12th International Conference on Information Security and Cryptology

12. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı

ISCTURKEY 2019

16-17 October/Ekim 2019
BTK Conference Center
BTK Konferans Merkezi
Ankara, TURKEY/TÜRKİYE

PROCEEDINGS

BİLDİRİLER KİTABI

https://www.iscturkey.org

Editors/Editörler

Prof. Dr. Şeref SAĞIROĞLU
Dr. Sedat AKLEYLEK
Dr. Yavuz CANBAY
Prof. Dr. Mustafa ALKAN
Prof. Dr. Ertuğrul KARAÇUHA
Prof. Dr. Ferruh ÖZBUDAK

ISCTURKEY 2019

ORGANIZER/ORGANİZASYON:

BİLGİ GÜVENLİĞİ DERNEĞİ

SSB 1985

T.C. Ulaştırma ve Altyapı Bakanlığı

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

GAZİ ÜNİVERSİTESİ Gazi 1926

ODTÜ

İTÜ İSTANBUL TEKNİK ÜNİVERSİTESİ 1773

ISCTURKEY 2019

SPONSORS/SPONSORLAR;

Ankara-Turkey/Türkiye, 16-17 October/Ekim 2019
https://www.iscturkey.org ISBN: XXX

SUPPORTER/DESTEKLEYEN:

enisa

ISCTurkey 2019

Bu konferans bildiriler kitabında yer alan bildiri tam metinleri kongre konu başlıklarına uygun olarak yazarlar tarafından hazırlanmıştır. Bildiri özetleri yazarların kendi fikirlerini yansıtır ve herhangi bir değişiklik yapılmadan aynı şekilde basılmıştır. Bu kitaptaki yazarların görüşlerinden ISCTurkey 2019 Düzenleme Kurulu sorumlu değildir.

The papers in this conference proceedings compromise the topics given in the conference web site. The articles reflect the authors' opinions and they are published as ithey are. Their inclusion in this publication does not necessarily constitute endorsement by the Organizing Committee of ISCTurkey 2019

Contact to/İrtibat:
Prof Dr. Şeref SAĞIROĞLU; Gazi University Engineering Faculty, Computer Engineering Department
06570 Maltepe ANKARA; +90 312 582 31 30
ss@gazi.edu.tr

ISCTurkey 2019

HONORORY BOARD MEMBERS / ONUR KURULU ÜYELERİ

Prof. Dr. Mehmet KARACA, İTÜ Rektörü,

Prof. Dr. İbrahim USLAN, Gazi Üniversitesi Rektörü

Prof. Dr. Mustafa Verşan KÖK, ODTÜ Rektörü

Dr. Ömer Fatih Sayan, Ulaştırma ve Altyapı Bakanlığı, Bakan Yardımcısı

Ömer Abdullah Karagözoğlu, BTK Başkanı

ORGANISING COMMITTEE MEMBERS / DÜZENLEME KURULU ÜYELERİ
Congress Chairs / Konferans Eş-Başkanları:

Prof. Dr. Mustafa ALKAN, Gazi Üniversitesi /Gazi University

Prof. Dr. Ertuğrul KARAÇUHA, İstanbul Teknik Üniversitesi/İstanbul Technical University

Prof. Dr. Ferruh ÖZBUDAK, Orta Doğu Teknik Üniversitesi/Middle East Technical University

Prof. Dr. Şeref SAĞIROĞLU, Bilgi Güvenliği Derneği/Information Security Association of Turkey, Gazi Üniversitesi/Gazi University

Congress Scientific Board Members / Konferans Bilim Kurulu:

Murat CENK, Orta Doğu Teknik Üniversitesi/Middle East Technical University

Sedat AKLEYLEK, Ondokuz Mayıs Üniversitesi/Ondokuz Mayis University

Abdullah Raşit GÜLHAN, Bilgi Güvenliği Derneği/Information Security Association

Burhanettin AL, Bilgi Güvenliği Derneği/Information Security Association

Mehmet GÜLŞEN, Bilgi Güvenliği Derneği/Information Security Association

Mehmet Ali İNCEEFE, Bilgi Güvenliği Derneği/Information Security Association

Mustafa ÜNVER, Bilgi Güvenliği Derneği/Information Security Association

Mehmet DEMİRCİ, Gazi Üniversitesi/Gazi University

Ramazan TERZİ, Gazi Üniversitesi/Gazi University

Yavuz CANBAY, Gazi Üniversitesi/Gazi University

Bilgehan ARSLAN, Gazi Üniversitesi/Gazi University

Duygu SİNANÇ, Gazi Üniversitesi/Gazi University

Murat AKIN, Gazi Üniversitesi/Gazi University

Merve Sedef DEMİRCİ, Gazi Üniversitesi/Gazi University

Sebahattin EKER, İstanbul Teknik Üniversitesi/İstanbul Technical University

Oğuzhan KÜLEKÇİ, İstanbul Teknik Üniversitesi/İstanbul Technical University

Lütfiye Ata DURAK, İstanbul Teknik Üniversitesi/İstanbul Technical University

Enver ÖZDEMİR, İstanbul Teknik Üniversitesi/İstanbul Technical University

Hakan Tekedere, Gazi Üniversitesi/Gazi University

Mustafa ŞENOL, Bilgi Güvenliği Derneği / Information Security Association, HAVELSAN

SCIENTIFIC COMMITTEE MEMBERS / BİLİM KURULU ÜYELERİ

Naci ÜNAL, Bahçeşehir Üniversitesi, Bahçeşehir University

Nurdan SARAN, Çankaya Üniversitesi/Çankaya University

Adnan Özsoy, Hacettepe Üniversitesi

Alper Uğur, Pamukkale Üniversitesi
Ahmet KOLTUKSUZ, Yaşar Üniversitesi/Yaşar University
Ahmet ÖZMEN, Sakarya Üniversitesi/Sakarya University
Ahmet Sınak, Necmettin Erbakan Üniversitesi
Akın MARSAP, Aydın Üniversitesi/Aydın University
Albert LEVI, Sabancı Üniversitesi/Sabancı University
Ali Aydın SELÇUK, TOBB ETÜ/TOBB University of Economics and Technology
Ali DOĞANAKSOY, Orta Doğu Teknik Üniversitesi/METU
Ali İNAN, Adana Bilim ve Teknoloji Üniversitesi
Ali ŞENTÜRK, Mersin Üniversitesi/Mersin University
Ali YAZICI, Atılım Üniversitesi/Atılım University
Ali Ziya ALKAR, Hacettepe Üniversitesi/Hacettepe University
Alisher KHOLMATOV, Sabancı Üniversitesi/Sabancı University
Alok TONGAONKAR, Symantec
Alper UĞUR, Pamukkale Üniversitesi/Pamukkale University
Alptekin KÜPCÜ, Koç Üniversitesi/Koc University
Ammar DAŞKIN, İstanbul Medeniyet Üniversitesi/ İstanbul Medeniyet University
Asaf VAROL, Fırat Üniversitesi, Fırat University
Atila BOSTAN, Atılım Üniversitesi/Atılım University
Atilla ELÇİ, Aksaray Üniversitesi/Aksaray University
Atilla ÖZGİT, Orta Doğu Teknik Üniversitesi/METU
Aydın ALATAN, Orta Doğu Teknik Üniversitesi/METU
Ayşe BAŞAR BENER, Boğaziçi Üniversitesi/Boğaziçi University
Barış Bülent KIRLAR, Süleyman Demirel Üniversitesi/Süleyman Demirel University
Bedri ÖZER, Fırat Üniversitesi/Fırat University
Berkant USTAOĞLU, İzmir Teknoloji Enstitüsü/İzmir Institute of Technology
Berna ORS YALÇIN, İstanbul Teknik Üniversitesi/İstanbul Technical University
Berrin YANIKOĞLU, Sabancı Üniversitesi/Sabanci University
Berry SCHOENMAKERS, Eindhoven University of Technology
Bimal ROY, Indian Statistical Institute
Bülent ÖRENCİK, İstanbul Teknik Üniversitesi /İstanbul Technical University
Bülent TUĞRUL, Ankara Üniversitesi/Ankara University
Cebrail ÇİFTLİKLİ, Erciyes Üniversitesi/Erciyes University
Cevat SENER, Orta Doğu Teknik Üniversitesi/METU
Cihangir TEZCAN, Ortadoğu Teknik Üniversitesi/METU
Cihan VAROL, Sam Houston State Universitesi / METU
Cüneyt BAZLAMAÇCI, Orta Doğu Teknik Üniversitesi/METU
Çağdaş ÇALIK, National Institute of Standards
Debasis GIRI, Haldia Institute of Technology
Deniz TAŞKIN, Trakya Üniversitesi/Trakya University
Derviş KARABOĞA, Erciyes Üniversitesi/Erciyes University
Ecir Uğur KÜÇÜKSİLLE, Süleyman Demirel Üniversitesi/Süleyman Demirel University
Eiji OKAMOTO, University of Tsukuba
Elif SAYGI, Hacettepe Üniversitesi/Hacettepe University

Emin ANARIM, Boğaziçi Üniversitesi/Boğaziçi University
Emin İslam TATLI, İstanbul Medipol Üniversitesi/İstanbul Medipol University
Emir DİRİK, Uludağ Üniversitesi/Uludağ University
Emrah ÇAKÇAK, Orta Doğu Teknik Üniversitesi/METU
Emre Yüce, Havelsan
Engin AVCI, Fırat Üniversitesi/Fırat University
Engin KIRDA, ISECLAB
Engin Şahin, Çanakkale Onsekiz Mart Üniversitesi
Enis KARAARSLAN, Muğla Üniversitesi/Muğla University
Ercan BULUŞ, Namık Kemal Üniversitesi/Namık Kemal University
Erdal IRMAK, Gazi Üniversitesi/Gazi University
Erdem ALKIM, Ege Üniversitesi/Ege University
Erdoğan DOĞDU, TOBB Ekonomi ve Teknoloji Üniversitesi/TOBB University of Economics and Technology
Erkan AFACAN, Gazi Üniversites/Gazi University
Erkan BEŞDOK, Erciyes Üniversitesi/Erciyes University
Erkay SAVAŞ, Sabancı Üniversitesi/Sabancı University
Ersan AKYILDIZ, Orta Doğu Teknik Üniversitesi/METU
Ersin ELBAŞI, TÜBİTAK/The Scientific and Technological Reseach Council of Turkey
Esra YOLAÇAN, Osmangazi Üniversitesi/Osmangazi University
Eşref ADALI, İstanbul Teknik Üniversitesi/ITU
Ertan ONUR, Orta Doğu Teknik Üniversitesi/METU
Eyüp Burak CEYHAN, Bartın Üniversitesi/Bartın University
Faruk GÖLOĞLU, ESAT-COSIC
Fatih Ertam, Fırat Üniversitesi
Fatih SULAK, TÜBİTAK/The Scientific and Technological Reseach Council of Turkey
Fatma Büyüksaraçoğlu SAKALLI, Trakya Üniversitesi/Trakya University
Fatoş Yarman VURAL, Orta Doğu Teknik Üniversitesi/METU
Ferruh ÖZBUDAK, Orta Doğu Teknik Üniversitesi/METU
Gökay SALDAMLI, Boğaziçi Üniversitesi/Boğaziçi University
Gökhan DALKILIÇ, Dokuz Eylül Üniversitesi/Dokuz Eylül University
Guangzhi QU, Oakland University
Hacer KARACAN, Gazi Üniversitesi/Gazi University
Hakan TEKEDERE, Gazi Üniversitesi/Gazi University
Halil İbrahim BÜLBÜL, Gazi Üniversitesi/Gazi University
Hamdi Murat YILDIRIM, Bilkent Üniversitesi/Bilkent University
Harold BAIER, TU DARMSTADT
Hayri SEVER, Hacettepe Üniversitesi/Hacettepe University
Hidayet TAKÇI, Cumhuriyet Üniversitesi/Cumhuriyet University
Hüseyin DEMİRCİ, TÜBİTAK/The Scientific and Technological Reseach Council of Turkey
Hüseyin HIŞIL, Yaşar Üniversitesi/Yaşar University
Hüsrev Taha SENCAR, TOBB ETÜ/TOBB University of Economics and Technology
Ion TUTANESCU, University of Pitesti
İbrahim Alper DOĞRU, Gazi Üniversitesi/Gazi University

İbrahim SOĞUKPINAR, Gebze Yüksek Teknoloji Enstitüsü/Gebze Institute of Technology
İlhami ÇOLAK, Nişantaşı Üniversitesi/Nisantasi University
İlkay ULUSOY, Orta Doğu Teknik Üniversitesi/METU
İhsan Yılmaz, Çanakkale Onsekiz Mart Üniversitesi
İsmail GÜLOĞLU, Doğuş Üniversitesi/Doğuş University
İsmail SAN, Anadolu Üniversitesi/Anadolu University
İzzet Gökhan ÖZBİLGİN, HAVELSAN Akademi Direktörü - Gazi Üniversitesi
Jianying ZHOU, ASTAR Institute for Infocomm Research
John A. CLARK, University of York
Jongsub MOON, Korea University
Jorge NAKAHARA, Universite' Libre de Bruxelles (ULB), Belgium
Kasım ÖZTOPRAK, KTO Karatay Üniversitesi/Karatay University
Katerina MITROKOTSA, Delft University of Technology
Kemal BIÇAKCI, TOBB Ekonomi ve Teknoloji Üniversitesi/TOBB University of Economics and Technology
Kerem KAŞKALOĞLU, Özyeğin Üniversitesi/Özyeğin University
Kıvanç MIHÇAK, Boğaziçi Üniversitesi/Boğaziçi University
Koray KARABINA, Florida Atlantic University
Leyla BERBER, Bilgi Üniversitesi/Bilgi University
Mehmet AKTAŞ, TÜBİTAK Bilgem, BTE/The Scientific and Technological Reseach Council of Turkey
Mehmet DEMİRCİ, Gazi Üniversitesi/Gazi University
Mehmet KİRAZ, TÜBİTAK-UEKAE/The Scientific and Technological Reseach Council of Turkey
Mehmet TEKEREK, KSU Üniversitesi/KSU University
Mehmet Emin DALKILIÇ, Ege Üniversitesi/Ege University
Mehmet Ufuk ÇAĞLAYAN, Boğaziçi Üniversitesi/Boğaziçi University
Melek D. YÜCEL, Orta Doğu Teknik Üniversitesi/METU
Melissa DANFORD, California State University
Meltem SÖNMEZ TURAN, National Institute of Standards and Technology (NIST)
Mert ÖZARAR, Konya Gıda ve Tarım Üniversitesi
Mine AKKAN, 9 Eylül Üniversitesi/9 Eylül University
Muhammet Ali AYDIN, İstanbul Üniversitesi/İstanbul University
Muhammet ÜNAL, Gazi Üniversitesi/Gazi University
Muharrem Tuncay Gençoğlu, Fırat Üniversitesi
Muhiddin UĞUZ, Ortadoğu Teknik Üniversitesi/METU
Murat AK, Akdeniz Üniversitesi/Akdeniz University
Murat AŞKAR, İzmir Ekonomi Üniversitesi/İzmir University of Economics
Murat AYDOS, Hacettepe Üniversitesi/Hacettepe University
Murat CENK, Orta Doğu Teknik Üniversitesi/METU
Murat KARAKAYA, Atılım Üniversitesi/ Atılım University
Mustafa ALKAN, Gazi Üniversitesi/Gazi University
Nazife BAYKAL, Orta Doğu Teknik Üniversitesi/METU
Oğuz YAYLA, Hacettepe Üniversitesi/Hacettepe University
Orhun KARA, TÜBİTAK-UEKAE/The Scientific and Technological Reseach Council of Turkey
Osmanbey UZUNKOL, TÜBİTAK/The Scientific and Technological Reseach Council of Turkey
Ömer Faruk BAY, Gazi Üniversitesi/Gazi University

Özgür AKAN, Orta Doğu Teknik Üniversitesi/METU
Peter COOPER, Sam Houston State University
Qinghan XIAO, Defence Research and Development Canada
Resul DAŞ, Fırat Üniversitesi/Fırat University
Sedat AKLEYLEK, Ondokuz Mayıs Üniversitesi/Ondokuz Mayis University
Selçuk BAKTIR, Bahçeşehir Üniversitesi/Bahçeşehir University
Selçuk KAVUT, Balıkesir Üniversitesi/Balıkesir University
Serap ŞAHİN, İYTE/Izmir Institute of Technology
Serdar BOZTAŞ, RMIT Üniversitesi/RMIT University
Serdar Süer ERDEM, GYTE/Gebze Institute of Technology
Sevil ŞEN, Hacettepe Üniversitesi/Hacettepe University
Shahram RAHIMI, Southern Illinois University
Suat ÖZDEMİR, Gazi Üniversitesi/Gazi University
Subhamoy MAITRA, Indian Statistical Institute
Süleyman ÖZARSLAN, Orta Doğu Teknik Üniversitesi/METU
Şaban EREN, Maltepe Üniversitesi/Maltepe University
Şeref SAĞIROĞLU, Gazi Üniversitesi/Gazi University
Şerif BAHTİYAR, İstanbul Teknik Üniversitesi /İstanbul Technical University
Taner ALTUNOK, Türk Hava Kurumu Üniversitesi / Turkish Aviation Association University
Tarık YERLİKAYA, Trakya Üniversitesi/Trakya University
Tekin MEMİŞ, Kadir Has Üniversitesi/Kadir Has University
Tolga SAKALLI, Trakya Üniversitesi/Trakya University
Tolga YALÇIN, Konya Gıda ve Tarım Üniversitesi
Tuğba Taşkaya TEMİZEL, Ortadoğu Teknik niversitesi/METU
Tuğkan TUĞLULAR, İzmir Yüksek Teknoloji Enstitüsü/Izmir Institute of Technology
Tuğrul YANIK, Celal Bayar Üniversitesi/Celal Bayar University
Türksel Kaya BENSGHİR, TODAİE
Umut ULUDAĞ, TÜBİTAK UEKAE/The Scientific and Technological Reseach Council of Turkey
Vasif NABİYEV, Karadeniz Teknik Üniversitesi/Karadeniz Technical University
Veysel ASLANTAŞ, Erciyes Üniversitesi/Erciyes University
Yadigar IMAMVERDIYEV, Institute of Information Technology, Azerbaijan National Academy of Sciences
Yavuz CANBAY, Gazi Üniversitesi/Gazi University
Yurdahan GÜLER, Ortadoğu Teknik Üniversitesi/METU
Yusuf İPEKOĞLU, Orta Doğu Teknik Üniversitesi/METU
Yusuf Murat ERTEN, İzmir Yüksek Teknoloji Enstitüsü/Izmir Institute of Technology
Yücel SAYGIN, Sabancı Üniversitesi/Sabancı University
Zaliha Yüce TOK, ASELSAN
Ziya AKTAŞ, Çankaya Üniversitesi/Çankaya University
Zülfükar SAYGI, TOBB ETÜ/TOBB University of Economics and Technology

