Finding a block of data by hash*: Cryptographic hashes are uniformly distributed regardless of input. We linearly scale the hash result range onto the size of `pmap` to get the initial probe location as follows: The first eight bytes of the hash are converted into a 64-bit integer x , which is then divided with a constant d . The `pmap` structure therefore has $\lceil 2^{64}/d \rceil$ entries. In the current implementation the constant is chosen as $d = \lfloor 2^{64}/(1.2n) \rfloor$, where n is the size of the physical disk. The initial index $i = \lfloor x/d \rfloor$ is called the “slot” of the hash h . When the physical disk fills up, the `pmap` table also fills up and two or more hashes try to use up the same slot i . The count of hashes in each slot is maintained in `pmap[i].scnt`.

```
uint64_t slot(h) {
    return *((uint64_t *) h) / d;
}
```

Pseudocode for the algorithm `find_by_hash()` for finding the entry in `pmap` that corresponds to hash h is given by.

```
s = slot(h) // our slot
c = pmap[s].scnt; // number of entries
i = s; // index
while (c > 0) {
    if (h == pmap[i].md)
        return i;
    // same slot? decrease count
    if (slot(pmap[i].md) == s)
        c--;
    if (++i >= pmapsiz) // wrap
        i = 0;
}
return NOT_FOUND
```

3) *Reading a Block*: When TWOVAULT receives a request to read from virtual location i , it simply translates it into a physical location p using the FragmentVault connection and performs an actual read operation. In FragmentVault:

```
p = find_by_hash(hmap[i]);
return pmap[p].ploc;
```

Note that if nothing has been written to block i yet, its `htab` entry is zero. In such a case FragmentVault simply returns “Not Available” and TWOVAULT writes a block of zeros to the bulk store.

4) *Writing a Block*: Write operation is slightly more complicated than the read operation. To write a block of data given by `*block` at virtual location i we do the following

```
h = hash(block); // hash it

if (hmap[i] != NOT_USED) {
    if (h == hmap[i])
        return; // NOP!
    j = find_by_hash(hmap[i]);

    // do we need to free this one?
    if (--pmap[j].pcnt == 0) {
        pmap[slot(hmap[j])].scnt--;
        rngq[rqend++] = pmap[j].ploc;
```

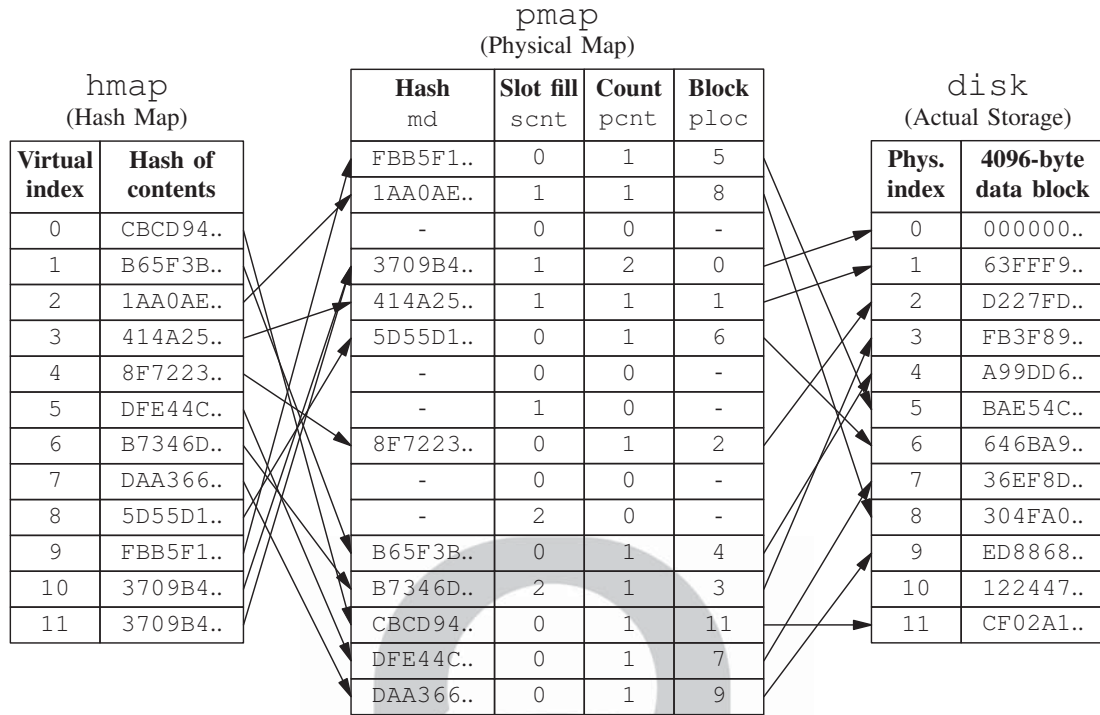



Fig. 5. An example of mapping a virtual block index into physical index via hmap and pmap inside the FragmentVault, also illustrating the hash table mechanism used. Blocks with the same content (10 and 11) are mapped to the same physical sector 0 in the picture.

```

if (rqend >= n) // wrap
    rqend = 0;
}
hmap[i] = h; // set it
j = find_by_hash(h);
if (j != NOT_FOUND) {
    pmap[j].pcnt++; // counter
    return; // done!
}
s = slot(h); // our slot
pmap[s].scnt++; // new
j = s;
while (pmap[j].pcnt > 0) {
    if (++j >= pmapsiz) // wrap
        j = 0;
}
pmap[j].md = h; // set the hash
pmap[j].pcnt = 1; // usage=1
// do NOT touch scnt!
pmap[j].rngq[rqtop++];
if (rqtop >= n) // wrap
    rqtop = 0;

```

III. PERFORMANCE ANALYSIS

In FragmentVault, the read operation is a simple table lookup and causes minimal effect on performance. The write operation involves a hash function computation and an $O(1)$ insertion algorithm. Since the algorithm eliminates a large proportion of media I/O required in the typical usage, there are significant speedups in write operations, especially with storage devices with relatively slow write speeds. The communication bandwidth required is minimal (less than 1 %) when

compared to device I/O or protocols such as the Network File System [12].

To estimate the storage requirements in FragmentVault, we give the ratio of the additional data structures to the actual stored data in our prototype implementation:

hmap	16 Bytes
pmap.md	16 Bytes
pmap.pcnt	8 Bytes
pmap.scnt	8 Bytes
pmap.ploc	8 Bytes
pmap total	40 Bytes
rngq	8 Bytes

$$\text{Fraction} = \frac{16+1.2 \times 40+8}{4096} \approx 1.758\%$$

However, probability that search count should exceed c when pmap expansion factor 1.2 is used is given by 1.2^{-c} . Hence only one byte is sufficient for scnt storage on essentially any future system as $1.2^{-256} \approx 2^{-67}$. By using 16k blocks and 32-bit addressing (max capacity 64 TB), and 72-bit hashes, the fraction can be reduced to 0.207%; 2.1 MB of tables in FragmentVault per each GigaByte stored on the removable device.

IV. SECURITY ANALYSIS

Finally, we will present short security arguments for TwoVault. These can be extended into security proofs in many realistic security models.

A. Confidentiality

In [13] Rogaway develops a tight security proof for XEX/XTS showing that if the underlying AES block cipher is secure against a powerful chosen plaintext/ciphertext adversary, so is the resulting XEX/XTS mode of operation. We note that AES has been approved by NSA to carry data up to Top Secret level in Governmental Use. We apply the XTS mode using the hash of the plaintext message as part of the tweak. This extra layer of protection increases the diffusion from the input bits across the entire allocation unit “block”.

B. Integrity

Our solution provides strong integrity protection for stored data using the RIPEMD-160 cryptographic hash. Most of the traditional disk encryption systems do not provide any integrity protection; random manipulation of ciphertext will not be detected, but simply be visible as corrupted “nonsense” when decrypted.

C. Access Control

In traditional encrypted filesystems the access to data is dependent only on a single user-specified key. In our solution on-line authentication is required to access each sector of envaulted data. Therefore off-line dictionary attacks are simply not feasible. Advanced access control mechanisms such as security tokens or smart cards can be used to authenticate the SSL/TLS connection, and all access to the device is traceable by the FragmentVault’s audit trail.

D. Selective Deniability

The TWOVAULT system provides selective deniability, even in forensic analysis. It can be seen that it is possible to hide data on the drive in a way that prevents the very existence of certain hidden volumes to be revealed even if FragmentVault authentication is successful. However, the data is not deniable to the organization that controls FragmentVault and owns the device. This was one of the original design criteria of TWOVAULT.

V. ACKNOWLEDGMENT

The author is deeply thankful to colleagues at Envault Corporation for the original inspiration, encouragement and support for “Project TWOVAULT”.

REFERENCES

- [1] C. E. Shannon, “A mathematical theory of communication,” *The Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, Oct. 1948.
- [2] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten, “Lest we remember: Cold boot attacks on encryption keys,” in *Proc. 17th USENIX Security Symposium*. USENIX Association, 2008, pp. 45–60.
- [3] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.
- [4] R. Anderson, R. Needham, and A. Shamir, “The steganographic file system,” in *Information Hiding, Second International Workshop, Portland, Oregon, USA, April 14-17, 1998, Proceedings*, ser. Lecture Notes in Computer Science, D. Aucsmith, Ed., vol. 1525. Springer, 1998, pp. 73 – 82.

- [5] A. D. McDonald and M. G. Kuhn, “Stegfs: A steganographic file system for linux,” in *Information Hiding, Third International Workshop, IH’99, Dresden, Germany, September 29 - October 1, 1999, Proceedings*, ser. Lecture Notes in Computer Science, A. Pfitzmann, Ed., vol. 1768. Springer, 2000, pp. 463–477.
- [6] T. Dierks and E. Rescorla, “The transport layer security (TLS) protocol version 1.2,” 2008. [Online]. Available: <http://tools.ietf.org/rfc/rfc5246.txt>
- [7] OpenSSL, “OpenSSL: The open source toolkit for SSL/TLS.” [Online]. Available: <http://www.openssl.org>
- [8] NIST, *FIPS 197, Specification for the Advanced Encryption Standard (AES)*, Nov. 2001. [Online]. Available: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- [9] IEEE, *Std 1619-2007: Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices*. IEEE, Apr. 2008.
- [10] H. Dobbertin, A. Bosselaers, and B. Preneel, “RIPEMD-160: A strengthened version of ripemd,” in *Fast Software Encryption, Third International Workshop, Cambridge, UK, February 21-23, 1996, Proceedings*, ser. Lecture Notes in Computer Science, vol. 1039. Springer, 1996, pp. 71 – 82.
- [11] NIST, “Announcing request for candidate algorithm nominations for a new cryptographic hash algorithm (SHA-3) family,” *Federal Register*, vol. 72, no. 212, pp. 62 212–62 220, Nov. 2007.
- [12] S. e. a. S, “Network file system (NFS) version 4 protocol,” 2003. [Online]. Available: <http://tools.ietf.org/rfc/rfc3530.txt>
- [13] P. Rogaway, “Efficient instantiations of tweakable blockciphers and refinements to modes ocb and pmac,” in *Advances in Cryptology – Asiacrypt 2004*, ser. Lecture Notes in Computer Science, vol. 3329. Springer, 2004, pp. 16–31.

CMS Tabanlı Kütüphane Kullanarak ETSI Uyumlu Elektronik İmza Modülü Geliştirmek

Hasan GÖLLE, Şeref SAĞIROĞLU

Özet—Dijital imzanın matematiksel altyapısı iyi tanımlanmıştır ve açık anahtar altyapısının sağladığı kriptografik metodlar, gizlilik, bütünlük, inkar edememezlik ve kimlik doğrulamada etkin olarak kullanılabilir. Veri nesnelerine uygulanan dijital imza için tanımlı genel standartlar (PKCS#7 veya CMS gibi) varsa da imzalanacak verinin formatını, imza formatını ve elektronik belge formatını tanımlayan bir standarda gereksinim vardır. Yalnızca uzun dönemli elektronik imza geçerliliğini destekleyen bir standart, farklı kullanıcı ortamlarda çalışan elektronik imza çözümlerinin birbirleri ile uyumlu çalışabilmelerine olanak sağlar. Bu noktada Telekomünikasyon Kurumu, atılan imzaların ETSI TS 101 733 standartına uygun olmasını tavsiye etmektedir. Bu bildiride CMS tabanlı MS CryptoAPI kütüphanesinin sağladığı temel kriptografik metodlar kullanılarak ETSI uyumlu elektronik imzanın nasıl oluşturulacağı açıklanmıştır.

Anahtar kelimeler—elektronik imza, CMS, ETSI, imzalama sertifikası.

Abstract—The mathematical aspects related to the calculation of digital signatures are well defined and the cryptographic methods, provided by public key cryptography, are effective in achieving scalable confidentiality, integrity, authentication and non-repudiation services. Even though there have been defined so far general standards for defining digital signature applied on data objects, like PKCS#7 or CMS, there still exist the need for a standard entirely defining the format of the data that is to be signed, the format of the signature and the format of the electronic documents. Only the existence of a widely accepted standard for the format of electronic signature that could remain valid over long periods could avoid the appearance of incompatible specifications and solutions for electronic signatures in different user environments. At this time, telecommunication institute advices generating electronic signatures compatible with ETSI TS 101 733. In this paper, it is explained that how to generate ETSI compatible electronic signature by using basic cryptographic methods provided from CMS based MS CryptoAPI.

Keywords—electronic signature, CMS, ETSI, signing certificate.

I. GİRİŞ

MS CryptoAPI [12] ile PKCS#7 / CMS standardı kullanılarak elektronik imza oluşturulmaktadır. Türkiye'de Tübitak'ın geliştirmiş olduğu imzager (java ve .net) e-imza kütüphaneleri [1] ETSI uyumlu e-imza üretip doğrulamaktadırlar.

H. GÖLLE, TÜBİTAK, Ankara
Ş. SAĞIROĞLU, Gazi Üniversitesi, Mühendislik Mimarlık Fakültesi,
Bilgisayar Mühendisliği Bölümü, Ankara

ETSI TS 101 733 [2] de belirtilen BES (basic electronic signature) formatının PKCS#7 / CMS formatından farklı olarak sahip olduğu ek imza nitelikleri nedeniyle Ms Crypto API nin ürettiği elektronik imza, Tübitak imza kütüphanesi tarafından doğrulanamamaktadır.

ETSI TS 101 733, Cryptographic Message Syntax (CMS) üzerine yazılmış bir standarttır. CMS'nin güncel RFC'si RFC 3852'dir. ETSI ise RFC 3369'u kullanmıştır. CMS [3] standartında, atılan imzalara "Attribute" olarak adlandırılan çeşitli nitelikler eklemek mümkündür. ETSI 101 733, attribute'larla ilgili çeşitli kısıtlar koyarak 9 farklı imza formatı tanımlamaktadır. Bunlardan en basiti BES(Basic Electronic Signature) yani Temel Elektronik İmzadır. BES imzası içinde bulunması zorunlu olan 3 attribute vardır. Bunlar CMS'de tanımlı Content-type, Message-digest attribute'ları ve RFC 2634'te [4] tanımlı signing-certificate ve other-signing-certificate attribute'larından biri olmalıdır.

MS CryptoAPI ile ETSI uyumlu imza atamamadaki problem de bu noktada ortaya çıkmaktadır. MS CryptoAPI, BES yapısı içine konması gereken 3 attribute'tan ilk ikisini imza içine koymasına rağmen, üçüncü olarak konması gereken signing-certificate veya other-signing-certificate attribute'larının ikisini de koymamaktadır. Bu nedenle MS CryptoAPI içinde bu attribute'ları direkt olarak tanımlamak mümkün değil. Fakat Microsoft, imza yapısına bir attribute eklemek için gerekli alt yapıyı oluşturmuştur ve eğer encoding'i de dahil olmak üzere attribute'u oluşturup MS CryptoAPI ye verilirse istenen attribute'un eklenmesi mümkündür.

II. PKCS#7 / CMS

En önemli kriptografik standartlardan biri, RSA veri güvenliğinin çıkardığı PKCS#7 dir. Bu standart, S/MIME [5] eposta güvenliği, kredi ödemeleri için (Secure Electronic Specification Transaction-SET) standardı yada gizli anahtar ve sertifikanın güvenli taşınmasında kullanılan PKCS#12 standardı gibi mekanizmalarda geniş kabul görmüş ve temel alınmıştır.

PKCS#7 standardı, (Internet Engineering Task Force-IETF)'ün S/MIME çalışma grubunun ürettiği ve sıradan bir mesajın dijital imzalanması, özetinin alınması, doğrulanması yada şifrelenmesi amacıyla kullanılan Kriptografik Mesaj Sözdizimi (Cryptographic Message Syntax- CMS) standardının evrimleşmiş halidir. Temelde PKCS#7 /CMS, elektronik verilere dijital imza gibi kriptografik düzenlemeler eklemek için farklı kullanışlı biçimler önermektedir. Standart, imzalama zamanı, mesaj içeriği ile birlikte doğrulanabilme, çoklu imza gibi niteliklere izin verir. Standart, PKIX çalışma grubunun [6] tanımladığı X.509 tabanlı PKI gibi farklı sertifika tabanlı mimarilere

destek verecek şekilde tasarlanmıştır. Tüm veri tipleri ASN.1 sözdizimine uygun olarak açıkça tanımlanmıştır ve şifreleme kuralları (DER ve/veya BER şifreleme nerede ve ne zaman kullanılır gibi.) da ayrıca belirlenmiştir.

Herhangi bir içeriğe dijital imza eklenmesi gerektiğinde PKCS#7/CMS standardında bulunan imzalı veri (signed-data) içerik tipini paralel olarak çok sayıda imzacı kullanabilir. İmzalanan veri formatı blobdur. PKCS#7/CMS de belge eklerine dijital imza desteklenmemiştir. Mesaj kendi içinde imza doğrulama için gerekli sertifikaları ve sertifika iptal listelerini (CRL) [7] içerebilir. Standartla ortaya çıkabilecek olumsuz bir durum da içerikte imzalayan olmadığı durumda sertifikalar ve CRL' ler anlamsızlaşabilir. Dahası veri ve imzasının *signed-data* içerik tipi içinde birarada gruplanmadığı ayırık imzalar da ortaya çıkabilir. Bu son durumda imza doğrulama işlemi uygulama bağımlıdır. Örneğin S/MIME'da tanımlı imzalı belgeler için tanımlı iki format *application/pkcs7-mime with SignedData* ve *multipart/signed*'dir. Sonuç olarak ya *multipart/signed* MIME içerik tipi[8] kullanılarak ayırık imza oluşturulabilir ya da *application/pkcs7-mime with SignedData*[5] tipi kullanarak tek CMS nesnesi oluşturulabilir.

III. ETSI ELEKTRONİK İMZA STANDARTI (CADES)

Elektronik imza, imzalayanla doğrulayan arasında uzun yıllar sonra bile oluşabilecek anlaşmazlıklarda kullanılabilir. Bu standartta elektronik imza üretmede açık anahtar altyapısı baz alınmıştır. Standartta ileri elektronik imza için kullanılan format olarak ASN.1 (Abstract syntax notation 1) belirtilmiştir. Bu format CMS (Cryptographic message syntax) tabanlı olup RFC 3852 [3] de tanımlıdır. Elektronik imzalar bu nedenle Cades "CMS Advanced electronic signature" olarak adlandırılır. Şekil 1 de temel elektronik imza formatı görülmektedir.

Standartta CMS (RFC 3852[3]) tabanlı Elektronik imza formatları tanımlanmıştır. Bu bağlamda temel olarak şu tanımlara yer verilmiştir:

- İmzalayan
- Doğrulayan
- Güvenilir servis sağlayıcı (trusted service providers)
- Hakem

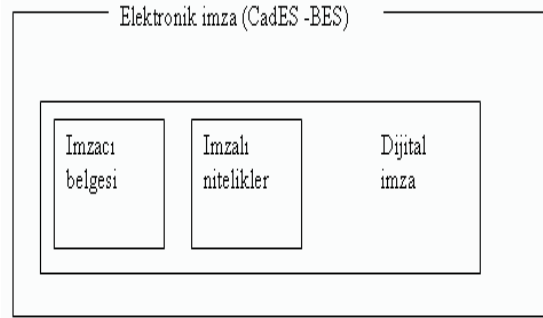
Güvenilir servis sağlayıcılar (TSPs), imzalayanla doğrulayan arasında güven ilişkisi sağlamaya yarayan varlıklardır. Bu güven ilişkisini şu hizmetleri sürdürerek sağlarlar:

- Kullanıcı sertifikaları
- Çapraz sertifikalar, zaman damgası tokenları
- CRL[7] ve OCSP[11] sorguları

Bu hizmetler aşağıdaki güvenilir servis sağlayıcıları vasıtasıyla sürdürülür:

- Sertifika makamı
- Kayıt makamı
- CRL yayınlayıcı
- OCSP sunucu
- İptal makamı
- Zaman damgası makamı
- Time-marking makamı
- İmza politikası yayınlayıcı

Cades-BES yapısı şu şekildedir:



Şekil 1: Elektronik imza (Cades -BES) formatı

Cades-BES, Avrupa elektronik imza yönergesi yasal gereksinimlerini karşılar. Temel kimlik doğrulama ve bütünlük denetimi sağlar.

IV. CADES-BES DE BULUNMASI ZORUNLU NİTELİKLER

Aşağıdaki niteliklerin imzalı belgede bulunması zorunludur.

A İçerik tipi (Content-type)

Content-type niteliği imzalı içeriğin tipini belirtir. Content-type niteliğinin sözdizimi CMS (RFC 3852 [3]) de tanımlıdır. Content-type niteliği, signed-data yada authenticated-data içindeki ContentInfo'nun içerik tipini gösterir. Content-type niteliği imzalı-veride (signed-data) imzalı nitelikler varsa yada doğrulanmış-veride (authenticated-data) doğrulanmış nitelikler varsa mutlaka bulunmalıdır. Content-type niteliği imzalı-veride ya da doğrulanmış verideki encapContentInfo eContentType değeriyle uyusmalıdır. Content-type niteliği imzalı olmalıdır.

Şu nesne belirteci content-type niteliğini belirtir:

```
id-contentType OBJECT IDENTIFIER ::= { iso(1)
member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs9(9) 3 }
```

ContentType ::= OBJECT IDENTIFIER

B Mesaj özeti (message-digest)

Mesaj özeti (Message-digest) niteliğinin sözdizimi CMS (RFC 3852 [3]) de tanımlıdır. Mesaj-özeti (message-digest) niteliği imzalı-veride (signed-data) imzalanacak encapContentInfo eContent OCTET STRING verisinin özetini gösterir. İmzalı-veri için mesaj-özeti, imzalayanın mesaj özeti algoritması ile hesaplanır. İmzalı-veride imzalı niteliklerin bulunması durumunda mutlaka mesaj özeti niteliği de bulunmalıdır. Mesaj özeti mutlaka imzalı olmalıdır.

Şu nesne belirteci content-type niteliğini belirtir:

```
id-messageDigest OBJECT IDENTIFIER ::= {
iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs9(9) 4 }
```

MessageDigest ::= OCTET STRING

C İmzalama sertifikası (signing-certificate) niteliği

İmzalama sertifikası (signing-certificate) niteliği, ESS imzalama-sertifika (ESS signing-certificate) yada ESS imzalama-sertifika-v2 (ESS signing-certificate-v2) ile desteklenmektedir. Bu niteliklerde imzalayan sertifikasına referans bulunmalıdır ve bu nitelikler yerine koyma ve yeniden yayınlama saldırılarına karşı koyan ve imza doğrulamada kısıtlı sayıda sertifikaya izin veren yapıda tasarlanmalıdır. Tam bir sertifikadan daha yoğun ve küçük bir yapıdadırlar ve kolayca ayırdedilebilirler.

- İmzalama sertifikası (ESS signing certificate) niteliği (Enhanced Security Services -ESS) RFC 2634 [4] de tanımlanmıştır ve özet algoritması olarak yalnızca SHA-1 e izin verir.
- İmzalama sertifikası-V2 (ESS signing certificate-V2) niteliği ise (ESS update: Adding CertID algorithm agility) RFC 5035 [9] de tanımlanmıştır ve diğer özet algoritmaları kullanıldığında kullanılmalıdır.

İmza doğrulamada kullanılacak sertifika, sertifika zincirinde bulunmalıdır ve sertifika zinciri de boş olmamalıdır. Signing-certificate RFC 2634 [4] (Enhanced Security Services for S/MIME) içinde şöyle tanımlanıyor:

```
SigningCertificate ::= SEQUENCE {
    certs SEQUENCE OF ESSCertID,
    policies SEQUENCE OF PolicyInformation
OPTIONAL
}
```

```
id-aa-signingCertificate OBJECT IDENTIFIER ::= { iso(1)
member-body(2) us(840) rsadsi(113549) pkcs(1)
pkcs9(9)
smime(16) id-aa(2) 12 }
```

```
ESSCertID ::= SEQUENCE {
    certHash Hash,
    issuerSerial IssuerSerial OPTIONAL
}
```

Hash ::= OCTET STRING -- SHA1 hash of entire certificate

```
IssuerSerial ::= SEQUENCE {
    issuer GeneralNames,
    serialNumber CertificateSerialNumber
}
```

Sertifika zincirindeki ilk sertifika imza doğrulama sertifikası olmalıdır. Bu sertifika için EssCertID kodlamasında issuerSerial alanı mutlaka bulunmalıdır. Böylece imzayı atan kişinin sertifikasına ulaşmak mümkün

olabilir. İmzalamaSertifika (SigningCertificate) niteliği mutlaka imzalı olmalıdır.

V. ASN1 ENCODE

Bu yapıyı encode edebilmek için DER encode fonksiyonları hazırlamak gereklidir. Bu fonksiyonlar MS CryptoAPI'de [12] tanımlı bir veri yapısı olan CRYPT_ATTR_BLOB üzerinde işlem yapmaktalar. Programda kullanılan EncodeLen, MakeTLV ve BasaTagEkle metodları öncelikle oluşturulmuştur. TLV, Tag, Length, Value kelimelerinin baş harflerinden oluşmaktadır. Der kodlaması böyle bir yapı kullanmaktadır.

VI. ETSİ UYUMLU ELEKTRONİK İMZA OLUŞTURMAK İÇİN KULLANILAN ALGORİTMA

Ms CryptoApi'nin[12] sağladığı en temel kriptografik medodlar kullanılarak şu işlem adımları ile ETSİ uyumlu elektronik imza gerçekleştirilebilir. Şekil 2 de bu işlem adımları gösterilmektedir.

Değişkenleri tanıtlıp ilk değer atadıktan sonra kullanıcıya sertifika seçtirilir.

- Sertifika store açmak için *CertOpenSystemStore* kullanılır.
- Store'daki sertifikaları liste halinde gösterip kullanıcının seçmesine imkan tanımak için *CryptUIDlgSelectCertificateFromStore* kullanılır.

Seçilen sertifika için iptal kontrolü yapılır. Sertifika geçerliyse devam edilir.

Microsoft'un ekleyemediği *signingCertificate* attribute oluşturulur. Bu attribute RFC 2634'de [4] tanımlıdır.

- Sertifika icinden blob olarak issuer'i ve serial'i alınır.
- Blob halindeki issuerdan *GeneralNames* yapisi oluşturulur.
- Blob halindeki serial'dan *CertificateSerialNumber=INTEGER* yapisi oluşturulur.
- *IssuerSerial* yapisi oluşturulur.
- Hash'i hesaplamak ve Hash yapısını oluşturmak için *CryptAcquireContext*, *CryptCreateHash*, *CryptHashData*, *CryptGetHashParam*, *CryptDestroyHash*, *CryptReleaseContext* metodları kullanılır.
- Hash ve *IssuerSerial* kullanarak *ESSCertID* yapisi oluşturulur.
- *SigningCertificate* yapisi elde edilir.

İmza sonucunun kaç byte olduğunu belirlemek için *CryptSignMessage* kullanılır.

- *CryptSignMessage(&SigParams,false,1,MessageArray, MessageSizeArray,NULL, &DataSize)*

İmzayı atmak için *CryptSignMessage* kullanılır.

- *CryptSignMessage(&SigParams,false,1,MessageArray,MessageSizeArray,sonuc->pbData,&DataSize))*

Her iki işlem için *CryptSignMessage* metodu kullanılıyor fakat girilen parametreler nedeniyle birinde imza büyüklüğü alınırken diğerinde imza atılıyor.

A Survey of Related-Key Attacks on AES

Ali DOĞANAKSOY, Aslı DARBUKA, Dilek ÖZBERK, Neşe ÖZTOP, Fatih SULAK

Abstract—In this paper, a survey of the related-key attacks on AES is given. In related-key attack model, attacker is assumed to know the relations between the keys which are related to each other. Since this model is stronger than normal attack scenarios, the complexities are better. In this survey, related-key impossible differential attack, related-key square attack, related-key rectangle attack and related-key differential-linear attack are covered. None of the attacks is a real threat to AES and can only break reduced round versions of AES. Also, all complexities of the mentioned attacks are tabulated.

Keywords —AES, cryptanalysis, related-key attacks.

I. INTRODUCTION

Rijndael, also known as Advanced Encryption Standard (AES), is the most widely used block cipher in the world. It is designed by Rijmen and Daemen in 2000. It has a block length of 128 bits and key lengths of 128, 192 and 256 bits (corresponding versions are called AES-128, AES-192, and AES-256, respectively).