ADVISORY COMMITTEE MEMBERS / DANIŞMA KURULU ÜYELERİ

Neşe SAYARI, BİZNET
Abdullah Raşit GÜLHAN, SİNERJİTÜRK
Ahmet Hamdi ATALAY, BGD, HAVELSAN
Batuhan TOSUN, ISSA Türkiye
Bilal ÖNAL, BGD
Burak ÇİFTER, BOA TEKNOLOJİ
Burhanettin AL, Turkcell
Cem AKOYMAK, Avea
Cemal AKYEL, Akyel Online
Doğan Ufuk GÜNEŞ, YASAD
Emine Yazıcı ALTINTAŞ, UDHB
Faruk ECZACIBAŞI, TBV
Ferhat YEŞİLLİ, BİH Grup
Füsun Sarp NEBİL, TİD
Gökhan ÖZBİLGİN, Havelsan
Hanzade SARIÇİÇEK, ODTÜ Teknokent
İlker TABAK, TBD
Kadriye Yıldız BARLAS, BGD
Kemal CILIZ, TÜBİSAD
Mehmet Ali İNCEEFE, BGD
Mesut DEMİRBİLEK, Vodafone
Metin TARAKÇI, ÇMD
Muhterem İLHAN, Vodafone
Mustafa MACAR, BGD
Mustafa YANARTAŞ, TÜBİFED
Nahit GÖK, SABİDER
Orhan TURAN, BGD
Selim ÜLKÜ, BGD
Tolga TÜFEKÇİ, TürkTrust

KONULAR / TOPICS

Siber Güvenlik
Kurumsal Sistem Güvenliği
Dağıtık ve Yaygın Sistem Güvenliği
Donanım Tabanlı Güvenlik
Olay İşleme ve Penetrasyon Testi
Yasal Sorunlar
Multimedya ve Belge Güvenliği
İşletim Sistemleri ve Veritabanı Güvenliği
Gizlilik sorunları
SCADA ve Gömülü Sistem Güvenliği
Güvenli Yazılım Geliştirme
Bulut Bilişim Güvenliği
Büyük Veri Güvenliği
Sosyal Ağlarda Güvenlik
Web Tabanlı Uygulamalar ve Hizmetlerin Güvenliği
Güvenlik Protokolleri
VOIP, Kablosuz ve Telekomünikasyon Ağ Güvenliği

Dijital Adli Bilişim
Siber Suçlar
Karşı-Adli Bilişim ve Karşı-Karşı Adli Bilişim Teknikleri
Veri sızıntısı ve Veri Koruma
Veritabanında Adli Bilişim
İçerik Filtreleme
Dosya Sistemi ve Bellek Analizi
Sanal ve Bulut Ortamlarında Adli Tıp
Bilgi Gizleme
Multimedia Adli Bilişimi
İçeriden Saldırıların İncelenmesi
Büyük Ölçekli Araştırmalar
Malware Adli Bilişimi ve Anti-Malware Teknikleri
Ağ Adli Bilişimi ve Trafik Analizi
Donanım Hassasiyeti ve Cihazların Adli Bilişimi
Yeni Tehditler ve Geleneksel Olmayan Yaklaşımlar

Bilgi Güvencesi ve Güvenlik Yönetimi
İş Sürekliliği ve Felaket Kurtarma Planlaması

Kurumsal Yönetim
Kritik Altyapı Koruma
Dijital Haklar Yönetimi ve Fikri Mülkiyet Koruması
Güvenlik Ekonomisi
Dolandırıcılık Yönetimi
Kimlik Yönetimi
Kanun ve Yönetmelikler
Güvenlik Politikaları ve Güven Yönetimi
Tehditler, Güvenlik Açıkları ve Risk Yönetimi

Siber Savaş ve Fiziki Güvenlik
Gözetleme Sistemleri
Biyometri Uygulamaları
Siber Savaş Eğilimleri ve Yaklaşımlar
Elektronik Pasaportlar, Ulusal Kimlik ve Akıllı Kart Güvenliği
Sosyal Mühendislik
Kimlik ve Erişim Kontrol Sistemleri
Biyometri Standartları
Yeni Teori ve Algoritmalar

IoT Destekli Teknolojiler
5G Ağlar ve IoT
Yazılım Tanımlı Ağ (SDN) ve IoT
Sensör ve Aktüatör Ağları
Ultra-düşük güç IoT Teknolojileri ve Gömülü Sistem Mimarileri
Giyilebilir Cihazlar, Vücut Algılayıcı Ağlar, Akıllı Taşınabilir Aygıtlar
IoT Cihazlar ve Sistemleri için Tasarım Uzayı Keşif Teknikleri
Heterojen Ağlar
IoT Protokolleri (IPv6, 6LoWPAN, RPL, 6TiSCH, W3C)
Iot için Adlı Veri Ağı (NDN)
Nano Şeylerin Interneti
Sensör Veri Yönetimi, IoT Madenciliği ve Analitiği
Adaptif Sistemler
Dağıtık Depolama
Veri Füzyonu
Yönlendirme ve Kontrol Protokolleri
Kaynak Yönetimi, Erişim Kontrolü
Kimlik Yönetimi ve Nesne Tanıma
Yerini Belirleme Teknolojileri
Uç Nokta Bilişimi, Sis Bilişimi ve IoT
Makineler Arası Haberleşme (M2M) ve IoT
Endüstriyel IoT

IoT Uygulama ve Hizmetleri
Siber-fiziksel sistemler
İşbirlikçi Uygulamalar ve Sistemler
Servis Deneyimleri ve Analizi
Akıllı Şehirler, Akıllı Kamu Yerleri, Akıllı Ev/Bina
e-Sağlık, Yaşam Desteği,
Akıllı Ulaşım
Akıllı Şebekeler, Enerji Yönetimi
Tüketici Elektroniği
Kırsal Hizmetler ve Üretim
Endüstriyel IoT Servis Oluşturma ve Yönetimi
Kitle Kaynaklı Algılama, İnsan Merkezli Algılama

Büyük Veri ve IoT Veri Analitiği
Semantik Teknolojiler
Mobil Bulut Bilişim ve IoT
IoT için Yatay Uygulama Geliştirme
IoT Uygulama Geliştirme için Tasarım Prensipleri ve En İyi Uygulamalar

IoT Toplumsal Etkileri
IoT'da İnsan Rolü, Sosyal Hizmetler
Değer Zinciri Analizi
IoT için Yeni İnsan-Aygıt Etkileşimleri
Sosyal Modeller ve Ağlar
Yeşil IOT: Sürdürülebilir Tasarım ve Teknoloji
Kent Dinamikleri ve Kitle Kaynaklı Hizmetler
IoT Sürdürülebilirliği ve ROI için Ölçümler ve Değerlendirmeler

IoT için Güvenlik ve Gizlilik
IoT Gizlilik ve Güvenlik Endişeleri
Kimlik Saptama ve Kimlik Doğrulama Sorunları
IoT Güvenliği için Kablosuz Sensör Ağı
IoT'da Saldırı Tespiti
IoT için kriptografi, anahtar yönetimi ve yetkilendirme
IoT'da Fiziksel / MAC / Ağ Saldırıları
IoT'da Çapraz Katmanlı Saldırılar
IoT'da QoS Optimizasyonu ile Güvenlik
IoT'da Gizlilik Tabanlı Kanal Erişimi
IoT Adli Bilişimi
IoT'da Büyük Veri ve Bilgi Bütünlüğü
IoT'da Haberleşme Güvenliği
IoT'da Güvenlik Standartları

IoT Deneysel Sonuçlar ve Dağıtım Senaryoları
Araştırma ve Uygulama Arasındaki Boşluğu Kapama
Deneysel Prototipler ve Sınama Ortamları
Çok amaçlı IOT Sistem Modelleme ve Analiz
IOT Ara Bağlantı Analizi
Gerçek Vaka Dağıtım Senaryoları ve Sonuçları
Standardizasyon ve Düzenleme

LANGUAGE/KONFERANS DİLİ

- Konferans dili İngilizce ve Türkçe'dir.
- Conference language is in Turkish and English

PREFACE / ÖNSÖZ

Bilgi güvenliği ve siber güvenlik alanında, ulusal ve uluslararası boyutta bilimsel, teknik, sosyal ve kültürel çalışmalar yürüterek kişisel, kurumsal ve ulusal farkındalığın oluşması ve ortak akıl ile çözüm önerilerinin geliştirilmesi amacı ile 2007 yılında kurulan Bilgi Güvenliği Derneği (BGD) her yıl Uluslararası Bilgi Güvenliği ve Kriptoloji (ISCTURKEY) Konferansı düzenlemektedir. Bu konferansın on ikincisi, Gazi Üniversitesi, İstanbul Teknik Üniversitesi ve Ortadoğu Teknik Üniversitesi işbirliğiyle ve T.C. Cumhurbaşkanlığı Savunma Sanayi Başkanlığı, T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ve Bilgi Teknolojileri ve İletişim Kurumu'nun destekleriyle 16-17 Ekim 2019 tarihlerinde BTK Kongre Merkezinde gerçekleştirilmiştir.

Uluslararası ISCTURKEY Konferansı, düzenlendiği ilk yıldan beri Türkiye'nin bilgi güvenliği alanındaki bilimsel ve sektörel çalışmalarının paylaşıldığı, üniversite-kamu-endüstri işbirliğinin geliştirildiği, kamuoyunun bilgilendirildiği, eğitildiği, ulusal ve uluslararası tüm bilim insanları, araştırmacılar ve sektörel uygulayıcılar arasında bilgi alışverişinin sağlandığı, ülkemizin bu alandaki en önemli etkinliğidir. Bu etkinlik ile bilgi güvenliği alanında, toplumun her kesiminin farkındalığının arttırılması, bilimsel bilgi birikimine katkı sağlanması, kurumlar ve sektörler arasında işbirliği imkânlarının oluşturulması ve en önemlisi bunu uluslararası boyutta yaparak uluslararası işbirliğinin arttırılması hedeflenmiştir.

ISCTURKEY 2019 Konferansı Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından da desteklenmiş ve Avrupa Birliği'nin her yılın Ekim ayı olarak belirlediği "Avrupa Siber Güvenlik Ayı" etkinlikleri kapsamına alınmıştır. ISCTURKEY 2019 Konferansının bu yılki ana teması "Siber Güvenlik ve Kuantum Sonrası Kriptoloji" olarak belirlenmiştir. Milli güvenliğin önemli bir parçası olan siber güvenlik konusunda zafiyet gösterilmemesi için hem nitelikli siber güvenlik uzmanları yetiştirilmesi hem de gerek donanım gerek yazılım alanında milli ve yerli çözümler üretilmesinin şart olduğu düşüncesinden hareketle ISCTURKEY 2019 Konferans programı oluşturulmuştur.

ISCTURKEY 2019 Konferansına, bu yıl 1500'ün üzerinde kişi elektronik kayıt yaptırmıştır. Konferans programında; 4 panel, 2 Kurul Toplantısı, 6 akademik oturum, 3 davetli konuşmacı, 4 eğitim oturumu gerçekleştirilmiştir.

Konferansa sunulmak üzere gönderilen bildiriler, Konferans Bilim Kurulu üyelerin tarafından en az iki üye tarafından incelenmiş ve sunulması önerilen bildiriler, akademik oturumlarda sunulmuş ve bu kitapçıkta basılmıştır.

Bu yıl on ikincisini yaptığımız bu uluslararası konferansın başta ülkemiz ve kurumlarımız olmak üzere tüm katımcılarına faydalı olmasını dileriz.

Prof. Dr. Şeref SAĞIROĞLU, Konferans Eş-Başkanı
Prof. Dr. Mustafa ALKAN, Konferans Eş-Başkanı
Prof. Dr. Ersan AKYILDIZ, Konferans Eş-Başkanı
Prof. Dr. Ferruh ÖZBUDAK, Konferans Eş-Başkanı

12th INTERNATIONAL CONFERENCE ON INFORMATION SECURITY AND CRYPTOLOGY *(ISCTURKEY 2019)*

12. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı

16-17 October / Ekim 2019

BTK Congress Center / BTK Kongre Merkezi, Ankara, Turkey

https://www.iscturkey.org

CONFERENCE PROGRAM

FIRST DAY / İLK GÜN
(16 OCTOBER/EKİM 2019)

08:30 - 09:00	**KAYIT**
09:00 - 11:00	**AÇILIŞ KONUŞMALARI / Ana Salon** Ahmet Hamdi ATALAY - Bilgi Güvenliği Derneği YK Başkanı Ömer Abdullah KARAGÖZOĞLU - BTK Başkanı Dr. Ömer Fatih SAYAN - Ulaştırma ve Altyapı Bakanlığı, Bakan Yardımcısı Mehmet Cahit TURHAN – T.C. Ulaştırma ve Altyapı Bakanı Recep Tayyip ERDOĞAN – T.C. Cumhurbaşkanı (*Teşrifleri Dahilinde)
11:00 - 11:15	**Siber Güvenlik Üstün Hizmet Ödülleri Töreni**
11:15 – 11:30	**İletişim Arası**
11:30 – 12:30	**Davetli Konuşmacı-Keynote Speaker Albay Jaak TRIEN – NATO Müşterek Siber Savunma Mükemmeliliyet Merkezi Direktörü**

12:30 – 13:00 **Öğle Arası**

13:00 – 13:45 **Davetli Konuşmacı-Keynote Speaker**
Doç. Dr. Sedat AKLEYLEK
Kuantum Bilgisayarların Güvenlik Üzerindeki Etkisi / Impact Of Quantum Computers On Security

13:45 – 15:00 **PANEL - 1 / Ana Salon**
"Siber Güvenlik ve Kuantum Sonrası Kriptoloji"

Panel Yöneticisi: Doç. Dr. Murat CENK - ODTÜ Öğretim Üyesi
Panelistler
Uğur ÇAĞAL - NETAŞ Siber Güvenlik Teknolojileri Geliştirme Direktörü
Emre YÜCE - HAVELSAN
Şadi Çağatay ÖZTÜRK - Rovenma CTO
Dr. Mert ÖZARAR - THK Üniversitesi Bilgisayar Mühendisliği Bölüm Başkan Yardımcısı
Doç. Dr. Orhun Kara - Ulusal Elektronik Kriptoloji Araştırma Enstitüsü (UEKAE)

15:00 – 15:30 **İletişim Arası**

15:30 – 18:00 **PANEL - 2 / Ana Salon**
"5G ve Siber Güvenlik"
Panel Yöneticisi: Rıdvan KAHVECİ - BTK Kurul Üyesi

ANA SALON (BTK Konferans Salonu, Ankara)	
1. GÜN	
16/Ekim/2019, Çarşamba	
08:30 - 09:00	KAYIT
09:00 - 10:45	AÇILIŞ KONUŞMALARI / Ana Salon
Açılış Konuşmaları	**Ahmet Hamdi ATALAY** - Bilgi Güvenliği Derneği YK Başkanı
	Ömer Abdullah Karagözoğlu, Bilgi Teknolojileri ve İletişim Kurumu Başkanı
	Mehmet Cahit TURHAN - T.C. Ulaştırma ve Altyapı Bakanı
	Recep Tayyip ERDOĞAN - T.C. Cumhurbaşkanı (*Teşrifleri Dahilinde)
10:45 - 11:00	**Siber Güvenlik Üstün Hizmet Ödülleri Töreni**
11:00-11:30	**İletişim Arası**
11:30-12:30	**Albay Jaak Tarien -** NATO Müşterek Siber Savunma Mükemmeliyet Merkezi Direktörü
	NATO Müşterek Siber Savunma Mükemmeliyet Merkezi'nin Siber Alanda Güvenlik ve Savaşlara Bakışı: Yeni Zorluklar ve Yeni Stratejiler
12:30-13:30	**Öğle Arası**
	PANEL - 1 / Ana Salon
13:30 - 15:00	*"Siber Güvenlik ve Kuantum Sonrası Kriptoloji"*
Panel Yöneticisi:	**Doç. Dr. Sedat AKLEYLEK,** 19 Mayıs Üniversitesi Öğretim Üyesi
Panelistler	**Dr. Mert Özarar,** THK Üniversitesi Bilgisayar Mühendisliği Bölüm Başkan Yardımcısı
	Doç. Dr. Orhun Kara, TÜBİTAK UEKAE
	Emre Yüce, HAVELSAN
	Şadi Çağatay Öztürk, ROVENMA CTO
	Prof. Dr. Süleyman Serdar Kozat, Bilkent Üniversitesi Elektrik Elektronik Mühendisliği
15:00 – 15:30	İletişim Arası

15:30 – 17:00	**PANEL - 2 / Ana Salon**
	"5G ve Siber Güvenlik"
Panel Yöneticisi:	**Abdullah Raşit Gülhan,** TNB Bilişim Teknolojileri Genel Müdürü
Panelistler	**Uğur Çağal,** NETAŞ Siber Güvenlik Teknolojileri Geliştirme Direktörü
	Dr. Pelin Angın, ODTÜ Bilgisayar Mühendisliği Öğretim Üyesi
	Bülent Arsal, BTK Bilgi Teknolojileri Dairesi Başkanı
	Dr. Metin Balcı, ULAK Haberleşme Genel Müdürü
	Prof. Dr. Lütfiye Durak Ata, İTÜ Bilişim Enstitüsü Müdürü
17 EKİM 2019 / 2. GÜN	
	PANEL - 3 / Ana Salon
09:00 - 10:30	***"Siber Güvenlik Sanayi ve Kümelenmesi"***
Panel Yöneticisi:	**Mustafa Özçelik,** SSB Siber Güvenlik ve Bilişim Sistemleri Grup Başkanı
	Veysel Ataytur, LOGSIGN CEO
	İbrahimCan Sönmez, IntelProb Genel Müdür Yardımcısı
	Kadir Murat Biçer, STM Siber Güvenlik Projeleri Grup Lideri
	Oğuz Yılmaz, Labris Networks Kurucu Ortağı
10:30 – 11:00	**İletişim Arası**
	PANEL - 4 / Ana Salon
11:00 - 12:30	***Dijital Türkiye ve Siber Güvenlik***
Panel Yöneticisi:	**Yavuz Emir Beyribey**, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkan Yardımcısı
Panelistler:	**Dr. Cemil Sağıroğlu,** TÜBİTAK BİLGEM YTE Müdürü
	Prof. Dr. Tuncay Yiğit, Süleyman Demirel Üniversitesi
	Dr. Tacettin Köprülü, HAVELSAN Strateji Yönetim Müdürü
	Dr. Emin İslam Tatlı, STM Siber Güvenlik ve Büyük Veri Direktörü
12:30 - 13:30	**İLETİŞİM ARASI**
	Ana Salon / Main Hall
13:30 – 14:30	***Siber Güvenlik Eğitimi Oturum 1 / Training on Cyber Security Session 1***
Konu Başlığı:	**Yeni Nesil Siber Saldırılar**
Eğitmenler:	**Korhan Gürler,** HAVELSAN
14:30 - 15:00	**İletişim Arası**
15:00 - 16:00	**Ana Salon / Main Hall**
	Siber Güvenlik Eğitimi Oturum 2/ Training on Cyber Security Session 2
Konu Başlığı:	**Açık Kaynak Kodlu Yazılımlar: Zorluklar ve Fırsatlar**
Eğitmenler:	**Ali Orhun Akkırman,** HAVELSAN
16:00 – 16:30	**İLETİŞİM ARASI**
16:30 – 17:30	**Ana Salon / Main Hall**
	Siber Güvenlik Eğitimi Oturum 3 / Training on Cyber Security Session 3
Konu Başlığı:	**Açık Kaynak Siber Tehdit İstihbaratı**
Eğitmenler:	**Şeref Can Özkaya,** STM
	İletişim Arası
17:45 - 18:00	**Kapanış Konuşmaları / Closing Remarks: Ana Salon**
	Prof. Dr. Şeref Sağıroğlu, ISC TURKEY 2019 Konferansı Eş Başkanı
	Prof. Dr. Mustafa Alkan, ISC TURKEY 2019 Konferansı Eş Başkanı
	Prof. Dr. Ertuğrul Karaçuha, ISC TURKEY 2019 Konferansı Eş Başkanı
	Prof. Dr. Ferruh Özbudak , ISC TURKEY 2019 Konferansı Eş Başkanı

Panelistler Uğur ÇAĞAL - NETAŞ Siber Güvenlik Teknolojileri Geliştirme Direktörü

SSB -
Cumhurbaşkanlığı Dijital Dönüşüm Ofisi -
Doç. Dr. Ertan ONUR - ODTÜ Bilgisayar Mühendisliği Bölümü Öğretim Üyesi

SECOND DAY / İKİNCİ GÜN
(17 OCTOBER/EKİM 2019)

Sözlü ve Poster Sunumları Programı

SALON 2:

09:00 – 10:30

Oturum: Kuantum Kriptografi

Oturum Başkanı: Doç. Dr. Murat Cenk, ODTÜ

- **Kuantum Kriptanalizin Siber Güvenlikteki Yeri,** (Muharrem Tuncay Gençoğlu, Fırat Üniversitesi)
- **Kuantum Dijital İmza Teknolojilerini Kullanarak Kuantum Elektronik İmza Geliştirmek** (Cumali Yaşar, Çanakkale Onsekiz Mart Üniversitesi - İhsan Yılmaz, Çanakkale Onsekiz Mart Üniversitesi)
- **Hassas Verilerin Korunmasında Klasik ve Kuantum Kriptoloji Yöntemleri Üzerine Bir Araştırma** (Ömer Kasım, Kütahya Dumlupınar Üniversitesi – Esma Coşgun, İstanbul Şehir Üniversitesi)
- **Secure Quantum Communication Based on Clifford Scrambling With Blind Trent** (İhsan Yılmaz, Çanakkale Onsekiz Mart Üniversitesi - Erdi Acar, Çanakkale Onsekiz Mart Üniversitesi)

11:00 – 12:30

Oturum: Kuantum Sonrası Kriptografi

Oturum Başkanı: Doç. Dr. Alptekin Küpçü, Koç Üniversitesi

- **Kuantum Sonrası Güvenilir ABC Şifreleme Sisteminin Farklı Platformlardaki Uygulamaları** (Sedat Akleylek, Ondokuz Mayıs Üniversitesi – Ramazan Koyutürk, Ege Üniversitesi)
- **Bazı Kod Tabanlı Kuantum Sonrası Algoritmaların Performans Analizleri** (Zülfükar Saygı, TOBB ETÜ – Burcu Ecem Yılmaz, TOBB ETÜ)
- **Kafes Tabanlı Kuantum Sonrası Algoritmaların Profil Analizi ve GPU Uygulamaları** (Aleaddin Özer, Hacettepe Üniversitesi – Adnan Özsoy, Hacettepe Üniversitesi – Oğuz Yayla, Hacettepe Üniversitesi)
- **Analyzing NIST 2nd-round Lattice-based Post-quantum KEM Algorithms** (Berkin Aksoy, ASELSAN – Yusuf Alper Bilgin, ASELSAN – Murat Cenk, ODTÜ - Murat Burhan İlter, ASELSAN – Neşe Koçak, ASELSAN – Yunus Emre Yılmaz, ASELSAN)
- **Enhanced AES with Arnold's CAT Map - Arnold's CAT Map ile Güçlendirilmiş AES** (Hakan Bostan, ODTÜ – Atila Bostan)

13:30 – 14:30

Oturum: Kriptografik Protokoller ve Uygulamaları

Oturum Başkanı: Prof. Dr. Ali Aydın Selçuk, TOBB ETÜ

- **Improving PKI, BGP, and DNS Using Blockchain: A Systematic Review** (Faizan Safdar Ali, Koç Üniversitesi – Alptekin Küpçü, Koç Üniversitesi)

- **BasGit: A Secure Digital ePassport Alternative** (Ceren Kocaoğullar, Koç Üniversitesi – Kaan Yıldırım, Koç Üniversitesi - Mert Atila Sakaoğulları, Koç Üniversitesi - Alptekin Küpçü, Koç Üniversitesi)
- **A Study on ID-Based Authenticated Key Agreement Protocols** (Gülnihal Öztürk, Famecrypt – Nurdan Saran, Çankaya Üniversitesi)

15:00 – 16:00

Oturum: Bilgi Güvenliği

Oturum Başkanı: Doç. Dr. Oğuz Yayla, Hacettepe Üniversitesi

- **Comparing PRESENT and LBlock block ciphers over IoT Platform** (Pejman Panahi, Sakarya Üniversitesi – Cüneyt Bayılmış, Sakarya Üniversitesi – Ünal Çavuşoğlu, Sakarya Üniversitesi – Sezgin Kaçar, Sakarya Üniversitesi)
- **Makine Öğrenmesi Yöntemleri İle Oltalama Websitesi Saldırı Tespiti** (Şevki Gani Şanlıöz, Milli Savunma Üniversitesi - Mustafa Kara, Milli Savunma Üniversitesi – Muhammed Ali Aydın, İstanbul Üniversitesi – Hasan Hüseyin Balık, Milli Savunma Üniversitesi)
- **BLE Teknolojisi ve Güvenliği** (Bengü Tacettin, İstanbul Üniversitesi – Cerrahpaşa – Muhammed Ali Aydın, İstanbul Üniversitesi)
- **Smart City Services** (Murat Dener, Gazi Üniversitesi)

16:00 – 18:00

Oturum: Bilgi Güvenliği Uygulamaları

Oturum Başkanı: Prof. Dr. Suat Özdemir, Gazi Üniversitesi

- **AB Komisyonu'nun Bilgi Güvenliğinin Sağlanması ve Bilginin Korunmasına İlişkin Politika Belgelerinin İncelenmesi (**Demet Soylu, Ankara Yıldırım Beyazıt Üniversitesi – Tunç Medeni, Ankara Yıldırım Beyazıt Üniversitesi – Tolga Medeni, Ankara Yıldırım Beyazıt Üniversitesi)
- **Docker Konteyner Teknolojisi Üzerine Yapılan Güvenlik Çalışmalarının İncelemesi** (Tamer Say, Gazi Üniversitesi – Mustafa Alkan, Gazi Üniversitesi – İbrahim Alper Doğru, Gazi Üniversitesi – Murat Dörterler, Gazi Üniversitesi)
- **Nesnelerin İnterneti (IoT) Ağlarında Veri Mahremiyetinin Korunması Üzerine İnceleme** (Ömer Faruk Ateş, Gazi Üniversitesi – Mehmet Arslan, Gazi Üniversitesi – Cengiz Paşaoğlu, KVKK)
- **Büyük Veri Analitiği Kullanan Bir SIEM Yazılımı Geliştirilmesi** (Burak Çayır, Gazi Üniversitesi – Bünyamin Ciylan, Gazi Üniversitesi)
- **Windows Sistemlerinde Post Exploitation İşlemleri İçin Bir Araç Geliştirilmesi** (Sedat Kızılçınar, Gazi Üniversitesi – Bünyamin Ciylan, Gazi Üniversitesi)
- **TLS Protokolü'ne Yapılan Güncel Kriptografik Saldırılar** (Duygu Özden, HAVELSAN)

PANELLER

SALON ANA:

09:30 – 10:30	**PANEL - 3 / Ana Salon** **"Siber Güvenlik Sanayi ve Kümelenmesi"**
Panel Yöneticisi:	Mustafa ÖZÇELİK - SSB Siber Güvenlik ve Bilişim Sistemleri Grup Başkanı
Panelistler	Bilgehan ÜSTÜNDAĞ - CHOMAR Antivirüs CEO Veysel Ataytur - Logsign CEO, Kurucu Ortak Kadir Murat BİÇER – STM Siber Güvenlik Müdürü Oğuz YILMAZ - Labris Networks Kurucu Ortağı
10:30 – 11:00	**İletişim Arası**
11:00 – 12:30	**PANEL - 4 / Ana Salon** **"Dijital Türkiye ve Siber Güvenlik"**
Panel Yöneticisi:	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi -
Panelistler	Murat GÜRAKAN - STM Siber Güvenlik Danışmanlık Grup Lideri

Seçkin GÜRLER - Labris Networks Kurucu Ortağı
Prof. Dr. Tuncay YİĞİT - Süleyman Demirel Üniversitesi
Dr. Tacettin KÖPRÜLÜ - HAVELSAN Genel Müdür Danışmanı

12:30 – 13:30 **İletişim Arası**

13:30 – 14:30 **Ana Salon**
Siber Güvenlik Eğitimi Oturum 1 / Training on Cyber Security Session 1
Konu Başlığı "Yeni Nesil Siber Saldırılar"
Eğitmenler Korhan GÜRLER, HAVELSAN

14:30 – 15:00 **İletişim Arası**

15:00 – 16:00 **Ana Salon**
Siber Güvenlik Eğitimi Oturum 2 / Training on Cyber Security Session 2
Konu Başlığı "Açık Kaynak Kodlu Yazılımlar: Zorluklar ve Fırsatlar"
Eğitmenler Ali Orhun AKKIRMAN, HAVELSAN

16:00 – 16:30 **İletişim Arası**

16:30 – 17:30 **Ana Salon**
Siber Güvenlik Eğitimi Oturum 3 / Training on Cyber Security Session 3
Konu Başlığı "Açık Kaynak Siber Tehdit İstihbaratı"
Eğitmenler Şeref Can Özkaya, STM

17:45 – 18:00 **Kapanış Konuşmaları / Closing Remarks : Ana Salon - Main Hall**
Prof. Dr. Şeref Sağıroğlu - ISC TURKEY 2019 Konferansı Eş Başkanı
Prof. Dr. Mustafa Alkan - ISC TURKEY 2019 Konferansı Eş Başkanı
Prof. Dr. Ertuğrul Karaçuha - ISC TURKEY 2019 Konferansı Eş Başkanı
Prof. Dr. Ferruh Özbudak - ISC TURKEY 2019 Konferansı Eş Başkanı

TABLE OF CONTENTS / İÇİNDEKİLER TABLOSU

ORAL PRESENTATIONS/ SÖZLÜ SUNUMLAR

Kuantum Dijital İmza Teknolojilerini Kullanarak Kuantum Elektronik İmza Geliştirmek

Cumali YAŞAR
Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
Çanakkale Onsekiz Mart Üniversitesi)
Çanakkale /Türkiye
cyasar@comu.edu.tr

İhsan YILMAZ
Bilgisayar Mühendisliği Bölümü
Çanakkale Onsekiz Mart Üniversitesi)
Çanakkale /Türkiye
iyilmaz@comu.edu.tr

***Özet*— Kuantum devriminde; kamu ve özel sektörde en çok kullanılan elektronik imzaların yerini kuantum dijital imza teknolojilerini kullanan kuantum elektronik imzalar alacaktır. Bu nedenle, bu çalışmada eski sistemle de uyumlu olabilecek Kuantum elektronik yazışma paketi(keyp) önerisi sunulmaktadır. Kuantum eyp paketinde kullanılacak kimlik doğrulaması için kuantum parmak izi, göz retinası ve DNA önerilmektedir.**

***Anahtar Kelimeler*—Kuantum elektronik yazışma paketi, Kuantum Elektronik İmza, Kuantum XML, Kuantum şifreleme.**

Abstract: In the quantum revolution; The most widely used electronic signatures in the public and private sectors will be replaced by quantum electronic signatures using quantum digital signature technologies. Therefore, in this study, a quantum electronic correspondence package (keyp) is proposed which can be compatible with the old system. Quantum fingerprint, eye retina and DNA are recommended for authentication in the quantum eyp package.

Keywords — Quantum electronic correspondence package, Quantum Electronic Signature, Quantum XML, Quantum Cryptography

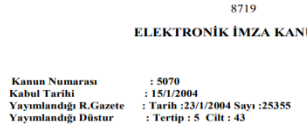
I. GİRİŞ

İmza, "Bir kimsenin, bir yazının altına bu yazıyı yazdığını veya onayladığını belirtmek için her zaman aynı biçimde yazdığı ad veya işarettir[1].

Elektronik İmza: Matematiksel fonksiyonları kullanarak tekil bir değer ya da değerlerin elde edilmesidir. [2].

Kuantum devriminde; kamu ve özel sektörde kullanılan elektronik imzaların yerini kuantum dijital imza teknolojilerini kullanan kuantum e-imzalar alacaktır. Kuantum dijital imza teknolojileri; kuantum mekaniği ilkelerini kullanır ve matematiksel olarak Hilbert uzayında tanımlı en az iki boyutlu vektörel fonksiyonlar ile üretilir. Vektörel fonksiyonları kullanma avantajı kuantum mekaniğinin doğasına uygun olmasıdır[3].

Günümüz teknolojilerinin geldiği en son nokta Kuantum Bilgi İletişimi tabanlı teknolojilerdir. Her zaman olduğu gibi bilginin iletiminde ve yönetiminde güvenlik ve hız ilk parametredir. Kuantum teknolojilerindeki gelişmelerden biri de kuantum mekaniğinin temel ilkelerine dayanan dijital imza şemalarının geliştirilmesidir. Bu kavramlar genel olarak kuantum dijital imza QDS) şemaları şeklinde ifade edilmektedir. Bu alandaki ilk kuantum dijital imza fikrini ortaya koyanlar Daniel Gottesman ve Isaac Chuang' dır[4]. Kuantum elektronik imza ise kuantum dijital imza teknolojileri ile üretilen sayısal veri kümesidir. Klasik anlamda elektronik imzalar dijital imza teknolojileri ile üretilen anahtarlardır[5]. Dijital imzalar üretmek için yetkili sertifika sahibi olması gerekir.


8719

ELEKTRONİK İMZA KANUNU (1)

Kanun Numarası : 5070
Kabul Tarihi : 15/1/2004
Yayımlandığı R.Gazete : Tarih :23/1/2004 Sayı :25355
Yayımlandığı Düstur : Tertip : 5 Cilt : 43

Fig. 1. Figure 1 Elektronik imza kanunu

Elektronik imza ile ilgili resmi tanımlama 5070 sayılı Elektronik İmza Kanununda tanımlanmıştır. Bu tanıma göre "Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi tanımlar. İlgili kanunun devamında; "Bir bilginin üçüncü tarafların erişimine kapalı bir ortamda, bütünlüğü bozulmadan (bilgiyi ileten tarafın oluşturduğu orijinal haliyle) ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşur[6]".

ABD Federal ESIGN Yasasına göre, "Elektronik ses, sembol veya süreç, bir sözleşmeye veya başka bir kayda bağlı veya mantıksal olarak iliştirilmiş kimlik doğrulama aracıdır"[7].

Tanımlardan hareketle Elektronik İmzanın Ortak Özellikleri[2];

•Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmaması,

•Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini sağlaması,

•Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesi, kullanılamaması ve elektronik imzanın sahteciliğe karşı korunması,

•İmzalanacak verinin imza sahibi dışında değiştirilememesi ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesi.

Elektronik imza kullanıcılarına aşağıda belirtilen üç temel özelliği sağlamaktadır:

•Veri Bütünlüğü: Verinin izinsiz ya da yanlışlıkla değiştirilmesini, silinmesini ve veriye ekleme yapılmasını önlemek,

•Kimlik Doğrulama ve Onaylama: Mesajın ve mesaj sahibinin iletiminin geçerliliğini sağlamak,

•İnkar Edilemezlik: Bireylerin elektronik ortamda gerçekleştirdikleri işlemleri inkar etmelerini önlemek.

Kuantum Elektronik İmza yazılımı, e-yazışma paketinin tüm bileşenlerini aynı anda imzalanmasını sağlamaktadır. Bu sayede resmi yazıya ait birden çok bileşen aynı anda imzalanarak paket içerisine eklenebilir ve süreç aynı anda yönetilebilir olmaktadır. Resmi yazılar, noter yazıları, şirket yazıları genelde birden çok dağıtımlı yazılardır. Bu belgelere ait ekler bulunmaktadır. Resmi yazıyı ekleriyle birlikte dağıtımda yer alan kurumlara gönderilmesi veya bir kısmına gönderilmemesi olası bir durum iken Kuantum elektronik imza sürecinde bu imkansızdır. Belgeye ait tüm bileşenler tek seferde eksiksiz olarak kuantum elektronik imza ile onaylanmış olmaktadır.

Benzer şekilde, kurum içi elektronik belge süreçlerinde e-Yazışma Paketi yapısının kullanılmadığı durumlarda, kurum dışına gönderilecek resmi yazının kurum içinde kalan kopyası, kullanılan dosya formatından bağımsız olarak, paket ile tek seferde imzalanabilir. Böylece, resmi yazının kurum içinde kalacak kopyası ve kurum dışına gönderilecek kopyası için ayrı ayrı imza atılması zorunluluğu ortadan kaldırılmış olur.

Yazışma Paketi'nin kurumlar arası iletimi sırasında güvenlik amacıyla kuantum şifreleme kullanılabilir. Kuantum kanallardan iletilir. Kuantum kanallardan iletim; kuantum mekaniği ilkelerine göre yapıldığından klasik kanallara göre çok daha güvenli olmaktadır. Çalışmamızı aşağıdaki şekilde özetleyebiliriz. Bu çalışmada öncelikle klasik elektronik yazışma paketi kısaca anlatılacak. Daha sonra önerilen kuantum elektronik yazışma paketinden bahsedilecek. Ayrıca kuantum elektronik yazışma paketinde imza olarak kullanılabilecek kauntum göz retinası, parmak izi ve DNA önerilmektedir. Sonuçlar ise son bölümde verilmektedir.

II. Klasik Elektronik İmza Altyapisinin Çalışma Şekli

1. Adım: Kullanıcı elektronik sertifika için yetkilendirilmiş olan elektronik sertifika hizmet sağlayıcısına başvurur.
2. Adım: Sertifika hizmet sağlayıcısı kullanıcının kimliğini geçerli ve güvenilir belgelerle onaylar.
3. Adım: Sertifika hizmet sağlayıcısı sertifikanın kaydını bir veri tabanında toplar.
4. Adım: Kullanıcı kendi gizli anahtarıyla mesaj sahibinin kimlik doğrulaması, mesajın bütünlüğünü ve inkar edilemezliğini sağlayarak mesajı imzalar ve karşı tarafa gönderir.
5. Adım: Karşı taraf mesajı alır. Elektronik imzasını kullanıcının açık anahtarıyla onaylar ve kullanıcının sertifikasının geçerliliğini ve durumunu kontrol etmek için veri tabanında sorgulama yapar.
6. Adım : Veri tabanında yapılan sorgulama sonucu sertifikanın geçerli/iptal durum bilgilerini karşı tarafa iletir.