AES is a very simple substitution-permutation network (SPN) type block cipher. It operates on bytes. S -box which is based on the inverse operation in $GF(2^8)$ is the only nonlinear part of AES and for diffusion, shift row and mix column operations are used. Despite its simple structure, it is secure against the known attacks.

In this paper, we deal with the related-key attacks on AES. In section 2, related-key impossible differential attack is presented. Related-key square attack and related-key rectangle attack are given in section 3 and section 4. In section 5, related-key differential-linear attack is covered and finally we conclude the paper and give all the complexities in Table II.

Notation: Let x_i^I denote the input of the i^{th} round, x_i^S , x_i^R , x_i^M and x_i^O denote the intermediate values after the operations SubBytes (SB), ShiftRows (SR), MixColumns (MC), and AddRoundKey (AR) of the i^{th} round, respectively and KS denote the Key Schedule.

Let K_i denote the subkey in the i^{th} round, and the initial whitening subkey is K_w . In some cases, the order of the MixColumns and the AddRoundKey operation in the same round is changed, so the subkey K_i is changed with $W_i = MC^{-1}(K_i)$ and in this case, x_i^W denotes the intermediate value after the operation AddRoundKey before the MixColumn.

Let $(x_i)_{col\ k}$ denote the k^{th} column of x_i , where $k=0, 1, 2, 3$ and $(x_i)_j$ the j^{th} byte of x_i ($j=0, 1, \dots, 15$). Here, Column(0) includes bytes 0, 1, 2, 3 and Column(1) includes bytes 4, 5, 6, 7 etc.

Ali Doğanaksoy, Aslı Darbuka, Dilek Özberk, Neşe Öztıp and Fatih Sulak are with the Department of Cryptography, Middle East Technical University, Ankara, Türkiye e-mail: {aldoks, aslid, dilek, noztop, sulak}@metu.edu.tr.

II. RELATED-KEY IMPOSSIBLE DIFFERENTIAL CRYPTANALYSIS OF REDUCED-ROUND AES

In related-key attacks, the attacker observes possible weaknesses of the encryption function and the key schedule algorithms, then chooses a relation between keys to derive information about the unknown keys. Related-key differential attacks exploit the propagation of differences between two encryptions under two related keys. Impossible differential attacks use differential relations which hold with probability 0 to eliminate wrong keys leaving the right key candidate. The attack which combines these two techniques is called the related-key impossible differential attack.

The security of AES-192 against related key attacks has inspired much research because of being more susceptible to related key attacks than other key variants. The reason is that AES-192 has longer related key differentials since the diffusion of the key schedule is slower than in other versions. More specifically, if the expanded keys are thought as a sequence of words, then the key schedule of AES-192 applies a non-linear transformation once every six words, while the key schedules of AES-128 and AES-256 apply non-linear transformations once every four words. Therefore, in recent years, several related key attacks on AES have been presented. In 2003, Jakimoski and Desmedt proposed related key impossible differential attacks on 7 and 8-round AES-192 [1]. In 2006, Biham et al. mounted attacks on again 7 and 8-round AES-192 [2] following the work in [1] but with an improvement of the data and time complexities. In [3], Zhang et al. presented related-key impossible differential attacks different from the ones in [1] and [2], by choosing another key difference between the two related keys and starting the attack from the first round which improved the data and time complexities. Moreover, Zhang et al. made a security analysis of AES-256 against related-key impossible differential attack [4] and they introduced an attack on 7-round AES-256 and four attacks on 8-round AES-256. All of these attacks were built on a 5.5-round impossible differential. Therefore, we begin by giving this impossible differential in detail.

A. A 5.5-Round Related Key Impossible Differential of AES-192

A 5.5-round related-key impossible differential can be constructed as combining a 4.5-round related-key differential (with probability 1) with a 1-round related key differential (with probability 1) in opposite direction where the intermediate differences give rise to a contradiction.

Choose the difference between two related keys K and K^* as $((a,0,0,0), (0,0,0,0), (a,0,0,0), (0,0,0,0), (0,0,0,0), (0,0,0,0))$.

TABLE I
SUBKEY DIFFERENCES

Round(i)	$\Delta K_{i,Col(0)}$	$\Delta K_{i,Col(1)}$	$\Delta K_{i,Col(2)}$	$\Delta K_{i,Col(3)}$
0	(a,0,0,0)	(0,0,0,0)	(a,0,0,0)	(0,0,0,0)
1	(0,0,0,0)	(0,0,0,0)	(a,0,0,0)	(a,0,0,0)
2	(0,0,0,0)	(0,0,0,0)	(0,0,0,0)	(0,0,0,0)
3	(a,0,0,0)	(0,0,0,0)	(0,0,0,0)	(0,0,0,0)
4	(0,0,0,0)	(0,0,0,0)	(a,0,0,0)	(a,0,0,0)
5	(a,0,0,0)	(a,0,0,0)	(a,0,0,0)	(a,0,0,0)
6	(a,0,0,b)	(0,0,0,b)	(a,0,0,b)	(0,0,0,b)
7	(a,0,0,b)	(0,0,0,b)	(a,0,c,b)	(a,0,c,0)
8	(0,0,c,b)	(0,0,c,0)	(a,0,c,b)	(a,0,c,0)

Then, propagation of the subkey differences is given in Table I.

The first 4.5-round differential is built as follows: The input difference Δx_1^M is cancelled by AR of the first round, so the difference in all bytes of Δx_2^I becomes zero. This is preserved through SB, SR and MC of the second and the third rounds until adding the subkey difference ΔK_3 . Then, we get a non-zero value in the first byte of Δx_4^I . After MC of round 4, this difference diffuses to all column. Finally, after MC and AR of the fourth round, there will be non-zero differences in bytes (1,2,3,5,6,7).

The second differential ends after the sixth round with output difference Δx_6^O as shown in figure 1. Applying AR, MC^{-1} , SR^{-1} and SB^{-1} to this difference, we find out that bytes (1,6) of Δx_6^I have zero difference while Δx_5^O has non-zero differences in these bytes, this is a contradiction.

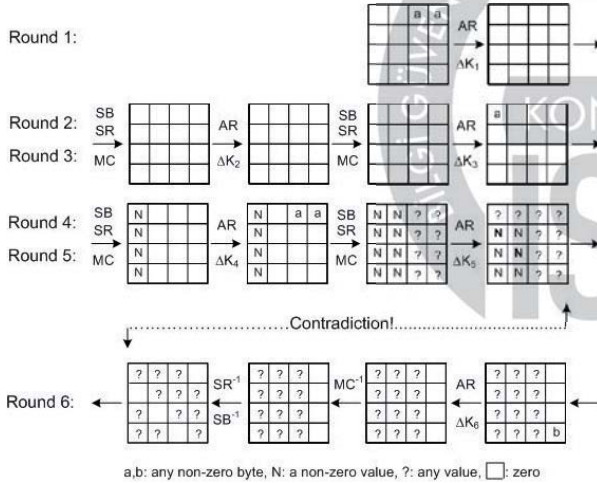


Fig. 1. 5.5-Round Related-Key Impossible Differential

B. A 7-Round Related-Key Impossible Differential Attack on AES-192

Main idea of this attack is applying the 5.5-round related key impossible differential given in figure 1 between the differences Δx_1^M and Δx_6^O , guessing some key bytes of the first and the last round for partial decryption, then eliminate all wrong keys using impossible differentials.

The attack procedure is as follows:

- Generate two sets S_1 and S_2 of m plaintexts such that for each plaintext pair $P_1 \in S_1$ and $P_2 \in S_2$, $P_1 \oplus P_2 = ((a, ?, ?, 0), (0, 0, ?, ?), (?, 0, 0, ?), (?, ?, 0, 0))$.
- Encrypt the set S_1 under key K and S_2 under key K^* and get the ciphertexts C_1 and C_2 .
- Store all the ciphertexts C_1 and $C_2^* = C_2 \oplus ((0, 0, 0, 0), (0, 0, 0, 0), (0, 0, 0, 0), (a, 0, 0, 0))$ in a hash table indexed by bytes 6,9,12.
- Guess the value of the subkey byte $(K_7)_3$ and decrypt the byte $(x_7^O)_3$ in all the ciphertexts to get the outputs of MC in the sixth round. Check for every C_1, C_2^* whether the difference in the corresponding byte is zero. If not, discard the pair C_1, C_2^* .
- For every remaining pair C_1, C_2^* , consider their plaintexts and use the precomputed hash table and the list of all 2^{64} possible values of the bytes (1,2,6,7,8,11,12,13) of K_0 to eliminate the wrong keys.

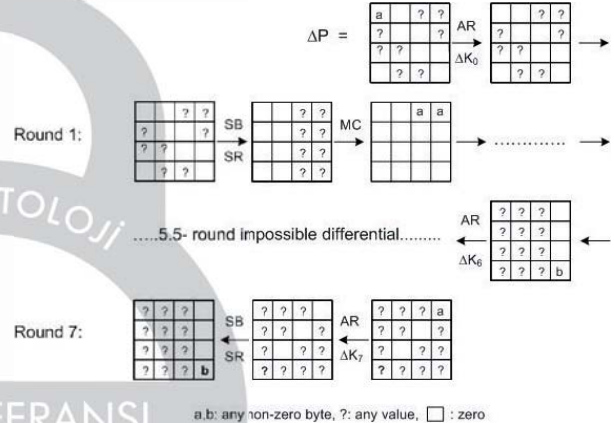


Fig. 2. 7-Round Related-Key Impossible Differential

Data complexity of this attack is 2^{52} chosen plaintexts, time complexity is 2^{80} encryptions, and the required memory is 2^{69} bytes.

For more details of the attack and the complexity analysis, we refer the reader to [3].

C. Extending 7-Round Attack to an 8-Round Attack

7-round attack can be extended to an 8-round attack as follows:

- Guess some bytes of the last round subkey K_8 .
- Partially decrypt these bytes in the last round so that we can obtain Δx_8^I .
- Check the difference in particular bytes of Δx_8^I . If that difference is not satisfied, discard the ciphertext pairs.
- For the remaining ciphertext pairs, apply the inverse of MC and guess some bytes of W_7 .
- Continue partial decryption and get Δx_6^O .
- Discard the wrong key guesses as in the 7-round attack.

In order to guess less subkey bytes, we interchange the order of MC and AR in the seventh round, so we change K_7 with W_7 .

In this attack, a data-time trade off can be performed by

guessing less bytes of the last round subkey K_8 which results in a decrease in the time complexity and an increase in the data complexity.

III. A 9-ROUND RELATED-KEY SQUARE ATTACK OF AES-256

A related-key square attack is a type of square attack that uses keys which are active in some particular bytes [5]. In [6], a related-key square attack on 9-round AES-256 is presented. The slowness of the diffusion of the key schedule helps to follow all the differences in round keys. In order to create a key difference pattern, any base key, denoted by L , is chosen first. Then, a set of 256 related keys, denoted by $L_0, L_1, \dots, L_{255}$ are constructed such that the difference $L_a \oplus L$ takes a nonzero value a in bytes 21, 25 and zero elsewhere. A total of 66 key bytes are computed by guessing just 27 bytes of the key. The key difference pattern is illustrated in figure 3. The dark grey bytes are the 27 bytes that will be guessed. The light grey bytes are the bytes that can be obtained by using the guessed bytes and the recurrence relationship between the expanded key bytes.

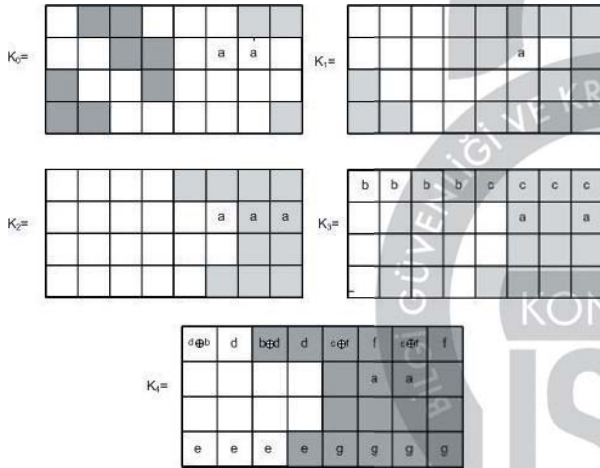


Fig. 3. Difference and Guessing Pattern in the Key of the 9-Round Attack

The b, c, d, e, f, g values mark outputs of non-linear S-box and all are known values for each given value of a . These values can be found gently using the key schedule. After guessing key, a plaintext is encrypted under each key and these plaintexts are chosen such that the corresponding states of them after the first round are all equal. It is observed that a single byte difference at the end of round 3 takes each value exactly once after 256 encryptions. This ensures that each byte of the output state of MC in round five takes all possible values. The key difference is a in bytes 5, 9 and 13 and zero elsewhere in the fifth round. So, the output of the fifth round takes all 256 values in every byte except the bytes 5, 9 and 13. The sixth round key takes value b in bytes 0, 4, 8 and 12. After computations, it is found that the sums of the values in bytes 13, 14 and 15 of the output in the sixth round over 256 values are zero. This is illustrated in figure 4. In figure 4, A denotes the bytes which are active, namely the bytes taking all values exactly once, $?$ denotes the

bytes that have unknown values and Z denotes the byte whose xor over all its values is zero.

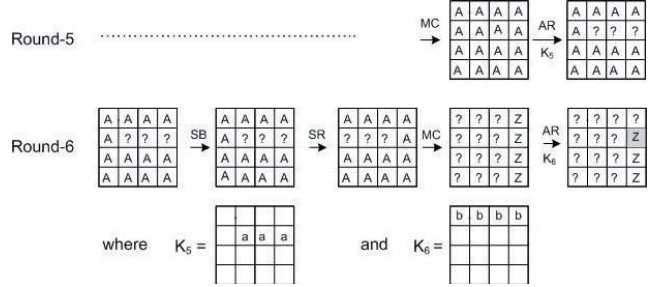


Fig. 4. Rounds 5-6 of the Attack

The attack is actualized at the end of the sixth round. At round 8, MC and AR are switched, so an equivalent key instead of the eighth round key is used in this round. The ninth round key is known because of the guesses of key bytes that is made before. Therefore, the output of AR in eighth round can be found by decrypting the ciphertexts. Then, the decryption is maintained by guessing 4 bytes of the equivalent key. Note that, several bytes of the original key bytes of the eighth round is known and this can be used to find the concerned key bytes of the equivalent key for the attack, because equivalent key is just result of an inverse MC on the original key. Now, investigating figures 4 and 5, the value of 13th byte shown as grey byte in figure 4 can be found.

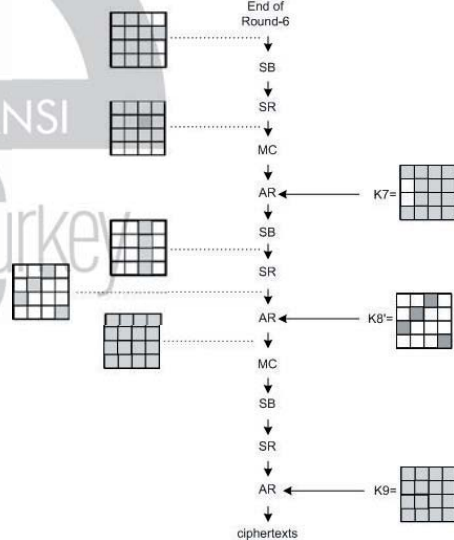


Fig. 5. Rounds 7-9 of the Attack

Finally, values of this byte are xored and checked whether the result is zero. If it is not zero, then the guesses are wrong. The complexity of the attack is 2^{248} and the number of chosen plaintexts used is 2^{72} .

A. An Improvement of the Attack

In order to improve this related-key square attack, the new technique so called "partial sums" which is described in the

previous sections of [6] is used. No guesses for the key are made in the first round, instead, all 2^{64} plaintexts are used for each of the keys and xored over all 2^{72} encryptions. The number of chosen plaintexts is increased to 2^{77} , namely 32 structures of 2^{72} texts, to identify the correct key uniquely. However, the complexity is reduced to $5 \cdot 2^{224}$ where multiplication with five is due to the fact that five of these structures are needed.

IV. RELATED-KEY RECTANGLE ATTACK ON REDUCED VERSIONS OF AES-192 AND AES-256

Up to now, related-key rectangle attacks have been applied to three versions of reduced round AES. The first attempt was made by J. Kim et al. and they attacked on 8-round AES-192 with four related keys. The attack given in [8] has $2^{86.5}$ data and $2^{86.5}$ time complexities. Then, a better attack was presented by Biham et al. [9] which is applied to 9-round AES-192 with 256 related-keys. This attack is different from the one given in [8] in a way that it uses more than one key difference in the differentials to make much better attacks. The attack needs 2^{87} related-key chosen plaintexts and has running time of 2^{125} encryptions. Furthermore, they attacked 10-round AES-256 with $2^{114.9}$ related-key chosen plaintexts encrypted under 256 related keys and $2^{171.8}$ time complexity. In 2007, the best known related-key rectangle attack was presented by J. Kim et al. [10]. Their attack reduces the complexity of the attacks [8] and [9]: for reduced AES-256 with 9 rounds, at the expense of decreasing number of attacked rounds from 10 to 9, they reduced the time and data complexities and the number of related keys required from 256 to 4. They also realized that the 9-round attack to AES-192 presented by Biham et al. has flaw in key guessing step and corrected time complexity as 2^{181} . Moreover, they attacked on 10-round AES-192 using 256 related keys with 2^{125} data complexity and 2^{182} time complexity and using 56 keys they made a data-time trade-off which reduces the data complexity to 2^{124} and increases the time complexity to 2^{183} . They also attacked to 9-round AES-256 and 10-round AES-256 with 4 and 64 related keys, respectively.

A. The Related-Key Rectangle Attack

The related-key rectangle attack introduced by J. Kim et al. [7] is a chosen plaintext attack based on two short related-key differentials with relatively high probabilities. The attack treats the cipher E as a cascade of two sub-ciphers E^0 and E^1 , that is $E = E^1 \circ E^0$. Assume that we have a related-key differential $\alpha \rightarrow \beta$ of E^0 with probability p and a related-key differential $\gamma \rightarrow \delta$ of E^1 with probability q . Using two related-key differentials, the related-key distinguisher can be described as follows:

- Take two randomly chosen plaintexts P and P' and obtain their corresponding ciphertexts $C = E_K(P)$ and $C' = E_{K'}(P')$.
- Form $P^* = P \oplus \alpha$ and $P'^* = P' \oplus \alpha$ and obtain their corresponding ciphertexts $C^* = E_{K^*}(P^*)$ and $C'^* = E_{K'^*}(P'^*)$, where $K^* = K \oplus \Delta K$, $K' = K \oplus \Delta K'$ and $K'^* =$

$K \oplus \Delta K \oplus \Delta K'$ for known key differences ΔK and $\Delta K'$.

- Check $C \oplus C' = \delta$ and $C^* \oplus C'^* = \delta$.

If a plaintext quartet (P, P^*, P', P'^*) satisfies the last δ test, we call such a quartet a *right quartet*. The probability P of the related-key distinguisher can be computed as follows: the probability that $I \oplus I^* = I' \oplus I'^* = \beta$ is about p^2 where $I = E_K^0(P)$, $I^* = E_{K^*}^0(P^*)$, $I' = E_{K'}^0(P')$ and $E_{K'^*}^0(P'^*)$. Since we choose P and P' randomly, the probability of $I \oplus I' = \gamma$ is expected to be 2^{-n} . These two above conditions imply the probability of $I^* \oplus I'^* = \gamma$ is 1. Moreover, the probability that $I \oplus I' = \gamma$ and $I^* \oplus I'^* = \gamma$ goes to $C \oplus C' = \delta$ and $C^* \oplus C'^* = \delta$ is q^2 . Therefore, the total probability becomes

$$\sum_{\beta, \gamma} p^2 \cdot 2^{-n} \cdot q^2 = \hat{p}^2 \cdot \hat{q}^2 \cdot 2^{-n}, \text{ where } \hat{p} = \sqrt{\sum_{\beta} p^2} \text{ and } \hat{q} = \sqrt{\sum_{\gamma} q^2}$$

Note that for a random permutation, the probability that δ test holds is 2^{-2n} . If the related-key distinguisher satisfies $\hat{p}^2 \cdot \hat{q}^2 \cdot 2^{-n} \geq 2^{-2n}$, that is $\hat{p} \cdot \hat{q} > 2^{-n/2}$, it can be used to distinguish E from a random cipher.

B. The Related-Key Rectangle Attack on 10-Round AES-192

8-Round Related-Key Rectangle Distinguisher:

The following two related-key truncated differentials as shown in figure 6 are constructed by exploiting the weakness of the key schedule of AES-192. The key scheduling algorithm of AES-192 propagates key differences slowly since the key schedule of AES-192 applies non-linear transformations once every six words which makes possible to find longer and better truncated differentials.

Let $E = E^b \circ E^0 \circ E^1 \circ E^f$ denote the 10 rounds of AES-192 where E^b is round 0 including the whitening addition key step and excluding the key addition step of round 0, E^0 is rounds 1-4 including the key addition step of round 0, E^1 is rounds 5-8 and E^f is round 9. Also in figure 6, the first related-key truncated differential is E^0 and the second one is E^1 , a is a fixed nonzero byte value, b and c are the output differences of S-box for the fixed nonzero input a and $*$ is a variable and unknown byte.

To construct an 8-round related-key rectangle distinguisher by using two related-key truncated differentials, the following three assumptions are made:

- 1) The key quartet (K, K^*, K', K'^*) satisfies $K \oplus K^* = K' \oplus K'^* = \Delta K$, and $K \oplus K' = K^* \oplus K'^* = \Delta K'$.
- 2) A plaintext quartet (P, P^*, P', P'^*) satisfies $P \oplus P^* = P' \oplus P'^* \in \Delta P$.
- 3) $E_K^b(P) \oplus E_{K^*}^b(P^*) = E_{K'}^b(P') \oplus E_{K'^*}^b(P'^*) = \Delta K_0$.

The probability of the 8-round related-key rectangle distinguisher is 2^{-231} and the computation of the probability is as follows:

- The probability of $x_5^I \oplus x_5^{*I} = x_5^{I'} \oplus x_5^{*I'}$ is about $(2^{-32} \cdot 2^{-7})^2 \cdot (2^7 - 2) \cdot 2^{32} + (2^{-32} \cdot 2^{-6})^2 \cdot 2^{32} \approx 2^{-39}$ where $x_5^I = E_K^0(E_K^b(P))$, $x_5^{*I} = E_{K^*}^0(E_{K^*}^b(P^*))$, $x_5^{I'} = E_{K'}^0(E_{K'}^b(P'))$ and $x_5^{*I'} = E_{K'^*}^0(E_{K'^*}^b(P'^*))$.
- The probability of $x_5^I \oplus x_5^{I'} = x_5^{*I} \oplus x_5^{*I'} \in \Delta x_5^{I'}$ is about 2^{-64} if the condition $x_5^I \oplus x_5^{*I} = x_5^{I'} \oplus x_5^{*I'}$ is satisfied.

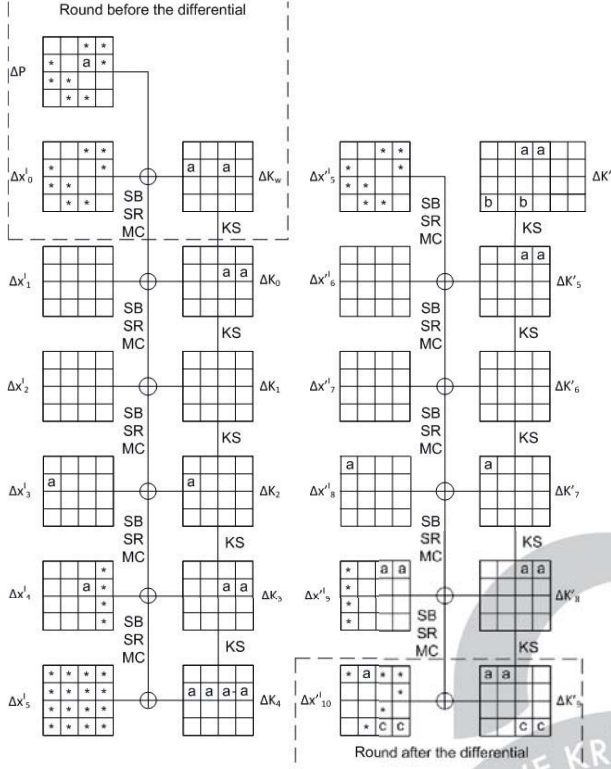


Fig. 6. The first figure is the first related-key truncated differential and the second figure is the second related-key truncated differential

- Let E^5 be the encryption function of round 5, the probability of $E_K^5(x_5^I) \oplus E_{K'}^5(x_5^{I'}) = 0$ is 2^{-64} and the probability of $E_{K^*}^5(x_5^{I'}) \oplus E_{K'^*}^5(x_5^{I'}) = 0$ is 2^{-64} if the condition $x_5^I \oplus x_5^{I'}$ and $x_5^{I'} \oplus x_5^{I'*} \in \Delta x_5^I$ is satisfied.
- Therefore, the probability of $E_K^1(x_5^I) \oplus E_{K'}^1(x_5^{I'})$, $E_{K^*}^1(x_5^{I'}) \oplus E_{K'^*}^1(x_5^{I'}) \in \Delta x_9^{II}$ is $2^{-39} \cdot 2^{-64} \cdot 2^{-64} \cdot 2^{-64} = 2^{-231}$.

C. Key Recovery Attack on 10-round AES-192

The aim of the attack is to capture 8 bytes of the whitening key quartet $(K_w, K_w^*, K_w', K_w^{**})$ and 6 bytes of the subkey quartet $(K_9, K_9^*, K_9', K_9^{**})$. These bytes correspond to * on ΔP and Δx_{10}^{II} . This attack needs 256 related keys to construct the difference $\Delta K'$ depicted in figure 6.

The attack algorithm can be summarized as follows:

- Choose 2^{54} structures of plaintexts which have fixed values in eight bytes, namely 0, 3, 4, 5, 9, 10, 14, 15 and obtain the corresponding ciphertexts under K . Then, form another structures by XORing difference a in byte 9 with these plaintexts and get their corresponding ciphertexts under K^* .
- Take 2^{54} structures of plaintexts which have fixed eight bytes listed in the previous step and encrypt them to get the corresponding ciphertexts under K' by guessing $\Delta K'$. Then, construct another structures by XORing difference a in byte 9 with these plaintexts and encrypt them under K'^* .

- Guess bytes, for the byte positions marked as *, of $(k_w, k_w^*, k_w', k_w^{**})$ and use third assumption and the difference Δx_{10}^{II} by making partial decryptions and encryptions, eliminate some wrong plaintext-ciphertext quartets which do not satisfy these two conditions.
- Guess 6 bytes of subkey quartet of round 9 and partially decrypt them one round to compare difference with Δx_9^{II} and ignore plaintext-ciphertext quartets that do not satisfy desired differences.
- If the remaining number of plaintext is more 16 then the guessed key quartet is the actual key quartet, if not, run all steps for the another key quartets.

This attack can be mounted with 2^{125} related-key chosen plaintexts and a running time of 2^{182} encryptions and with a success rate of 0.99. For further details of the attack algorithm one can see [10].

Furthermore, the attackers decrease the number of related keys from 256 to 64 by making a data-time trade-off that decrease the required number of plaintexts-ciphertexts to 2^{124} and increase the required time to 2^{183} encryptions.

V. RELATED-KEY DIFFERENTIAL-LINEAR CRYPTANALYSIS OF REDUCED-ROUND AES

Differential-linear cryptanalysis technique was first introduced by Langford and Hellman [11] which makes use of both differential and linear cryptanalysis. They have combined these two cryptanalysis methods in such a way that the differential part creates a linear approximation with probability 1. Then differential-linear cryptanalysis is unified with the idea of related-key which exploits the weaknesses of the key scheduling algorithm to mount better attacks. Related key impossible differential attacks and related key rectangle attacks are the most popular attacks on AES that have been presented recently. However, there was not any research result on the security of AES against differential-linear attack. In 2007, Zhang et al. proposed a related key differential-linear attack on reduced round AES-192 [12]. Since this attack was the first attempt using this technique, the results of the attacks are not better than the other related key attacks but improvements of these attacks can be made to get more desirable results. They have presented two different attacks on 7-round AES-192 and one attack on 8-round AES-192 using a 5-round related key differential-linear distinguisher. Now, we begin by giving this 5-round distinguisher.

A. A 5-Round Related Key Differential-Linear Distinguisher

A 5-round related key differential-linear distinguisher is constructed as combining a 4-round related-key differential with a 1-round related-key linear approximation where the differential part creates the linear approximation with probability 1. The fact that the equality of the coefficients in two bytes of one column of the MDS matrix constitutes the main point in using this distinguisher.

Choose the difference between two related keys K and K^* as $((0,0,0,0), (0,0,0,0), (a,0,0,0), (a,0,0,0), (0,0,0,0), (0,0,0,0))$.