Elektronik imza üretilirken dikkat edilirse birinci adımda olduğu gibi dijital imza üreten bir sertifikaya başvurmak gerekir. Kuantum devriminde de kuantum dijital sertifika üreten yetkili merkezler hem güvenlik hem de yasanın koşullarını yerine getirmiş olacaktır.

Klasik Dijital imza için kullanılan Elektronik Belge tanımı kuantum bilgisayarlar için de geçerli olacaktır. Klasik bilgisayarlarda üretilen elektronik belgeler kuantum bilgisayarlar için de çalışma şekli aynı olacaktır.

Kullanıcı bir bilgisayar yazılımı ile bir belge oluşturacak ve bunu bir birime ya da bir kullanıcıya gönderecektir. Gönderim sırasında belgeyi üretene ait temel üst verileri de karşıya gönderecektir. Elektronik yazışma paketi olarak tanımlanan ifadede belgeye ait üstveriler korunacaktır. Kuantum bilgisayarlar için elektronik belgeye ait üstveri yapısı kuantum xml formatında olması gerekir. Ayrıca kuantum bilgisayarlar arası veri gönderme protokol tipleri belgeye ait üstverileri kuantum veri yapısı da eklenecektir.

2 Şubat 2015 tarih ve 29255 sayılı Resmi Gazetede yayımlanan "Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik[8]" resmi yazışmalarını elektronik ortamda gerçekleştirecek kamu kurum ve kuruluşlarının zorunlu olarak uyması gereken üstveri yapısının kuantum bilişim sistemlerinde uygulamalarının yapısına ait olmasıdır. Şekil -2 de bunun yapısı görülmektedir. Bu yapı süreci tüm elektronik imza üreten kuruluşlar için geçerlidir.

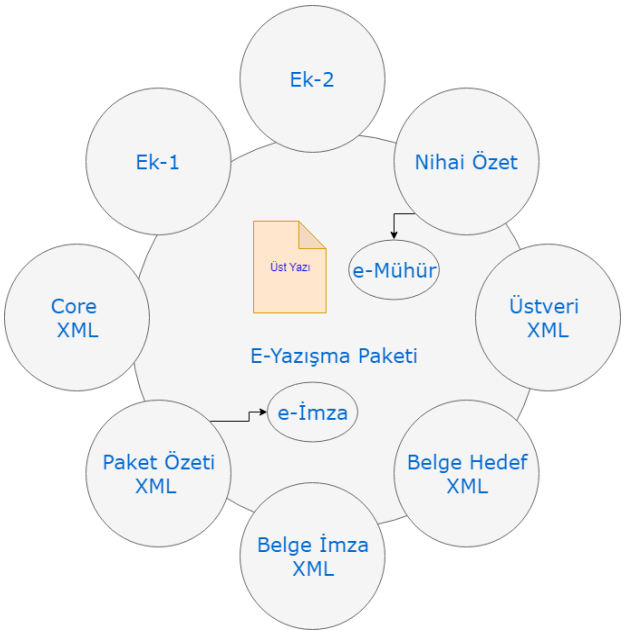


Fig. 2. Klasik e-yazışma paket yapısının içeriği

III. Kuantum Elektronik Yazışma Paketinin Matematiksel Modeli

Yasayla tanımlanan elektronik yazışma paketi OPC(Open Packaging Conventions) standartlarını sağlamalıdır. OPC Yaygın bir biçimde kullanılan ZIP dosya yapısını temel alan geniş amaçlı dosya/bileşen paketleme kurallarıdır. OPC standartlarına göre elektronik belgeler bileşenlerden oluşur. Bu bileşenlerin her biri XML formatındadır. Bileşen yapıları makinelerce okunabilir bir formattadır.

Kuantum bilgisayarlarda üretilecek bu belgelerin bileşenleri için bir model önerisi aşağıdaki şekilde verilebilir.

$Ikeyp >= \text{Ik}paket(p_i) >$ .keyp :kuantum elektronik yazışma paketine verilen genel isimdir. Kuantum Paket fonksiyonu p_i değerleri pakete ait bileşenlerin veri yapılarını içeren değerlerden oluşmaktadır. Bu bileşenlerin her bir $p_i(k_j)$ kendi içinde birer fonksiyon olarak tanımlanmaktadır. Örneğin;

p_0 üst yazı bileşenini,
p_1. Üst veri bileşenini,
p_2 belge hedefi bileşenini,
….
p_8 nihai özet bileşenini
temsil eder.

Paket bileşeninin her birine ait bilgileri k_j'ler ile gösterebiliriz. k_j'ler verinin kendisini temsil eder.

Örneğin;
k_0 Belge Id değerini;
k_1 konu değerini;
k_2 tarih değerini;
…
k_{50} dosya adını temsil eder.
$k_j = \cup_{j=0}^{n} l_j$
şeklinde tanımlanabilir.

l_j'ler verilerin satır numaralıdır. Kuantum XML yapısındadır.

Birleşim sembollerini matematiksel olarak art arda yapılacak işlem olarak gösterirsek

$Ikeyp >= \sum_{i=0}^{20} Ip_i > (\sum_{j=0}^{n} Ik_j > (\sum_{j=0}^{n} Il_j >))$

Şeklinde denklem elde ederiz. Bu denklemin şematik gösterimi aşağıdaki şekilde verilebilir.

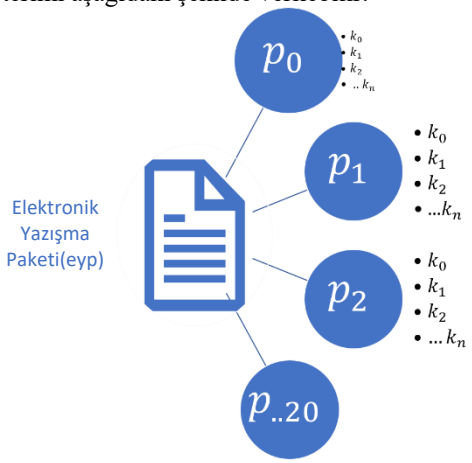


Fig. 3. keyp paketinin şematik gösterimi

02/02/2015 tarihli ve 29255 sayılı Resmi Gazete'de yayımlanan "Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik"in 26'ncı maddesinin üçüncü fıkrasında çıktısı alınabileceği ifade edilen üstveriler bu paket bileşeninin elemanlarıdır. Bu paketin kuantum durum olarak gösterimi ve kuantum XML yapı şekli aşağıdaki şekilde gösterilebilir.

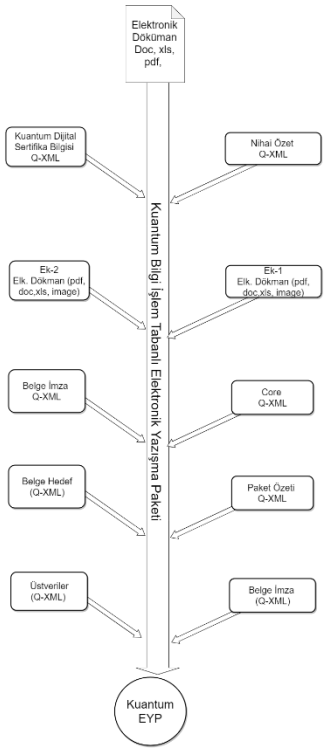


Fig. 4. KEYP Paket yapısı[9]

Kuantum XML[10], Kuantum Bilişim Bilimleri (KBB) alanındaki üstverilerin yönetimi için geliştirilen XML'dir. Kuantum XML'in amacı, kuantum programlama için gerekli olan veri modelini tanımlamak ve Elektronik belgelerin bileşenlerini OPC standartlarında yapılandırmaktır[9]. Kuantum bilgisayarların veri işlemesinde; veriyi anlamsal yapıda bilgiyi dönüştürmesindir. Tanımlanan bilgiler yazılım olarak işlenerek uygun bir çıktıyı elde etmeyi amaçlamaktadır[10].

Kuantum EBYS sisteminde bileşen olarak bulunan Üstveri modelinin örnek kuantum durum yapısı aşağıdaki şekilde verilebilir.

Belgeld, konu, tarih, BelgeNo, GuvenlikKodu ve mimeturu kuantum XML olarak aşağıdaki gibi ifade edilebilir.

<BelgeId> : $\Psi_{belgeid} = \alpha|belgeid\rangle + \beta|belgeid\rangle$
<BelgeId>101001010010</BelgeId>
<konu>: $\Psi_{konu} = \alpha|konu\rangle + \beta|konu\rangle$
<Konu>Tez Yönergesi </Konu>
<tarih>: $\Psi_{tarih} = \alpha|tarih\rangle + \beta|tarih\rangle$
<Tarih>2019-06-12…</Tarih>
<BelgeNo>: $\Psi_{belgeno} = \alpha|belgeno\rangle + \beta|belgeno\rangle$
<BelgeNo>69471265-902-E.4752</BelgeNo>
<GuvenlikKodu>: $\Psi_{gvkkodu} = \alpha|gvkkodu\rangle + \beta|gvkkodu\rangle$<GuvenlikKodu>HZO</BelgeNo>
<GuvenlikKoduGTar> $\Psi_{gkgt} = \alpha|gkgt\rangle + \beta|gkgt\rangle$
<GuvenlikKoduGTar> </GuvenlikKoduGTar>
<MimeTuru> $\Psi_{mimeturu} = \alpha|mimeturu\rangle + \beta|mimeturu\rangle$ <MimeTuru> application PDF</MimeTuru>
<OzId> $\Psi_{ozid} = \alpha|ozid\rangle + \beta|ozid\rangle$ <OzId schemeID="GUID">6A690BBB-FA820EFE4CB9</OzId>

Elektronik belgelerin paket yapısı OPC standartlarında oluşturulması gerekmektedir[9]. Kuantum bilişimi için bu yapı aynen korunmaktadır. Paket oluşturma şekli, Şekil-5 oluşturulan yapıya uygundur. Kuantum elektronik imza ile imzalanan elektronik yazışma paketi için veri modelinde kuantum dijital imza algoritmalarından üretilmiş olan kuantum elektronik imza değeri kuantum xml formunda olmaktadır. Bu değer kuantum sürekliliğe bağlı olarak rastgele olarak üretilecektir. Bu elektronik imza için elde edilen değerler bir ikili şeklinde değil bir matris formundadır[10].

```
<g:Gate>
<r:Identification>
<r:ID>H</r:ID>
</r:Identification>
<g:Name>Hadamard</g:Name>
<r:Transformation size="1">
<r:Multiplier r="0.707106781">
<r:Symbolic syntax="odf">1/sqrt(2)</r:Symbolic>
<r:Symbolic syntax="html">1/sqrt(2)</r:Symbolic>
</r:Multiplier>
<r:Cell row="1" col="1" r="1"/>
<r:Cell row="1" col="2" r="1"/>
<r:Cell row="2" col="1" r="1"/>
<r:Cell row="2" col="2" r="-1"/>
</r:Transformation>
</g:Gate>
```

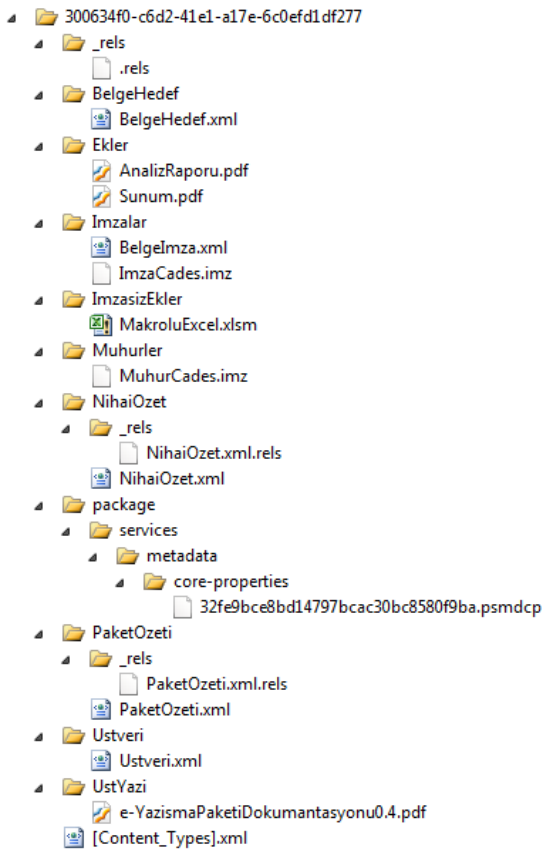


Fig. 5. Paket içeriği aynen korunmalıdır[9].

IV. DİGİTAL İMZA ÜRETME SÜREÇLERİ

Kuantum dijital imza algoritmalarında klasik imza algoritmalarında olduğu gibi genel ve özel anahtar oluşturma işlemleri tek seferlik olarak yapılmaktadır. Kuantum dijital imzalar genel olarak kuantum anahtar dağıtımı olarak tanımladığımız yapılar üzerine kurgulanmıştır[11].

Bir kuantum İmza protokolü, bir grup katılımcı tarafından gerçekleştirilir ve iki aşamaya ayrılır[11]; dağıtım aşaması ve mesajlaşma aşaması. Dağıtım aşaması, tarafların protokol kurallarına göre kuantum ve klasik sinyaller alışverişinde bulunduğu kuantum iletişim aşamasıdır. Prensipte, alınan kuantum durumları bir kuantum hafızasında saklamış olsalar da, katılımcıların durumları üzerinde ölçümler gerçekleştirdikleri ve sonuçları klasik bir belleğe kaydettiği daha pratik protokoller varsayımını kabul edilir[12].

Sistem kullanıcıları verilerini işleyebilir ve klasik olarak birbirleriyle iletişim kurabilirler. Genel olarak, her katılımcı mesajı imzalamak ve imzaları doğrulamak için aralarında bir ortak kural belirlemişlerdir. Bu kuralların geçerliliği genelde ölçüm sonuçlarına ve klasik iletişime bağlıdır[13].

Dağıtım aşamasının sonunda taraflar, mesajlaşma aşamasına devam edip etmeyeceğini veya protokolü iptal edip etmeyeceğine karar verirler. Mesajlaşma aşamasında, katılımcılardan biri (imzalayan) mesaja klasik bir dize (imza) ekleyerek bir mesaj imzalar. Bir katılımcı imzalanmış bir mesaj aldığında, protokol kurallarına göre geçerliliğini doğrular[14].

Kuantum dijital imzalar genel olarak yoğunluk matrisleri veya dalga denklemleri şeklinde iki formda üretilmektedirler[15]. Kuantum Mekaniğinin en önemli özelliklerinden biri dalga denklemine dayalı olmasıdır. Dalga denkleminin herhangi bir andaki ölçümü, sistemin o andaki durumu hakkında bilgi vermektedir. Doğal olarak sürekli olan kuantum hesaplama mimarisi, sürekli değişkene (CV: continuous variable) bağlı olan modeldir. Sürekli değişkene bağlı modelin kullanım nedeni kuantum mekaniğinin dalga fonskiyonu özelliklerinden yararlanır. Konum ($\vec{x}$) ve ($\vec{p}$) momentum gibi sürekliliğe dayalı değişkenler örnek olarak verilebilir.

Sürekli değişkene bağlı kuantum anahtar üretimi ile mevcut klasik sistemin yapısına uygun olarak kuantum bilgi işlem tabanlı sertifikadan değer üretimi Kuantum EBYS için yeni bir model önerebiliriz. Üretilen kuantum sürekli değişken değerler fiziksel objelerin modellemesine uygun olmaktadır. Bu modeller günümüzde kullanılan göz retinası, DNA yapısı, parmak izi gibi karmaşık değerlerin kuantum değerler için girdi olarak kullanılabilir.

Modelimizde kimlik doğrulama için kuantum parmak izi, göz retinası ve DNA eşleştirmesi önerilmektedir. Bu işlemi sertifika üretme yetkisi olan kurum ya da kuruluşlar yapabilir. Çünkü yeni elektronik cipli kimlikler için parmak izleri verileri mevcuttur. Yapılması ı gereken bu verilerin kuantum veri olarak ifade edilmesidir. Ayrıca bu modelde tek seferlik kuantum anahtar üretimi ve dağıtımı için güvenliği yüksek olan sürekli değişkenlere dayalı anahtar üretim ve dağıtımının kullanılması önerilmektedir.

V. SONUÇ

Kuantum devriminde üretilecek olan kuantum dijital imza ve kuantum elektronik imza teknolojileri güvenliği ispatlanmış teknolojileri kullanacaktır. Özellikle klasik dijital üretmek için kullanılan teknolojilerin yerine kuantum mekaniği içinde var olan süper pozisyon, kuantum dolanıklık, kuantum teleportasyon, süper yoğun kodlama gibi iletişim teknolojileri kullanılacaktır.

Kuantum elektronik imza sürecinde kuantum tabanlı dijital sertifikalar kullanılacaktır. Gelecekte kuantum dijital sertifika üreten kuruluşların hakem olarak seçilmesi, kuantum network alt yapısının gelecek için veri transferinde kuantum XML teknolojilerini paket olarak kabul etmesi öngörülmektedir.

Bu modelde Kuantum XML elektronik belgelerin üstverilerini tanımlamak için kullanılacaktır. Klasik elektronik imza teknolojilerinde kullanılan anahtar ikilileri yerine vektörel tabanlı yoğunluk matrislerini kullanan bileşenler yerini alacaktır. Sistemin girdileri parmak izi, göz retinası ve DNA gibi değerlerin oluşturduğu bir şema olacaktır.

$k \mapsto |f_k\rangle$ girdileri fiziksel nesnelerin kuantum data olarak tanımlamasıdır. f tek yönlü bir kuantum fonksiyonudur. Yani, sonucun hesaplanması kolaydır, ancak klasik şemanın aksine, kuantum fonksiyonun tersinin bulunması imkansızdır[1].

VI. TEŞEKKÜR

Bu çalışma Çanakkale Onsekiz Mart Üniversitesi BAP birimi tarafından FDK-2018-2462 nolu proje kapsamında desteklenmektedir.

Kaynakça

[1] "TÜRK DİL KURUMU". [Çevrimiçi]. Erişim adresi: http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c4950fb8de0b5.57947749. [Erişim: 24-Oca-2019].

[2] T. B. Kamusm, "Elektronik Belgeleri Açık Anahtar Altyapısı Kullanarak Güvenli İşleme Rehberi". TÜBİTAK BİLGEMBilişimve Bilgi Güvenliği İleri TeknolojilerAraştırma Merkez, 2016.

[3] M. Nadeem ve X. Wang, "Quantum digital signature scheme", s. 11.

[4] L. Chen *vd.*, "Report on Post-Quantum Cryptography", National Institute of Standards and Technology, NIST IR 8105, Nis. 2016.

[5] "Difference Between Digital Signature and Electronic Signature (with Comparison Chart) - Tech Differences". [Çevrimiçi]. Erişim adresi: https://techdifferences.com/difference-between-digital-signature-and-electronic-signature.html. [Erişim: 03-Şub-2019].