The first 4-round differential is built as follows: Choosing the plaintext difference

$((0, 0, 0, 0), (0, 0, 0, 0), (a, 0, 0, 0), (a, 0, 0, 0))$, the input difference Δx_1^I is cancelled by the whitening subkey difference, so the difference in all bytes of Δx_1^I becomes zero. This is preserved through SB, SR and MC in the first and the second rounds until adding the subkey difference ΔK_2 . Then, we get a non-zero value in the first byte of Δx_3^I . After the MC in round 3, this difference diffuses to all column. Let's call the non-zero byte position zero of the fourth round as δ . Then, after MC, the first column will be $(02 \cdot \delta, \delta, \delta, 03 \cdot \delta)$. Finally, applying the key addition, we get equal differences in byte 1 and 2 of Δx_4^O . Therefore, $\Delta(x_4^O)_1 = \Delta(x_4^O)_2 \neq 0$ holds with probability 1. In the following SB in the fifth round, a linear approximation is used. We have

$$(x_4^O)_1 \oplus (x_4^O)_2 = (x_4^O)_1 \oplus (x_4^O)_2 \neq 0$$

For every possible 8-bit linear mask λ , the equation

$$\lambda \cdot \{(x_5^S)_1 \oplus (x_5^S)_2 \oplus (x_5^S)_3 \oplus (x_5^S)_4\} = 0$$

is satisfied with a bias of 2^{-9} .

Since the value of the subkeys keep unchanged in the attacks, after SR and AR in the fifth round, finally we obtain the following 5-round differential-linear distinguisher with a bias of 2^{-9} :

$$\lambda \cdot \{\Delta(x_5^W)_{13} \oplus \Delta(x_5^W)_{10}\} = 0$$

B. A 7-Round Related Key Differential-Linear Attack on AES-192

Main idea of this attack is applying the 5-round related-key differential-linear distinguisher given above starting from the first round, guessing some key bytes of the sixth and the seventh round for partial decryption, then using the linear approximation to find the key.

The attack procedure is as follows:

- Construct m plaintext pairs (P, P^*) such that $P \oplus P^* = ((0, 0, 0, 0), (0, 0, 0, 0), (a, 0, 0, 0), (a, 0, 0, 0))$.
- Encrypt the plaintexts P 's under key K and P^* 's under key K^* and get the ciphertexts.
- Initialize an array of 2^{160} counters to zeros.
- Guess bytes in positions 8, 9, 12, 15 of W_6 and all bytes of K_7 . Then, for each ciphertext pair, decrypt to get two bytes $(x_5^W)_{10}$ and $(x_5^W)_{13}$ and check whether $\lambda \cdot \{\Delta(x_5^W)_{10} \oplus \Delta(x_5^W)_{13}\} = 0$ is satisfied, where λ is fixed. If this equation holds, increment the counter of the array.
- If $|T_{max} - m/2| > |T_{min} - m/2|$, then adopt the key candidate corresponding to T_{max} where T_{max} is the highest entry. Otherwise, adopt the key candidate corresponding to T_{min} where T_{min} is the lowest entry.

Data complexity of this attack is 2^{22} chosen plaintexts and the time complexity is 2^{187} encryptions.

VI. CONCLUSION

In this paper, we try to cover all related-key attacks on AES. In this attack scenario, the attacker is assumed to choose keys which are related to each other. Because of

this strong assumption, the number of rounds for which an academic attack is possible is larger than normal attacks. The complexities of the attacks are given in Table II. None of the attacks given in this paper is a real threat to full round AES.

TABLE II
COMPARISON OF ATTACK COMPLEXITIES

AES	Paper	Rou	Type	Data	Time	Memory
192	[2]	7	RK-ImpDif	2^{56}	2^{94}	2^{69}
	[12]	7	RK-DifLin	2^{22}	2^{187}	-
	[3]	7	RK-ImpDif	2^{52}	2^{80}	2^{69}
	[8]	8	RK-Rect	$2^{86.5}$	$2^{86.5}$	-
	[12]	8	RK-DifLin	2^{118}	2^{165}	-
	[3]	8	RK-ImpDif	$2^{64.5}$	2^{177}	2^{69}
	[9]	9*	RK-Rect	2^{85}	2^{182}	-
	[10]	10	RK-Rect	2^{125}	2^{182}	-
	[10]	10	RK-Rect	2^{124}	2^{183}	-
	[13]	8	RK-ImpBoo	$2^{122.4}$	2^{160}	-
256	[4]	8	RK-ImpDif	2^{112}	2^{143}	-
	[6]	9	RK-Squ	2^{85}	2^{224}	-
	[9]	9	RK-Rect	2^{99}	2^{120}	-
	[13]	9	RK-ImpBoo	$2^{122.8}$	$2^{242.5}$	-
	[10]	10	RK-Rect	$2^{113.9}$	$2^{172.8}$	-

*corrected complexity

REFERENCES

- [1] G. Jakimoski, Y. Desmedt, *Related-Key Differential Cryptanalysis of 192-bit Key AES Variants*, SAC 2003, LNCS 3006, pp. 208-221, Springer-Verlag, 2004.
- [2] E. Biham, O. Dunkelman, N. Keller, *Related-Key Impossible Differential Attacks on 8-round AES-192*, CT-RSA 2006, LNCS 3860, pp. 39-49, Springer-Verlag, 2006.
- [3] W. Zhang, W. Wu, L. Zhang, D. Feng, *Improved Related-Key Impossible Differential Attacks on Reduced-Round AES-192*, SAC 2006, LNCS 4356, pp. 15-27, Springer-Berlin, 2007.
- [4] W. Zhang, W. Wu, L. Zhang, *Related-Key Impossible Differential Attacks on Reduced-Round AES-256*.
- [5] E. Biham, *New Types of Cryptanalytic Attacks Using Related Keys*, Advances in Cryptology-EUROCRYPT'93, volume 765 of Lecture Notes in Computer Science, pages 398-409. Springer-Verlag 1993
- [6] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner and D. Whiting, *Improved Cryptanalysis of Rijndael*, Fast Software Encryption 2000, volume 1978 of Lecture Notes in Computer Science, pages 213-230, Springer-Verlag 2001
- [7] J. Kim, G. Kim, S. Hong, S. Lee and D. Hong, *The Related-Key Rectangle Attack-Application to SHACAL-1*, Proceedings of International Conference on Information Security and Privacy 2004, LNCS vol. 3108, pp. 123-136, Springer Verlag, 2004.
- [8] S. Hong, J. Kim, S. Lee, and B. Preneel, *Related-Key Rectangle Attacks on Reduced Versions of SHACAL-1 and AES-192*, Proceedings of Fast Software Encryption 2005, LNCS vol. 3557, pp. 368-383, Springer-Verlag, 2005.
- [9] E. Biham, O. Dunkelman, and N. Keller, *A Related-Key Boomerang and Rectangle Attacks*, Advances in Cryptology - Proceedings of EUROCRYPT 2005, LNCS vol. 3494, pp.507-525, Springer-Verlag, 2005.
- [10] J. Kim, S. Hong and B. Preneel, *Related-Key Rectangle Attacks on Reduced AES-192 and AES-256*, FSE'07, LNCS vol. 4593, pp.225-241, Springer-Verlag, 2007.
- [11] S.K. Langford, M.E. Hellman, *Differential-Linear Cryptanalysis*, CRYPTO 94, LNCS vol.839, pp.17-25, Springer,Heidelberg (1994).
- [12] W. Zhang, L. Zhang, W. Wu, D. Feng, *Related-Key Differential-Linear Attacks on Reduced AES-192*, INDOCRYPT 2007, LNCS 4859, pp.73-85, Springer,Heidelberg (2007).
- [13] J. Lu, *Cryptanalysis of Block Ciphers* Ph.D. Thesis

A Survey of the Attacks on AES

Ali DOĞANAKSOY, Aslı DARBUKA, Dilek ÖZBERK, Neşe ÖZTOP, Fatih SULAK

Abstract—In this paper, a survey of the attacks on AES is given. The aim of the paper is to make a collection of the academic cryptanalysis of 3 different variants of AES. In this survey, side-channel attacks and related-key attacks are not covered. Most efficient attacks such as square attack, impossible differential attack, boomerang attack, algebraic attack and meet in the middle attack are given. All attacks can only break reduced variants of AES. Also, complexities of the mentioned attacks are tabulated.

Keywords —AES, cryptanalysis, square attack, impossible differential attack, boomerang attack, algebraic attack, meet in the middle attack.

I. INTRODUCTION

After the cryptanalysis of Data Encryption Standard (DES), NIST made a competition for the new standard for block ciphers. Rijndael, a block cipher designed by Rijmen and Daemen, won the competition and was adopted as Advanced Encryption Standard (AES) in 2000. It is the most widely used block cipher in the world.

AES has a block length of 128 bits and 3 different key sizes; 128 bits (AES-128), 192 bits (AES-192) and 256 bits (AES-256). Since the most powerful attacks for block ciphers are differential and linear cryptanalysis, AES is designed to be provably secure against these attacks.

AES is a very simple substitution permutation network (SPN) type block cipher and operates on bytes. S -box which is based on the inverse operation in $GF(2^8)$ is the only nonlinear part of AES and for diffusion, shift row and mix column operations are used. Despite its simple structure, it is secure against known attacks.

In this paper, we collect all important attacks on AES. All of the attacks are for reduced round versions of AES and complexities are not realistic. Due to space limitations, we omit the description of AES. In section 2, square attack is given, in section 3, impossible differential attack on AES is presented. Boomerang attack is presented in section 4. Section 5 is for algebraic attack and in section 6, meet in the middle attack is given. After that, we conclude the paper and give all the complexities in Table I.

Notation: Let SB, SR, MC and AR denote the operations SubBytes, ShiftRows, MixColumns, and AddRoundKey, respectively.

Let K_i denote the subkey in the i^{th} round, and K_w denote the initial whitening subkey. In some cases, the order of the MixColumns and the AddRoundKey operations in the same round is changed so, the subkey K_i is changed with

Ali Doğanaksoy, Aslı Darbuka, Dilek Özberk, Neşe Öztıp and Fatih Sulak are with the Department of Cryptography, Middle East Technical University, Ankara, Türkiye e-mail: {aldoks, aslid, dilek, noztop, sulak}@metu.edu.tr.

$$W_i = MC^{-1}(K_i)$$

Let $(x_i)_{col\ k}$ denote the k^{th} column of x_i , where $k=0,1,2,3$ and $(x_i)_j$ is the j^{th} byte of x_i ($j=0,1,\dots,15$). Here, Column(0) includes bytes 0,1,2,3 and Column(1) includes bytes 4,5,6,7 etc.

II. SQUARE ATTACK ON REDUCED-ROUND AES

Square attack is a chosen plaintext attack invented by Lars Knudsen particularly for breaking substitution-permutation network cryptosystems. It was originally applied to the block cipher Square [1], so named as Square attack. The attacker uses complete sets of carefully chosen plaintexts and the concept of multisets, where a multiset is a group of values which can appear more than once. In the original proposal of AES [2], a square attack on 4-round AES-128 and its extension up to 6 rounds are presented. Then, this attack is applied to AES-192 and AES-256. Moreover, a 7-round attack on AES for all key sizes is introduced. However, exhaustive search is much faster than the 7-round attacks on AES-128 and AES-192 [3]. So, they are impractical. Lastly, the attacks presented in [2] and [3] are further improved and 8-round attacks on AES-192 and AES-256 are given in [4].

A. A 3-Round Distinguisher of AES-128

To build a 3-round distinguisher, a Λ -set, which is defined as a collection of 256 states that differ in only one byte and equal in all the other bytes is constructed. The byte which takes all 256 values is called an active byte. To see the attack in a more clear way, consider a Λ -set in which only the first byte is active and all the other bytes take a constant value. One should understand the effects of round transformations on the sets of bytes to follow the steps of the attack. In the first round, the input of MC is again a Λ -set. Since SB is bijective, it leaves the types of sets of bytes unchanged. Also note that SR does not have an effect on the values of bits in the bytes. So, it does not change the type of the sets of bytes. Then, MC converts all the bytes of the first column into active bytes and hence, after one round encryption, the bytes in the first column take all 256 values, while the other 12 bytes take constant values. In the second round, the active bytes in the first column are diffused by SR so that all columns include one active byte. Then, the active bytes of these columns spread over all the bytes of the state by MC. Therefore, each byte of the input of the third round is active and this is also the case after the SB and SR of this round. Now, the sum of all bytes is zero because they take all 256 encryptions. Since MC and AR are linear transformations, the sum of each byte at the end of round three is zero. So, a 3-round distinguisher is constructed. These are illustrated in figure 1. A denotes the active bytes, C

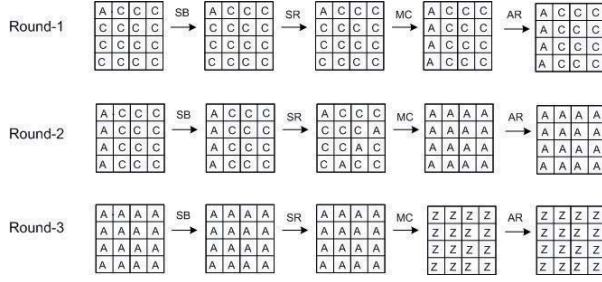


Fig. 1. A 3-round distinguisher for AES-128

denotes the bytes that take all constant values and Z denotes the bytes whose sum over all 256 encryptions is zero.

B. The Basic 4-Round Attack on Reduced-Round AES-128

The 4-round attack in [2] is based on the 3-round distinguisher which is described in the previous section and goes as follows:

For the attack, it is desired to compute a particular byte at the end of round 3. So, start decryption from round 4 by guessing a key byte corresponding to that particular byte. Then, add this key byte to the corresponding byte of the 256 ciphertexts one by one. Note that the last round, namely the fourth round, does not include MC and SR does not have an effect on the sum of the bytes. Therefore, continue with going backwards through the S-box. Then, check if the sum of all the decrypted values of this byte which corresponds to the output of the third round equals to zero or not. If it is not zero, then conclude that the guessed key byte is wrong. This can be achieved for finding other bytes of the key. This 4-round attack uses 2^9 plaintexts and their corresponding ciphertexts. The memory used is negligible.

C. A 6-Round Attack on AES-128

The 4-round attack is extended by first adding one round to the end of the cipher. The ciphertexts are partially decrypted up to end of round three by guessing the value of four bytes of the fifth round key and one byte of the fourth round key. Then, as in the previous attack, the values of the particular byte are summed together to check if the sum is zero. Number of required plaintexts is 2^{11} and number of ciphertext executions is 2^{40} since 40 key bits are guessed. Then, add one more round to the beginning. The output of this additional round should be a Λ -set in order to apply the basic 4-round attack after the first round. So, the output of MC in the first round has one active byte. This byte depends on four bytes of the plaintext and four bytes of the round key. A set of 2^{32} plaintexts are constructed by taking all possibilities of the four bytes which affect the active byte of the input of the second round. Then, a set of 256 plaintexts can be selected which result in a Λ -set in the second round by using the 2^{32} plaintexts and making an assumption for the value of the 4 relevant bytes of the first round key. This 6-round attack requires 2^{32} plaintexts and uses 2^{72} ciphertext executions. The memory used is 2^{32} .

D. Improvements of the 6-Round Attack

The 6-round attack presented in the original proposal is improved in [3] and [4]. First, the 6-round attack is adapted to AES-192 and AES-256 [3]. The writer takes the advantage of changing the order of round transformations and dependencies between the expanded key bytes. The key addition is achieved before SR. In this addition, a key which is equivalent to the actual round key is used. This attack uses 2^{32} chosen plaintexts and the time complexity is 2^{80} . In [4], an improved Square attack on 6-round AES suitable for all key sizes is described. Different from the previous attacks, this attack uses a new technique called ‘partial sum’ and all the 2^{32} chosen plaintexts, guesses just five bytes of the round keys at the last two rounds instead of guessing four round key bytes at the beginning. 2^{32} ciphertexts are partially decrypted two rounds by guessing one byte of the fifth round and four bytes of the sixth round. Then, the single byte determined at the end of decryption is summed over all ciphertexts. Now, this sum can be written in this way:

$$\sum_i S^{-1}[S_0[c_{i,0} \oplus k_0] \oplus S_1[c_{i,1} \oplus k_1] \oplus S_2[c_{i,2} \oplus k_2] \oplus S_3[c_{i,3} \oplus k_3]]$$

where S_i , $i \in \{0, 1, 2, 3\}$, are bijective S-boxes such that each one is composed of an inverse AES S-box which is followed by a multiplication with a field element from the inverse MDS matrix, $c_{i,j}$ is the j^{th} attacked byte of the i^{th} ciphertext, and k_i , $i \in \{0, 1, 2, 3\}$ denote the five guessed key bytes.

This sum is organised by introducing the ‘partial sum’ in a more effective way. For each k , a partial sum is defined as;

$$x_k := \sum_{j=0}^k S_j[c_j \oplus k_j]$$

here the subscript i of $c_{i,j}$ is not used since it is not considered about a particular text. The desired sum is computed by using the map $(c_0, c_1, c_2, c_3) \rightarrow (x_k, c_{k+1}, \dots, c_3)$ which is obtained from the partial sum and counting on some particular images of that map by guessing the stated key bytes. The complexity for this 6-round attack is 2^{44} which shows the attack was improved vigorously.

E. 7-Round and 8-Round Attacks on AES-192 and AES-256

The 6-round attack presented in the proposal can be extended to 7-round AES-192 and AES-256 [3]. It is similar to 6-round attack, but this time the attacker simply starts decryption from the seventh round by guessing all bytes of the last round key. Naively, this causes guessing 128 more key bits. However, since there are dependencies between the expanded key bytes, the complexity of the attack is 2^{176} for AES-192 and 2^{192} for AES-256. In [4], two improvements are made for this 7-round attack. First improvement uses the new technique partial sum. This new technique helps to save work if there are more ciphertexts than possible values for the intermediate result. For AES-192, the guesses of the last round key give four key bytes in round 6 and one key byte in round 5. Then, using the partial sum technique, each structure is reduced to 2^{24} counters after guessing the last round key. This can be done for each of the 128 key bits guesses in about 2^{32} memory lookups by using some precomputed tables. Overall cost of the attack is in order of 2^{163} S-box lookups because there are three phases

each of which costs 2^{160} . This overall cost is approximated with 2^{155} trial encryptions. For AES-256, knowing the last round key does not provide any information about the sixth round key but gives most of the fifth round key. After guessing the last round key, the four bytes are computed for each of the 2^{32} texts for a total cost of 2^{160} lookups. Each of the next phases has cost of 2^{176} . So, the cost per structure is 2^{178} lookups, namely about 2^{170} trial encryptions. Since five structures are used, the overall complexity is 2^{172} . Then, a second improvement is made by introducing a new concept, "herd". The attacker focuses on a particular byte in round 1 after MC and fixes a value on this byte. Then, a set of 2^{120} encryptions are made. This set consists of a list of 2^{88} packs where each pack contains 2^{24} groups of 2^8 encryptions varying in a single byte of the output of MC in round 2. This structure of 2^{120} encryptions is called a herd. Using this concept and some properties of the cipher, a second improvement for the 7-round attack can be made. By this improvement, one can break all key sizes with lower overall complexity but this requires the entire codebook of texts. Using these improvements, an 8-round attack can be mounted faster than exhaustive search. For AES-256, 2^{204} and for AES-192, 2^{188} work is needed. However, since again one needs the entire codebook of texts ($2^{128} - 2^{119}$ texts), the attack is impractical.

III. IMPOSSIBLE DIFFERENTIAL CRYPTANALYSIS OF REDUCED-ROUND AES

Impossible differential cryptanalysis exploits differentials that hold with probability 0 (impossible differentials) to eliminate the wrong keys and leave the right key candidate. Up to now, several impossible differential attacks on AES have been proposed. In 2000, Biham and Keller presented an attack on 5-round AES-128 using a 4-round impossible differential which is the first impossible differential attack on AES [5]. The attack eliminates wrong keys of the first round by showing that the impossible differential property holds in the last four rounds. In [6], this impossible differential attack was expanded to six rounds by using the same 4-round impossible differential. They put this impossible differential in the middle of six rounds and covered some bits of the first and last round's subkeys. Both in [5] and [6], the attacks were applied to AES-128 and based on the weaknesses which results from the characteristic of the optimal linear layer. These attacks are chosen plaintext attacks and they are independent of the specific choice of S-box, the multiplication polynomial of MC and the key schedule. Therefore, the same attacks in [5] and [6] can also be applied to AES-192 and AES-256. However, in [9], R.C.-W.Phan proposed an impossible differential attack on 7-round AES-192 and AES-256 which works by exploiting the weaknesses in the AES key schedule and improves the data and time complexities significantly. In 2007, Zhang et al. presented some new results on impossible differential cryptanalysis of AES. They introduced new attacks on 6-round AES whose complexity is much lower than that in [6]. Moreover, they extended the attack to both 7-round (which can be applied to all key variants of AES) and 8-round AES-256 and made an improvement of the 7-round attack on AES-192 which was given in [9]. Also again in 2007, Chen et al.

presented two methods of impossible differential cryptanalysis of 7-round AES-192 and 8-round AES-256 combined with time-memory trade off by exploiting weaknesses in their key schedule [12]. Complexities of their attacks are slightly better than that of [10]. However, since the attacks given by Zhang et al. [10] can be applicable to all key variants of AES and we do not want to go into the details of the AES key schedule, in this paper we will deal with the attacks given in [10]. In [7], Phan and Siddiqi proved that there exists no impossible differential greater than four rounds that can be constructed with the miss-in-the-middle technique. In all of the above attacks, the same impossible differential property is used, so it is better to give these 4-round impossible differentials at first.

A. 4-Round Impossible Differentials of AES

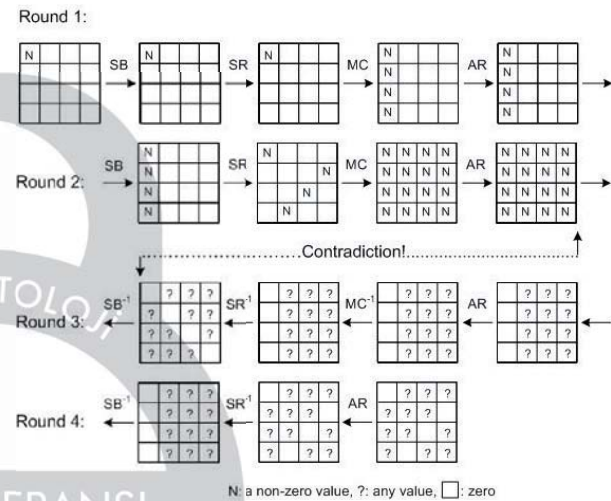


Fig. 2. A 4-Round Impossible Differential of AES

4-round impossible differentials are constructed as combining two 2-round probability-1 differentials in opposite direction where the intermediate differences induce a contradiction. This 4-round impossible differential states that given a pair of plaintexts which are equal in all bytes except one, then the ciphertexts after four rounds can not be equal in any of the following combination of impossible byte positions: (0,7,10,13), (1,4,11,14), (2,5,8,15) nor (3,6,9,12). This can be explained as follows: The difference before the first MC is in one byte, it diffuses to one column after MC. In the second round, after SR, every column has a difference in different bytes; when the second MC applied, the data differs in all bytes. On the other hand, if the ciphertexts are equal in one of the four impossible combinations of bytes, then before SR in the fourth round, the data is equal in one column and so is after SR in the third round. When SR^{-1} and then SB^{-1} are performed, the data is equal in four different bytes. This contradicts with the fact that the data differs in all bytes after the second MC.

B. An Impossible Differential Attack on 6-Round AES

Main idea of this attack is applying the 4-round impossible differential given in figure 2 between the second and the fifth

round, guessing some key bytes of the first and the last round for partial decryption, then eliminating all wrong keys by using impossible differentials. Illustration of the 6-round attack in which the prob. means that the probability is different from 1, is given in figure 3.

The attack procedure is as follows:

- Choose a set of 2^{32} plaintexts which have all different values in bytes (0,5,10,15). Generate n such structures.
- Choose the plaintext pairs whose ciphertext pairs have zero difference in all but the two bytes (3,6).
- Guess the value of the subkey bytes $(K_6)_3, (K_6)_6$ and partially decrypt these ciphertext pairs in order to get the outputs of the fifth round.
- Check whether the difference in at least one of the four 4-byte sets is zero where the four sets are (0,7,10,13), (1,4,11,14), (2,5,8,15) and (3,6,9,12). If not, discard the pairs.
- For every remaining ciphertext pair, consider their plaintexts and using the precomputed hash table and the list of all 2^{32} possible values of the bytes (0,5,10,15) of K_0 get rid of the wrong keys.

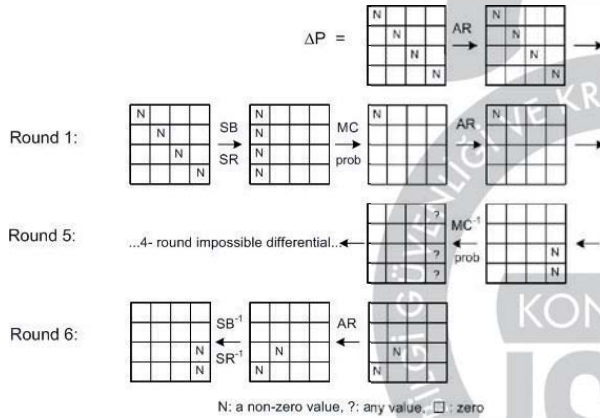


Fig. 3. Impossible Differential Cryptanalysis of 6-round AES

Data complexity of this attack is $2^{114.5}$ chosen plaintexts, time complexity is 2^{50} encryptions, and the required memory is 2^{45} bytes. In this attack, a data-time trade off can be done by guessing more bytes of subkey K_6 so that after partial decryption the number of nonzero bytes in the output of the fifth round reach the most possible. This trade-off reduces the data complexity to $2^{75.5}$ chosen plaintexts and increases the time complexity to 2^{104} encryptions.

C. Extending 6-round attack to 7-round

The above attack can be improved to attack 7-round AES. The main idea is guessing some bytes of the last round subkey K_7 , decrypt the last round and apply the 6-round attack as described above. In this extension, different from the 6-round attack, the order of MC and AR in the fifth and sixth rounds is changed in order to guess less key material and the subkeys K_5 and K_6 are replaced with equivalent subkeys. Data complexity of this attack is $2^{115.5}$ chosen plaintexts, time

complexity is 2^{119} encryptions, and the required memory is 2^{45} bytes.

Note that, these two attacks are applicable to all key variants of AES and can be improved to attack 8-round AES-256.

IV. THE BOOMERANG ATTACK ON 5 AND 6-ROUND REDUCED AES-128

A. Overview of the Boomerang Attack

The Boomerang attack introduced in 1999 by Wagner [13] is a chosen plaintext-adaptive chosen ciphertext attack based on differential cryptanalysis. The attack treats the block cipher as a cascade of two sub-ciphers which have short, high probability differentials and combines these two differentials to make a successful attack on the given cipher. However, the boomerang attack has a strong assumption states that in order to attack a cipher, the attacker should have decryption box of the cipher besides the encryption box and this assumption makes this attack unrealistic. Furthermore, the boomerang attack can also be performed by using truncated differentials instead of using conventional differentials.

B. The Boomerang Attack on 5 and 6-Round Reduced AES-128

The attack presented by A. Biryukov [14] is a generic method to attack 5 and 6-round substitution-permutation networks (SPNs). In this study, the boomerang distinguisher is constructed by exploiting incomplete diffusion property of SPNs (including AES), not the properties of S-boxes or other components of the cipher. This attack is better than square attack in terms of speed, however, it has much more data complexity than square attack.

C. Attacking to 5-Round AES-128

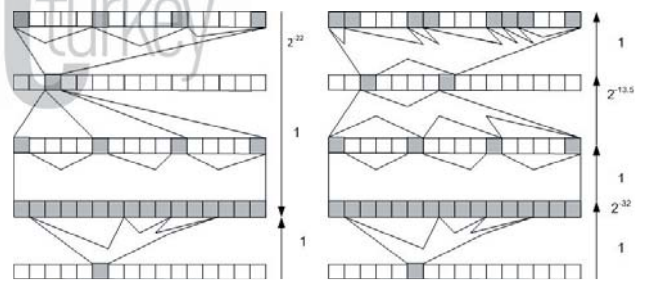


Fig. 4. The Boomerang Quartet for AES Reduced to 5-Rounds

Truncated differentials are used in the construction of the boomerang distinguisher. (For further details about the construction of the boomerang distinguisher, see [14]). The probability of the above boomerang distinguisher is $2^{-22} \cdot 2^{-32} \cdot 2^{-13.5} = 2^{-67.5}$.

The attack algorithm goes as follows:

- Choose a pool of 2^{32} plaintexts P_i which have all possible values in the four bytes depicted in figure 4 and find their corresponding ciphertexts C_i .

- Construct a pool of ciphertexts C_i^* which have Δ difference between C_i , i.e. $C_i^* = C_i \oplus \Delta$, Δ is a one-byte difference, and find their corresponding plaintexts P_i^* .
- Choose the pairs P_i^* and P_j^* which have non-zero differences in eight bytes.
- For each quartet P_i, P_j, P_i^* and P_j^* that pass third stage, guess 32-bit of the first round subkey corresponds to non-constant bytes.

The attack needs 2^6 pools of plaintexts, that is, in total 2^{38} chosen plaintexts and adaptively chosen ciphertexts. It necessitates 2^{39} running time of encryptions and 2^{36} bytes for the memory required.

In addition, by using the same boomerang distinguisher, this attack can be extended by adding one round at the bottom to attack 6-round reduced AES-128. In this way, by guessing extra 32-bit of the sixth round subkey, the attack on 6-round reduced AES-128 can be mounted with 2^{71} data and time complexities.

V. ALGEBRAIC ATTACK

Algebraic attack uses the algebraic structure of the cipher. In most of the block ciphers only nonlinear part is S -box. Algebraic attack uses this property and writes S -box as a Boolean function. If the degree of this function is low (2 for example), then one can rename the quadratic terms as other unknowns and try to solve this huge number of linear equations using mathematical methods, such as Gauss elimination. Actually algebraic attacks depends on algebraic structure of S -boxes, not the structure of the cipher. AES also has only nonlinear part as its S -box. However, since this S -box is based on inverse operation, algebraic degree is 254 in $\text{GF}(2^8)$. Assume that S -box has input $x_1, x_2, \dots, x_8$ and output $y_1, y_2, \dots, y_8$. y_i has high algebraic degree in the x_i , but there are other implicit multivariate equations of the form $P(x_1, \dots, x_8, y_1, \dots, y_8)$ that are for low algebraic degree $d \leq 2$. Assume that the number of such equations is r and t is the number of monomials that appear in these equations. In general, t is around $\binom{s}{d}$. If t is very low, then we say that the equations are sparse. Also, if $r = s$, then equations give enough information about the S -box. However, if $r \gg s$, then we say that the system is overdefined. In [16], a method for representing AES-128 with 8000 quadratic equations and 1600 variables is presented. The problem is solving multivariate quadratic equations which is known to be NP-hard. The most obvious way is to use linearization and eXtended Linearization (XL) with Gauss elimination. Using this method these equations can be solved in 2^{330} time. In [16], the authors show that if the MQ is sparse it is easy to solve and present a new method called eXtended Sparse Linearization (XSL). In normal XL method, all equations are multiplied by all possible monomials of some degree $D-2$, but in XSL only carefully chosen monomials are multiplied. However, for AES no results better than 2^{256} is found. Still, algebraic analysis of AES is a hot topic and researchers are trying to combine algebraic attacks with different type of attacks.

VI. MEET IN THE MIDDLE ATTACK ON REDUCED ROUND OF AES

In square attack, using 3-round distinguisher, one can attack to four rounds then, extend this attack to six rounds. Due to the special structure of AES, searching for more square like properties is essential.

A. 4-Round Distinguisher

In [15], Gilbert and Minier presented a 4-round distinguisher. By considering how plaintext changes over four rounds, they observed that in a set of 256 plaintexts with only the first byte is active (takes all possible values) and other bytes are passive, after four rounds the first byte is determined by nine fixed 1-byte parameters.

Gilbert and Minier also observed that four of these constant bytes depend on the values in the first column, but four of them are independent of these values. Using this information they form a pool of 2^{16} plaintexts where the values are given randomly to the first column and the other columns are fixed. Using birthday paradox, a collision will be found with high probability and this distinguishing property is used to attack AES up to seven rounds.

B. 5-Round Distinguisher

Demirci and Selçuk improved this attack [17]. They expanded the attack one more round and under the same assumptions of [15], they observed that after five rounds, the first byte depends on 25 fixed 1-byte parameters instead of 36. In order to make an exhaustive search on these bytes, 2^{200} time complexity is needed. Therefore, this distinguisher can only work for AES-256.

C. A Meet in the Middle Attack on 7-Round AES

Attack on AES-256 can be summarized as follows:

- Considering 5-round AES as a function, first, all possible functions from the first byte before encryption to the first byte after five rounds is precomputed.
- Similar to the other attacks, one round is added before and after the distinguisher.
- The subkey blocks in both of the new rounds are guessed.
- By using the guessed subkeys, plaintext and ciphertext pairs are encrypted and decrypted one round, respectively.
- Using precomputed tables, keys are checked whether the distinguishing property is satisfied or not.

The attack needs 2^{40} chosen plaintext-ciphertext pairs which is not so many, but the critical part of the complexity is the precomputation part which is 2^{216} . Time and memory complexities are 2^{80} and 2^{218} respectively.

D. Extension to 8-Round

By guessing the last round key, 8-round AES can be broken with 2^{200} time complexity since the time complexity on 7-round attack is only 2^{80} . The attack described here can not be applied to AES-192. Demirci and Selçuk also present a time memory trade off approach in [17]. Since the complexity is dominated by the precomputation phase, this approach can be effectively applied. The results are given in Table I.

VII. CONCLUSION

In this paper, we try to cover all attacks on AES. The complexities of the attacks are given in Table I. None of the attacks is a real threat to AES, but these are used to understand the security margin of the number of the rounds used. The best attack for AES is time memory trade off attacks, however since they are applicable to all block ciphers we did not cover it. We plan to study deeply meet in the middle attack and algebraic attack as a future work.

TABLE I
COMPARISON OF ATTACK COMPLEXITIES

AES	Paper	Rou	Type	Data	Time	Memory
128	[2]	4	Squ	2^9	2^9	-
	[2]	5	Squ	2^{11}	2^{40}	-
	[2]	5	Squ	2^{32}	2^{40}	2^{32}
	[14]	5	Boo	2^{39}	2^{39}	2^{33}
	[2]	6	Squ	2^{32}	2^{72}	2^{32}
	[3]	6	Squ	2^{32}	2^{80}	2^{32}
	[4]	6	Squ	$6 \cdot 2^{32}$	2^{44}	-
	[14]	6	Boo	2^{71}	2^{71}	2^{33}
	[10]	6	ImpDif	$2^{114.5}$	2^{50}	2^{45}
	[18]	6	ImpBoo	$2^{112.2}$	$2^{112.3}$	-
	[3]	7	Squ	2^{32}	2^{208}	-
	[10]	7	ImpDif	$2^{115.5}$	2^{119}	2^{45}
	[18]	7	ImpDif	$2^{115.5}$	2^{119}	-
192	[3]	7	Squ	2^{32}	2^{184}	2^{32}
	[4]	7	Squ	$19 \cdot 2^{32}$	2^{155}	-
	[9]	7	ImpDif	2^{92}	2^{186}	2^{157}
	[10]	7	ImpDif	2^{92}	2^{162}	-
	[18]	7	ImpDif	$2^{91.2}$	$2^{145.5}$	-
	[12]	7	ImpDif	$2^{94.5}$	2^{157}	2^{129}
	[17]	7	MitM	2^{32}	2^{80}	2^{217}
	[17]	7	MitM-TM	2^{33+n}	2^{82+n}	2^{217-n}
	[4]	8	Squ	$2^{128} - 2^{119}$	2^{188}	-
256	[3]	7	Squ	2^{32}	2^{200}	2^{32}
	[4]	7	Squ	$19 \cdot 2^{32}$	2^{172}	-
	[17]	7	MitM	2^{32}	2^{80}	2^{218}
	[17]	7	MitM-TM	2^{34+n}	2^{82+n}	2^{218-n}
	[4]	8	Squ	$2^{128} - 2^{119}$	2^{204}	-
	[18]	7	ImpBoo	$2^{112.8}$	$2^{186.9}$	-
	[10]	8	ImpDif	$2^{166.5}$	$2^{247.5}$	-
	[18]	8	ImpDif	2^{89}	$2^{247.5}$	-
	[17]	8	MitM	2^{32}	2^{208}	2^{216}
	[17]	8	MitM-TM	2^{34+n}	2^{210+n}	2^{216-n}
	[12]	8	ImpDif	2^{101}	2^{228}	2^{201}

REFERENCES

- [1] J. Daemen, L. Knudsen and V. Rijmen. *The Block Cipher Square*. Fast Software Encryption '97, pp. 149-165. Springer-Verlag, 1997.
- [2] J. Daemen and V. Rijmen, *AES Proposal: Rijndael*, Second Version, AES submission.
- [3] S. Lucks, *Attacking Seven Rounds of Rijndael under 192-bit and 256-bit keys*. The Third Advanced Encryption Standard Candidate Conference, pp. 215-229. NIST April 2000.
- [4] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner and D. Whiting, *Improved Cryptanalysis of Rijndael*, Fast Software Encryption 2000, volume 1978 of Lecture Notes in Computer Science, pp. 213-230, Springer-Verlag 2001
- [5] E. Biham, N. Keller, *Cryptanalysis of Reduced Variants of Rijndael*, 3rd AES Conference, 2000.
- [6] J.H. Cheon, M. Kim, K. Kim, J.-Y. Lee, S. Kang, *Improved Impossible Differential Cryptanalysis of Rijndael and Crypton*, in: ICISC 2001, LNCS, vol.2288, pp. 39-49, Springer-Verlag.
- [7] R.C.-W. Phan, M.U. Siddiqi, *Generalized Impossible Differentials of Advanced Encryption Standard*, Electronics Letters 37 (14)(2001), pp. 896-898.
- [8] R.C.-W. Phan, *Classes of Impossible Differentials of Advanced Encryption Standard*, Electronics Letters 38 (11)(2002), pp. 508-510.
- [9] R.C.-W. Phan, *Impossible Differential Cryptanalysis of 7-round AES*, Information Processing Letters 91 (1)(2004), pp. 29-32.
- [10] W. Zhang, W. Wu, D. Feng, *New Results on Impossible Differential Cryptanalysis of Reduced AES*, in: ICISC 2007, LNCS, vol.4817, pp. 239-250, Springer-Verlag.
- [11] B. Bahrak, M.R. Aref, *Impossible Differential Attack on Seven-Round AES-128*, IET.Inf.Secur., 2008, Vol.2, No.2, pp. 28-32.
- [12] J.Chen, Y. Hu, Y. Zhang, *Impossible Differential Cryptanalysis of Advanced Encryption Standard*, Science in China Series F:Information Sciences, 2007, vol.50, No.3, pp.342-350.
- [13] D. Wagner, *The Boomerang Attack*, FSE'99, LNCS vol.1636, pp. 156-170, Springer-Verlag, 1999
- [14] A. Biryukov, *The Boomerang Attack on 5 and 6-Round Reduced AES-128*, FSE'99, LNCS vol. 4593, Springer-Verlag, 2007.
- [15] H. Gilbert, M. Minier *A collision Attack on 7 Rounds of Rijndael*, 3rd AES Conference, 2000
- [16] N.T. Courtois, J. Pieprzyk *Cryptanalysis of block ciphers with overdefined system of equations*, in ASIACRYPT 2002 volume 2501 of LNCS, pages 267-287. Springer-Verlag, 2002.
- [17] H. Demirci, A. A. Selçuk *A Meet-in-the-Middle Attack on 8-round AES*, in FSE 2008
- [18] J. Lu, *Cryptanalysis of Block Ciphers* Ph.D. Thesis, 2008.

Algebraic Cryptanalysis of Reduced AES

Ameneh FARHADIAN, M.R. AREF

Abstract—Algebraic attack on AES was proposed, recently. It was called XSL attack. The suggested computational complexity of this attack on AES is not dependent on the number of cipher rounds, roughly. So the implementation of attack is not practical even for the low number of AES round. In addition, the estimate given for the number of linearly independent equations generated by XSL technique has not been proved exactly and it can not be checked even for reduced AES, because the mentioned reason. But there is a question: weather it may be possible to have another equation system expressing the AES that enable the algebraic attack on reduced AES with computational complexity proportional to the number of rounds. In this paper a new equation system for AES is proposed that results in new algebraic attack on reduced AES up to 5 rounds. Solving this equation system even by worst method like guessing the unknowns is faster than the brute force attack.

Keywords — Algebraic cryptanalysis, AES, Closed form representation, Ground idea.

I. INTRODUCTION

Algebraic attack on ciphers has gained more and more attention in cryptography[1]-[6]. The idea of algebraic attack is to express a cipher by a system of equations whose solution reveals the secret key. So the differences in the way of generating the equation system or in the methods of solving the equation may result in different algebraic attacks. The algebraic attack on AES [7] was proposed by Courtois and Pieprzyk in [1], it was called XSL attack. The computational complexity of this attack has not been proved, perfectly. Because the estimates given for the number of linearly independent equations generated by the XSL technique, appears to be inaccurate. Murphy and Robshaw have improved this attack by rewriting the equations in $GF(2^8)$ instead of $GF(2)[2]$. They argue that it should be possible to break 128-bit AES with an effort equivalent to 2^{100} AES encryption, of course if the estimates for XSL technique are valid.

In [8], a simple closed form of AES was presented. But solving this equation or using it in cryptanalysis has remained as an open problem, until now. In this paper we use solving such closed form of equation by some difference to

cryptanalysis reduced AES. The obtained equation system could be solved faster than brute force attack even by guessing the unknowns.

The equation system is established in the next section. The Section 3 deals with solving discussion of the obtained equation. An improved attack is presented in Section 4. Finally we summarized the paper in the Section 5.

II. GENERATING THE EQUATION SYSTEM

In algebraic cryptanalysis of block cipher, usually a big equation system with large number of equations and unknowns is established. But here, only one equation is written to describe the cipher and cryptanalysis is done by solving this equation for some chosen plaintexts.

In AES encryption, all the operations can be expressed in $GF(2^8)$ field. So every intermediate byte or output byte can be expressed in closed form of input bytes, easily. In [4], Ferguson et al. derived a closed formula for AES (rijndael) that can be seen as a generalization of continued fractions. We use such closed form equation by some modifications. Before generating the equation, let define the notation that will be used. We refer to FIPS 197 [7] for a full description of the cipher.

$p_{i,j}$ One byte of plaintext which is placed in i -th row and j -th column of block.

$c_{i,j}$ One byte of ciphertext which is placed in i -th row and j -th column of block.

$S(x)$ S-box function by input byte x .

$p_{i,j}^{(r)}$ The input byte of r -th round which is placed in i -th row and j -th column of block.

$\alpha_i, \beta_i, \gamma_i$ Coefficients of the mix column operation.

λ_i Coefficients of the mix column inversion operation.

$k_{i,j}^{(r)}$ One byte of subkey in r -th round, which is placed in i -th row and j -th column of block.

Using the defined notation and description of the cipher, the $p_{i,j}^{(3)}$, one input byte of the third round can be written as

$$\begin{aligned} p_{m,n}^{(3)} = & \alpha_1 S \left(\sum_e \beta_{1,e} S(p_{i_{1,e},j_{1,e}} + k_{i_{1,e},j_{1,e}}) + k_{i_1,k_1}^{(1)} \right) \\ & + \alpha_2 S \left(\sum_e \beta_{2,e} S(p_{i_{2,e},j_{2,e}} + k_{i_{2,e},j_{2,e}}) + k_{i_2,k_2}^{(1)} \right) \\ & + \alpha_3 S \left(\sum_e \beta_{3,e} S(p_{i_{3,e},j_{3,e}} + k_{i_{3,e},j_{3,e}}) + k_{i_3,k_3}^{(1)} \right) \\ & + \alpha_4 S \left(\sum_e \beta_{4,e} S(p_{i_{4,e},j_{4,e}} + k_{i_{4,e},j_{4,e}}) + k_{i_4,k_4}^{(1)} + k_{p,q}^{(2)} \right) \end{aligned} \quad (1)$$

Manuscript received November 9, 2008. This work was supported in part by ITRC under Grant T500/5990.

A.Farhadian received the B.S., and M.S. degrees, in Electrical Engineering, from Sharif University of Technology of Iran. (Phone: +98-21-44990823; e-mail: afarhadian@yahoo.com).

M.R. AREF is with the Electrical Engineering Department, Sharif University of Technology. (phone: +98-21-66165935; e-mail: aref@sharif.ir).

Now we want to simplify this equation. For this reason, we choose only plaintexts which are identical in all bytes except one, say $p_{i_{1,1},j_{1,1}}$. We call it “active byte”. Choosing plaintexts in this way enables us to summarize the equation. Now, we have some constant components in the equation for this set of chosen plaintexts. We summarize these constant parts in equation by assigning a new simple constant parameter. One constant part in the (1) within such chosen plaintexts are shown by underling. Using this idea, equation (1) is rewritten to

$$p_{m,n}^{(3)} = \alpha_1 S(\beta_1 S(\underline{p_{i_{1,1},j_{1,1}}} + k_{i_{1,1},j_{1,1}}) + \text{const}_1) + \text{const}_2 \quad (2)$$

In (2), const_2 is equal to the part that is underlined in (1). As we see, the number of unknowns are reduced in (2), notably. If we consider the reduced 4-round AES, the $p_{i,j}^{(3)}$ byte can be expressed by ciphertext bytes, too. The expression of $p_{i,j}^{(3)}$ according to ciphertext bytes is

$$S(p_{m,n}^{(3)}) = k_{m,n}^{(3)} + \sum_{1 \leq y \leq 4} \lambda_y S^{-1}(c_{k_y, l_y} + k_{k_y, l_y}^{(4)}) \quad (3)$$

Please note that $k_{m,n}^{(3)}$ is the subkey that is obtained after transposition of two linear operations in 3-th round. “Add round key” operation and “Mix column” operation are transported together. Since both of them are linear, this transposition doesn’t have any effect on cipher. Just, we should notice that replacing these two operations requires changing the corresponding subkey. (By performing the mix column inversion operation on corresponding subkey) Combining (2) and (3), we have

$$S(\alpha_1 S(\beta_1 S(\underline{p_{i_{1,1},j_{1,1}}} + k_{i_{1,1},j_{1,1}}) + \text{const}_1) + \text{const}_2) = k_{m,n}^{(3)} + \sum_{1 \leq y \leq 4} \lambda_y S^{-1}(c_{k_y, l_y} + k_{k_y, l_y}^{(4)}) \quad (4)$$

Now, we could find a relation between plaintext bytes and ciphertext bytes for 4-round AES. Let develop this equation to 5-round AES. We know that each output byte of mix column operation in 3-th round is a linear combination of $S(p_{i,j}^{(3)})$ s. thus

$$b_{m,n}^{(3)} = \gamma_1 S(p_{i,j}^{(3)}) + \gamma_2 S(p_{i,j}^{(3)}) + \gamma_3 S(p_{i,j}^{(3)}) + \gamma_4 S(p_{i,j}^{(3)}) \quad (5)$$

And Substituting (5) into (4), it gives

$$b_{m,n}^{(3)} = \gamma_1 S(\alpha_1 S(\beta_1 S(\underline{p_{i_{1,1},j_{1,1}}} + k_{i_{1,1},j_{1,1}}) + \text{const}_1) + \text{const}_2) + \gamma_2 S(\alpha_2 S(\beta_2 S(\underline{p_{i_{1,1},j_{1,1}}} + k_{i_{1,1},j_{1,1}}) + \text{const}_1) + \text{const}_2) + \gamma_3 S(\alpha_3 S(\beta_3 S(\underline{p_{i_{1,1},j_{1,1}}} + k_{i_{1,1},j_{1,1}}) + \text{const}_1) + \text{const}_2) + \gamma_4 S(\alpha_4 S(\beta_4 S(\underline{p_{i_{1,1},j_{1,1}}} + k_{i_{1,1},j_{1,1}}) + \text{const}_1) + \text{const}_2) \quad (6)$$

In other hand, $b_{m,n}^{(3)}$ can be represented by ciphertext bytes as follows

$$b_{m,n}^{(3)} = S(k_{m,n}^{(4)} + \sum_{1 \leq y \leq 4} S^{-1}(c_{k_y, l_y} + k_{k_y, l_y}^{(5)})) + k_{m,n}^{(3)} \quad (7)$$

Combining [6] and [7] results in

$$S^{-1}(k_{m,n}^{(4)} + \sum_{1 \leq y \leq 4} \lambda_y S^{-1}(c_{k_y, l_y} + k_{k_y, l_y}^{(5)})) + k_{m,n}^{(3)} = \gamma_1 S(\alpha_1 S(\beta_1 S(\underline{p_{i_{1,1},j_{1,1}}} + k_{i_{1,1},j_{1,1}}) + \text{const}_{1,1}) + \text{const}_{2,1}) + \gamma_2 S(\alpha_2 S(\beta_2 S(\underline{p_{i_{1,1},j_{1,1}}} + k_{i_{1,1},j_{1,1}}) + \text{const}_{1,2}) + \text{const}_{2,2}) + \gamma_3 S(\alpha_3 S(\beta_3 S(\underline{p_{i_{1,1},j_{1,1}}} + k_{i_{1,1},j_{1,1}}) + \text{const}_{1,3}) + \text{const}_{2,3}) + \gamma_4 S(\alpha_4 S(\beta_4 S(\underline{p_{i_{1,1},j_{1,1}}} + k_{i_{1,1},j_{1,1}}) + \text{const}_{1,4}) + \text{const}_{2,4}) \quad (8)$$

The resulted equation is very interesting. We could find an equation that relates the plaintext bytes and cipher text bytes together, with low number of unknown variables. The number of unknown variables in this equation is only 15.

After generating the equation for 4-round and 5-round AES, let's investigate the solving strategy. In the next section we deal with the strategy of solving.

III. SOLVING THE EQUATIONS

Since the number of unknowns in the equations is low, the first way that appears to solve the equation is to guess the unknowns. The equation corresponding to 4-round AES has 8 unknowns. And other equation corresponding to 5-round AES has 15 unknowns.

The second way is to substitute the $S(x)$ relation in the equation. From [7], we know that

$$S(x) = '63'x^{254} + '05'x^{253} + '09'x^{251} + '25'x^{247} + 'f'4'x^{239} + '01'x^{223} + 'b5'x^{191} + '8f'x^{127} \quad (9)$$

Substituting $S(x)$ relation in original Equation results in a multivariate polynomial over $\text{GF}(2^8)$ with maximum possible degree. Solving the resulted multivariate polynomial seems to be very difficult. We don't have any proper tool to solve such equation.

Another way is to use $xy = 1$ relation for nonlinear part of s-box. This idea was used in establishing the equation system for XSL attack on AES. According to [1], it is possible to have 23 implicit quadratic equations with 80 distinct terms for each s-box. We define new variables and expand the equation to be possible to use such above-mentioned implicit equation system for s-box. Each s-box should be assigned to a new defined variable like as follows for 4-round AES equation

$$S(\alpha_1 S(\beta_1 S(\underline{p_{i_{1,1},j_{1,1}}} + k_{i_{1,1},j_{1,1}}) + \text{const}_1) + \text{const}_2) = \underbrace{\underbrace{\underbrace{\gamma_1}_{y_1} S(\alpha_1 S(\beta_1 S(\underline{p_{i_{1,1},j_{1,1}}} + k_{i_{1,1},j_{1,1}}) + \text{const}_1) + \text{const}_2)}_{y_2}}_{y_3} = k_{m,n}^{(3)} + \sum_{1 \leq j \leq 4} \lambda_j S^{-1}(c_{k_j, l_j} + k_{k_j, l_j}^{(4)}) \quad (10)$$

Thus

$$\begin{cases} y_1 = S(p_{i_{1,1},j_{1,1}} + k_{i_{1,1},j_{1,1}}) \\ y_2 = S(v_1), \quad v_1 = \beta_1 y_1 + const_1 \\ y_3 = S(v_2), \quad v_2 = \alpha_1 y_2 + const_2 \\ z_1 = S^{-1}(c_{k_1,j_1} + k_{k_1,j_1}^{(4)}) \\ z_2 = S^{-1}(c_{k_2,j_2} + k_{k_2,j_2}^{(4)}) \\ z_3 = S^{-1}(c_{k_3,j_3} + k_{k_3,j_3}^{(4)}) \\ z_4 = S^{-1}(c_{k_4,j_4} + k_{k_4,j_4}^{(4)}) \\ y_3 = k_{m,n}^{(3)} + \lambda_1 z_1 + \lambda_2 z_2 + \lambda_3 z_3 + \lambda_4 z_4 \end{cases} \quad (11)$$

In above equation system, there are 10 equations over $GF(2^8)$. Each equation over $GF(2^8)$ is equal to 8 equation over $GF(2)$. We have 7 s-box relations that each of them can generate 23 implicit quadratic equations. Therefore this equation system is equal to an equation system over $GF(2)$ with $185 (7 \times 23 \text{ implicit quadratic} + 3 \times 8 \text{ linear})$ equations and 136 unknown bits and nearly 591 distinct terms. The number of equations is more than the number of unknowns by 49, so the XL method can be successful to solve the system. But it seems that the work load will be more than to be acceptable. In future, may be, one can solve this equation system better.

Let come back to first way, guessing the unknowns. In the equation corresponding to 4-round AES, there are 8 unknown bytes, so the search space has $(2^8)^8$ elements. Each element should be tested by computing the equation and check the equality for it. To overcome the answers by chance, we should iterate the test at least 8 times for 8 different chosen plaintexts. Because the probability that equality holds by chance is 2^{-8} . The computation of equation takes $1/8$ of work load taken for one 4-round AES encryption. Therefore the work load of this attack is 2^{64} .

There are 15 unknown bytes in 5-round expressing equation. So, 15 bytes should be guessed. To overcome the answers by chance, we should iterate the test at least 15 times for 15 different chosen plaintexts. Finally, the work load will be $2^{121.5}$. This is lower than exhaustive search by factor of $2^{6.5}$.

In the next section we will improve this attack.

IV. THE ATTACK IMPROVEMENT

As we saw in the previous section, the resulted equation can be solved by guessing the unknowns with computational complexity lower than exhaustive key search attack. Here, we want to improve the prior attack.

Equation (4) can be rewritten as follows

$$k_{m,n}^{(3)} = S(\alpha_1 S(\beta_1 S(p_{i_{1,e},j_{1,e}} + k_{i_{1,e},j_{1,e}}) + const_1) + const_2) + \sum_{1 \leq y \leq 4} \lambda_y S^{-1}(c_{k_y,j_y} + k_{k_y,j_y}^{(4)}) \quad (12)$$

We see that the left hand side of the above equation is a byte of subkey and is constant for every plaintext. Therefore it doesn't need to guess the $k_{m,n}^{(3)}$. It is sufficient to compute the

right hand side of the equation and to check if the computed values for right hand side are identical for all chosen plaintexts. If they are the same, the guessed values for unknowns can be correct. So it is sufficient to guess only 7 bytes and to compute the right hand side. By means of this idea, the number of unknown is reduced. The number of chosen plaintexts that the right hand side is computed for them should be enough to overcome the answers by chance. The probability that n bytes take the same value by chance is $2^8 / (2^8)^n$. And the search space for 7 unknown bytes has $(2^8)^7$ elements. Thus n should be at least 8 to overcome the wrong solutions. In this case, the computational complexity would be 2^{56} . It shows that the attack is improved by factor of 2^8 to prior attack.

We define the $k_{m,n}^{(3)}$ term as "Ground" of the equation [9]. Since it is constant within all chosen plaintexts and can be considered as a ground for our computations.

Now we want to use the "Ground" idea to improve the 5-round AES cryptanalysis, too. In (8), $k_{m,n}^{(3)}$ can be taken as a "Ground". Thus

$$\begin{aligned} \text{Ground} &= k_{m,n}^{(3)} = \\ &S^{-1}(k_{m,n}^{(4)} + \sum_{1 \leq y \leq 4} \lambda_y S^{-1}(c_{k_y,j_y} + k_{k_y,j_y}^{(5)})) \\ &+ \gamma_1 S(\alpha_1 S(\beta_1 S(p_{i_{1,j_1}} + k_{i_{1,j_1}}) + const_{1,1}) + const_{2,1}) \\ &+ \gamma_2 S(\alpha_2 S(\beta_2 S(p_{i_{1,j_1}} + k_{i_{1,j_1}}) + const_{1,2}) + const_{2,2}) \\ &+ \gamma_3 S(\alpha_3 S(\beta_3 S(p_{i_{1,j_1}} + k_{i_{1,j_1}}) + const_{1,3}) + const_{2,3}) \\ &+ \gamma_4 S(\alpha_4 S(\beta_4 S(p_{i_{1,j_1}} + k_{i_{1,j_1}}) + const_{1,4}) + const_{2,4}) \end{aligned} \quad (13)$$

Now, there are 14 unknowns, which should be guessed, to compute the "Ground" value. Since the search space has $(2^8)^{14}$ elements, we should compute the Ground parameter for at least 14 chosen plaintexts to escape from accidental wrong outcomes. If the guessed variables are correct, the computed Ground for all chosen plaintexts will be the same. In this case, the computational complexity is 2^{112} that is improved by factor of 2^8 rather prior attack. It is better than brute force attack by factor of 2^{16} .

V. CONCLUSION

In this paper, a new algebraic attack on reduced AES is proposed. It was shown that for the reduced AES up to 5 rounds, it is possible to write an equation that relates the plaintext and ciphertext bytes together. Solving this equation even by guessing the unknown is faster than brute force attack. The attack was improved by the Ground idea. The proposed algebraic Ground attack could break 4-round and 5-round AES by respectively 2^{56} and 2^{112} computational complexity. The number of required chosen plaintexts for cryptanalysis the 4-round and 5-round AES is 8 and 15, respectively.

Although, some more efficient structural attacks such as square attack [10], impossible differential attack [11] and

collision attack [12] were proposed on reduced AES before, but the new proposed attack in this paper is the first successful algebraic attack on reduced AES. It seems to be hard to extend the attack to more than 5 rounds. But may be, one can do it some years ago.