[6] Telekomünikasyon Kurulu, *ELEKTRONİK İMZA KANUNU*, c. 43. 2016, s. 8719.

[7] "eSignature | Digital Signature | electronic signature | Compliant Online Signature". [Çevrimiçi]. Erişim adresi: https://www.suitebox.com/esignatures. [Erişim: 02-Şub-2019].

[8] T. C. KALKINMA BAKANLIĞI, *Resmi Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik*, c. 29255. 2015, s. 83.

[9] KALKINMA BAKANLIĞI, ŞUBAT 2016, ve Kalkınma Bakanlığı, *e-Yazışma Projesi - T.C. Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı*, c. 26242. 2006, s. 73.

[10] P. Heus ve R. Gomez, "QIS-XML: A metadata specification for Quantum Information Science", s. 26.

[11] D. Gottesman ve I. Chuang, "Quantum Digital Signatures", May. 2001.

[12] S. Cobourne ve C. Cid, "Title: Quantum Key Distribution – Protocols and Applications", s. 95.

[13] N. Kaya, "KAFES TABANLI YENİ ANAHTAR DEĞİŞİM PROTOKOLLERİ VE VERİMLİ POLİNOM ÇARPIMI", Tez, ONDOKUZ MAYIS ÜNİVERSİTESİ FEN BİLİMLERİ ENSTİTÜSÜ, Samsun, 2018.

[14] A. A. Zhukov, E. O. Kiktenko, A. A. Elistratov, W. V. Pogosov, ve Y. E. Lozovik, "Quantum communication protocols as a benchmark for quantum computers", *Quantum Inf. Process.*, c. 18, sy 1, Oca. 2019.

[15] R. J. Collins *vd.*, "Experimental transmission of quantum digital signatures over 90 km of installed optical fiber using a differential phase shift quantum key distribution system", *Opt. Lett.*, c. 41, sy 21, s. 4883, Kas. 2016.

Makine Öğrenmesi Yöntemleri İle Oltalama Websitesi Saldırı Tespiti

Attack Detection of Web Phishing With Machine Learning Methods

Şevki Gani ŞANLİÖZ
MSÜ Hezarfen Havacılık ve Uzay Teknolojileri Enstitüsü
Bilgisayar Mühendisliği
İstanbul, Türkiye
ganisanlioz@hotmail.com

Mustafa KARA
MSÜ Hava Harp Okulu
Bilgisayar Mühendisliği
İstanbul, Türkiye
mkara@hho.edu.tr

Muhammed Ali AYDIN
İstanbul Üniversitesi
İstanbul, Türkiye
Bilgisayar Mühendisliği
aydinali@istanbul.edu.tr

Hasan Hüseyin BALIK
MSÜ Hava Harp Okulu
İstanbul, Türkiye
hasanbalik@gmail.com

***Abstract*—Phishing is defined as a fraudulent method by which fraudulent persons send personal information to the victim's e-mail box using known e-mail addresses of known web sites, banks, companies or internet service providers. Although there are many applications to detect phishing attacks today, there are difficulties in preventing attacks. In order to detect Phishing attacks at certain rates, some machine learning methods are discussed. The purpose of this work is to compare machine learning techniques used against web phishing attacks. These methods, including Classification and Regression Trees (CART), J48 (C4.5) Algorithm, Adaboost Algorithm, Random Forest (RF) and Neural Networks (NNet), were used to estimate web phishing attacks. The accuracy rate has been tested. In this study, a total of 1353 emails were used in a phishing attack website, 702 of which were malicious and 548 were legitimate websites and 103 suspicious websites in the data set. In addition, 10 properties were used to train and test the classes. 9 features have been addressed and 1 reference has been used to specify the classification.**

Keywords—Cyber Attack, Web Phishing, Machine Learning

***Özet*—Oltalama (Phishing), bilinen web sitelerinden, bankalardan, büyük çaplı firmalardan veya internet servis sağlayıcıları benzeri kuruluşlardan gönderilmiş gibi gelen mailler aracılığı ile kişisel bilgilerin elde edilmesini sağlayan dolandırıcılık yöntemi olarak tanımlanmaktadır. Günümüzde oltalama saldırısının tespiti için birçok uygulama mevcut olmasına rağmen hala önüne geçmekte zorluklar yaşanmaktadır. Bu çalışmanın amacı, web oltalama saldırılarına karşı kullanılan makine öğrenme tekniklerini karşılaştırmaktır. Web oltalama saldırı tespitinde Sınıflandırma ve Regresyon Ağaçları (CART), J48 (C4.5) Algoritması, Adaboost Algoritması, Rastgele Orman (RF) ve Sinir Ağları (NNet) olmak üzere 5 farklı mekine öğrenme yöntemi kullanılarak, bunların tahmin doğruluğu karşılaştırmalı test edilmiştir. Yapılan bu çalışmada toplamda 1353 mail üzerinden 702 oltalama yapmak isteyen web sitesi, 548 ise meşru web sitesi ve 103 şüpheli web sitesi veri kümesinde kullanılmıştır. Ayrıca, sınıfları eğitmek ve test etmek amacıyla kullanılan 10 öznitelik üzerinden değerlendirme yapılmıştır. 9 öznitelik ele alınmış ve 1 özniteklik sınıflandırmayı belirtmek için kullanılmıştır.**

Anahtar Kelimeler—Siber Saldırı, Web Oltalama, Makine Öğrenmesi

I. INTRODUCTION

Phishing is an online theft and fraud. It is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords [1]. With end-user training, web phishing attacks can be prevented to a certain extent. However, this is not highly secure. In this respect, web sites should be marked with machine learning methods. Thus, less work is provided to the end user in terms of security measures.

As a result of the significant increase of the internet in our lives, machine learning has started to be seen in every aspect of our lives. For example, recommendations through web banners use machine learning to personalize online ad delivery in almost real time. However, web sites can be damaging to a large extent by capturing our sensitive data through phishing [2,3].

The method used in phishing is often redirecting the user to fake web sites that are similar to original ones. Best way for redirecting them to these fake sites is convincing them with some offers that they cannot reject, like as if they won in a lottery or similar kind of games [4].

Some of the simple measures that can be taken against the web phishing attacks are;

- Not responding to unsolicited emails requesting your personal information
- Counterfeiting attacks take a variety of ways to keep users in doubt and gain their trust. Not to click on the address links in suspicious emails
- Not to provide personal information to suspicious or unfamiliar websites
- When you visit the websites of bank, credit card and service providers to enter your personal information, it goes through methods such as not typing the address of the site directly into the internet browser.

In recent years, through attacks on website phishing billions of dollars are harmed to individuals and corporations that conduct transactions such as online banking [5]. These attacks are increasing day by day. The measures listed above

can provide a certain level of safety. In this respect, with machine learning methods, we can prevent this attack by reducing the attack rate before it reaches the end user.

In addition, even if many network solutions are proposed and implemented for detection and prevention of phishing attacks, the effectiveness of these methods cannot be calculated. These solutions cannot be reinforced with more clear and computable methods that increase the error rate. The contribution of this study to literature is comparing the efficiency and accuracy of five different machine learning methods including J48, Classification and Regression Trees (CART), Adaboost Algorithm, Random Forest (RF), and Neural Network [6,7,8].

The rest of the article is organized as follows: Section 2 deals with the concept phishing with a web site. In the third chapter, the logic of machine learning methods and algorithms used in the study is mentioned. Chapter 4 describes the methods of machine learning for detecting website attacks by phishing. In the fifth chapter, the findings showing our experimental studies are expressed and the methods are presented. The result evaluation is presented in Chapter 6.

II. Web Phishing

One of the best cyber attacks used for obtaining the personal sensitive data of others is Phishing attack [9]. In this type of attack, an attacker attacks his victim through a fake website. These fake websites are almost identical to the original sites that actually exist. The victim is requested to click on the link in the e-mail to access the forms requested to enter or update personal information on these web sites. In this way, the victim's information is sent to the attacker [10].

People can use the internet for a variety of purposes, such as sending e-mails, conducting e-banking activities, selling products, or purchasing on-site [11]. Despite all these advantages of the Internet, there are some disadvantages. One of them is internet fraud, a type of crime executed on the internet. There are many ways that online users can be exposed to Internet fraud. Disclosure of these users 'sensitive information is also one of these attackers' intentions. Therefore, the Internet is a very good platform to trick people and capture private account information [12].

In recent years, only some of these researches against phishing attacks are focused on detection of phishing attacks on the website, which causes serious risks [13,14].

We've used both known and new features to classify fake websites. This study demonstrates the use of selected machine learning algorithms to test the features we specify. Table 1 describes preventive and corrective solutions that investigate phishing attacks.

TABLE I. Solutions for Phishing Attack

Solutions	Preventive Solutions	Corrective Solutions
Process Monitoring	Verification	Unpublishing The Website
Web Copy Disabling	Change Management	Forensic Investigation
Content Filtering	E-Mail Authentication	Internal Network Security Measures
Anti-Spam Feature	Web Application Security	External Network Security Measures

III. Machine Learning Methods And Algorithms

Machine learning is a type of artificial intelligence that makes software applications more accurate in predicting results without explicit programming. Algorithms that can receive input data and use statistical analysis to estimate an output value within an acceptable range are the mainstay of machine learning.

To fully understand the logic of machine learning algorithms and use it against cyber threats will reduce our error rate considerably. In this respect, the objectives and methods for using machine learning algorithms in attacks should be evaluated. These will be explained under three methods: accurate evaluation of data through classification, aggregation of data sets by clustering and establishing a relationship between data through proximity analysis [15].

A. *Accurate Evaluation of Data on Classification*

It is an evaluation obtained by making a classification which aims to estimate a result by creating separate classes in a data set. Using classification algorithms is beneficial for some methods such as spam email detection and health risk analysis. First, after scanning an email text and tagging recognized words and phrases, the classification algorithms are very effective way to determine whether the "signature" of the email is considered as spam. On the other hand, a network's instant statistics, security status, activity levels, and attack data can be run with an algorithm to determine a risk score for specific data [16].

B. *Aggregate Data Sets by Clustering*

One of the most effective algorithms of machine learning methods is clustering logic. The purpose of a cluster analysis algorithm is to consider entities in a single large pool and to form smaller groups that share similar characteristics [17]. For example, a television company that wants to determine the demographic distribution of watchers or watchers of different broadcasts can do so by building clusters based on available data about subscribers and broadcasts they watch. A restaurant chain can cluster its customers according to their menu choices based on geographic locations, and then change their menus accordingly. It can facilitate attacker analysis by aggregating requests to a website under cyber-attack [18]. Figure 1 shows the machine learning process.

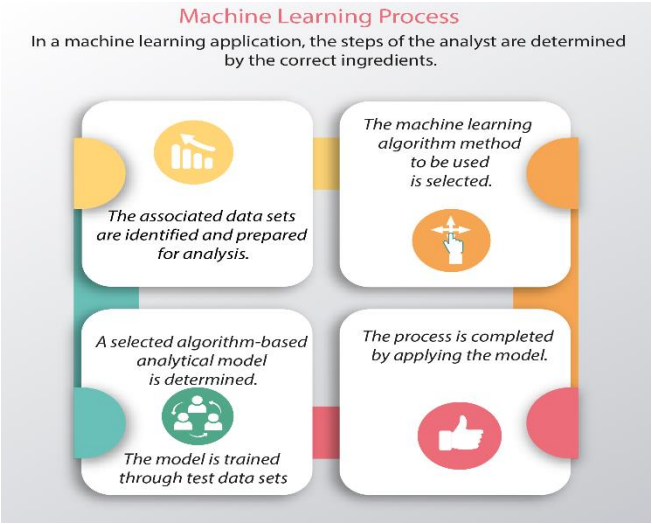


Fig. 1. Machine Learning Process

C. Establishing Relationship with Proximity Analysis

Proximity analysis is another approach to mining and analyzing data that can be made through machine learning. The purpose of this approach is exploring correlations between data features or transactional events. For example, it can often be used by retailers in market-basket analysis applications to identify products purchased at the same time. An online vendor can use the results to apply product placement on the website [19].

Cyber security efforts also often involve proximity analysis. Sequences of network operations prior to cyber attacks are analyzed to identify process patterns that occur close to each other. It can be used to formulate prescriptive analytic applications designed to evaluate similar attacks in similar attacks. In addition to these machine learning algorithms and approaches, there are many other algorithm methods that can be used to perform similar analysis results. Applying the right method in the right area will work best.

In this study, the accuracy of machine learning methods was tested by using Classification and Regression Trees (CART), J48 (C4.5) Algorithm, Adaboost Algorithm, Random Forest (RF) and Neural Networks (NNet) methods to predict phishing web sites. A total of 1353 e-mail and 542 legitimate websites and 103 suspicious websites were used in the data set.

IV. Machine Learning Methods for Detecting Phishing Attacks

The classification methods used in our study are mentioned. AdaBoost, Random Forest, J48, Artificial Neural Network Classification and Regression methods will be explained in general terms.

A. AdaBoost

Adaboost method is one of the techniques of learning with consecutive communities from the perspective of machine learning methods.The estimation speed is plays an important role for choosing this method. In addition, it can be applied in many data sets and uses memory space efficiently [20].

B. Random Forest

Random Forest (RF) is a classification algorithm that covers many concepts. It is mainly used for classification and regression methods. It brings together multiple trees while training. Multiple decision tree structure is used on the training side over real data sets. It is basically based on two features [20,21]. These features are the number of trees created and the number of predictors randomly selected when differentiating at each node.

C. J48 Classification Algorithm

J48 is a decision tree algorithm based on the very popular C4.5 algorithm. Decision trees are a classic way of representing information from a machine learning algorithm and offer a powerful and fast way of expressing data structures. This algorithm classifies the data as recursive. This ensures maximum accuracy of training data, but may create excessive rules that define only certain behavioral characteristics of the data [22].

D. Neural Networks

Neural Network (NN) includes the logic of self-learning in addition to previous machine learning methods. Memorize the problem and establish a relationship between the information that the problem has [23]. NN consists of 5 basic elements. These are;

- Inputs
- Outputs
- Addition Function
- Activation Function
- Weights

The xi symbol inputs are shown in Figure 2, which describes the structure of the NN. The input values are multiplied by the coefficient wi and the threshold value is obtained. The activation function is then applied. This is the basic logic in the structure of neural networks.

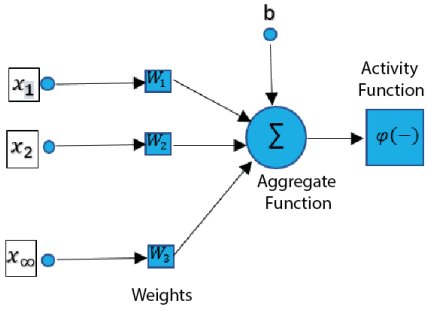


Fig. 2. Neural Network Process

E. Classification Via Regression (CART)

The most important feature of the CART algorithm, known as classification and regression tree, is its ability to create regression trees. Considering the values contained in the features, the training set is divided into two separate branches called candidate divisions. A node t has two branches of clusters, right ($t_{(right)}$) and left ($t_{(left)}$). Each data to be used in the creation of a regression tree is candidate to be divided into right and left branches. The twoing rule first calculates the probability for each candidate to be on the right and left branches. The probability for each candidate to divide the data into the left-hand branch is expressed as ($P_{(left}$) and P(j/ t_{left}), and the probability of right-hand branching ($P_{(\text{right})}$ and P(j / t_{right}). After calculating the probabilities, the measure of suitability of candidate divisions s at node t is shown in formula 1:

$$\cup(\sigma / \tau) = 2P_{left}\, P_{right}\, \alpha\nu\delta\, \Pi(\varphi / t_{(right)} \sum_{j=1}^{n} |P(j/t_{left}) - P(\tfrac{j}{t_{right}})| \quad (1)$$

V. Methods And Findings

In this study, various tested has been done on a computer with Intel (R) Core (TM) i7-3610QM 2.30 Ghz processor, 6 GB RAM with Windows 8.1 operating system. Different methods were applied in WEKA environment with the necessary data set and different parameters. With the tests performed, a model was created on the data set of the algorithms. Comparative analyzes have been carried out in various aspects with the methods described in the previous sections.

A. Method

The methods for classifying phishing attacks on the website with the data set obtained will be specified. In

addition, the evaluation techniques used in the comparison will be explained. In these comparisons, performance criterion, F-Criterion and ROC area were analyzed.

B. Data Set

The data set was used for detection of phishing website. The data set was evaluated over 10 features, including one for classification. Our data set consists of a total of 1353 records. 548 of these are classified as legitimate URLs, 702 of them are phishing URLs and 103 of them are classified as suspicious URLs. This data set was taken from UCI repository [24]. In addition, each feature is distinguished in that it contains at least one of the features that indicate that it is legitimate (1), suspicious (0) and Phishing (-1).

The need to observe how the algorithms to be applied acts on a data set, including all features in the specified data set, was effective in selecting all of these features. The features of the data set are given in Table 2.

TABLE II. WEB PHISHING DATASET FEATURES

No	Features
1	Having_IP_Address
2	URL_Length
3	PopUpWidnow
4	Age_of_Domain
5	Web_Traffic
6	SFH
7	SSLfinal_State
8	Request_URL
9	URL_of_Anchor
10	Result

Having_IP_Address: If the URL contains an IP address, this may be the indication of web phishing. This tag is -1 (Phishing) if the IP address exits in the domain, 1 (Legitimate) in other cases [25].

URL_Length: Generally, attackers hide the insecure part of the URL to capture data sent by a user. They can also redirect the web page to a suspicious domain. Normally, there is no measure for URL length, but recent studies have found that an acceptable limit can be used for URL length [26].

PopUpWidnow: When a pop-up prompts the user to add some certain data, this is generally the indicator of a fraudulent activity. Consisting of pop up window with text field may indicate the Phishing (-1) web page. [26].

Age_of_Domain: The duration of the web page may be an indicator. For example, if a web page has been in use for less than a month, this may indicate that it is a fake web page [26].

Web_traffic: When a website has high density traffic, then this webpage is really safe, and users can feel safe while browsing the site. Phishing websites normally have low navigation traffic and can be measured by rank in Alexa database. For example, a web page can be considered as Legitimate (1) if Alexa ranking is below 100.000 or Phishing (-1) if Alexa ranking is above 100.000 or Suspicious (0) if there is no Alexa record about that web page in Alexa ranking list [26].

SFH: Indicates that the empty string feature is hosted in the Server Form Handler. SFH is displayed or -1 (Phishing) if the string value is as 'about: blank' or empty, 0 (Suspicious) if referring to a different field, and 1 (Legitimate) in other cases [26].

SSLfinal_State: Indicates the existence of the HTTPS protocol. Using the HTTPS is Legitimate (1) if it is used, the provider is trusted, and the certificate age is one year or higher, Suspicious (0) if https is used and the provider is untrusted, otherwise Phishing (-1) [26].

Request_URL: Represents the state that the web page will attract different objects from different field names. The percentage of object request URLs pulled from external websites is shown as Legitimate (1) if the percentage is less than 22%, Suspicious (0) if the percentage is between 22% and 61%, Phishing (-1) in other cases [26].