REFERENCES

- [1] N. Courtois, J. Pieprzyk, "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations." In: *Proceedings of Asiacrypt 2002*, LNCS 2501, Springer-Verlag 2002, pp. 267-287.
- [2] S. Murphy, J.B. Robshaw, "Essential Algebraic Structure Within the AES", *Proceedings of CRYPTO 2002*, LNCS 2442, Springer-Verlag 2002, pp.17-38.
- [3] A. Biryukov, and C. De Canniere, "Block ciphers and systems of quadratic equations", in *Fast Software Encryption, FSE 2003*, pp. 274-289.
- [4] C. Carlos, S. Murphy, M. Robshaw, *Algebraic Aspects of the Advanced Encryption Standard*, 2006, Approx. 155 p., Hardcover, ISBN:0-387-4363-1.
- [5] C. Cid, S. Murphy, and M. Robshaw, "Computational and Algebraic Aspects of the Advanced Encryption Standard", *Seventh International Workshop on Computer Algebra in Scientific Computing, CASC 2004*, Petersburg, Russia, 2004, pp. 93-103.
- [6] I. Toli, and A. Zanzi, "An Algebraic Interpretation of AES-128", *AES 4th International Conference*, AES 2004 Bonn, Germany, pp. 84-97.
- [7] National Institute of Standards and Technology, "Advanced Encryption Standard", *FIPS 197*, 26 November 2001.
- [8] N. Ferguson, R. Schroepel, D. Whiting, A Simple algebraic representation of Rijndael, *Proceeding of the Eighth International Workshop on selected areas in cryptography (SAC 2001)*, LNCS 2259, Springer-Verlag, 2001, pp. 103-111.
- [9] A. Farhadian, "Algebraic Cryptanalysis of AES" M.S. thesis, Dept. Electrical. Eng., Sharif University of Technology, Tehran, Iran, 2006.
- [10] J. Daemen, L.R. Knudsen, and V. Rijmen, "The Block Cipher Square", *Fast Software Encryption*, LNCS 1267, Springer-Verlag, 1997, pp. 149-165.
- [11] E. Biham, and N. Keller, "Cryptanalysis of Reduced Variants of Rijndael", *3rd AES Conference*, New York, USA, 2000.
- [12] H. Gilbert and M. Minier, "A Collision Attack on 7 Rounds of Rijndael", *Proceeding of the Third Advanced Encryption Standard Candidate Conference*, NIST, 2000, pp. 230-241.

Cryptanalysis of Strengthened Magenta

Orhun KARA

Abstract—In this paper we mount a reflection attack on a modified version of Magenta. Magenta was one of the block ciphers submitted for the AES contest. Indeed, Magenta has been already broken during the AES contest and hence has been disqualified. We first strengthen Magenta by double encryption and by adding two more rounds. We call this new cipher as MagentaP2. We claim that MagentaP2 is strong against any attack including the attack mounted on Magenta, except reflection type attacks.

One prevalent adoption in crypto community is that increasing the number of rounds of a block cipher enhances the security level. In fact, we give a counter example against this adoption. Magenta stands well against reflection attacks whereas MagentaP2 is vulnerable to reflection attacks even though its number of rounds is more than twice the number of original Magenta. The workloads of our attack are 2^{65} , 2^{131} and 2^{196} encryptions with at most 2^{66} known plaintexts for 128-bit, 192-bit and 256-bit key lengths, respectively.

Keywords —Block Cipher, Round Function, Round Key, Key Schedule, Cryptanalysis, Self-similarity.

I. INTRODUCTION

In this paper we mount a reflection attack on a fortified version of Magenta by means of increasing its round numbers and double encryption. The reflection attack is a new type of self-similarity attack and the attack idea has been first appeared in [13]. The first applications with extensions have been presented in FSE 2007 [14] and in INDOCRYPT 2008 [12].

Apart from reflection attacks, there are two more generic attack types exploiting some degree of self-similarity among round functions: One of them is the slide attack [5], [6]. The typical slide attack can be applied if the sequence of round keys has a short period. The other attack type is the related-key attacks proposed by Biham [1]. Unlike slide attacks and related-key attacks, reflection attack exploits similarities of some round functions of encryption process with those of decryption. This is the main difference from the previous self-similarity attacks, which exploit the similarities among round functions only in encryption process. Consequently, some ciphers resistant to related-key attacks or slide attacks can be vulnerable to reflection attacks.

Magenta was one of the candidate algorithm for AES during NIST-AES contest and has been broken immediately after the commencement of the contest [2]. The major pitfall of the algorithm was not a weakness of the round function but was

its extremely simple key-schedule algorithm. We strengthen Magenta by double encryption and by adding two more rounds in order to foil the attack in [2]. It is also interesting that slide attacks and related-key attacks are probably not applicable to the strengthened version. On the other hand, we mount a reflection attack on the strengthened version.

It is quite unusual that increasing the number of rounds may cause weaknesses in terms of reflection analysis in some cases. Magenta is strong against reflection analysis. However, reflection attack works quite well on MagentaP2, having more rounds. The attack exploits extremely large number of the fixed points produced by the encryption function of Magenta. The workloads are 2^{65} , 2^{131} and 2^{196} encryptions with at most 2^{66} known plaintexts for 128-bit, 192-bit and 256-bit key lengths, respectively.

Organization. We give a brief description of the algorithm Magenta in section II and then describe the modified version MagentaP2 in the forthcoming section. After giving preliminary results for the attack in Section IV, we explain the attack in Section V. Then, we conclude the paper.

II. A BRIEF DESCRIPTION OF MAGENTA

Magenta is a block cipher submitted for the AES contest by Deutsche Telekom AG [10]. It is a Feistel cipher with 128 bit block size and 128, 192 or 256 bit key sizes. In this section we give a high level description of Magenta and construct a distinguisher for the whole cipher. This distinguisher does not assist key recovering. We modify Magenta and call it MagentaP2 (meaning Magenta Plus 2). MagentaP2 is double encryption of Magenta plus two more rounds. The modified Magenta is expected to be more secure than Magenta against most of the attack methods including the attack in [2] on Magenta. However, it is surprising that MagentaP2 is weaker than Magenta itself in terms of reflection attacks.

We give a short description of Magenta. We do not enter into details of round function since we do not exploit it in cryptanalysis. Magenta is a Feistel network where the last swap operation is included unlike DES. When the key length of Magenta is of 128, 192 or 256 bits then it is divided into two, three or four equal parts as (K_1, K_2) , (K_1, K_2, K_3) or (K_1, K_2, K_3, K_4) , respectively. The encryption functions are

$$E_K = \begin{cases} F_{K_1}^2 F_{K_2}^2 F_{K_1}^2 & \text{if key size is 128,} \\ F_{K_1} F_{K_2} F_{K_3}^2 F_{K_2} F_{K_1} & \text{if key size is 192,} \\ F_{K_1} F_{K_2} F_{K_3} F_{K_4}^2 F_{K_3} F_{K_2} F_{K_1} & \text{if key size is 256.} \end{cases}$$

O. KARA, TÜBİTAK UEKAE

National Research Institute of Electronics and Cryptology, Gebze 41470
Kocaeli/Turkey, orhun@uekae.tubitak.gov.tr

Each round function F_{K_i} is defined as

$$F_{K_i} : GF(2)^{128} \longrightarrow GF(2)^{128}$$

$$F_{K_i}(x, y) = (y, R_{K_i}(y) \oplus x) \quad (1)$$

where $\oplus$ is the “XOR” operation.

Magenta was cryptanalyzed during the AES conferences by Biham *et. al.* [2] and hence eliminated. The attack is a divide and conquer type attack. One can extract the outer keys, independently from the inner key. The complexity is 2^{m_k-31} encryptions for a known plaintext attack where m_k is the key length.

III. DESCRIPTION OF MAGENTA2

The modified Magenta, which we call MagentaP2, is a double encryption of Magenta including two more rounds. Let $E_K^{(M)}$ and $E_K^{(M2)}$ denote the encryption functions of Magenta and MagentaP2, respectively. Then, MagentaP2 encryption is defined as

$$E_K^{(M2)}(x) = F_{(K_t \ll_m)} E_K^{(M)} E_K^{(M)} F_{K_t}(x) \quad (2)$$

where F is the round function of Magenta and

$$K_t = \begin{cases} K_2 & \text{if key size is 128,} \\ K_2 \oplus K_3 & \text{if key size is 192,} \\ K_2 \oplus K_3 \oplus K_4 & \text{if key size is 256.} \end{cases}$$

$\ll_m$ is cyclic rotation to left by m bits where m can be chosen any positive integer less than 64. The new cipher depends on m , but we call all the ciphers simply as “MagentaP2” by abuse of terminology.

IV. PRELIMINARY WORK FOR THE ATTACK

We give a general framework of the reflection attack on Feistel networks as a preliminary section for the next section where the attack is described. The extensions of the statements in this section can be found in [12].

Let a plaintext $x \in GF(2)^n$ be given as $x = (x_0, x_1); x_0, x_1 \in GF(2)^{n/2}$. The Feistel structure can be stated as a recursive function defined as $x_i = R_{k_{i-1}}(x_{i-1}) \oplus x_{i-2}$ with the initial conditions given by $x = (x_0, x_1)$. The function $R : GF(2)^{n/2} \rightarrow GF(2)^{n/2}$ is the encryption function. The i -th round operation is defined as

$$(x_i, x_{i+1}) = F_{k_i}(x_{i-1}, x_i) = (x_i, R_{k_i}(x_i) \oplus x_{i-1}) \quad (3)$$

for $i \leq r$. In general, the swap operation is excluded in the last round and (x_{r+1}, x_r) is the corresponding ciphertext. With some abuse of terminology, R is also called the round function. We call the stream $x_0, x_1, \dots, x_r, x_{r+1}$ the *encryption stream* of $x = (x_0, x_1)$ with respect to K .

Proposition 1: For a given natural number $m < r$, assume that $k_{m-i} = k_{m+i}$, $\forall i : 1 \leq i \leq \min\{r-m, m-1\}$. Let $x = (x_0, x_1)$ be encrypted and $x_0, x_1, \dots, x_r, x_{r+1}$ be its encryption stream. If $R_{k_m}(x_m) = 0$, then $x_{m-i} = x_{m+i}$, $\forall i : 1 \leq i \leq \min\{r-m, m-1\}$. Conversely, if $x_{m-i} = x_{m+i}$ and $x_{m-i+1} = x_{m+i-1}$ for some i , then $R_{k_m}(x_m) = 0$.

Proposition 1 has already been known during the studies on cycle structures of DES (see [8], [19]). Hence, the notion of the fixed points of the weak keys of DES is well known. However,

the studies were focused on algebraic properties of DES permutations and their short cycles rather than developing a key recovery attack [8], [19], [11], [18]. The following corollary points out the opposite direction of this old phenomenon.

Corollary 1: Assume that each round key k_i determines a round function R_{k_i} randomly. Let $x = (x_0, x_1)$ be encrypted and $x_0, x_1, \dots, x_r, x_{r+1}$ be its encryption stream. Assume that the round number r is even, $r = 2r' > 4$, and $k_{r'-i} = k_{r'+i}$ $\forall i : 1 \leq i < r'$. Let $s_{r'}$ be the cardinality of the pre-image set, $R_{k_{r'}}^{-1}(0)$. Then, $\Pr(x_0 = x_r) = 2^{-\frac{n}{2}}(s_{r'} + 1 - 2^{-\frac{n}{2}} \cdot s_{r'})$ and

$$\Pr(R_{k_{r'}}(x_{r'}) = 0 \mid x_0 = x_r) = \frac{s_{r'}}{s_{r'} + 1 - 2^{-\frac{n}{2}} \cdot s_{r'}}.$$

Proof: Assume that the round function is random. Then, the probability that $x_0 = x_r$ is given as

$$\Pr(x_0 = x_r) = s_{r'} \cdot 2^{-n/2} + 2^{-n/2}(1 - s_{r'} \cdot 2^{-n/2})$$

$$= 2^{-\frac{n}{2}}(s_{r'} + 1 - s_{r'} \cdot 2^{-\frac{n}{2}})$$

since it is equal to

$$\Pr(x_0 = x_r \mid R_{k_{r'}}(x_{r'}) = 0) \Pr(R_{k_{r'}}(x_{r'}) = 0) +$$

$$\Pr(x_0 = x_r \mid R_{k_{r'}}(x_{r'}) \neq 0) \Pr(R_{k_{r'}}(x_{r'}) \neq 0).$$

Note that $\Pr(x_0 = x_r \mid R_{k_{r'}}(x_{r'}) \neq 0) = 2^{-n/2}$ since $r > 4$. On the other hand, $\Pr(x_0 = x_r \mid R_{k_{r'}}(x_{r'}) = 0) = 1$ by Proposition 1. Hence, we conclude that

$$\Pr(R_{k_{r'}}(x_{r'}) = 0 \mid x_0 = x_r) =$$

$$\frac{\Pr(x_0 = x_r \mid R_{k_{r'}}(x_{r'}) = 0) \cdot \Pr(R_{k_{r'}}(x_{r'}) = 0)}{\Pr(x_0 = x_r)}$$

$$= \frac{s_{r'}}{s_{r'} + 1 - 2^{-\frac{n}{2}} \cdot s_{r'}}.$$

The following theorem illustrates the property exploited to mount an attack on a Feistel network with palindromic round keys.

Theorem 1: Assumptions are as in Corollary 1. Then the equality $x_0 = x_r$ implies that the equation

$$x_1 = R_{k_r}(x_r) \oplus x_{r+1}. \quad (4)$$

is true with probability

$$\frac{s_{r'}}{s_{r'} + 1 - 2^{-\frac{n}{2}} \cdot s_{r'}}.$$

Proof: Assume that $x_0 = x_r$. Then by Corollary 1, we have $R_{k_{r'}}(x_{r'}) = 0$ with probability

$$\frac{s_{r'}}{s_{r'} + 1 - 2^{-\frac{n}{2}} \cdot s_{r'}}.$$

Thus the equality $x_1 = x_{r-1}$ is true with probability

$$\frac{s_{r'}}{s_{r'} + 1 - 2^{-\frac{n}{2}} \cdot s_{r'}}.$$

by Proposition 1. On the other hand $x_{r+1} = R_{k_r}(x_r) \oplus x_{r-1}$. Thus, the probability that $x_1 = R_{k_r}(x_r) \oplus x_{r+1}$ is

$$\frac{s_{r'}}{s_{r'} + 1 - 2^{-\frac{n}{2}} \cdot s_{r'}}.$$

V. THE ATTACK

Define an intermediate function

$$I_{K_i} : GF(2)^{128} \longrightarrow GF(2)^{128}$$

$$I_{K_i}(x, y) = (R_{K_i}(R_{K_i}(y) \oplus x) \oplus y, R_{K_i}(y) \oplus x). \quad (5)$$

The function I_{K_i} is indeed two rounds of encryption with key K_i such that the second swap is ignored. That is, I_{K_i} is $F_{K_i}F_{K_i}$ without the last swap. We use this function as the intermediate function. It has many fixed points:

Lemma 1: The function I_{K_i} has 2^{64} fixed points.

Proof: The fixed points of the function I_{K_i} are those $(x, y) \in GF(2)^{128}$ such that

$$x = R_{K_i}(R_{K_i}(y) \oplus x) \oplus y \text{ and } y = R_{K_i}(y) \oplus x. \quad (6)$$

These are the same equations and the points $(R_{K_i}(y) \oplus y, y)$ are fixed points of $I_{K_i} \forall y \in GF(2)^{64}$.

The intermediate function of MagentaP2 chosen as

$$I_{K_1}(x, y) = (R_{K_1}(R_{K_1}(y) \oplus x) \oplus y, R_{K_1}(y) \oplus x) \quad (7)$$

also has 2^{64} fixed points by Lemma 1. If the first half of a plaintext is equal to second half of its corresponding ciphertext through encryption of Magenta, then the remaining other halves are also equal with probability nearly one half by Corollary 1. This distinguisher does not depend on the number of Magenta encryptions.

The reflection attack on MagentaP2 is to get an equation similar to Equation 4 and solve it to extract the subkey K_t . The following proposition leads to a reflection attack on MagentaP2.

Theorem 2: Assume that Magenta is a random function. Let a plaintext $x = (x_0, x_1)$ be encrypted by MagentaP2 and the ciphertext $y = (y_0, y_1)$ be produced. Assume that $x_1 = y_0$. Then x and y satisfy the equation

$$R_{K_t}(x_1) \oplus R_{K_t \ll m}(y_0) = x_0 \oplus y_1. \quad (8)$$

with probability

$$\frac{1}{2 - 2^{-64}}.$$

Proof: Observe that the equations $R_{K_t}(x_1) \oplus R_{K_t \ll m}(y_0) = x_0 \oplus y_1$ and $x_1 = y_0$ together come from a fixed point $(R_{K_t}(x_1) \oplus x_0, x_1)$ of double encryption Magenta function $E_K^{(M)}E_K^{(M)}$ without the last swap. We have the equality of probabilities:

$$\Pr(F_{K_t}(x) \text{ is fixed point} \mid x_1 = y_1) = \frac{\Pr(F_{K_t}(x) \text{ is fixed point})}{\Pr(x_1 = y_1)}$$

since $\Pr(x_1 = y_1 \mid F_{K_t}(x) \text{ is fixed point}) = 1$. On the other hand, $\Pr(x_1 = y_1) = 2^{-63} - 2^{-128}$ by Theorem 1 and the result follows.

Equation 8 in Theorem 2 leads to a divide and conquer type attack that can be mounted on MagentaP2. Encrypt a plaintext $x = (x_0, x_1)$ and obtain the corresponding ciphertext $y = (y_0, y_1)$. If $x_1 = y_0$ then Equation 8 is satisfied for x and y with probability nearly one half by Theorem 2. Solve

the equation and extract the subkey K_t and then recover the remaining key bits by searching exhaustively. Let the key length be $64 \cdot i$ for $i = 2, 3, 4$. Then, by using $i \cdot 2^{64}$ plaintexts we obtain approximately $2i$ equations of the form Equation 8 and expect half of them to be correct by Proposition 2. By collecting the subsets of i equations and solving them we obtain a unique solution for K_t . Note that false alarm probability is almost zero since the probability that a false key is a solution of all the i equations is 2^{-64i} . The time complexity of recovering K_t is $\binom{2i}{i} \frac{i \cdot 2^{64i-63}}{r}$ where r is the number of rounds, namely 14 or 18 depending on the key size. The remaining key material (i.e., K_1) can be deduced by exhaustive search. As a result, one can recover the key by $2^{64.78}$, $2^{131.1}$ and $2^{196.96}$ encryptions using 2^{65} , $2^{65.58}$ and 2^{66} known plaintexts for 128 bit, 192 bit and 256 bit key lengths, respectively.

VI. CONCLUSION AND DISCUSSION

The algorithm Magenta is doubled in the modified version. Indeed, the number of Magenta encryption does not affect the attack complexity. Therefore, one may use triple or more Magenta encryptions. Still, the attack will work. It is also interesting that other self-similarity attack methods whose complexities are independent of round number, such as related key attacks or slide attacks probably do not work for MagentaP2.

One design criterion introduced in [13] is the self similarity degree of functions. It is expected that the round functions of a block ciphers should not be similar of high degree with high probability. Indeed, the Magenta round functions are even same with probability one. This property results from the key schedule of Magenta and is exploited in the attack.

REFERENCES

- [1] E. Biham, New Types of Cryptanalytic Attacks Using Related Keys. *J. of Cryptology*, Vol.7, pp.229-246, 1994.
- [2] E.Biham, A. Biryukov, N. Ferguson, L.R. Knudsen, B. Schneier and A. Shamir. Cryptanalysis of Magenta. In *Proc. Second AES conference*, NIST, 1999.
- [3] E.Biham, O. Dunkelman and N. Keller. Improved Slide Attacks, In *Proc. FSE'07*, LNCS 4593, pp. 153-166, Springer, 2007.
- [4] E. Biham and A. Shamir. *Differential Cryptanalysis of Data Encryption Standard*. Springer, 1993.
- [5] A. Biryukov and D. Wagner. Slide Attacks. In *Proc. FSE'99*, LNCS 1636, pp.245-259, Springer, 1999.
- [6] A. Biryukov and D. Wagner. Advanced Slide Attacks. In *Proc. EURO-CRYPT 2000*, LNCS 1807, pp.589-606, Springer, 2000.
- [7] G. Carter, E. Dawson and L. Nielsen. Key Schedules of Iterated Block Ciphers. In *Proc. Information Security and Privacy, ACISP'98*, LNCS 1438 pp. 80-89, Springer, 1998.
- [8] D. Coppersmith. The Real Reason for Rivest's Phenomenon. In *Proc. CRYPTO'85*, LNCS 218, pp. 535-536, Springer, 1985.
- [9] M. Henricksen. *Design, Implementation and Cryptanalysis of Modern Symmetric Ciphers*. PhD Thesis, ISRC, Faculty of Information Technology, Queensland University of Technology, 2005.
- [10] M.J. Jacobson Jr. and K. Huber. The Magenta Block Cipher Algorithm. In *Proc. First AES conference*, NIST, 1998.
- [11] B.S. Kaliski, R.L. Rivest and T. Sherman. Is DES a Pure Cipher? (Results of More Cycling Experiments on DES). In *Proc. CRYPTO'85*, LNCS 218, pp. 212-222, Springer, 1985.
- [12] O. Kara. Reflection Cryptanalysis of Some Ciphers. In *Proc. IN-DOCRYPT 2008*, LNCS 5365, pp. 294-307, Springer, 2008.
- [13] O. Kara. Self-Similarity Analysis of Block Ciphers. In *Proc. II. National Cryptology Symposium*, METU Ankara 2006.

- [14] O. Kara and C. Manap. A new class of Weak Keys for Blowfish, In *Proc. FSE'07*, LNCS 4593, pp. 167-180, Springer, 2007.
- [15] J. Kelsey and B. Schneier. Key-Schedule Cryptanalysis of DEAL. In *Proc. SAC'99*, pp.118-134, Springer, 2000.
- [16] Y. Ko, S. Hong, W. Lee, S. Lee and J. Kang. Related Key Differential Attacks on 27 Rounds of XTEA and Full-Round GOST. In *Proc. FSE'04*, LNCS 3017, pp.299-316, Springer, 2004.
- [17] M. Matsui. Linear Cryptanalysis Method of DES Cipher. In *Proc. EUROCRYPT'93*, LNCS 765, pp. 386-397, Springer, 1994.
- [18] J.H. Moore and G.J. Simmons. Cycle Structure of the DES with Weak and Semi-Weak Keys. In *Proc. CRYPTO'86*, LNCS 263, pp.9-32, Springer, 1986.
- [19] J.H. Moore and G.J. Simmons. Cycle Structure of the DES for Keys Having Palindromic (or Antipalindromic) Sequences of Round Keys. *IEEE Transactions on Software Engineering*, pp. 262-273, No 13, 1987.



Security of Critical Information Infrastructures: E-Governance and Standardization

Serap ATAY, Marcelo MASERA

Abstract— Critical Information Infrastructure - CII is a key enabler of e-Governance. This infrastructure is composed of the Information and Communication Technologies –ICT– underpinning the higher level services to end users, and encompasses the Internet, fixed and mobile telecommunications and other systems. The gap between security solutions and security risks is continuously growing due to evolution of the ICT. Each new technology and application can include many flaws. Each flaw may pave the way to unauthorized users to accessing critical data and/or may mistakenly provide them with the ability to perform some harmful action. Nowadays, the CII is in a conversion phase towards the so-called Next Generation Networks – NGNs. With this development, all telecommunication services will be built upon IP based networks. Naturally, these developments force the standardization bodies to adapt their rules and policies and thus to meet the security needs of these new CII components. E-government services such as administration, health, education etc. either create new services or replace existing manual procedural systems. These new services should offer higher availability, security and reliability with respect to current operations due to their increasing criticality. This criticality should be managed in innovative e-Governance arrangements among public and private actors: mainly the authorities and the operators of the CII, but also including all relevant stakeholders. In the meantime, the governments should be prepared for this new paradigm of e-Governance. The aim of this paper is to summarize the benefits and security risks of NGNs and emphasize the basis and requirements for that e-Governance.

Keywords — Communication system security, Government information systems, Internet, Security.

I. INTRODUCTION

The aim of this paper is to define the importance of Critical Information Infrastructure – CII and the developments of NGNs for the availability, security, and reliability of the e-governance services.

First of all, the difference between e-government and e-governance should be explained. E-government refers to the

use of Internet technologies for expediting the links of the government (executive, legislative, judiciary, local administration) with citizens and the private sector. It integrates the interactions and the interrelations between and among government and citizens, companies, customers, and public intuitions through the application of modern information and communication technologies. E-governance refers to the process of using information technology for facilitating the joint operations of government, nonprofit, and private-sector entities, as well as the interactions with citizens, other authorities and organizations [1]. The main distinction is that in E-Governance all participants are part of a network, while in E-Government the main actor is the government.

E-governance is understood as a powerful tool to overcome existing barriers for development of countries with the following properties;

- automation and citizen centric service delivery,
- accessing to these services from anywhere and anytime,
- increasing accountability and
- in order to achieve much more citizen participation.

Therefore, e-governance can be accepted as a new culture for governments for dealing with problems where the actors are multiple and where the government is not the only, privileged participant.

E-governance services create new services or replaces manual procedural systems for aforementioned objectives. For the usability of e-governance services, the confidentiality, integrity, authentication, non-repudiation, availability, reliability, responsiveness and assurance should also be created. Also, these properties should be supported by laws.

The governments tend to maintain e-governance services for many critical infrastructures - CI such as transportation, water, energy, finance, justice, health etc. However, all these CIs use another common critical infrastructure which is called as Critical Information Infrastructure – CII. Consequently, these infrastructures are interrelated or interdependent through CII. Therefore, the Critical Information Infrastructure Protection – CIIP is so important for the governments. The Fig. 1 depicts these relations.

Manuscript received November 10, 2008. This work was supported in part by the TUBITAK (Turkish Science and Technological Research Program) under Grant of Bideb2219 Post-Doctorate Research Fellowship.

S. ATAY, Author is with the Institute for the Protection and the Security of the Citizen, Joint Research Center, Via E. Fermi, 21020, Ispra, Italy (e-mail: serap.atay@irc.it) and Izmir Institute of Technology, Department of Computer Engineering, Izmir, Turkey (mail: serapatay@iyte.edu.tr).

M.MASERA, Autor is with the Institute for the Protection and the Security of the Citizen, Joint Research Center, Via E. Fermi, 21020, Ispra, Italy (e-mail: marcelo.masera@ec.europa.eu)

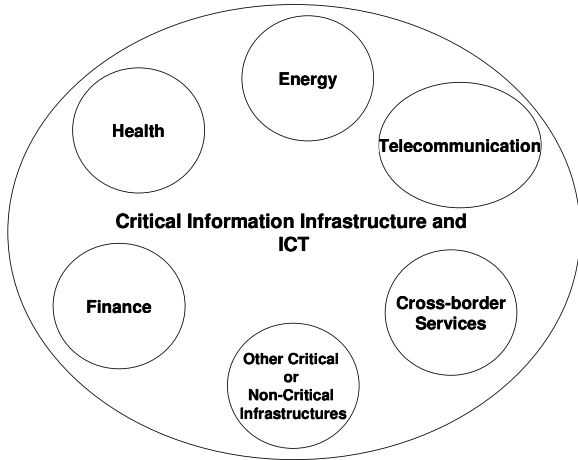


Fig. 1. The critical and non-critical infrastructures have an information infrastructure which uses the common information and communication technologies.

CII can be easily affected by the any changing or development of Information and Communication technologies such as communication, hardware or software technologies. In the mean time these technologies are very fast changing and improving. These improvements, changes and new interconnections between infrastructures may be causes new vulnerabilities, threats or attacks through directly or indirectly.

According to survey report is prepared by Secure Computing; 'when asked about the interconnection of control networks and corporate networks, over 60% of the Secure Computing survey respondents said their networks were already interconnected and 98% said that interconnection increased their security risks'¹. Survey data of this report had collected from attendees at the Process Control Systems Industry Conference held August 26-28, 2008 in La Jolla, California; attendees at the 1st Annual Cyber Security Conference held September 8-9 in Calgary, Alberta; and an online survey of critical infrastructure cybersecurity experts in Europe, the Middle East, and Africa during September 10-25, 2008. A total of 199 respondents had completed the survey.

Additionally U.S. Department of defence -DoD reported the number of incidents of malicious cyber attacks in May 20, 2008. As shown from the Fig. 2 the rate of attacks is increasing %31 between 2006 and 2007.

Nowadays, the telecommunication infrastructure is in a conversion phase for the Next Generation Networks – NGNs. Naturally, these developments will come with lots of unknown vulnerabilities, threats, and security risks.

According to aforementioned reports and the definition of the high consequence risks facing the UK in the report of Centre for the Protection of National Infrastructure – CPNI [13]; the interconnectivity among networks is expanding and the probabilities and impacts of attacks with NGN reach higher values as illustrated in Fig. 3.

¹ Critical Infrastructure Cybersecurity: Survey Findings and Analysis Whitepaper Sponsored by: Secure Computing, Rick Nicholson, November 2008.

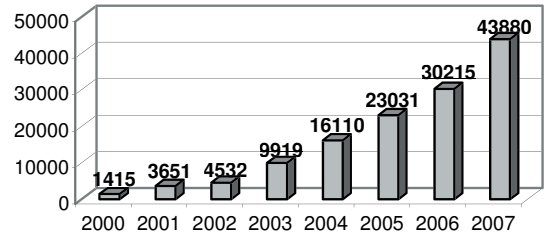


Fig. 2. U.S. Department of Defence (DoD) Reported Incidents of Malicious Cyber Activity [14].

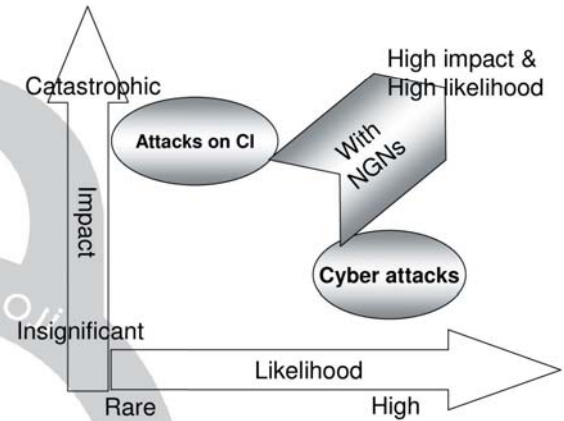


Fig. 3 An illustration of the high consequence risks with NGNs.acing

This situation forces the research institutes and standardization bodies adapt their rules and policies to meet the security needs of the new CII. Currently, the governments are planning to improve the ICT and the e-governance services and for that, they should do some preparations for the security of e-governance and NGNs.

This paper is organized with the following sections; the section 2 includes information about the NGNs and their benefits for the e-governance and CII. The section 3 defines the security risks of CII and e-governance services. The section 4 defines the standardization studies for NGNs. Section 5 concentrates on the definitions of requirements of e-governance and security with a proposed solution list. Section 6 presents the conclusions of this study.

II. NEXT GENERATION NETWORKS AND BENEFITS OF E-GOVERNANCE

The requirement of ICT is growing for e-governance, global market, industry, education, health and multimedia services etc. These requirements expand the digital traffic and costs. Therefore, the telecommunication sector has a plan about the convergence and optimization of traditional networks.

The aim of telecommunication sector with the NGN is collection of existing networks (such as fixed, mobile, broadcast, data, internet etc.) into unitary network architecture. This new architecture is to be a packet-based network and will be using multiple broadband technologies. As shown in Fig. 4, the idea of NGN is to have an infrastructure a reusable and services centralized and avoid discrete networks overlaid on existing network for each new service.

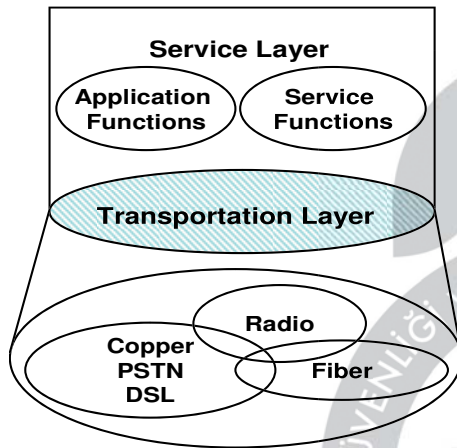


Fig. 4. NGNs transform communication technologies to service-centric unitary network architecture.

NGN are being developed by using a number of different technologies, including wireless and mobile, fiber and cable, or by upgrades to existing copper lines. The service-related functions in NGNs are independent of transport technologies when providing telecommunication services to users. So, from a more technical point of view, NGN is defined by the International Telecommunication Union-ITU as a “packet based network able to provide services including telecommunication services and able to make use of multiple broadband, quality of service - QoS enabled transport technologies and in which service related functions are independent from underlying transport-related technologies.”²

According to ITU report “Trends in Telecommunication Reform: the Road to NGN” published in September 2007, it is predicted that full implementation of NGN in fixed line networks in developed countries will be deployed by 2012 and in mobile networks by 2020. Developing countries are also seeking to deploy NGN technology, although not necessarily following the same path as developed countries [3].

² ITU-T Recommendation Y.2001, approved in December 2004, available at <http://www.itu.int/ITU-T/studygroups/com13/past-results.html>

Benefits of NGNs for e-Governance

One of the objectives of the NGN is to establish higher quality communication infrastructure for everyone and from everywhere.

- The ICT supports all economic sectors, is crucial to the national and international exchange of goods and services and economic interrelationships through related services. As a result, it has become a key economic and social infrastructure for all countries and citizens with this property.

The unitary and completely IP based infrastructure will decrease usage costs for the communication infrastructure. But, first investments of NGN and NGN access are high for the operators [4]. The aim of the NGNs is to have an access for every place with higher bandwidth.

- In this case, the e-governance services can be reachable from the rural places. This property helps to the availability of e-governance services.
- High speed networks with NGN will increasingly help to resolve ongoing social concerns in areas such as the environment, healthcare, education and are increasingly playing a role in social networking (facebook etc.).

In the mean time, this innovative technology is expected to bring about greater energy efficiency than legacy networks. By improving the energy efficiency of Information and Communication Technologies (ICTs), NGN can potentially make a significant contribution in the battle against global warming [3].

III. THE SECURITY RISKS OF CII AND E-GOVERNANCE

The formal definition of Critical Infrastructure-CI for the European Countries is ‘critical infrastructures which disruption or destruction would significantly affect two or more Member States or a single Member State if the critical infrastructure is located in another Member State’³. Now, this includes effects resulting from cross-sector dependencies on other types of infrastructure therefore for the potential of NGNs, some services required closed to the national or universal coverage.

The Supervisory Control and Data Acquisition – SCADA networks can be taken as a good example to show the risks. The system monitoring, control, and status data gathering in most CI are now automated processes with reduced reliance on human effort. These processes rely on SCADA networks and these are closed networks. So security was not addressed in great depth compared to conventional ICT systems. Unfortunately, today many corporate network and their leased lines are parts of SCADA network. These parts provide direct or indirect connectivity points to the internet and other networks. So, many examples exist about security vulnerabilities of SCADA network. For instance; in January 2003 the Slammer worm disrupted SCADA traffic causing operators to temporarily lose some degree of control of the

³ European Commission 2006a, p. 15

Davis-Besse nuclear power plant in Ohio USA. As a result, there is now increased acknowledgment of the possibility of external attacks on SCADA networks by CI owners and notable surge in interest in SCADA systems by terrorist groups.⁴

The physical cross-borders between governments are removed by ICT. Many e-governance services will be deployed over national borders. See for instance the offer of e-health to international tourists. Interconnection across borders means that attacks can come from anywhere and anytime, infiltrating the public (governmental) and private sections of the CII. This risk is coming from 'multi-party cross-border' relations of the governments and the risks become to have unpredictable dimensions with NGNs. The Fig. 5 depicts the multi-party cross-border relation for the security risks. This highlights the need for developing international approaches for the protection of the CII, and the prevention and management of related incidents.

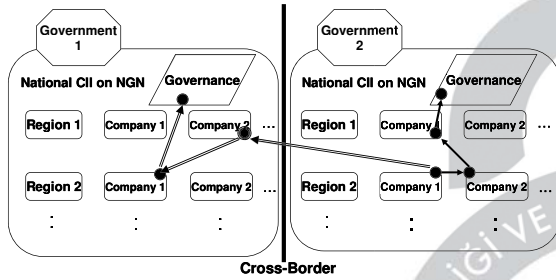


Fig. 5. NGNs have unique communication infrastructure and its affect on national CIIs is 'multi-party cross-border'.

Each new ICT technology inevitably includes new vulnerabilities. Threats are either to exploit these vulnerabilities directly or indirectly to create an attack. Therefore, many vulnerability, threat and risk analysis should be done for NGNs – and these should also include infrastructures and multi-party situations. Typical ICT security assessment approaches do not contemplate these situations, and new methodologies are needed. The most important part of this process is that the results of these analyses should be employed for reshaping the related security standards and common criteria.

IV. STANDARDIZATION STUDIES FOR NGNs

Standardization is a consensus-driven activity and an important mean for achieving and establishing trust between the parties involved. It is based on openness and transparency within independent organizations. Some of the important objectives of standardization are the establishment of compatibility and interoperability, the removal of barriers through harmonization, and the safety and health of citizens. As a consequence, the three groups of stakeholders primarily

benefiting from standardization processes are industry, consumers and governments.

Telecommunication services are created on IP networks in NGNs. This creates a demand on standardization bodies to adapt and meet the needs of these emerging networks. The goal is to develop specifications that are ready for an assurance audit and, using the common criteria for security evaluation as well [7]. International Standard Development Organizations - SDOs such as ITU, ETSI, ISO, IETF, and 2GPP/3GPP2 are working to integrate security into the definition of NGN standards and protocols, in order to appropriately address security in the design phase of the new generation of networks.

ITU has ITU Global Cybersecurity Agenda – GCA which is an ITU framework for international cooperation aimed at proposing strategies for solutions to enhance confidence and security in the information society. It will build on existing national and regional initiatives to avoid duplication of work and encourage collaboration amongst all relevant partners.

At ITU-T, the international standardization of NGNs is underway as part of the NGN Global Standards Initiative⁵ - NGN-GSI, involving various standards organizations. The NGN-GSI focuses on developing the detailed standards necessary for NGN deployment so that service providers can offer the wide range of services expected from NGN.

ETSI TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking) has been the key standardization body in creating the NGN specifications since its creation in 2003. NGN Release #1 was finalized in December 2005, provided the robust and open standards that industry required for the development, testing and implementation of the first generation of NGN systems. NGN Release #2 was finalized in early 2008, and added key element to the NGN such as IP Multimedia Subsystem - IMS and non IMS based IPTV, Home Networks and devices, as well as NGN interconnect with Corporate Networks.

A major part of any security specification and of a security product is the measure of assurance it provides with respect to the security it offers. The Common Criteria as identified in ISO/IEC 15408. This is the best known tool for evaluation of security [6].

V. REQUIREMENTS OF E-GOVERNANCE SERVICES AND SECURITY

This section discusses the definition of security requirements for e-governance. Firstly the objectives of the governments, other related service providers and the expectations of the end users should be clearly defined. The e-governance services may cover the many type of users such as; from inside of the government, civilization (from cities, rural areas or from other countries), military forces, justice departments, national security units and some services from other governments etc.

The services of e-governance and its requirements have to

⁴ Critical Infrastructure Protection in the Baltic Sea Regions, chapter 3, 2007.

⁵ <http://www.itu.int/ITU-T/ngn/>

establish the availability, reliability and privacy from the point of view of the users, which can be classified according to different categories. Therefore,

- The security standards and policies are to be used by the all involved parties in the governments and industry. As presented in section 1, all critical and non-critical information infrastructures use the common CII.
- The governments should have incident response systems and policies for the emergency cases. Private actors should be involved, always in respect of business confidentiality and fair market rules. Specific e-Governance arrangements for security should be put in place.
- The public and private suppliers and users of e-government and e-governance services should be aware about the related security risks. The training for everybody is important requirement for the security, reliability and availability of e-governance services.
- The governments are doing investments to build e-governance services and its technological infrastructure, so the usage rates of these services are very important. To improve the usage rates, the training of the end users is an important aspect. Education system and methods should be evaluated for all level from first school to universities and for the public by the government. Dedicated e-Inclusion policies (for the elders, people with temporary or permanent disabilities, etc.) should be studied.
- ICT will give important possibilities to access all people to educate them. All citizens should be empowered from the functional and security viewpoints. Education can and should continue for the whole life-span of the people.

The security professionals, research and accreditation centers, service companies and organizations are necessary for the secure systems design, detection of vulnerabilities, threats and risks. For this objective;

- The universities and their departments and curriculums should be evaluated and updated. Security studies should be recognized as a key component of all relevant curricula – and not only the particular computer science department.
- Global research activities about ICT should be closely followed. The specific organizations, research centers and universities should join to global standardization organizations and follow the developments; since the earlier experiences are so valuable at the beginning of transformation to NGNs infrastructure and e-governance.
 - There are some early NGN implementations in UK and Japon. Their early NGN implementations -including field trials- were established in 2006 such incumbent operators as BT in the UK, NTT in Japan, and AT&T in the US. By the end of 2008, NTT expects to

offer complete NGN services on a full scale, and BT has announced that it expects half of its customer base to have migrated by 2008, and the migration to be "substantially complete" by the end of the decade[3].

- To use the same internationally approved terminology, concepts and security standards are other important facilitators of the e-governance.

The governments should reorganize the civil and governmental policies and should update the laws to support e-governance services and establish the security requirements as harmonized with inside and outside of the government regulations. So, the governments should sign all relevant international agreements for tracing criminals, and cyber warriors across borders.

VI. CONCLUSIONS

Standards and common criteria agreed at the international level should be accepted and be used globally in a harmonized structure. This requires a change in mentality in governments; since they have their own national traditions, institutional structures, policies and strategies, vocabulary, technical and methodological approaches.

In addition, e-governance requires the close interaction of public and private actors, and a shared approach to security. In an e-governance setting, governments had to take into consideration the opinions, concerns and positions of private actors. In the field of NGN, the security of the resulting critical infrastructure will depend on the convergence of positions among public and private actors.

Typically countries prefer not to publish their research results about vulnerabilities and threats as they might affect their national security, but to detect all vulnerabilities and threats is impossible for each individual country. Therefore, there is the need to develop the right arrangements for sharing their experiences in a global environment. The sharing of these information and usage should be regulated by international agreements and rules.

The CII security problem will never be solved completely, because the nature of the problem is NP-complete [8]. The governments therefore should:

1. Recognise that the security problem should be approached by complementing the best available science and technology with heuristic methods, as it is a NP-complete problem. So, as Einstein said that "The significant problems we have cannot be solved at the same level of thinking with which we created them", then we will do much more research on the problem with the new technologies which will have the heuristic abilities except Turing computational model.
2. Recognise that the security of CII and e-governance needs urgent solutions. The governments should support standardization research, other security-related research, and security education. New regulations,

standards should be created to force minimal level security goals for all ICT solutions. And, the governments should have an action plan and should do some investments to establish the requirements which are presented in section 5.

ACKNOWLEDGMENT

Thanks for the support of Assoc. Prof. Koltuksuz, A., Ph.D. from İzmir Institute of Technology Department of Computer Engineering, Turkey.

REFERENCES

- [1] G.Narayan, A.N.Nerurkar, "Value-proposition of e-governance services" International Journal of Education and Development using Information and Communication Technology (IJEDICT), 2006, Vol. 2, Issue 3, pp. 33-44.
- [2] ITU-T Recommendation Y.2001, approved in December 2004, available at <http://www.itu.int/rec/T-REC-Y.2001-200412-I/en>.
- [3] Next-Generation Networks and Energy Efficiency, ITU-T Technology Watch Briefing Report Series, No. 7, August 2008.
- [4] "Next-Generation Network Architecture: What and When?", Analysys Mason Group, Jan 2008, <http://www.researchandmarkets.com/reports/c82216>.
- [5] International Standards Organization. ISO/IEC 18045, Information Technology – Security techniques – Evaluation criteria for IT security, 2005.
- [6] S. Cadzow, "Security assurance and standards - design for evaluation", Secure Mobile Communications Forum: Exploring the Technical Challenges in Secure GSM and WLAN, 2004. The 2nd IEEE (Ref. No. 2004/10660) Volume, Issue , 23 Sept. 2004 Page(s): 8/1 - 8/6
- [7] International Standards Organization. ISO/IEC 18045, Information Technology – Security techniques – Evaluation criteria for IT security, 2005.
- [8] N.Li, Q.Wang, "Beyond Separation of Duty: An Algebra for Specifying High-Level Security Policies", Journal of the ACM, vol. 55, No 3, article 12, July 2008.
- [9] M.Masera, I.N.Fovino, R.Sgnaolin, "A Framework for the Security Assessment of Remote Control Applications of Critical Infrastructure", 2005.
- [10] E. P. Rathgeb, A.Krupp, H.Chair, "Dependable communication – vision or illusion?", Proceedings of the 32nd EUROMICRO Conference on Software Engineering and Advanced Applications, 2006.
- [11] P.Stuckmann, R.Zimmermann, "Towards Ubiquitous and Unlimited-capacity Communication Networks- European Research in FP7", European Commission, 2007.
- [12] "Trends in Telecommunication Reform 2007 The road to Next-Generation Networks (NGN), Summary", ITU Publication, September 2007.
- [13] National Risk Register of UK government, last updated 09 Nov. 2008 http://www.cabinetoffice.gov.uk/media/cabinetoffice/corp/assets/publications/reports/national_risk_register/national_risk_register_introduction.pdf
- [14] U.S. e- China Economic and Security Review Commission, Hearing on China's Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities, testimony of Colonel Gary McAlum, Washington, DC, May 20, 2008.

Türkiye’de Siber Güvenlik Yönetimine Yönelik Kurumsal Bir Yapılanma Önerisi

Türksel KAYA BENSGHİR, Sema ÖNAL ALTINSOY

Özet–Bu bildiride, bilişim uygulamaları önde olan bazı ülkelerde bilgi ve iletişim sistemleri ile bu sistemler üzerindeki bilgilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması olarak tarif edilen siber güvenliğin yönetiminde yer alan kuruluşlar ve bu kuruluşların etkinlikleri incelenmiş ve özellikle 2000’li yıllarda bilişim uygulamaları hız kazanan ülkemiz için, siber güvenliğin yönetimden sorumlu kurumsal bir yapılanma modeli önerilmiştir.

Anahtar Kelimeler–Siber güvenlik, bilgi, güvenlik yönetimi, örgütsel yapı, Türkiye.

Abstract–In this paper, it is examined the applications of some countries in cyber security management and organizational structures. A cyber security organizational structure model is proposed for Turkey.

Keywords–Cyber security, information, security management, organizational structure, Turkey.

I. GİRİŞ

Bilgi ve iletişim teknolojilerindeki (BİT) gelişmeler, bilgiye dayalı ekonomiyi ve bilgi toplumuna dönüşümü tetiklemiştir. BİT’lerin yaygın kullanımı, dünya üzerinde fiziksel mesafelerin önemini kaybetmesini sağlayarak farklı coğrafi konumlarda yaşayan bireyler ve topluluklar arasındaki etkileşimi artırmıştır. Teknolojik gelişmeler ve giderek artan küreselleşme olgusu ile birlikte dünyada, güvenlik yönetiminde de köklü değişim gündeme gelmiştir. Daha önce toprak bütünlüğü ve rejim güvenliği bağlamındaki milli güvenlik tanımı yeterli sayılırken; günümüzde bu tanım, devletin anayasal düzeninin, milli varlığının ve bütünlüğünün uluslararası alanda her türlü iç ve dış tehditlere karşı korunması ve kollanması şeklinde genişletilmiştir. Devletlerin sahip oldukları bilginin de iç ve dış tehditlere karşı korunması, güvenliğinin sağlanması ihtiyacı doğmuştur.

Bilgi toplumunda ulusların diğer güvenlik alanlarında olduğu gibi, bilgi güvenliği yönetiminde de tek başlarına etkili olamayacakları olgusu giderek daha yoğun bir şekilde hissedilmektedir. Ulusal ve uluslararası arenada “karşılıklı bağımlılık” ilkesi gereği, ancak zincirin tüm halkalarının güvenliğinin sağlanması durumunda başarılı bir güvenlik yönetimi, kabul görmüş bir yaklaşım olarak dikkat çekmektedir. Bu bağlamda, 90’lı yıllarda yoğun olarak bilgi güvenliği kavramı kullanılırken, 2000’li yılların

başlarından itibaren sadece bilginin değil bilginin üzerinde tutulduğu, işlem gördüğü, iletildiği tüm ortamların(küresel) güvenliğini anlatmaya yönelik sistemin tamamını temsil edecek şekilde, *siber güvenlik* kavramı kullanılmaya başlanmıştır. *Siber güvenlik*, bilginin üzerinde tutulduğu, iletildiği, işlem gördüğü bilgi ve iletişim sistemlerinin ve bu sistemler üzerindeki bilgilerin *erişilebilirlik*, *gizlilik*, *bütünlük* ilkelerine uygun bir şekilde korunması olarak tanımlanmaktadır.

Dünya üzerinde bilgi ekonomisi hız kazanırken gerek uluslararası kuruluşlar gerekse ülkeler siber güvenliğin sağlanmasında yeni yol ve yöntem arayışına girmekte ve yönetilmesi oldukça zor olan bu alan için farklı kurumsal yapılar ortaya koymaktadırlar.

Bu bildiride, bilgi toplumu içinde ağırlıklı yer edinen ve bilişim uygulamaları açısından önde olan kimi ülkelerin mevcut kurumsal yapıları ve uygulamaları incelenmiştir. Ülkemizde siber güvenlik alanında bu güne kadar yapılan çalışmalar değerlendirilerek siber güvenlik yönetiminden sorumlu bir kurumsal yapı önerisi ortaya konulmuştur.

II. YÖNTEM

Bildiri kapsamında gerek ulusal gerek uluslararası alanda yapılan çalışmalara ulaşmak için ayrıntılı yazın taraması yapılmıştır. Bu kapsamda güvenlik, bilgi teknolojileri literatürü taranmış, raporlar ve strateji belgeleri incelenmiştir. İnternet üzerinden araştırma yapılırken öncelikle ülkelerin resmi, kurumsal sayfalarına; strateji geliştirme merkezlerinin, web sayfalarına erişilmiştir. Güncel bilgileri kullanabilmek amacı ile dokümanların yakın dönemde hazırlanmış olmasına dikkat edilmiştir. Ağırlıklı olarak 2000-2008 yılları arasındaki dönem kapsayan kaynaklar kullanılmıştır. Ülkemize yönelik öneri geliştirme aşamasında alanda uzman kişilerle yapılan görüşmelerden elde edilen bilgiler de dikkate alınmıştır.

III. BAZI ÜLKELERİN SİBER GÜVENLİK KURUMLARI

Bildiri kapsamında ABD, Finlandiya, Fransa, İngiltere ve Japonya’nın özellikle 2000–2008 yılları arasındaki dönemde siber güvenliğe ilişkin kamu teşkilatları incelenmiştir. Bu ülkelerin neden inceleme kapsamına alındığının gerekçelerini şöyle özetleyebiliriz:

- ABD, tek kutuplu dünya düzeninde bilişim uygulamalarında lider konumda olduğu,
- Finlandiya, özellikle iletişim sektöründeki öncü İskandinav ülkelerinden biri olduğu,
- Fransa, ülkemizin mevcut kamu yönetimi yapılanması ile benzerlik gösterdiği,

TÜRKİYE'DE SİBER GÜVENLİK YÖNETİMİNE YÖNELİK KURUMSAL BİR YAPILANMA ÖNERİSİ

2

- İngiltere, Türkiye'deki e-devlet yapılanmasında örnek ülke olarak alındığı,
- Japonya ise 20. yüzyılda bilim ve teknoloji alanında gerçekleştirdiği ilerlemelerle dikkat çektiği için araştırma kapsamına alınmıştır.

Bu ülkelerin siber güvenlikle ilgili kuruluşları, kuruluşların bağlı olduğu üst birimler ve temel görevleri EK'de sunulan Tablo-1'de özetlenmiştir.

Ülkelerin siber güvenlik stratejilerinde kamu, özel sektör, sivil toplum örgütleri, vatandaş vb. tüm aktörlerin katılımı ile gerçekleştirilecek ortak çalışmalar ile siber güvenliğin daha sağlıklı yürütülebileceği üzerinde durulmaktadır. Bu belgelerde uluslararası kuruluşlar ile birlikte çalışmanın da önemine değinilmektedir.

Bu ülkelerin hemen tümünde;

- Teknolojik gelişmelere paralel olarak siber güvenlikle ilgili kurumlarda sürekli bir yeniden yapılanma çalışmasına gidildiği;
- Siber güvenliğe ilişkin politika ve stratejileri belirleyen, uygulanmasını takip eden, yönetime rapor sunup gerektiğinde stratejiyi güncelleyen birer kurul olduğu;
- Siber güvenliğe ilişkin yapılan çalışmaların diğer kamu kurum ve kuruluşları, özel sektör, sivil toplum örgütleri, üniversiteler vb. ile koordine edilerek yürütüldüğü ve bunları koordine eden birimler kurulduğu,
- Konu ile ilgili uluslararası kuruluşlarla ilişkiyi sağlayacak birimlerin teşkil edildiği,
- Kamu ve özel sektöre yardımcı olmak üzere bilgisayar acil durum müdahale ekiplerinin oluşturulduğu,
- Emniyet teşkilatları içinde ileri teknoloji suçları ile mücadele amaçlı teknolojiyi takip eden birimlerin kurulduğu görülmüştür.

IV. TÜRKİYE'DE SİBER GÜVENLİK YÖNETİMİ

Ülkemizde bilgi güvenliği konusuna Yedinci Beş Yıllık Kalkınma Planı'ndan itibaren her geçen dönem artan bir şekilde yer vermeye başlanmıştır[1]. Ancak kavram olarak siber güvenlik, son dönemde konuşulmaya başlanmıştır.

Türkiye'de yalnızca siber güvenlikten sorumlu ve görevli bir kamu kurumu bulunmamaktadır. 1999 yılında yayınlanan TUENA Sonuç Raporunda[2], Bilgi Toplumu Bakanlığı, Bilgi Teknolojileri Konseyi, Düzenleyici Kuruluş ve Bilgi Toplumu Kurumu'nun oluşturulması, güvenlik hizmetinin de Bilgi Toplumu Kurumu görevleri arasında yer alması önerilmektedir. Yine bu rapor içinde Güven Çalışma Grubu[3] tarafından önerilen Ulusal Bilgi Güvenliği Üst Kurulu ve Bilgi Güvenliği Kurumu teşkiline ilişkin teklif [4] değerlendirilmektedir. Kanun tasarısında tanımlanan görevlerin tamamlanması yapılmasının zorunlu olduğu belirtilmekte ancak bilgi altyapısına yönelik

yapılanmanın daha öncelikli olduğu vurgulanmaktadır. TUENA Projesi Sonuç Raporu uygulamaya konulmadığı için bilgi altyapısına yönelik bir teşkilatlanma yoluna da gidilmemiştir.

Kritik tesislerin belirlenmesi ve bu tesislerin çevresinde özel güvenlik bölgesi tesis edilmesine yönelik çalışmalarda, ilgili kurumlar arası koordinasyonu, MGK Genel Sekreterliği birimleri gerçekleştirmektedir.

2003 yılından itibaren uygulamasına geçilen e-Dönüşüm Türkiye Projesinde siber güvenliği sağlamak üzere sorumlu ya da ilgili kuruluş olarak tanımlanan kurumsal yapılara ilişkin bilgiler, EK'de sunulan Tablo-2'da özetlenmiştir.

Bu çalışmada edinilen bilgiler ışığında ülkemizdeki mevcut durumun ana hatları şöyle özetlenebilir:

- Türkiye'de özel bir siber güvenlik politikası bulunmamakla birlikte, kritik altyapıların korunması ve e-Dönüşüm Türkiye Projesi kapsamında konu ile ilgili faaliyetler icra edilmektedir. Ancak bu faaliyetler, tüm kurum ve kuruluşlardaki bilgi ve iletişim sistemlerinin güvenliğini sağlayacak nitelikte, temel politikaların oluşturulmasından, takibinden, ilgili kurumlar arası koordinasyonu başarılı bir şekilde gerçekleştirecek uzun vadeli politikalardan uzak olup; daha çok kısa süreli, günlük çözümlere yöneliktir.
- Türkiye'de sadece siber güvenlikten sorumlu, politikalar ve stratejiler üreten, bunları takip eden bir kurum bulunmamaktadır. DPT Bünyesinde görev yapmakta olan Bilgi Toplumu Dairesi tarafından koordine edilmekte olan Bilgi Toplumu Stratejisi kapsamında konuya yönelik eylemler tanımlanmıştır. Her eylem için sorumlu ve ilgili kamu kurum kuruluşları belirlenmiştir. Ancak belirlenen bu kurumların temel görevleri siber güvenliği sağlamak değildir ve tümünün uyması gereken bir siber güvenlik stratejisi bulunmamaktadır. Bilgi Toplumu Dairesinin ilgilendiği konuların çokluğu ve yoğunluğu, buna karşılık personel sayısının kısıtlılığı nedenleri ile bilgi güvenliğine yönelik eylemlerin takip ve koordinasyonunu sağlıklı bir şekilde gerçekleştiremediği, bu alanda önemli boşluğun ortaya çıktığı gözlenmektedir.
- Ulusal Bilgi Güvenliği Yönetimine ilişkin Ulusal Bilgi Güvenliği Teşkilatının Tesisi Kanun Tasarısı, 1997 yılından bu yana üzerinde çalışılıyor olmasına rağmen henüz kanunlaşmamıştır. Bu süreç içerisinde, dünyadaki siber güvenlik kurumlarının teşkilatlanmasında değişiklikler olmuş, ülkemizde de bu kanun tasarısı ile oluşturulması planlanan Ulusal Bilgi Güvenliği Kurumu tarafından gerçekleştirilmesi öngörülen görevlerin büyük çoğunluğu TÜBİTAK UEKAE, TÜRKSAT, TK, TSE gibi mevcut başka kurumlar tarafından gerçekleştirilmeye başlanmıştır.