URL_of_Anchor: The existence of the HTML anchor tag (<a> tag) usage in the URL. The percentage of URL presence in anchor tags is 1 (Legitimate) if the percentage is below 31%, 0 (Suspicious) if the percentage is between 31% and 67%, and -1 (Phishing) in other cases [26].

Result: The last parameter in our table, Result, is the class field that indicates whether it is marked as phishing or not. If the web page is fraud, the result is -1 (Phishing); if it is marked as good, the result is 1 (Legitimate); and if it is not clear whether the web page is Phishing or not, then the result is 0 (suspicious).

In order to process the data set and test the classification algorithms, Weka application and machine learning programs were used.

1) Performance Criteria: The presented classification algorithms were tested using k cross-validation. With the results obtained, True Positive Rate (TP Rate), False Positive Rate (FP Rate), F-Criteria, ROC Area and Accuracy Rate (Accuracy)) parameters were compared [27].

a) TP Rate: Based on the information obtained from the complexity matrix, the algorithm is a method used to calculate the correct estimation rate for the selected class [31]. Equation (8) is calculated using the formula 2.

$$TP\ Rate = TP/(TP + FP) \quad (2)$$

b) FN Rate: Similar to the TP Ratio, the complexity is obtained from the matrix. It is used to calculate the wrong estimate rate of the selected class. The following formula is seen on the calculation process [31].

$$FN\ Rate = FN/(TP+FN) \quad (3)$$

c) F-Measure: It is calculated as the harmonic mean of Precision and Recall. Calculation of the accuracy (A), precision (P) and F-criterion (Fm) values is shown by formulas 4,5 and 6 [28].

$$A = TP/(TP + FN) \quad (4)$$

$$P = TP/(TP + FN) \quad (5)$$

$$Fm = 2 * (\frac{A*P}{A+P}) \quad (6)$$

d) ROC: It is one of the criteria used to measure the accuracy of algorithms calculated on the curve graph obtained from TP ratio and FP ratio. ROC Field value is

between 0 and 1 and convergence with 1 indicates the increase in the success of the test.

C. Experimental Results

In this section, comparative analysis is performed on the results obtained with the experimental environment. After the analysis, the success and failure rates of classification algorithms used for detection of phishing attacks are shown graphically. Comparison of classification algorithms according to evaluation criteria is shown in Table 3.

In addition, the comparison of the success measures of classification algorithms according to the classifications of "Phishing", "Legitimates" and "Suspicious" is presented in the graphs in Figure 3, Figure 4 and Figure 5.

TABLE III. COMPARISON OF CLASSIFICATION ALGORITHMS ACCORDING TO PARAMETER VALUES

ALGORITHMS	Class	TP Rate	FP Rate	F-Measure	ROC	Accuracy
Classification and Regression Trees	0	0,689	0,017	0,728	0,708	0,772
	1	0,914	0,099	0,888	0,808	0,862
	-1	0.907	0,066	0,922	0,841	0,937
AdaBoost	0	0.000	0,000	-	0,545	-
	1	0.849	0,150	0,820	0,929	0,794
	-1	0.913	0,194	0,873	0,930	0,836
Neural Network	0	0.845	0,019	0,813	0,973	0,784
	1	0.872	0,078	0,878	0,957	0,884
	-1	0.906	0,100	0,907	0,959	0,907
Random Forest	0	0,854	0,014	0,842	0,991	0,830
	1	0,892	0,075	0,892	0,968	0,891
	-1	0,912	0,089	0,914	0,966	0,917
J48	0	0,932	0,015	0,881	0,986	0,835
	1	0,892	0,065	0,898	0,958	0,904
	-1	0,916	0,083	0,919	0,958	0,923

When the results of test attack packets are analyzed in Figure 3; it is seen that the best TP Ratio is obtained by J48 algorithm with 0.916 and the worst accuracy rate is obtained by Neural Network algorithm with 0.906.

In addition, when the detection of attack packets in terms of error rate (FP Ratio); Classification and Regression Trees algorithm is the best with the lowest error rate of 0.066, whereas AdaBoost is found to be a very inefficient algorithm with the highest error rate of 0.194.

Regarding the F-Measure, where the precision and sensitivity criteria are calculated; Classification and Regression Trees algorithm is the most successful algorithm with 0.922, while AdaBoost is the worst algorithm with 0.873.

Regarding ROC value;, Random Forest algorithm gives the best results with 0.966, while Classification and Regression Trees algorithm gives the worst results with 0.841.

When the accuracy rates are compared, in addition to the criterias mentioned above; the Classification and Regression Trees algorithm is the best with the highest accuracy rate of 0.937 and AdaBoost algorithm is the worst with the lowest accuracy rate of 0.836.

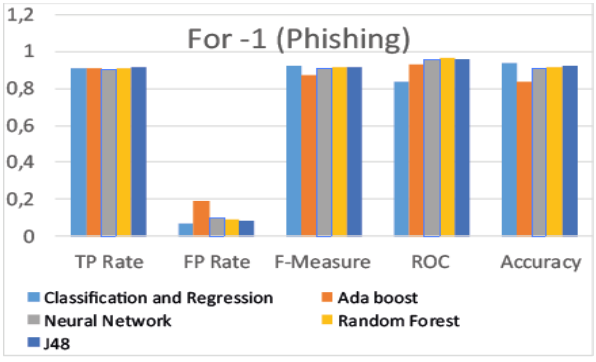


Fig. 3. Success measurement of classification algorithms according to "Phishing" (Class Value: -1) website detection

When the results of legitimate packets are examined in the experiment performed in Figure 4; Classification and Regression Trees algorithm is the best with the highest accuracy (TP Ratio) ratio of 0.914 and the AdaBoost is the worst algorithm with the lowest accuracy ratio of 0.849.

In addition, when the legitimate packet detection error rate (FP Ratio) is examined; J48 algorithm is the most successful with the lowest error rate of 0,065, while AdaBoost is the most unsuccessful algorithm with the highest error rate of 0,150.

In terms of F-Criterion value; J48 algorithm is the most successful algorithm with 0.898, while AdaBoost is the most unsuccessful with the lowest success rate of 0.820.

About ROC value; Random Forest algorithm gives the best result with 0.968, while Classification and Regression Trees algorithm gives the worst result with 0.808.

In addition, when the accuracy rates are compared, the J48 algorithm has the highest accuracy rate of 0.904, while the AdaBoost algorithm has the lowest accuracy rate of 0.794.

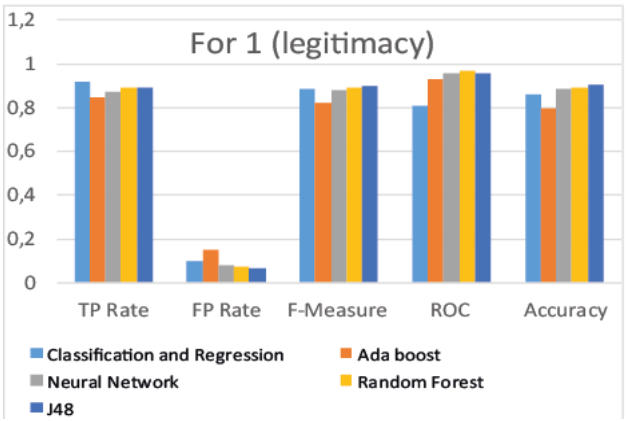


Fig.4. Success measurement of classification algorithms according to "legitimate" (Class Value: 1) website detection

As it is seen in Figure 5, when the results of the legitimate packets are examined in the experiment; J48 algorithm is the best with the highest accuracy (TP Ratio) with 0.932 and Classification and Regression Trees is the worst algorithm with the lowest accuracy rate of 0.689.

In addition, when the legitimate packet detection error rate (FP Ratio) is examined; AdaBoost algorithm is observed to be the most successful with the lowest error rate of 0, while Neural Network is observed as the most unsuccessful algorithm with the highest error rate of 0,019.

In terms of F-Criterion value; J48 algorithm is the most successful algorithm with 0.881, while Classification and Regression Trees is the most unsuccessful algorithm has the lowest success rate with 0.728.

About ROC value; Random Forest algorithm gives the best result with the rate of 0.991, while Classification and Regression Trees algorithm gives the worst result with 0.708.

In addition, when the accuracy rates are compared, J48 algorithm has the highest accuracy rate of 0.835, while the Classification and Regression Trees algorithm has the lowest accuracy rate of 0.772.

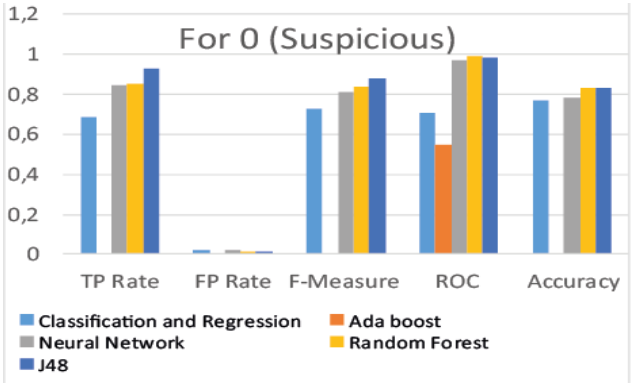


Fig.5. Success measurement of classification algorithms according to "Suspect" (Class Value: 0) website detection.

Table 4 shows the duration of model creation with the data sets used in the classification algorithms. These values are very important in terms of bandwidth, energy and resource usage. With this data set, the duration of creating the model reaches the highest value in Neural Network algorithm with 20.84 seconds, while the lowest value is obtained by J48 algorithm with 0.07 seconds.

TABLE 4. THE DURATION OF MODEL CREATION WITH THE DATA SETS USED IN THE CLASSIFICATION ALGORITHMS

Algorithm	Model Creation Time
Classification And Regression	1.38
Ada boost	0.12
Neural Network	20.84
Random Forest	0.65
J48	0.07

VI. RESULT

In recent years, billions of dollars are lost by individuals and corporations that conduct transactions such as online banking through websites on the web phishing attacks. These attacks are increasing day by day. To be able to get effective results against cyber-attacks with certain methods, the most effective techniques should be determined by performing experimental analyzes.

In this study, we searched for the predictive accuracy of five classifiers in a phishing dataset. Some methods are discussed to give an idea of existing machine learning techniques, comparison and most deterministic method between them. In this paper experimented with various Machine Learning algorithms and found Classification and Regression Trees algorithm as the best. And J48 is the lowest value.

In our research a dataset that has 10 features and a total of 1353 raw websites, 548 of which were legitimate, 702 of which were harmful and 103 of which were suspicious, was used to be able to estimate the probability of detecting phishing attacks with J48, Classification and Regression Trees (CART), AdaBoost, Random Forests (RF) and Neural Networks (NNet) Classification methods.

In this study, different methods on web phishing detection have been tested and achieved successful results in various aspects. These results were compared, and the best solutions have been revealed.

REFERENCES

[1] Patil, S., & Dhage, S. (2019, March). A Methodical Overview on Phishing Detection along with an Organized Way to Construct an Anti-Phishing Framework. In 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS) (pp. 588-593). IEEE.

[2] Dua, S., & Du, X. (2016). Data mining and machine learning in cybersecurity. CRC press.

[3] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.

[4] Hink, R. C. B., Beaver, J. M., Buckner, M. A., Morris, T., Adhikari, U., & Pan, S. (2014, August). Machine learning for power system disturbance and cyber-attack discrimination. In Resilient Control Systems (ISRCS), 2014 7th International Symposium on (pp. 1-8). IEEE.

[5] Xiang, G., Hong, J., Rose, C. P., & Cranor, L. (2011). Cantina+: A feature-rich machine learning framework for detecting phishing web sites. ACM Transactions on Information and System Security (TISSEC), 14(2), 21.

[6] Miyamoto, D., Hazeyama, H., & Kadobayashi, Y. (2008, November). An evaluation of machine learning-based methods for detection of phishing sites. In International Conference on Neural Information Processing (pp. 539-546). Springer, Berlin, Heidelberg.

[7] Fette, I., Sadeh, N., & Tomasic, A. (2006). Learning to detect phishing emails (No. CMU-ISRI-06-112). Carnegie-Mellon Univ Pittsburgh Pa Dept Of Computer Science.

[8] Sanglerdsinlapachai, N., & Rungsawang, A. (2010, January). Using domain top-page similarity feature in machine learning-based web phishing detection. In Knowledge Discovery and Data Mining, 2010. WKDD'10. Third International Conference on(pp. 187-190). IEEE.

[9] Chandrasekaran, M., Narayanan, K., & Upadhyaya, S. (2006, June). Phishing email detection based on structural properties. In NYS Cyber Security Conference (Vol. 3).

[10] Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. Big Data & Society, 3(1), 2053951715622512.

[11] Peiravian and Zhu, X. (2013, November). Machine learning for android malware detection using permission and api calls. In Tools with Artificial Intelligence (ICTAI), 2013 IEEE 25th International Conference on (pp. 300-305). IEEE.

[12] Wang, A. H. (2010, June). Detecting spam bots in online social networking sites: a machine learning approach. In IFIP Annual Conference on Data and Applications Security and Privacy (pp. 335-342). Springer, Berlin, Heidelberg.

[13] Ma, L., Ofoghi, B., Watters, P., & Brown, S. (2009, July). Detecting phishing emails using hybrid features. In Ubiquitous, Autonomic and Trusted Computing, 2009. UIC-ATC'09. Symposia and Workshops on (pp. 493-497). IEEE.

[14] Fette, I., Sadeh, N., & Tomasic, A. (2007, May). Learning to detect phishing emails.

[15] Sebastiani, F. (2002). Machine learning in automated text categorization. ACM computing surveys (CSUR), 34(1), 1-47.

[16] Tong, S., & Koller, D. (2001). Support vector machine active learning with applications to text classification. Journal of machine learning research, 2(Nov), 45-66.

[17] Fisher, D. H. (1987). Knowledge acquisition via incremental conceptual clustering. Machine learning, 2(2), 139-172.

[18] McGregor, A., Hall, M., Lorier, P., & Brunskill, J. (2004, April). Flow clustering using machine learning techniques. In International Workshop on Passive and Active Network Measurement (pp. 205-214). Springer, Berlin, Heidelberg.

[19] Kotsiantis, S. B., Zaharakis, I., & Pintelas, P. (2007). Supervised machine learning: A review of classification techniques. Emerging artificial intelligence applications in computer engineering, 160, 3-24.

[20] Aytuğ, O. N. A. N., & Korukoğlu, S. (2016). Makine öğrenmesi yöntemlerinin görüş madenciliğinde kullanılması üzerine bir literatür araştırması. Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi, 22(2), 111-122.Basnet, R., Mukkamala, S., & Sung, A. H. (2008). Detection of phishing attacks: A machine learning approach. In Soft Computing Applications in Industry (pp. 373-383). Springer, Berlin, Heidelberg.

[21] Pal, M. (2005). Random forest classifier for remote sensing classification. International Journal of Remote Sensing, 26(1), 217-222.

[22] Patil, T. R., & Sherekar, S. S. (2013). Performance analysis of Naive Bayes and J48 classification algorithm for data classification. International Journal of Computer Science and Applications, 6(2), 256-261.

[23] Rowley, H. A., Baluja, S., & Kanade, T. (1998). Neural network-based face detection. IEEE Transactions on pattern analysis and machine intelligence, 20(1), 23-38.

[24] UCI Machine Learning Repository. "Phishing Websites Dataset".https://archive.ics.uci.edu/ml/datasets/Phishing+Websites (26.03.2016).

[25] Web:https://archive.ics.uci.edu/ml/machine-learning-databases/00327/Phishing%20Websites%20Features.docx, Accessed 02 09 2019.

[26] Davis J, Goadrich M. "The relationship between Precision-Recall and ROC curves". 23rd international Conference on Machine Learning, Pennsylvania, USA, 25-29 June 2006.

[27] Powers, D.M.. "Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation". Journal of Machine Learning Technologies, 2(1), 37-63. 201.

Kafes Tabanlı Kuantum Sonrası Algoritmaların Profil Analizi ve GPU Uygulamaları

Profiling and GPU Implementation of Lattice-Based Post-Quantum Algorithms

Aleaddin ÖZER ve Adnan OZSOY
Hacettepe Üniversitesi, Bilgisayar Müh.
06800, Beytepe Ankara

Oğuz YAYLA
Hacettepe Üniversitesi Matematik
06800, Beytepe Ankara

***Özet*— Kuantum sonrası kriptoloji son zamanların en revaçta araştırma konuları arasında yer almaktadır. Özellikle, kuantum bilgisayar üretildiğinde bu bilgisayarların dahi kıramayacağı kriptosistem tasarımları bilim insanları ve firmalar tarafından yoğun bir şekilde araştırılmaktadır. Hatta 2016 yılında NIST'in çağrısıyla kuantum sonrası için anahtar değişimi ve imzalama algoritmaları farklı araştırma grupları tarafından NIST'e değerlendirilmek üzere gönderilmiştir. Bu algoritmalar, 30/11/2018 yılından itibaren diğer araştırmacıların analizine ve değerlendirmesine açıktır. 30/01/2019 tarihinde ise ikinci aşamaya geçenler duyurulmuştur. Bu çalışmada, ikinci aşamaya geçebilen kafes tabanlı kripto sistemlerin performans analizi yapılmıştır. Bu performans analizi için öncelikle CPU profil analizi yapılmıştır, diğer bir ifade ile algoritmaların CPU üzerinde kullandıkları yöntemler kullanım sürelerine ve çağrı sayısına göre sıralanmıştır. Bu profil analizinin tabloları ve grafik gösterimleri çıkarılmıştır. Böylece bu algoritmalarda en fazla zaman harcayan yöntemler belirlenmiştir. Bu çalışmanın ikinci bölümünde ise en fazla zaman harcayan yöntemler için GPU hızlandırmaları önerilmiştir. Özellikle Fourier dönüşümü, modüler çarpma, polinom çarpma ve matris çarpma gibi yöntemlerin GPU hızlandırılmasının önemli olduğu görülmüştür. Bu yöntemlerden matris çarpması için GPU uygulaması bu çalışmada verilmiştir.**

Anahtar Kelimeler— kuantum sonrası kriptoloji, kafes tabanlı kriptografi, profil analizi, GPU

***Abstract*— Post-Quantum Cryptology is a trending topic nowadays. In particular, design of a cryptosystem resistant to quantum computers is heavily researched by scientists and companies. In fact, many post-quantum key exchange and signature algorithms are submitted to the NIST call in 2016 . Analysis and evaluation period of these algorithms are open to researchers since 30/11/2018. Second round submissions are announced on 30/01/2019. In this study, performance of lattice-based cryptosystems submitted to second round is analyzed. First of all, we perform CPU profiling of these algorithms, in other words, the methods used by the algorithms are listed according to time consumption and number of calls. Then we tabulate and plot graphically these results so that the most time consuming methods are marked. In the second part of this study, alternative GPU implementations of some of the most time consuming methods are given. In particular, the methods including Fourier transformation, modular multiplication, polynomial multiplication and matrix multiplication are required to be implemented in GPU. In this study, we give only the implementation of matrix multiplication in GPU.**

Anahtar Kelimeler— kuantum sonrası kriptoloji, kafes tabanlı kriptografi, profil analizi, GPU

I. GİRİŞ

Kuantum sonrası kriptografi algoritmalarının GPU üzerine hızlandırılması bu sistemlerin etkili ve verimli çalıştırılması için önemlidir. Bu çalışmada NIST çağrısı [1] kapsamında sunulan kaynak kodlu algoritmalardan kafes tabanlı algoritmalar üzerinde kodun performans açısından değerlendirmesi yapılmıştır. Bu değerlendirmeler ışığında çok zaman tutan işlemlerin GPU gibi paralel işlem yapılmasına olanak tanıyan bir ortam üzerine yapılacak geliştirme çalışmalarına yön verilebilecektir.