TÜRKİYE'DE SİBER GÜVENLİK YÖNETİMİNE YÖNELİK KURUMSAL BİR YAPILANMA ÖNERİSİ

3

- Ulusal siber alan müdahale ve alarm sistemi çalışmaları, TÜBİTAK UEKAE[5] sorumluluğunda yakın zamanda kurulan Bilgisayar Olayları Müdahale Ekibi (BOME)[6] tarafından yürütülmektedir. Siber güvenliğe ilişkin risk yönetimi, danışmanlık hizmeti verecek profesyonellerin özel olarak eğitilmesi, tüm siber alan kullanıcıları için farkındalık ve eğitim programlarının hazırlanması; bilgi sistemleri ve güvenlik planları ile uyumlu rehber uygulamaların ve referansların geliştirilmesi gibi çalışmalar TÜBİTAK UEKAE tarafından yürütülmektedir. Yeni dünya düzeni içinde güçlü devletler arasına girebilmek için bilgi ve iletişim teknolojilerinin sadece kullanıcı değil aynı zamanda üreticisi ve geliştiricisi de olmak gerekmektedir. Bu hedefe yönelik olarak gerekli araştırmaları yapmak, teknolojik ürünleri geliştirmek üzere TÜBİTAK, siber alanın güvenliğine yönelik teknolojiyi geliştirme ana hedefi ile de UEKAE kurulmuştur. Siber güvenlik yönetiminde TÜBİTAK UEKAE önemli aktörlerden birisidir. Ancak, başka kurumsal yapılar tarafından yürütülebilecek görevler de bu kuruma yüklenerek kendi görevlerini yapamaz ya da geciktirir duruma getirilmemelidir.

Devletin siber alanının güvenli hale getirilmesi ve güvenilirliğinin artırılması konusunda TÜRKSAT A.Ş.[7] görevlendirilmiş olmakla birlikte bu görevlendirmenin sadece e-devlet kapısı kapsamında olduğu, bu proje dışında kalan kamu bilgi ve iletişim sistemlerinin güvenli kullanımı için Türkiye'de bütünleşik bir yapılanmanın bulunmadığı gözlenmektedir.

İletişim sektöründe serbestleşme ve rekabetin korunmasına yönelik çalışmalar yapmak üzere kurulan Telekomünikasyon Kurumu[8], kendi görev alanını kapsayacak şekilde e-imzaya ilişkin düzenlemeleri yapmış olup uluslararası kuruluşlar ile işbirliği çalışmalarına ağırlık vermektedir. Ancak bu kurumun kuruluş amacı farklı olduğu için doğrudan siber güvenlik konusu ile ilgili çalışmaları bulunmamaktadır.

Türk Standartlar Enstitüsü[9], diğer standartların yanı sıra bilgi güvenliğine yönelik uluslararası kuruluşların geliştirdiği standartları da Türkçe'ye çevirerek yayınlamakta, konu ile ilgili farkındalık yaratıcı çalışmalar gerçekleştirmektedir. Kamu ve özel sektör kurumları için Bilgi Güvenliği Yönetim Sistemi(BGYS) kurulum denetimini de yapmaktadır. Ancak tüm kamu kurumlarına yönelik bir çerçeve plan ve bu planın uygulanmasını takip edecek sorumlu bir kurumsal yapı bulunmadığı için BGYS kurulumları verimli bir şekilde gerçekleştirilememektedir.

Emniyet Genel Müdürlüğü'nün siber suçlarla mücadele ve adli analiz konularında son dönemde kayda değer yapılanma içinde olduğu ve personelin bu yönde eğitiminde önemli mesafeler kaydettiği gözlenmektedir.

Siber güvenliği sağlamak üzere kamu, özel sektör, üniversiteler, sivil toplum örgütleri vb. ile diğer ülkeler ve

uluslararası kuruluşlarla bölgesel ve uluslararası işbirliğini geliştirecek sorumlu bir kuruluş bulunmamaktadır.

Siber güvenliğin ihlal edildiği durumlar sonrasında normale dönüş uygulamalarını kapsayan kriz yönetimi, Başbakanlık Kriz Yönetim Merkezi tarafından gerçekleştirilmekte olan genel tatbikatlarda kısıtlı bir şekilde alt konu başlıklarından biri olarak ele alınmaktadır. Ancak bu alanda asıl sorumlu kurum belli değildir.

V. ÜLKEMİZDE SİBER GÜVENLİK YÖNETİMİNE İLİŞKİN KURUMSAL YAPI ÖNERİSİ

Ülkemizde siber güvenlik yönetiminde kurumsal yapılanma modeli diğer ülke uygulamalarında olduğu gibi tüm aktörlerin katılımını sağlayacak şekilde yönetim yaklaşımı ile geliştirilebilir. Bu bağlamda öncelikle ulusal düzeyde siber güvenlik strateji ve politikaları geliştirmekle sorumlu bir *Siber Güvenlik Kurul'u* oluşturulmalıdır. (Çizim 1, Bkz EK) Bu kurul, yaptırımcı etkisinin güçlü kılınması için Başbakan tarafından görevlendirilecek bir Devlet Bakanı başkanlığında, ilgili Bakanlıkların, Milli Güvenlik Kurulu Genel Sekreterliği, TSK, Milli İstihbarat Teşkilatı Müsteşarlığı, Türkiye Bilimsel ve Teknik Araştırma Kurumu Başkanlığı ve konu ile ilgili diğer kurumların en üst düzey yöneticilerinden oluşturulmalıdır.

Siber Güvenlik Kurulunun sekreteryası hizmetlerini yürütecek; konu ile ilgili kurumlararası koordinasyonu gerçekleştirecek; üst düzey politikanın ve stratejinin ilgili tüm paydaşların katılımı ile hazırlanmasını sağlayacak; bu politika ve strateji doğrultusunda tüm kamu kurumları tarafından uygulanacak çerçeve planları hazırlayacak ve bu planların uygulanmasını takip ve koordine edecek bir kurumsal yapıya ihtiyaç bulunmaktadır.

Böyle bir kurumsal yapı, Ulusal Bilgi Güvenliği Teşkilatının Tesisi Kanun Tasarısı Taslağı kapsamında tanımlanan şekilde, görev alanında bazı kısıtlamalara gidilerek gerçekleştirilebileceği gibi mevcut kurumlardan birine de bu görev verilerek gerçekleştirilebilir. Bu görev, halihazırda Başbakan'a doğrudan bağlı ya da Başbakanlığa[10] bağlı olarak görev yapmakta olan, güvenlik işleri ile ilgili politikalar üreten, çalışmalar yapan bir kurumsal yapı altında oluşturulacak Siber Güvenlik Birimi'ne de verilebilir.

Siber Güvenlik Birimi'nde, bilişim teknolojilerinin kullanımı ve siber güvenlik konularında uzmanlaşmış, aynı zamanda kamu yönetimi alanında da eğitilmiş, yeni kamu yönetimi yapısına uygun çalışmalar içinde bulunabilecek görevliler ile hukuk ve uluslararası ilişkiler konularında deneyimli, yeniliklere açık uzmanların oluşturduğu çekirdek bir kadro yapısı kurulmalıdır.

Siber Güvenlik Kurulu, daha önce belirlenen gündeme uygun olarak belli periyotlarla toplantılar yapmalıdır. Toplantılara sorumlu Devlet Bakanı, onun olmadığı durumlarda Siber Güvenlik Biriminin bağlı olduğu kurumun en üst düzey yöneticisi başkanlık etmelidir. İhtiyaç duyulması halinde bu toplantılara, konu ile ilgili özel sektör kuruluşları, sanayi temsilcileri, sivil toplum

TÜRKİYE'DE SİBER GÜVENLİK YÖNETİMİNE YÖNELİK KURUMSAL BİR YAPILANMA ÖNERİSİ

4

örgütlerinin temsilcileri de davet edilebilmelidir. Toplantılarda alınan kararlar doğrultusunda, Siber Güvenlik Biriminin koordinasyonu ile katılımcı kurumların temsilcilerinden Çalışma Grupları teşkil edilmelidir.

Temel olarak kamu kurumları tarafından uygulanacak ancak, özel sektör, üniversiteler, STK, kullanıcılar vb. tüm paydaşlar için de yol gösterici olacak şekilde, Siber Güvenlik Stratejisi ile uyumlu çerçeve planlar hazırlanmalı ve uygulamalar izlenmelidir. Ayrıca siber güvenlik ile ilgili farkındalığın artırılması, personelinin eğitilmesi, uluslararası kuruluşlarca kabul görmüş siber güvenlik standartların benimsenmesi, güvenlik risk analizlerinin yapılarak gerekli önlemlerin alınması gibi konular kamu kurumlarının Strateji Geliştirme birimlerinde tesis edilecek siber güvenlik birimlerinin sorumluluğunda olmalıdır. Uygulamanın takibi, bu birimlerden alınacak geribildirimler kullanılarak Siber Güvenlik Birimi tarafından yapılmalıdır.

Siber alanın güvenliğine yönelik Bilgisayar Olayları Müdahale Ekibi'nin TÜBİTAK bünyesi yerine, normal duruma dönüş çalışmalarını da kapsayan kriz yönetimi görevini de üstlenecek şekilde Türkiye Acil Durum Yönetimi Genel Müdürlüğü bünyesinde kurulması, ancak TÜBİTAK UEKAE ile çok sıkı işbirliği içinde çalışması düşünülebilir. Bu birimin edindiği tecrübelerin diğer tüm kurumlarla paylaşılmasının da, Siber Güvenlik Birimi tarafından sağlanması yerinde olacaktır.

Kamu kurumlarına yönelik siber güvenlik standartlarına uygun risk yönetiminin ilgili kurumların Strateji Geliştirme Birimleri tarafından yapılması ya da yaptırılması, uygulamanın takibinin ise Siber Güvenlik Birimi tarafından gerçekleştirilmesi yoluna gidilebilir. Siber güvenlik

alanında profesyonellerin eğitimi, yine TÜBİTAK UEKAE tarafından vermeye devam edilmelidir. Kamu kurumlarındaki siber güvenliğin sağlanması ile görevlendirilen Strateji Geliştirme Birimleri kapsamındaki çalışanların konu ile ilgili eğitimi, yine Siber Güvenlik Birimi tarafından yapılacak çalışmalar sonucu hazırlanan çerçeve planlar doğrultusunda, bu birimin koordinasyonu ile TODAİE tarafından verilmesi düşünülebilir. Kamu kurumlarındaki son kullanıcıların eğitimi ve farkındalık yaratılması işlemi de yine kurumların Strateji Geliştirme Birimleri tarafından, Siber Güvenlik Birimi'nin koordinesi ile çalışma grupları tarafından hazırlanmış olan çerçeve planlar dahilinde gerçekleştirilmelidir.

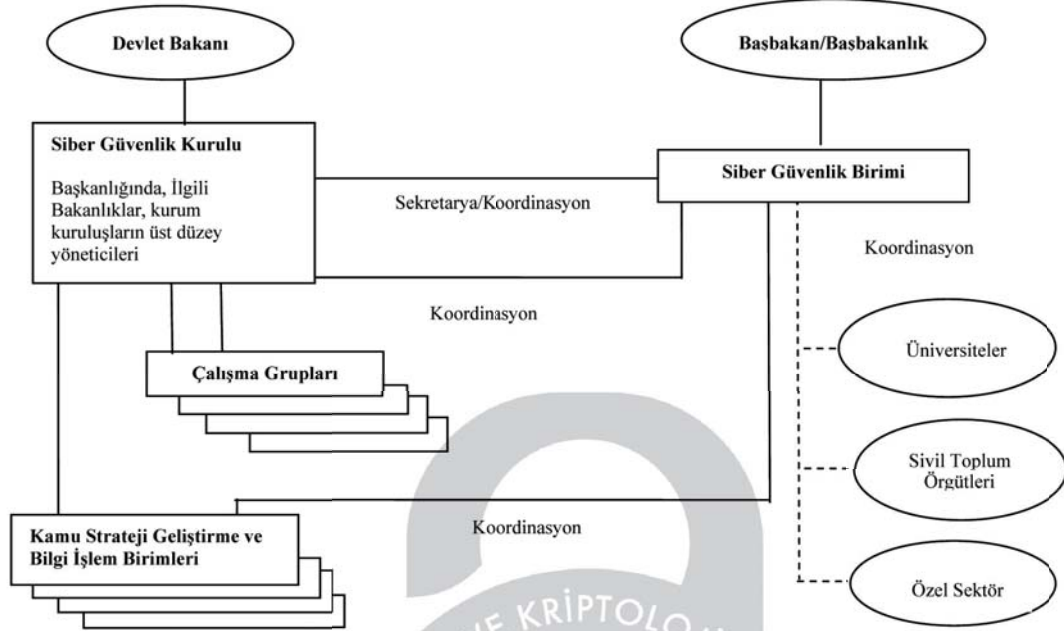
Devlet, tüm vatandaşlarının bilgilerinin güvenliğinden de sorumlu olduğu için siber alan kullanıcıları tüm vatandaşlara yönelik çözümleri kapsayan çerçeve planların hazırlanması da Siber Güvenlik Birimi'nin çalışma alanı içinde olmalıdır.

VI. SONUÇ

Bilgi çağında, dünyanın önde gelen ülkeleri arasında yer almayı hedefleyen Türkiye'nin başarılı bir siber güvenlik politikası uygulayabilmesi için, yönetsel düzeyde siber güvenlik politikalarını oluşturacak bir Siber Güvenlik Kurulu ile bu kurulun sekretarya hizmetlerini yürütecek, belirlenen politikaların takibini ve ilgili ulusal-uluslararası kuruluşların koordinasyonunu gerçekleştirecek bir Siber Güvenlik Birimi'nin görevlendirilmesi için gerekli yasal çerçeve ivedilikle hazırlanmalıdır.

EKLER

Çizim-1:Türkiye İçin Siber Güvenlik Yönetimi Kurumsal Yapı Önerisi:



Tablo 1: İncelenen Ülkelerde Siber Güvenlik Kuruluşları

Ülke	Üst Birim	Kuruluş	Görevleri
ABD	İç Güvenlik Bakanlığı	İç Güvenlik Danışma Konseyi Ulusal Altyapı Danışma Konseyi [11] Kritik Altyapı Ortaklığı Danışma Komitesi [12]	Danışmanlık ve koordinasyon
		Politika Ofisi [13]	Danışmanlık ve Koordinasyon
		Ulusal Koruma ve Programlar Direktörlüğü Ulusal Siber Güvenlik ve İletişim Ofisi [14]	Koordinasyon Ulusal Siber Alan Müdahale Sistemi Siber risk yönetimi
		Ulusal Koruma ve Programlar Direktörlüğü Altyapı Koruma Ofisi [15]	Standart Belirleme Kritik altyapı varlıklarının korunması Önleyici tedbirlerin belirlenmesi Koordinasyon
		Ulusal Koruma ve Programlar Direktörlüğü Yönetim Birimleri Arası Programlar Ofisi [16]	Devletin tüm birimleri için savunma, Farkındalık yaratma Koordinasyon
		Ulusal Koruma ve Programlar Direktörlüğü Risk Analizi ve Yönetimi Ofisi [17]	Ulusal seviyede risk yönetimi standartları ve metriklerinin belirlenmesi Risk analizi ve değerlendirmesinin yapılması
		Bilgisayar Olayları Acil Durum Müdahale Ekibi [18]	Operasyonel siber tehditleri ve zafiyetleri azaltmak, analiz etmek, Uyarı bilgilerini yayınlamak, Olay müdahale etkinliklerinin koordinesi
	ABD Kongresi	Gerçekleşen Tehditler, Siber Güvenlik ve Bilim Teknoloji Alt Komitesi [19] Devlet Saymanlık Ofisi [20]	Danışmanlık Denetleme
	Başbakanlık	Ulusal Güvenlik Ajansı [21]	Devlet Sistemlerinin bilgi güvenliğinin sağlanması Kriptoloji eğitimi Siber tehditlerin araştırılması, raporlanması Kriptografik kod geliştirme
	Adalet Bakanlığı	Bilgisayar Suçları ve Fikri Mülkiyet Bölümü [22]	Bakanlığın ulusal stratejisinin geliştirilmesi, Bilişim suçlarının önlenmesi, Tetik ve kovuşturma işleminin tüm kamu kurumları ile koordineli bir şekilde gerçekleştirilmesi

Finlandiya	İletişimi Düzenleme Otoritesi (FICORA) [23]	Bilgi Teknolojileri Bölümü Ağlar ve Güvenlik Bölümü	Farkındalığı artırmak, İlgi ve iletişim sistemleri güvenliğinin sağlanması Tehditlerin raporlanması Uluslararası ilişkilerin sağlanması
		Bilgisayar Olayları Acil Durum Müdahale Ekibi(CERT-FI) [24]	Tüm dünyadaki bilgi güvenliği olaylarını takip etmek, Kılavuzlar yayınlamak, Problem çözümüne destek, İhlalleri önleme amaçlı bilgi yayınlamak.
	Sanayi Ticaret Bakanlığı	Ulusal Acil Durum Destek Ajansı (NESA) [25]	Kritik altyapılara yönelik tehdit ve risklerin yönetimi.
	Maliye Bakanlığı	Kamu Bilgi Güvenliği Yönetim Konitesi (VAHTI) [26]	Kullanım kılavuzlarının yayınlanması
	Başbakanlık	Ulusal Bilgi Güvenliği Danışma Kurulu [27]	Ulusal Bilgi Güvenliği Stratejisinin uygulanması etkinliklerinin koordinasyonu ve takibi
Fransa	Başbakanlık	Ulusal Savunma Genel Sekreterliği Bilgi Sistemleri Güvenliği Merkez Yönetimi [28]	BS güvenlik politikaları hakkındaki hükümet kararlarının hazırlanması, koordinasyonu, uygulanması ve takibinde Başbakan'a danışmanlık
	Ulusal Savunma Genel Sekreterliği Bilgi Sistemleri Güvenliği Merkez Yönetimi	Bilgisayar Acil Durum Müdahale Takımları [29] CERT-Renater CERT-A CERT-IST	BG bilgilerini toplama, uyarılar, müdahale ve önleme konularında danışmanlık
	Başbakanlık	BT Stratejik Danışmanlık Kurulu [30] (Kamu Özel Sektör Yöneticileri)	Koordinasyon, Eylem önceliklerinin belirlenmesi Kritik bilgi altyapılarının korunmasında uygulamayı takip
		Fransa Güvenilirlik Enstitüsü [31] Otomotiv,askeri, uzay sanayi, profesyonel örgüt temsilcileri, sanayi temsilcileri	Proje geliştirme Uluslararası temsil Forum düzenleme
	İçişleri Bakanlığı	İleri Teknoloji Suçları ile Savaş Merkez Ofisi [32]	Yasal soruşturmalara destek, yargıfama (emniyet-jandarma-interpol)
İngiltere	Başbakanlık	Ulusal Altyapı Güvenliği Koordinasyon Merkezi [33] (Kamu ve Özel Sektör Temsilcileri)	Koordinasyon Saldırı alarmları yayınlamak Tehdit-Zafiyet araştırması Ciddi saldırılara cevap vermede destek
	Ulusal Altyapı Güvenliği Koordinasyon Merkezi	Birleştirilmiş Olay Raporlama ve Alarm Grubu (UNIRAS) [34]	Kamu kurumları ve kritik ulusal altyapı işleri yapan firmalara ulusal teknik destek
		İletişim-Elektronik Güvenlik Grubu (CESG) [35]	BG politikasını yayınlama, Risk değerlendirmesinde teknik öneriler
		Sanayi ve Ticaret Bakanlığı [36]	ISO 17799'u geliştirme, Küçük ve orta ölçekli işletmeler için BG sistemi kurulması
		İçişleri Bakanlığı [37]	Yönetim Kurulu'na başkanlık etme, Basın merkezi hizmeti
		Savunma Bakanlığı [38]	Teknik araştırmalara katkı
		Polis Teşkilatı (Ulusal Yüksek Teknoloji Suç Birimi) [39]	Suç önleme, Saldırı tespit
		Güvenlik Servisi (Ulusal Güvenlik Danışma Merkezi)	Tehdit, sorgulama, istihbarat, koruyucu güvenlik için teknik destek
	(Bakanlar Kurulu) Bilgi Güvenilirliği Merkez Sponsoru (CSIA)	Ulusal İleri Teknoloji Suç Birimi [40]	Polis teşkilatı altında, e-suç önleme, raporlama, sorgulama
		İçişleri Bakanlığı [41]	Kritik ulusal altyapıların korunmasına yönelik faaliyetler
		İletişim Elektronik Güvenlik Grubu [42]	Kamu işlerinin güvenliğini sağlamak üzere önerilerde bulunmak.
Japonya	Başbakanlık	Kriz Değerlendirme ve Takip Sekreteryası [43]	Mukavemeti artırmak
		Ulusal Bilgi Güvenliği Merkezi (NISC) [44]	Kamu-özel sektör koordinasyonu Temel strateji belirleme Çerçeve plan oluşturma Müdahale kapasitesi Kritik bilgi altyapısının korunması Uluslararası strateji geliştirme
	Bakanlar Kurulu	Bilgi Güvenliği Politika Konseyi (Başbakan, Devlet Bakanları, İçişleri ve İletişim Bakanı, Özel Sektör temsilcileri, Ulusal Kamu Güvenliği Komisyon Başkanı) [45]	Temel strateji geliştirme Politikanın uygulanmasının takibi Kılavuz yayınlama Acil durum müdahale
		Bilgi Politikaları Bölümü [46]	BG stratejisinin uygulanması, olay müdahale ve değerlendirme sistemi siber saldırılara karşı özel sektör ve kullanıcılara bilgi sağlama
		Ulusal Polis Ajansı (İleri Teknoloji Suçları Önleme Bölümü) [47]	Siber terör:steri yakalama, etkilerini azaltma, farkındalık yaratma
	Bakanlar Kurulu	Ulusal Bilgisayar Olayları Müdahale Ekibi [48]	Güvenlik claylarını incelemek Teknik önlemler geliştirmek Danışmanlık
		Bilgisayar Olayları Acil Durum Müdahale Ekibi Koordinasyon Merkezi	Güvenlik clayları ve zafiyetlere ilişkin bilgi toplamak Uyarılar yayınlamak

Tablo 2: Türkiye'nin Siber Güvenlik Kurumları

Bağlı/İlgili/İlişkili Olduğu Kurum	Siber Güvenlik Kurumu	Amacı
Başbakan	e-Dönüşüm Türkiye İcra Kurulu (Devlet Bakanı, Milli Eğitim Bakanı, Ulaştırma Bakanı, Sanayi ve Ticaret Bakanı, Başbakanlık Müsteşarı, DPT Müsteşarı, Başbakanlık Başmüşaviri)	BT Stratejisinin uygulanması sürecinde en üst düzey politika belirleme, karar alma, değerlendirme, yönlendirme
Başbakanlık	DPT Bilgi Toplumu Dairesi Başkanlığı	e-Dönüşüm Türkiye Projesinin koordinasyonu ve BT Stratejilerinin belirlenmesi
Başbakanlık	TÜBİTAK UEKAE	BG, haberleşme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim teknoloji üretim merkezi olmak
Ulaştırma Bakanlığı	TÜRKSAT A.Ş.	Kamu güvenli ağı kurulması, BS'leri olağanüstü durum merkezi kurulması
Ulaştırma Bakanlığı	TK	e-imza yapılmasına ilişkin tüm kamu kurum ve kuruluşlarının aynı kurumsal sertifika yapısı altında toplanmasının sağlanması.
Sanayi ve Ticaret Bakanlığı	TSE	Kamu ve özel sektör kuruluşları için BGYS ve Ortak Kriterler Belgelendirmesi ve kurulunun denetimini yapmak.
Başbakanlık	DTM	e-Ticaret güvenlik altyapısının sağlanması
İçişleri Bakanlığı	EGM	Bilişim suçları hakkında bilgi toplamak, değerlendirmek ve bu faaliyetleri önlemek amacıyla gerekli tedbirleri almak ve operasyonlar düzenlemek.

KAYNAKLAR

- [1] DPT, *Yedinci Beş Yıllık Kalkınma Planı*, Resmi Gazete Yayın Tarihi: 25. 07. 1995, Sayısı: 22354 Mükerrer, s.88.
- [2] DPT, *Sekizinci Beş Yıllık Kalkınma Planı*, Resmi Gazete Yayın Tarihi: 05. 07. 2000, Sayısı: 24100 Mükerrer, s. 130-131. DPT, *Dokuzuncu Kalkınma Planı*, Resmi Gazete Yayın Tarihi: 01. 07. 2006, Sayısı: 26215 Mükerrer, s.77,97-98.
- [3] Başbakanlığın, 5 Şubat 1996 tarihli bir yazısı ile *Türkiye'de Enformasyon Politikası ve Enformasyon Altyapısı Master Planı'nın oluşturulması* direktifi gereğince Ulaştırma Bakanlığı koordinatörlüğü ve TÜBİTAK Başkanlığı'nın sekreteryasında 1996 da başlayan çalışmalar ile oluşturulmuştur. (Ayrıntılı bilgi için Bkz. T.C.Ulaştırma Bakanlığı, *Türkiye Ulusal Enformasyon Altyapısı Anaplanı Sonuç Raporu*, Ekim 1999, TUENA Ofisi, ANKARA.
- [4] Türkiye'de bilgi güvenliğine yönelik ilk kurumsal yapılanma önerisini getiren ve Genel Kurmay Başkanlığı bünyesinde oluşturulan çalışma grubudur. (Ayrıntılı bilgi için Bkz. Pelin Ögüt, Yüksek Lisans Tezi, *Küreselleşen Dünyada Bilgi Güvenliğine Yönelik Politikalar: Sayısal İmza Teknolojisi ve Türkiye*, 2006, Ankara, s. 76.
- [5] http://www.tbd.org.tr/genel/bizden_detay.php?kod=245&tipi=5&sube=0
- [6] <http://www.uekae.tubitak.gov.tr/hakkimizda.php>
- [7] Mehmet ERİŞ, "Türkiye-Bilgisayar Olayları Müdahale Ekibi (TR-BOME)" başlıklı sunum, 3. TÜBİTAK-UEKAE Bilgi Teknolojileri Güvenlik Konferansı Sunumları - Kamu (6 Haziran 2008) http://www.bilgiguvenligi.gov.tr/index.php?option=com_content&task=view&id=252&Itemid=6
- [8] 20 Nisan 2006 tarihli 26145 sayılı Resmi Gazete'de yayınlanarak yürürlüğe giren 2006/10316 sayılı Başbakanlık Genelgesi
- [9] http://www.tk.gov.tr/Kurum_Hakkinda/Kurulus.htm
- [10] "Güvenlik Yönetim sistemleri, Ürün ve Hizmet Güvenliğinde TSE" başlıklı sunum, Dilek ÖZEREN, 6/7 Mart 2007 "Bilgi Güvenliği ve Yazılım Kalitesi Sempozyumu, TSE ANKARA) <http://www.tse.org.tr/turkish/duyuruyayin/bilgiguvenligi/dozeren.pdf>
- [11] <http://www.basbakanlik.gov.tr>
- [12] http://www.dhs.gov/xinfo/share/committees/editorial_0331.shtm
- [13] http://www.dhs.gov/xinfo/share/committees/editorial_0353.shtm
- [14] http://www.dhs.gov/xabout/structure/editorial_0870.shtm
- [15] www.ncs.gov; ww.dhs.gov/xabout/structure/editorial_0839.shtm
- [16] http://www.dhs.gov/xabout/structure/editorial_0794.shtm
- [17] http://www.dhs.gov/xabout/structure/editorial_0794.shtm
- [18] <http://www.uscert.gov/aboutus.html>
- [19] <http://www.hsc.house.gov/about/subcommittees.asp>
- [20] I. Abele-Wigert, M. Dunn, 13 April 2006, s. 325.
- [21] <http://www.nsa.gov/about/>
- [22] <http://www.usdoj.gov/criminal/cybercrime/index.html>
- [23] <http://www.itu.int/cybersecurity/search/search.aspx?StrCountry=FIN>
- [24] Cybersecurity Gateway –Finlandiya-For Government, <http://www.itu.int/cybersecurity/search/search.aspx?StrCountry=FIN>
- [25] I. Abele-Wigert, M. Dunn, 13 April 2006, s. 90.
- [26] I. Abele-Wigert, M. Dunn, 13 April 2006, s. 91.
- [27] Cybersecurity Gateway –Finlandiya-For Government, <http://www.itu.int/cybersecurity/search/search.aspx?StrCountry=FIN>
- [28] www.ssi.gouv.fr/en/dcssi/indexes.htm
- [29] I. Abele-Wigert, M. Dunn, 13 April 2006, s.103–104.
- [30] I. Abele-Wigert, M. Dunn, 13 April 2006, s. 103.
- [31] I. Abele-Wigert, M. Dunn, 13 April 2006, s.103–104.
- [32] I. Abele-Wigert, M. Dunn, 13 April 2006, s. 102.
- [33] I. Abele-Wigert, M. Dunn, 13 April 2006, s.297– 300.
- [34] http://www.dh.gov.uk/en/Policyandguidance/informationpolicy/informationsecurity/DH_4015419
- [35] <http://www.cesg.gov.uk/site/about/index.cfm>
- [36] http://www.cabinetoffice.gov.uk/csia/key_organizations
- [37] http://www.cabinetoffice.gov.uk/csia/key_organizations
- [38] http://www.cabinetoffice.gov.uk/csia/key_organizations
- [39] http://www.cabinetoffice.gov.uk/csia/key_organizations
- [40] http://www.cabinetoffice.gov.uk/csia/key_organizations
- [41] http://www.cabinetoffice.gov.uk/csia/key_organizations
- [42] <http://www.cesg.gov.uk/site/about/index.cfm>
- [43] I. Abele-Wigert, M. Dunn, 13 April 2006, s. 301.
- [44] "Japanese Government's Efforts to Address Information Security Issues", October 2006, Japan, <http://www.nisc.go.jp/eng/>, s. 5.
- [45] Mobito Yoshida, "Information Security Policies in Japan", IT Security Office, Information and Communications Policy Bureau, MIC, 29 June 2005, s. 12.
- [46] I. Abele-Wigert, M. Dunn, 13 April 2006, s.164
- [47] http://www.cyberpolice.go.jp/english/action01_e.html
- [48] http://www.cyberpolice.go.jp/english/action01_e.html

E-Devlet Güvenliği

Ayşe İNALÖZ, Mustafa ÜNVER, Mustafa ALKAN

Özet— Küreselleşme ile gelen hızlı değişim içerisindeki dünyada bilgi tabanlı ekonomi hem özel sektör hem de kamu sektörüne bazı zorlukların yanı sıra bazı fırsatlar da sunmaktadır. Bu makalede bilgi ve haberleşme teknolojilerinin kamu sektöründe yarattığı reform olarak kabul edebileceğimiz Elektronik Devlet ya da kısaca “e-devlet” konusunun gelişimi irdelenmiş, e-devlet sistemleri için arttırılmış güvenlik çerçevesi kapsamında E-Devlet Güvenlik Riskleri ve Risk Yönetimi Prosedürleri incelenmiştir.