II. bölümde latis tabanlı algoritmalardan NIST ikinci aşamasına geçen anahtar değişim algoritmalarından NewHope, Kyber ve Frodo'nun CPU üzerinde profile çalışmaları verilecektir. III. bölümde ise imzalama algoritmalarından qTESLA ve Dilithium için yapılan CPU profil çalışmaları sunulmuştur. Yapılan profil çalışmaları aşağıda paylaşılmıştır. V. bölümde GPU ortamlarında çalışılan algoritmaların en yavaş çalışan metodlarının paralel hesaplamaya uygunluğu tartışılmıştır. Ek bölümünde ise grafikler ve bu grafiklerin elde edilme yöntemleri belirtilmiştir.

II. AÇIK-ANAHTAR ŞİFRELEME VE ANAHTAR-KURMA ALGORİTMALARI

Bu kısımda açık-anahtar şifreleme ve anahtar kurmaya dayalı algoritmaların profil çıkarma işlemleri sunulacaktır. Bu kapsamda NIST ikinci aşamaya geçmiş NewHope, Crystal-Kyber ve Frodo algoritmaları incelenmiştir.

Öncelikli olarak bakılan algoritmalardan NewHope [2], Hatalarıyla Halka Öğrenme (Ring-Learning-with-Errors, Ring-LWE) problemini temel alan bir anahtar değişim protokolüdür. NIST çağrısında sırasıyla 1. seviyeyi ve 5. seviyeyi hedefleyen IND-CPA güvenli anahtar kapama mekanizmaları olan NewHope512-CPA-KEM ve NewHope1024-CPA-KEM ile AES-128 ve AES-256'nın kaba kuvvet güvenliğini eşleştirmek veya aşmayı hedeflemektedir. *Tablo 1. NewHope512-CCA-KEM üzerinde yapılan profil çıkarma işlemleri sonucu CPU üzerinde çalışma zamanları*

Each sample counts as 0.01 seconds.

% time	cumulative seconds	self seconds	calls	self us/call	total us/call	name
50.02	0.02	0.02	700	28.58	35.25	invntt
25.01	0.03	0.01	1344000	0.01	0.01	barrett_reduce
25.01	0.04	0.01	9200	1.09	1.09	KeccakF1600_StatePermute
0.00	0.04	0.00	2905600	0.00	0.00	montgomery_reduce
0.00	0.04	0.00	2854400	0.00	0.00	fqmul
0.00	0.04	0.00	281600	0.00	0.00	csubq
0.00	0.04	0.00	230400	0.00	0.00	basemul

Tablo 2. Kyber512-CCA-KEM üzerinde yapılan profil çıkarma işlemleri sonucu CPU üzerinde çalışma zamanları

Each sample counts as 0.01 seconds.

% time	cumulative seconds	self seconds	calls	self us/call	total us/call	name
50.02	0.04	0.04	819200	0.05	0.05	hw
12.51	0.05	0.01	3148800	0.00	0.00	montgomery_reduce
12.51	0.06	0.01	900	11.12	18.44	ntt
12.51	0.07	0.01	300	33.35	33.35	poly_uniform
12.51	0.08	0.01	100	100.05	100.05	verify
0.00	0.08	0.00	358400	0.00	0.00	coeff_freeze
0.00	0.08	0.00	223800	0.00	0.00	load64
0.00	0.08	0.00	176200	0.00	0.00	store64

Tablo 3. Frodo-640-CCA-KEM üzerinde yapılan profil çıkarma işlemleri sonucu CPU üzerinde çalışma zamanları

Each sample counts as 0.01 seconds.

% time	cumulative seconds	self seconds	calls	self ms/call	total ms/call	name
88.75	0.63	0.63	200	3.15	3.15	frodo_mul_add_sa_plus_e
4.23	0.66	0.03	60300	0.00	0.00	KeccakF1600_StatePermute
2.82	0.68	0.02	100	0.20	0.20	frodo_mul_add_as_plus_e
1.41	0.69	0.01	400	0.03	0.03	frodo_unpack
1.41	0.70	0.01	300	0.03	0.03	frodo_pack
1.41	0.71	0.01				crypto_kem_enc
0.00	0.71	0.00	2000	0.00	0.00	clear_bytes

Benzer şekilde NewHope512 - CCA - KEM ve NewHope1024 - CCA - KEM ile NIST teklif çağrısında sırasıyla 1. seviye ve 5. seviyeyi hedefleyen IND-CCA güvenli anahtar kapama mekanizmaları sunulmaktadır.

Profili çıkarılan Crystal-Kyber [3] Algoritması, güvenli anahtar kapsülleme mekanizması(KEM) ve güvenli dijital imza algoritması(Dilithium) olmak üzere iki algoritma içermektedir. Her iki algoritma da kafes tabanlı problemlere yönelik oluşturulmuş ve büyük kuantum bilgisayar saldırılarına dayanacak şekilde tasarlanmıştır.

Frodo [4] algoritması ise, güvenliği iyi çalışılmış hatalarıyla öğrenme algoritmalarından türetilen, pratik kuantum sonrası yapılar olacak şekilde tasarlanmış, anahtar kapsülleme mekanizmalarının bir ailesidir.

Tablo 1'de NewHope512-CCA-KEM üzerinde yapılan profil çıkarma işlemleri sonucu CPU üzerinde çalışma zamanlarını görmekteyiz. Bu sonuçlara bakıldığında %50 çalışma süresinin inverse-number-theoretic-transform (InvNtt) işlemi için harcandığını, geri kalan süresinin de yarı kısmı indirgeme (reduction) işlemi için harcanmaktadır. Benzer şekilde Kyber-512-KEM için yapılan profil sonuçları Tablo-2'de verilmiştir. Kyber için Montgomery indirgemesi ve NTT en çok zaman alan işlemlerdir. Frodo için yapılan profil çalışmasında ise SA+E matris çarpma-toplama işlemi en fazla zaman harcayan işlemdir, bkz. Tablo 3.

NewHope, Kyber ve Frodo algoritmaları içerisindeki işlemlerin harcadıkları zamanlara göre ağaç diyagramları Şekil A1-A2-A3'te sunulmuştur.

Tablo 4. qTESLA-CCA üzerinde yapılan profil çıkarma işlemleri sonucu CPU üzerinde çalışma zamanları

Each sample counts as 0.01 seconds.

% time	cumulative seconds	self seconds	calls	self us/call	total us/call	name
78.27	0.18	0.18				randombytes_init
8.70	0.20	0.02				crypto_sign_keypair
4.35	0.21	0.01	30661	0.33	0.33	KeccakF1600_StatePermute
4.35	0.22	0.01	1157	8.64	8.64	sparse_mul16
4.35	0.23	0.01	324	30.87	34.79	kmxGauss

Tablo 5. Dilitihium512-CCA üzerinde yapılan profil çıkarma işlemleri sonucu CPU üzerinde çalışma zamanları

Each sample counts as 0.01 seconds.

% time	cumulative seconds	self seconds	calls	self us/call	total us/call	name
73.09	0.19	0.19				frame_dummy
7.69	0.21	0.02	526462	0.04	0.04	br_aes_ct64_bitslice_Sbox
7.69	0.23	0.02	34646	0.58	1.11	aes_ctr4x
3.85	0.24	0.01	9492736	0.00	0.00	montgomery_reduce
3.85	0.25	0.01	2929	3.41	4.49	ntt
3.85	0.26	0.01	500	20.00	20.00	shake256
0.00	0.26	0.00	570624	0.00	0.00	csubq

III. SAYISAL İMZALAMA ALGORİTMALARI

Bu kısımda sayısal imzaya dayalı üç algoritmanın profil çıkarma işlemleri sunulacaktır. Bu kapsamda NIST ikinci aşamayı geçmiş qTesla ve Crystal Dilithium algoritmaları incelenmiştir. qTesla [5] algoritması, karar-hatalarıyla halka öğrenme (decision Ring-Learning-with-Errors) probleminin zorluğuna dayanan güvenli kuantum kriptografi sonrası imza oluşturma algoritmalarının bir ailesidir. Dilithium [6] ise kafes problemlerinin modül kafesler üzerindeki zorluğuna bağlı olarak çalışan bir dijital imza şemasıdır. qTesla ve Dilithium için profil analizleri Tablo 4 ve 5 olarak aşağıda sunulmuştur. qTesla'da çarpma işlemi oldukça zaman harcarken, Dilithium için Montgomery indirgemesi ve NTT işlemleri en fazla zaman almaktadır. Bu algoritmaların işlem diyagramları ise Şekil A4 ve A5'te sunulmuştur.

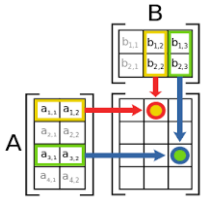
IV. GPGPU PARALEL YAKLAŞIM

Performans elde etme adına paralel programlama araçları ve farklı donanımlar tercih edilmektedir. Donanımlardan son yıllarda özellikle çok kullanılmaya başlayan grafik kartlarının (GPU) genel amaçlar için kullanımı (GPGPU) ile çok yüksek performanslara erişilebilmektedir [7]. Grafik kartlarının hemen hemen her sistemde olması, modern CPU'ya göre binler seviyesinde fazla işlemci ünitesi içermesi ve bu sayede binlerce iş parçacığını aynı anda işleyebilme kapasitesi GPU'ların öne çıkan yönleridir. GPGPU amacı için en öne çıkan NVIDIA şirketinin çıkardığı CUDA framework ile grafik kartları grafik işlemleri dışında genel amaç için programlanabilmekte ve yüksek performans elde edilebilmektedir.

CUDA mimarisinin yüksek performans alma adına bazı gereksinimleri mevcuttur. CUDA üzerinde çalışacak programda birbirinden bağımsız işlemlerin olması, işlenecek verinin belli bir büyüklükte olması, ve veri üzerinde yapılacak işlemin aynı olması sayılabilir. Bu şartları sağlayan uygulamalara özellikle Fourier dönüşümü, modüler çarpma, polinom çarpma ve matris çarpma işlemleri birebir uymaktadır. Bu nedenle bu bölümde, önceki bölümlerde incelediğimiz algoritmaların zaman açısından uzun işlemlerinden CUDA uyumlu grafik kartı üzerinde paralel olarak çalıştırarak yüksek oranda performans elde edebileceğimiz işlemlerini inceleyeceğiz.

İlk olarak çok yüksek oranda parallel çalıştırmaya uygun matris işlemleri ile başlayacağız. Verilen algoritmalarda özellikle matris çarpma ardından toplama işlemlerinin (matris-multiply-

add) kısmı için parallel bir çözüm sunulabilir. Bu işlemleri iki kısımda incelersek matris çarpımında kullanılan iki matrisin, A ve B olsun, ilk A matrisindeki her bir sıranın B matrisindeki her bir sütun üzerindeki her bir sayının çarpımlarının toplanarak sonuç C matrisinin ilgili sıra-sütun kısmına yazılmasını içerir. Şekil 1'de de görülebileceği gibi sonuç matrisinin her bir elemanının hesaplaması farklı bir iş parçacığı tarafından yapılabilir.



Şekil 1 Matris çarpımının paralelleştirilmesi. Her bir sonuç matrisi elemanın hesaplaması farklı bir iş parçacığı tarafından yapılabilir.

Bu şekilde tasarlanan matris çarpımının CUDA üzerinde çalıştırılması sonucu elde edilen hızlanmaları deneyimleme adına Intel Xeon Silver 4114 2.20 GHz işlemcili 128 GB Ram kapasiteli ve grafik kartı olarak Geforce GTX 1080 Ti kartı bulunan bir sunucu üzerinde testler gerçekleştirdik. GTX 1080 Ti 1.5 GHz de çalışan 3584 adet işlemci içermektedir.
Gerçekleştirilen kodlama sonucunu gösterir sonuçlar Tablo 6'da verilmiştir.

Tablo 6 Matris Multiply-Add CPU ve GPU testleri

	512	1024	2048
CPU	499,78ms	7053,26ms	118230,50ms
GPU	0,76ms	2,96ms	16,74ms
Speedup	653x	2381x	7060x

Tablo 6'da görüldüğü üzere artan matris boylarına bağlı yüksek oranda performans artırımı elde etmek mümkündür.

V. SONUÇ

Bu çalışmada NIST çağrısında ikinci aşamaya kalmış latis tabanlı kuantum sonrası NewHope, Kyber, Frodo, qTesla ve Dilithium algoritmalarının profil analizleri yapılmıştır. Bu profil çalışmaları ilgili algoritmalarının yavaşladığı noktaları (yöntemleri) yüzdesel olarak ortaya çıkarmıştır. Bu yöntemlerin paralel hesaplamaya olanak tanıyan GPU gibi ortamlarda çalıştırılması ile bu algoritmalarda hızlanma oranları için gözlem yapılmıştır. Matris çarpması, indirgeme, NTT gibi işlemlerin algoritmaları yavaşlatan işlemlerde olduğu görülmüştür. Özel olarak matris çarpması için GPU üzerinde denemeler yapılmıştır ve hızlanma oranları verilmiştir.

TEŞEKKÜR

Bu çalışma ve yazarları TÜBİTAK 117E636 nolu proje tarafından desteklenmektedir.

KAYNAKLAR

[1] NIST round 2 adayları resmi web sayfası https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions, Erişim tarihi: 01.08.2019

[2] Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). Post-quantum key exchange - a new hope. In 25th USENIX Security Symposium (USENIX Security 16) (pp. 327-343).

[3] Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., ... & Stehlé, D. (2018, April). CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. In 2018 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 353-367). IEEE.

[4] Joppe Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, Douglas Stebila. Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE. 23rd ACM Conference on Computer and Communications Security 2016

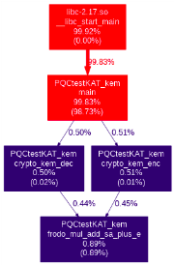
[5] Bindel, N., Akleylek, S., Alkim, E., Barreto, P. S. L. M., Buchmann, J., Eaton, E., ... & Ricardini, J. E. (2018). Submission to NIST's post-quantum project: lattice-based digital signature scheme qTESLA.

[6] Ducas, L., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). Crystals–dilithium: Digital signatures from module lattices.

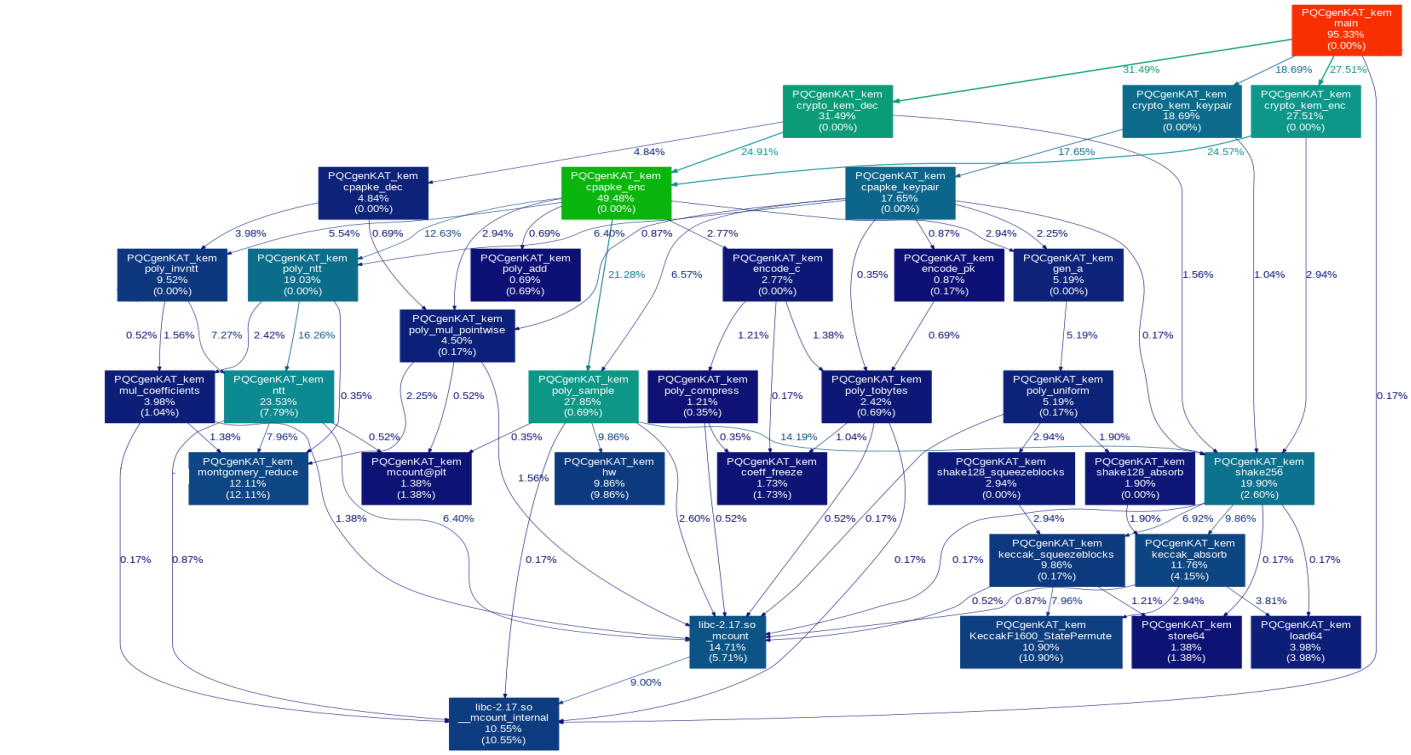
[7] NVIDIA CUDA Paralel Programlama https://docs.nvidia.com/cuda/cuda-c-programming-guide/index.html, Erişim tarihi: 06.06.2019