Anahtar Kelimeler—E-devlet, güvenlik çerçevesi, güvenlik hedefleri, güvenlik politikaları

I. GİRİŞ

Çağımızda tüm dünyada gerçekleşen teknolojik gelişmeler kamu sektöründe bilgi ve haberleşme teknolojilerinin kullanılmasının yaygınlaşması ile yeni bir çeşit rasyonelizasyonun doğmasına yol açmıştır. Bilgi ve haberleşme teknolojileri araçlarının kullanımı kamu politikası, işlemleri ve fonksiyonlarında dönüşümsel kaymalara yol açmıştır. Bilginin yönetimi belirli bir süreden beri hükümetlerin ana görevlerinden birisi olmuştur.

“e-Devlet” kavramı, vatandaşların ve aynı zamanda özel kurum ve kuruluşların kamu kurumları ile olan mal, hizmet ve bilgi alışverişi şeklindeki ilişki ve işlemlerinin bilgi ve iletişim teknolojilerinin yardımıyla elektronik ortamda gerçekleştirilmesidir [1].

E-Devlet sadece vatandaşlar için hizmetler sağlamakla kalmayıp, kamu sektörünün de hükümet fonksiyonlarında şeffaflık ve hesap verilebilirliğin sağlanması, hükümet yönetiminde masrafların azaltılmasının sağlanması v.b. gibi verimlilik amaçlarının gerçekleştirilmesini sağlamaktadır [2].

Bu makalenin I. Bölümünde E-Devlet oluşumunun aşamalarına değinilmiş, E-devlete hazırlık göstergeleri kapsamında dünya geneli ve ülkemizdeki duruma ait bazı istatistiksel veriler sunulmuştur. II. Bölümde E-Devlet için Arttırılmış Güvenlik Çerçevesi konusu incelenmiş, III. Bölümde E-Devlet Güvenlik Riskleri ve Risk Yönetim Prosedürlerine değinilmiştir. IV. Bölümde ise Sistem Güvenliği Altyapısı konusu irdelenmiştir.

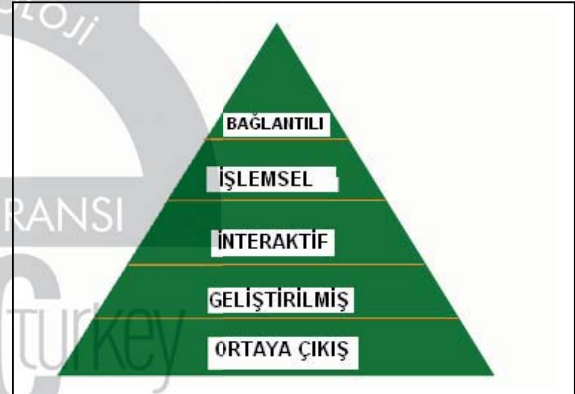
Bilgi Teknolojileri ve İletişim Kurumu, Maltepe, Ankara
ainaloz@tk.gov.tr, munver@tk.gov.tr, malkan@tk.gov.tr

II. E-DEVLETİN GELİŞİMİ

Endüstrileşmiş ülkelerin popülasyonunun büyük bir yüzdesi web’e dayalı ekonomi ile iç içe yaşamaktadır. 2007 yılında Avrupa Birliği popülasyonunun %55’i ve ABD popülasyonunun %71’i internet erişimine sahiptir. Aralık 2007 sonu itibarıyla ABD popülasyonunun % 78’i dünya popülasyonunun ise %69 ‘unun elektronik posta kullandığı bildirilmektedir [2]. Bilgi ve haberleşme teknolojilerinin kullanımının artması e-devlet oluşumunun gelişimini hızlandırmaktadır.

E-Devlet Oluşumu aşağıda Şekil I’de gösterilen beş ana aşamadan meydana gelmektedir.

ŞEKİL I
E-DEVLET OLUŞUMU



I. Aşama: Ortaya Çıkış

Hükümetin çevrimiçi varlığı bir web sayfası ya da Bakanlıklar, eğitim enstitüleri, sağlık, sosyal yardım, iş ve finans kuruluşlarına bağlantıları da içeren resmi bir web sayfasından oluşmaktadır. Bilgilerin çoğu statiktir ve vatandaşlar ile etkileşim azdır.

II. Aşama: Geliştirilmiş

Hükümetler kamu politikası ve yönetimle ilgili pek çok bilgi sağlarlar. Vatandaşlar için dokümanlar, formlar, raporlar, yasa ve düzenlemeler ve gazeteler v.b. gibi arşivlenmiş bilgilere erişme imkanı sağlarlar.

III. Aşama: İnteraktif

Hükümetler hizmetlerini vergi ödemeleri ve lisans yenileme uygulamaları için indirilebilir formlar v.b. gibi çevrimiçi sunarlar. Buna ek olarak interaktif portalın ya da web sitesinin başlangıcı vatandaşların rahat etmesini sağlamaya yöneliktir.

IV. Aşama: İşlemsel

Hükümetler kendileri ve vatandaş arasında iki yönlü etkileşim sağlaya başlarlar. Buna vergileri ödeme seçeneği, sayısal kimlik başvurusu, nüfus kağıdı, pasaport başvurusu dahil olmak üzere bu hizmetlere vatandaşların 7/24 çevrimiçi olarak ulaşmasını sağlamaktadır. Tüm işlemler çevrimiçi yapılır.

V. Aşama: Bağlantılı

Hükümetler kendilerini vatandaşlarının tüm ihtiyaçlarına karşılık veren bağlantılı bir varlık olarak görürler. Bu e-devlet girişimlerinin en sofistike aşamasıdır ve aşağıda yer alan bağlantılara sahiptir.

- 1.Yatay bağlantılar (Hükümet kuruluşları arasında)
- 2.Dikey bağlantılar (Merkezi ve bölgesel hükümet kuruluşları arasında)
- 3.Altyapı bağlantıları (Birlikte çalışabilirlik konuları)
4. Hükümetler ve vatandaşlar arasındaki bağlantılar
- 5.Paydaşlar (Hükümet, özel sektör, akademik enstitüler ve sivil toplum örgütleri) arasındaki bağlantılar [3]

Birleşmiş Milletlerin 2008 yılı E-Devlet Araştırması [3] 192 üye ülkenin daha iyi kalitede hizmet ve ürün alması için vatandaşlarının, işletmelerinin ihtiyaçlarına ilişkin cevaplarını içermektedir.

TABLO I
Ülkelerin Sunduğu İnteraktif Hizmetler

	Ülke Sayısı	Yüzde (%)
GSM Telefonlara Mesaj Gönderimi	14	7
WAP PDA Erişimi	19	10
Güvenli Bağlantı	33	17
Güncellemeler İçin E-Posta Kayıt Opsiyonu	58	30
Hükümetlerin kayıtların gizli kalacağına ait garantisi	29	15
Elektronik İmza	19	10

Ülkemiz E-Devlet Hazırlık Göstergesi 2008'de 76 ncı sırada yer almaktadır (Bknz. Tablo II). Ülkemiz E-Devlet Kullanım kapasitesi açısından %33- % 66 lık Grupta yer almaktadır (Bknz. Tablo III).

TABLO II
E-DEVLET HAZIRLIK GÖSTERGESİ

	Ülke	Gösterge
1	İsveç	0.9157
2	Danimarka	0.9134
3	Norveç	0.8921
4	ABD	0.8644
5	Hollanda	0.8631
6	Kore Cumhuriyeti	0.8317
7	Kanada	0.8172
8	Avusturalya	0.8108
9	Fransa	0.8038
10	İngiltere	0.7872
76	Türkiye	0.4834

TABLO III
E-DEVLET KULLANIM KAPASİTESİ

Ülke	Kullanım Yüzdesi					
	I Ortaya Çıkış	II Geliştirilmiş	III İnteraktif	IV İşlemsel	V Bağlantılı	Toplam
% 34-%66 Kullanım Oranına Sahip Ülkeler- Kullanım Oranı (%)						
Malta	100	92	63	40	44	65
Birleşik Arap Emirliği	88	68	68	60	37	64
Meksika	100	86	65	38	41	63
İspanya	100	79	68	39	41	62
Malezya	100	84	65	35	26	60
Avusturya	100	85	60	38	22	59
İsrail	88	82	56	43	44	59
Portekiz	100	84	53	32	4	53
El Salvador	100	75	56	21	33	52
Almanya	100	75	56	20	30	51
Peru	100	82	58	11	19	50
Bolivya	100	78	50	11	19	47
Bahreyn	88	70	44	27	26	46
İtalya	100	79	48	2	37	46
Filipinler	100	72	49	14	22	46
Çin	100	76	52	4	26	45
Venezuela	88	60	52	5	37	42
Suudi Arabistan	100	58	53	8	19	41
İzlanda	75	74	46	8	0	41
Letonya	100	70	48	1	7	40
Mogolistan	88	73	33	7	19	38
Türkiye	63	59	37	17	26	38
Yunanistan	100	74	35	4	4	37
Kuveyt	0	60	40	14	26	37
Panama	88	65	36	7	22	37

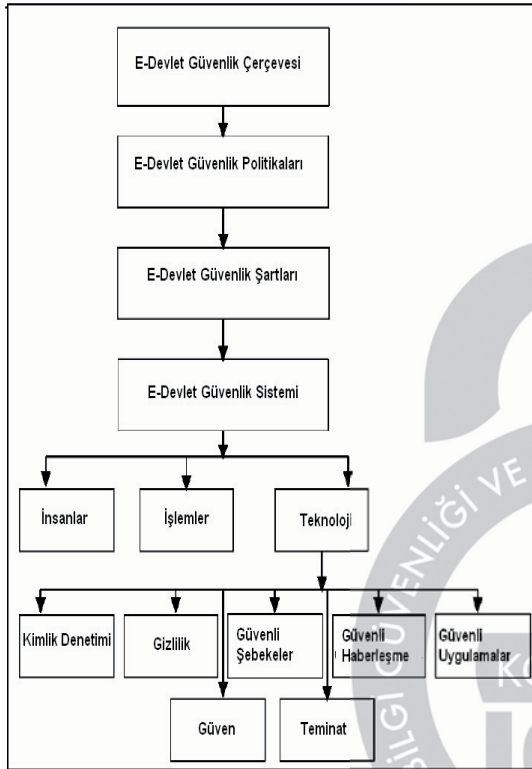
III. E-DEVLET İÇİN ARTTIRILMIŞ GÜVENLİK ÇERÇEVESİ

Hükümetlerin çoğu vatandaşları ve işletmelerinin ihtiyaçlarını karşılamaya yönelik sunmuş oldukları hizmetleri kendilerine uygun olan güvenli yer ve zamanlarda vermektedirler.

E-Devlet internetin en önemli başarılardan biridir. E-Devlet güvenliği, e-Devlet oluşumunun ileri aşamalarına ulaşılmasını sağlayan çok önemli faktörlerden biridir. E-Devletin başarılı olarak uygulanması işlemlerde yer alan tüm taraflar üzerinde bir güvenlik seviyesini gerektirmektedir. E-Ticaret kapsamında geliştirilmiş olan bazı güvenlik teknikleri ve araçları bulunmaktadır. Ancak güvenli e-devlet sistemleri proje yaşam döngüsünden itibaren yürürlüğe konulabilecek olan kapsamlı bir model gerektirmektedir. Bu makalede e-devlet sistemleri için artırılmış güvenlik çerçevesi modeli sunulmaktadır. Bu tip bir güvenlik çerçevesi karar alıcılar ve e-devlet sistemlerini dizayn edenler tarafından kullanılacak olan temel bir araçtır.

E-Devlet için arttırılmış güvenlik çerçevesi güvenlik şartlarının en üst düzeyde ifade edildiği ve e-devlet güvenlik beyanlarına uzanan bir dokümandır. Bu çerçevenin amacı e-devlet hizmetleri ve işlemlerinin güvenliğini sağlamak olup hükümet kurum ve kuruluşları ve işletmeler tarafından kullanılan bir kılavuzdur. Söz konusu çerçeve e-devlet web sitelerinin güvenlik seviyesini ölçmede kullanılabilir.

ŞEKİL II E-DEVLET GÜVENLİK ÇERÇEVESİNİN ANA BİLEŞENLERİ



“İnsanlar” bileşeni e-Devleti kullanan insanları temsil etmektedir. Hükümetler tarafından e-devlet kullanıcılarının güvenlik problemleri ve sonuçlarından haberdar olmasını sağlayacak farkındalık programlarının uygulanmasına ihtiyaç vardır.

“İşlemler” bileşeni E-Devlet kullanımını sağlayan güvenlik politikası ve prosedürleri tarafından yönetilen uygulamalardır.

Teknoloji E-Devlet güvenliğini kuvvetlendirmek için kullanılır ancak en zayıf halka kadar iyidir. Güvenliği arttırmak için kullanılacak teknoloji çok katmanlı olmalı ve her seviyede uygun şekilde uygulanmalıdır [3].

Teknolojinin Şekil ‘de yer alan altbileşenlerine aşağıda kısaca değinilmektedir.

1. Kimlik Denetimi: Sadece yetkilendirilmiş kişiler sisteme erişebilmelidir.

2. Gizlilik: Sadece yetkilendirilmiş kişiler sisteme erişebilir. Bilgi güvenli olarak depolanır ve yetkisiz kişi ya da işlemlere kapalıdır.

3. Güvenli Uygulamalar: E-Devlet hizmet ve uygulamalarının sağlam ve güvenli bir biçimde dizayn edilip geliştirilmesi ve uygulanmasıdır.

4. Güvenli Şebeke: Bilgi ve işlemlerin her türlü saldırıdan korunmasıdır.

5. Güvenli Haberleşme: İşlemlerdeki bilginin tahrif ve ifşa edilmeden korunması

6. Güven: İşlemlerin yetkilendirilmiş kişilerce izlenebilir ve hesap verilebilir olması ve daha sonradan inkar edilememesi

7. Teminat: Güvenlik bileşenlerinin uygulanmasında güvenin de dahil edilmesi

Şekilde II’de sunulmuş olan E-Devlet güvenlik çerçevesi kullanıcıları üzerinde güven ve itimat kazanmak isteyen hizmet sağlayıcıları için anahtar bir kılavuz mahiyetindedir.

Öte yandan herhangi bir E-devlet sisteminin güvenlik şartları karşılaşılabilecek tehdit ve saldırıları da analiz etmelidir. Bu ise modern bir yazılım risk analiz metodolojisini kullanan güvenli uygulama geliştirme ile bütünleşmiştir.

IV. E-DEVLET GÜVENLİK RİSKLERİ

İnternete dayalı E-devlet’in gelişimi ile şebekenin kompleksliği ve açıkları sebebiyle önemli güvenlik problemleri ile karşılaşmaktadır.

E-devletin karşılaştığı güvenlik riskleri aşağıda sıralanmaktadır:

1. Bilginin Yolunun Kesilmesi (Durdurulması): İlgili e-devlet kullanıcılarının ya da saldırganların bilgileri kullanıcılardan ya da devletten çalmaları ya da ele geçirmeleridir.

2. Bilginin Tahrifatı: İnternet saldırganlarının bilgi bütünlüğünün tahrif edilmesi amacıyla orijinal bilgiyi çeşitli metotlar vasıtasıyla tahrif etmesi, bilgiye ekleme ya da çıkartma yapmasıdır.

3. Hizmetlerin İnkâr Edilmesi: Şebeke sisteminin yada sistemdeki sunucuların belirli bir periyot zarfında tamamen hükümsüz kılınmasıdır. Çoğunlukla hacker saldırıları ya da virüs ya da insan yapımı yıkıcı araçlar vasıtasıyla gerçekleştirilen saldırılardır.

4. Sistem Kaynaklarının Çalınması: Şebeke sistemi çevresinde sistem kaynaklarının çalınması sık rastlanır bir durumdur.

5. Bilginin Taklidi: saldırganların şebeke bilgisi içerisindeki veri kurallarını bilmesi ya da e-devlet bilgisinin kodunu çözdükten sonra yasal kullanıcı gibi davranması ya da diğer kullanıcıları aldatmak için yanlış bilgi vermesidir. Ana formlar kullanıcıların yasal olmayan sertifikaları, yanıltıcı e-postaları almasını da içerir [5].

A. Risk Yönetimi Prosedürleri

Risk yönetimi riskleri tanımlamak, analiz etmek ve risk yönetimi planlarını hazırlamayı içeren bir süreçtir. E-devlet güvenlik risk yönetimi prosedürleri üç adımdan oluşmaktadır. Risk tanımlanması, Risk Analizi ve Risk Kontrolü

A.1.Risk Tanımlaması: İlgili çeşitli tehditlerin ve çözümlerinin toplanmasına ve e-devlet sistemindeki muhtemel riskleri ve tehditlerin tanımlanmasına dayanmaktadır.

Risklerin belirlenmesini sağlayan çeşitli metotlar bulunmaktadır. Risklerin belirlenmesinin amacı şebeke içindeki, veri ya da veri alışverişindeki var olan riskleri tanımlamaktır.

Risklerin belirlenmesi tüm e-devlet sistemi risklerinin belirlenmesini sağlayamaz. Risk belirlenmesi halihazırda bilinen ya da bilinen risklerden kaynaklanabilecek muhtemel riskleri bulabilir.

Risk analizi ve risk kontrolü bilinmeyen riskleri azaltmak ya da çözmek için kullanılır.

A.2. Risk Analizi: Analiz, karşılaştırma ve değerlendirme gibi çeşitli nicel ve nitel yöntemler vasıtasıyla e-devlet risklerinin her faktörünün önemine karar vermek ve e-devlet sistemi için muhtemel sonuçlarını değerlendirmektir.

Tehdit kaynakları insan, doğa v.b. her türlü çevre olabilir.

TABLO IV ÇEŞİTLİ TEHDİT KAYNAKLARI

Tehdit	Muhtemel Kaynak
Kasıtlı Tehditler	Teröristler Organizasyondan memnun olmayan, akıl sağlığı yerinde olmayan insanlar Suçlular Yabancı düşmanlarla işbirliği yapan işbirlikçiler
Kasıtlı olmayan Tehditler	Sistem kullanıcılarının yanlış işlemleri Sistem koruyucularının ya da sorumlularının yanlış işlemleri
Doğal Tehditler	Deprem Volkanik Patlama Hortum Sel Yıldırım Düşmesi Dolu

Güvenlik açıkları hakkındaki bilgilere mevki araştırması, personel araştırması, penetrasyon testi, ilgili dokümanların analizi ve diğer açık bilgi kaynaklarından ulaşılabilir.

A.3. Risk Kontrolü

Risk kontrolü bazı risk kontrol metotlarını seçerek riskin kabul edilebilir bir seviyeye azaltılmasının sağlanmasıdır. Risk kontrolü risk yönetiminin en önemli adımıdır. E-Devlet güvenlik risk kontrolünün amacı e-devlet projelerinin maruz kalacağı risk derecesini azaltmaktır.

İki çeşit risk kontrolü metodu bulunmaktadır.

Birincisi risk azaltımı, kaçınma ya da transfer etme ve kayıp yönetimi gibi risk kontrolü ölçüleridir.

İkincisi risk telafisi için sigorta ya da riski kendilerinin üstlenmesi gibi fon önlemleridir. E-devlet güvenlik risk yönetiminde idareciler sigorta ya da riski kendilerinin üstlenmesine dair hangi önlemi alacaklarına karar vermelidirler.

V. SİSTEM GÜVENLİĞİ ALTYAPISI

Kamu perspektifinden bakıldığında hükümet bir kuruluş olarak kabul edilebilir. Bir devlet kuruluşunda oluşacak olan bir güvenlik problemi tüm hükümet işlemlerinin başarısızlığı olarak görülebilir. Bu bakımdan tüm kamu kurum ve kuruluşlarında bilgi güvenliğinin sağlanması ve korunması bir ana proje olarak kabul edilebilir [6].

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS)

Kurum ve Kuruluşların hassas bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşım olan Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) amacı sistem çalışanları, iş süreçlerini ve bilgi teknolojileri (BT) sistemlerini kapsayan hassas bilgilerin korunmasıdır.

Kurum ve Kuruluşların fiziksel alan güvenliği, veri güvenliği, donanım-yazılım güvenliği ve güvenilirliği ile personel güvenliğinin sağlanması için tehditlerden ve/veya zafiyetlerden kaynaklanan risklerin bertaraf edilmesi veya azaltılmasına yönelik kullanılan bazı standartlar bulunmaktadır.

Bilgi güvenliği yönetimi konusunda en yaygın olarak kullanılan standart, "ISO/IEC 27002:2005 Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri" standardıdır. Bu standart, işletmeler içerisinde bilgi güvenliği yönetimini başlatmak, gerçekleştirmek, sürdürmek ve iyileştirmek için genel prensipleri ve yönlendirici bilgileri ortaya koyar. ISO/IEC 27002:2005 rehber edinilerek kurulan BGYS'nin belgelendirmesi için "ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler" standardı kullanılmaktadır [7]. Bu standart, dokümanite edilmiş bir BGYS'ni kurumun tüm iş riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsamaktadır. İş risklerini karşılamak amacıyla ISO/IEC 27002:2005'te ortaya konan

kontrol hedeflerinin kurum içerisinde nasıl uygulanacağı ve denetleneceği ISO/IEC 27001:2005'te belirlenmektedir [8].

Her iki standardın Türkçe hali TSE tarafından sırasıyla TS ISO/IEC 17799:2005 ve TS ISO/IEC 27001:2005 isimleri ile yayınlanmıştır.

Pratik Uygulamalar:

Bilgi Teknolojileri ve İletişim Kurumu tarafından hazırlanan 20 Temmuz 2008 tarih ve 26942 sayılı Resmi Gazetede yayımlanan ELEKTRONİK HABERLEŞME GÜVENLİĞİ YÖNETMELİĞİ ile elektronik haberleşme güvenliğine ilişkin usul ve esaslar düzenlenmektedir.

Bu Yönetmelik, işletmecilerin fiziksel alan güvenliği, veri güvenliği, donanım-yazılım güvenliği ve güvenilirliği ile personel güvenilirliğinin sağlanması için tehditlerden ve/veya zafiyetlerden kaynaklanan risklerin bertaraf edilmesi veya azaltılmasına ilişkin olarak alacakları tedbirlere yönelik usul ve esasları kapsamaktadır. Yetkilendirilen işletmeciler yetkilendirme tarihinden itibaren bir yıl içerisinde Elektronik haberleşme güvenliğini sağlama kapsamında TS ISO/IEC 27001 veya ISO/IEC 27001 standardına uygunluğu sağlamakla yükümlü kılınmışlardır.

27001 Bilgi Güvenliği sertifikası kapsamında; bilgi envanterinin hazırlanması ve bilgilerin sınıflandırılması, Zaafiyet – Sızma Test ve Analizlerinin yapılması, Risk Analizinin yapılması ve Güvenlik Önlemlerinin tespit edilmesi, Bilgi Güvenliği Politika, Prosedür, Talimat ve Formlarının Oluşturulması, TS ISO/IEC 27001 Ek dokümanlarının hazırlanması, TS ISO/IEC 27001 Sertifikasyonu kapsamında değerlendirilmesi gereken konulardır.

Ayrıca ISO bünyesinde ISO/IEC 27012 – Bilgi Teknolojileri-Güvenlik Teknikleri-E-Devlet için Bilgi Güvenliği Yönetim Sistemleri Kılavuzu'nun hazırlanması çalışmaları sürdürülmektedir. ISO/IEC 27012'nin ilk taslağı Ocak 2009 tarihinde yayınlanacak olup Nisan 2009 tarihine kadar kamuoyu görüşlerine açılacaktır [9].

VI. SONUÇ

İnternet günümüzde hem bilgi hem de tehditlerin kaynağı durumuna gelmektedir. Bu makalede güvenli e-devlet hizmet ve uygulamalarının ana bileşenlerini adresleyen kapsamlı bir güvenlik çerçevesi ortaya konulmuştur. Bu çerçeve hükümetlerin güvenliği e-Devlet sistemlerine tüm anahtar güvenlik bileşenlerini göz önünde bulundurarak etkin bir şekilde dahil etmelerinde yardımcı olacaktır. E-devletin karşılaştığı güvenlik riskleri risk yönetimi prosedürleri yardımıyla azaltılabilir. Etkin ve elverişli risk kontrolü metodlarından biri riski azaltmak üzere bütüncül bir güvenlik planı hazırlamak, güvenlik garantisi olarak bazı temel teknolojilere hakim olmak ve özel güvenlik kazaları olduğunda hükümetin kabul edebileceği çözümler hazırlamaktır.

Ülkemiz E-Devlet Hazırlık Göstergesi 2008'de 192 ülke arasında 76 ncı sırada yer almakta ve E-Devlet Kullanım kapasitesi olarak %34- %66 kullanım oranına sahip ülkeler sınıfında bulunmaktadır. E-Devlet güvenliğinin sağlanması, makalenin I inci bölümünde kapsamlıca anlatılan e-Devlet oluşumunun ileri aşamalarına ulaşılmasını sağlayan en önemli faktörlerin başında gelmektedir. Bu bağlamda ülkemizdeki e-Devlet oluşumunun ileri aşamalara ulaşabilmesi için E-Devlet Güvenliğinin sağlanmasına özel bir önem verilmesi yerinde olacaktır. Bu bağlamda makalenin II inci bölümünde vurgulanan E-Devlet Güvenlik çerçevesinin belirlenerek, E-Devlet Güvenlik politikaları ve güvenlik şartları oluşturulması, kullanıcılar, işlemler ve teknolojiyi bir arada göz önünde bulunduran bir E-Devlet Güvenlik sistemi kurulması yerinde olacaktır. E-Devlet Güvenlik sisteminin kurulmasının en önemli safhasını kamu kurum ve kuruluşlarının hassas bilgilerini yönetebilmesi, bilgi güvenliğinin sağlanması ve korunması oluşturmaktadır. Kamu Kurum Kuruluşlarının kendi Bilgi Güvenliği Yönetim Sistemlerini kurmaları ve bu konuyla ilgili olarak Elektronik Haberleşme Güvenliği Yönetmeliği ile yetkilendirilen işletmecilerin halihazırda uygunluğu sağlamakla yükümlü kılındıkları TS ISO/IEC 27001 veya ISO/IEC 27001 sertifikasyonlarını almaları devlet bünyesinde bir sistematğin oluşturulmasını sağlayacaktır. Ayrıca ISO bünyesinde sürdürülen ISO/IEC 27012 – Bilgi Teknolojileri-Güvenlik Teknikleri-E-Devlet için Bilgi Güvenliği Yönetim Sistemleri Kılavuzu'nun hazırlanması faaliyetlerinin dikkatle takip edilmesi, Ülkemiz E-Devlet Güvenlik sistemi kurulması çalışmalarında katkı sağlayacaktır.

KAYNAKLAR

- [1] C. Can Aktan, "Etkin Devlet", Çizgi Kitabevi, 2003
- [2] David S. Evans, " Antitrust Issues Raised by the emerging global Internet Economy" , Copyright 2008 by Northwestern University School of Law Vol. 102Northwestern University Law Review Colloquy
- [3] "UN e-Government Survey", United Nations, New York, 2008
- [4] Walid Al-Ahmad and Reem Al-Kaabi, "An Extended Security Framework for E-Government", ISI 2008, June 17-20, 2008, Taipei, Taiwan, 2008 IEEE
- [5] Zhitian Zhou, Congyang Hu, "Study on the E-government Security Risk Management", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.5, May 2008
- [6] Stephen Smith, "Key Factors in E-Government Information System Security", 18th Bled eConference eIntegration in Action Bled, Slovenia, June 6 - 8, 2005
- [7] Fikret Ottekin Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü ISO/IEC 27001 Denetim Listesi, Sürüm 1.00, 21.02.2008
- [8] Dinçer Önel, Ali Dinçkan, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Bilgi Güvenliği Yönetim Sistemi Kurulumu, Sürüm 1.00, 28.08.2007
- [9] <http://www.iso27001security.com/html/27012.html>