EK

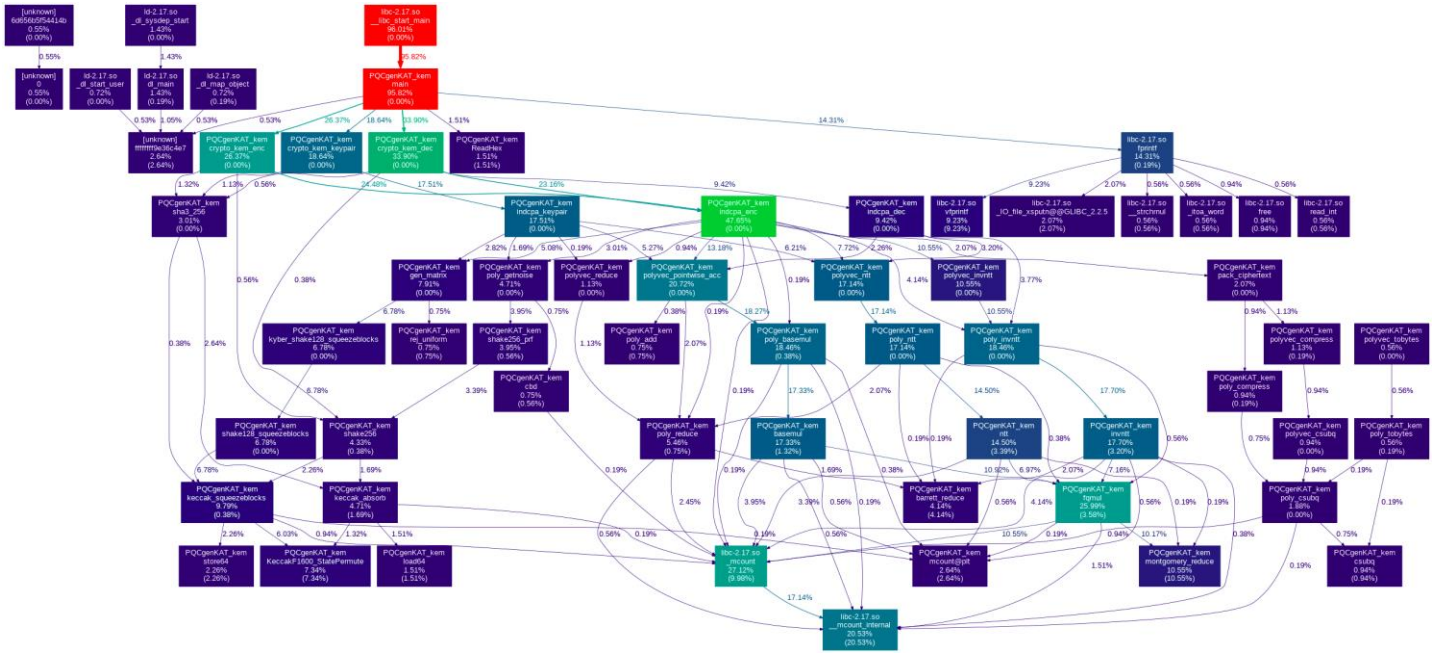
Bu araştırmada belirlenen algoritmaların analizinin yapılması, bellek kullanımlarının ölçülmesi, ağaç yapılarının çıkarılması için belirli araçlar kullanılmıştır. Bunlar temel olarak bellek kullanımı ve derinlemesine bilgi elde etmek için **pref** aracı, CPU üzerindeki incelemeler için **gprof** ve **nvprof** araçları, GPU üzerindeki incelemeler içinde yine **nvprof** ve **nsight** monitor ve grafik oluşturmak ve ilişkilendirmek için **gprof** ve **gprof2dot** araçları kullanılmıştır. Bu araçlara **github** paylaşım ortamından ulaşılabilir.



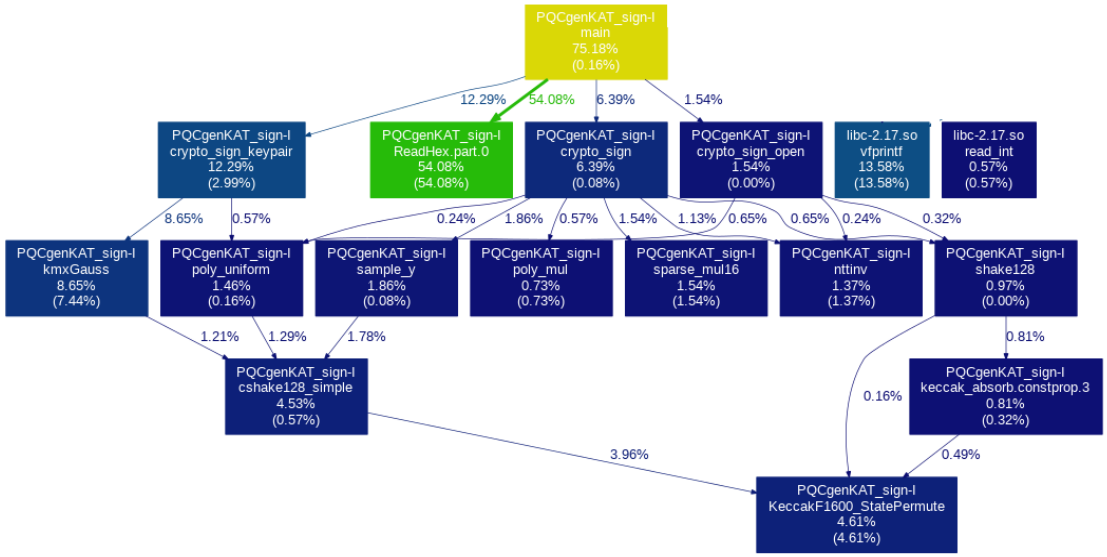
Şekil A1. Frodo-512-CCA üzerinde yapılan profil çıkarma işlemleri sonucu CPU üzerinde çalışma zamanları



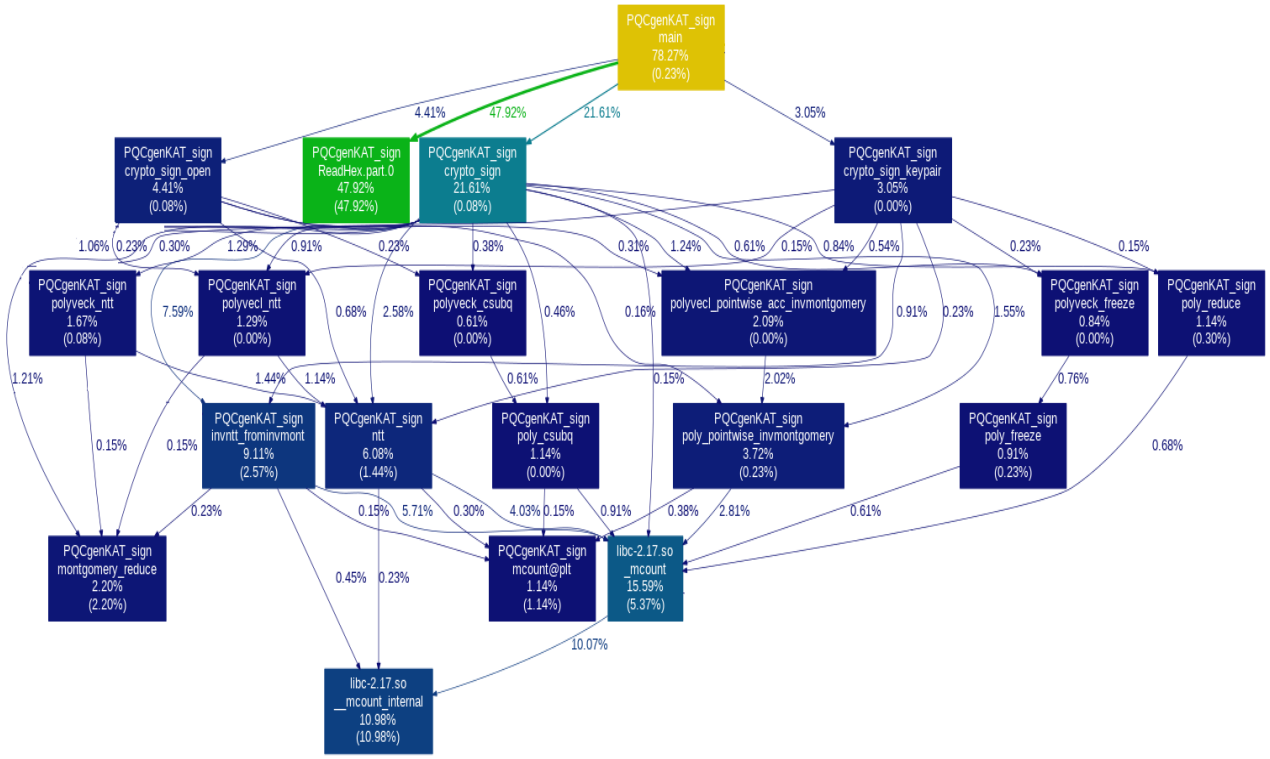
Şekil A2. NewHope512-CCA-KEM üzerinde yapılan profil çıkarma işlemleri sonucu CPU üzerinde çalışma zamanları



Şekil A3. Kyber512-CCA-KEM üzerinde yapılan profil çıkarma işlemleri sonucu CPU üzerinde çalışma zamanları



Şekil A4. Dilithium-512-CCA üzerinde yapılan profil çıkarma işlemleri sonucu CPU üzerinde çalışma zamanları



Şekil A5. qTESLA-512-CCA üzerinde yapılan profil çıkarma işlemleri sonucu CPU üzerinde çalışma zamanları

BasGit: A Secure Digital ePassport Alternative

BasGit: Alternatif Güvenli Elektronik Pasaport Sistemi

Ceren Kocaoğullar, Kaan Yıldırım, Mert Atila Sakaoğulları, Alptekin Küpçü
College of Engineering, Koç University, İstanbul, Turkey 34450
{ckocaogullar15,kyildirim14,msakaogullari14,akupcu}@ku.edu.tr

***Abstract*—This paper discusses a new passport program that allows the passports to be printed on paper or carried in a smartphone application by the passport holders, without any interference or use of specialized equipment. The security and privacy implications, usability, and practicality of the proposed BasGit Passport Program are compared and contrasted with the already existing ePassport system that is widely used in the world. The paper then concludes with the overview of a proof-of-concept implementation and test results of it.**

***Index Terms*—e-Passport, border security, customs security, electronic visa.**

***Öz*—Bu makalede pasaportların evde kağıda yazdırılabilmesini veya mobil bir uygulamada tutulabilmesini sağlayan, kullanımı kolay ve maliyeti düşük alternatif bir güvenli elektronik pasaport sistemi öne sürüyoruz. Önerdiğimiz BasGit Pasaport Sistemi'nin güvenlik, gizlilik, kullanılabilirlik analizlerini yapıyor ve günümüzde yaygın olarak kullanılan ePasaport sistemi ile kıyaslıyoruz. Prototip kodlamamızın tartışması ve güvenlik testleri sonuçlarıyla makalemizi sonlandırıyoruz.**

***Anahtar Sözcükler*—e-Pasaport, sınır güvenliği, gümrük güvenliği, elektronik vize.**

I. Introduction

Passports are official travel documents that governments issue for their citizens to use for international travels. Passports contain information such as, but not limited to, the holder's name, photograph, date of birth, and signature. Started as a paper-based document, passports were rather recently enhanced with contactless Integrated Circuit (IC) chips and named electronic passport (or ePassport) for this reason. As of May 2017, 120 countries were using ePassports [1]. The standards for e-passports are set and managed by the International Civil Aviation Organization (ICAO) which is a specialized agency of the United Nations [2]. Prevention of counterfeiting and fraud is crucial for safeguarding national and international security. Several studies discussing the security and privacy issues of the ePassports exist [3]–[6].

The current ePassport system is constructed on the physical presence of a passport. Most counties register travel visas on the physical passport. The visa approval and issuing processes, which may take up to several weeks, withholds the holder from traveling abroad, as the original passport is kept by the visa issuing agency/country.

The security, privacy, and usability related issues indicate the necessity for a more reliable and convenient system for validating identity and crossing borders. Considering the ease of use and high-security requirements based on computers and mobile devices, this paper proposes a new passport system.

II. Literature Review

A recent research on mobilizing travel credentials by Bissessar et. al solely focuses on visas and electronic travel authorizations, and does not include mobilizing ePassports [7].

The most comprehensive effort on mobilizing ePassports has been done by the World Economic Forum. This initiative is a self-sovereign identity system that has no central authority. A distributed ledger technology with blockchain, pointers and hubs are used [8].

Also, an application named Mobile Passport is being offered as a free and paid service to United States passport owners and Canadian passport owners entering United States [9]. This mobile application aims to accelerate the customs operations and does not qualify as an ePassport. The travelers are required to present their ePassports as well as the mobile application upon inspection, whereas BasGit is a replacement to the current ePassport system.

III. Preliminaries

Digital signatures are algorithms that are used for validating integrity and authenticity of data [10]. They are based on asymmetric (public key) cryptography. The core idea of digital signature concept is, the signing party *A* distributes a public key for verification and keeps the matching private key secret. *A* digitally signs data using the private key, and this signature can be validated using the public key. This way, only *A* is able to sign data, and everyone who has access to the public key can assure that the data source is *A* and the data is unmodified.

In the paper, $info$ denotes the passport information, ssk denotes secret signing key and pvk denotes public verification key.

The passport signature function is:

$$\sigma = Sign_{ssk}(UUID, info) \tag{1}$$

The passport verification function is:

$$0/1 = Verify_{pvk}(UUID, info, \sigma) \tag{2}$$

If the verification function yields true and the obtained $UUID$ matches the passport holder's UUID, the passport is authentic. However, passport holder's legitimacy is a different concern. The current passport system requires either a visual validation by the control officer, or biometric verification. This topic will be further discussed in the following sections.

The managerial component of BasGit, the Administrative Web Interface (AWI) requires HTTPS connection for encryption, integrity checking, and server authentication. Whenever an internet connection to the AWI is mentioned, it is presumed that all parties have access to the genuine SSL (Secure Sockets Layer) certificate of the AWI, and can exchange and validate it through a legitimate PKI (Public Key Infrastructure).

IV. Objectives

Prevention of tampering and forgery in a passport system is crucial for national and international security. Weaknesses mainly arise from the validation mechanisms based on the contactless IC chip. The contactless IC chip and current access control mechanisms are prone to security and privacy compromises such as unauthorized communication with the chip, eavesdropping, skimming, and brute-force attacks [3]–[6].

One of the main objectives of the proposed BasGit system in this paper is to prohibit tampering and forgery by using the physical passport to only link individuals to the passport information stored in a secure central system. The proposed system does not claim safety against theft nor copying, however, an attacker retrieving an original or copied document does not cause any security risk. For each verification, the passport data is obtained from the central system and any biometric data mismatch can be quickly detected by the authorized staff. This also provides security against forgery, since the data carried by a physical passport is meaningful only if it has correspondence on the central system. For the same reason, the proposed system also does not require the same level of physical protection on the documents. Therefore, losing access to a physical passport should not constitute a major problem for the proposed system.

The proposed system aims to restrict the access to sensitive personal data only to authorized personnel. The existing ePassports contain identity information as plain text on the physical passport and includes biometric data in the embedded chip. This constitutes a threat to exploitation of sensitive personal data, including identity theft [5], [6]. Moreover, the current passports require the first page of the passport to be closed for security. Because the key for the initial authorization step for the IC chip, Basic Access Control, is calculated by reading information from the first page of the passport [6]. BasGit system aims to eliminate this privacy risk by not displaying or storing identity information on the passport and only giving access to this information to authorized readers. BasGit also aims to keep log of crucial information such as the identity of reader and time of access of each instance of passport reading. The ePassport system does not ensure recording this information in cases that the passport is inspected offline.

One major usability issue of ePassports is their financial cost, which can be as high as $333 or 125% of annual per capita national income [11]. Moreover, acquiring a passport usually has a high time cost because of the required bureaucratic processes. All these factors complicate the availability of ePassports for travelers. The proposed program in this paper aims to increase the availability of passports for the citizens.

In addition, in case of a stolen or lost ePassport, cancelling and reissuing may take up to several weeks. As a usability improvement, BasGit aims to reduce the duration of these actions down to seconds.

V. Specifications of The Proposed System

The main administrative element of the structure is a web-based system named Administrative Web Interface (AWI) (Fig.1c). It poses as the passport issuing, verifying, and maintaining authority.

The proposed system offers two different types of passport implementations: a printable, and a mobile application-based passport (Fig. 1a). Obtaining the former requires a printer and internet connection to access the AWI, while the latter requires a smartphone and also an internet connection to access the mentioned web interface.

The system proposes to employ a mobile application to be used by the control points (Fig. 1b).

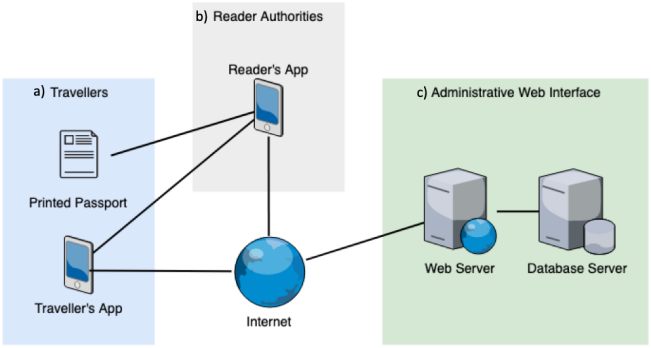


Figure 1. Architecture diagram showing the proposed system.

A. Administrative Web Interface (AWI)

Governing bodies of the participant nations must adopt the AWI in order to manage and supervise the proposed system. AWI is either a central or a distributed system that is capable of fulfilling the requirements of the program. In case of a distributed system, the participating nations have to determine the protocols for data exchange. The current ePassport system is a distributed system and utilizes ICAO Public Key Directory (PKD) to handle data exchange between states [12].

AWI has the features specified below:

- Contain the biographic information of the holder of a passport, including the full name of the holder, the birthplace and date, sex, nationality, and national ID number.
- Contain a digital biometric photograph of the holder that is compliant with the ICAO Machine-Readable Travel Documents Photo Guidelines [2].
- Contain information about the generated passport including at least the generation date, date of expiry, type of the passport, and the serial number.
- Keep log of each access to a passport by an authorized reader securely [13]–[21]. Log entries should include at least the access time and identity of the accessing personnel.
- Generate and contain a private/public key pair for digitally signing passport information, and share the public key with the readers.
- Authorize reader devices to prevent unintended devices from being used to read passports or act maliciously in the system.
- Support administrative operations such as passport revocation and travel restriction.
- Operate role based clearances that allow multiple types of authorities to use the system in parallel.

Separating all actions into roles as in Table I allows many government bodies to work together on the same system without causing security risks.

Table I
ROLES AND THEIR RIGHTS IN THE BASGIT AWI.

Security Authority	Reader Authority	Statistics Authority
Revoke Passport	Active Readers	Active Passports
Restrict Travel	Revoke Reader	Revoked Passports
Arrest Warrant	Reader Users	Expired Passports

1) Passport Issuing: The proposed system does not determine the means of registering citizens into the AWI. This can be handled similar to the web-based governmental systems in use [22]. However, the system requires each passport data stored in the central database to be digitally signed by the passport issuing authority. The issuing body can then decide whether a candidate is eligible for a passport using any information it has; this process is neither specified in this proposal nor by ICAO. Once the passport data is registered in the system, issuing a passport consists of the following steps:

1) A universally unique identifier is generated (UUID) for each passport. As the name suggests, UUID promises spatially and temporally unique identifiers of 128 bit length. UUID version 4 is generated randomly or pseudo-randomly, which is sufficient for backwards-compatibility and preventing predictability [23].
2) The system securely maps each UUID to the corresponding passport $info$.

B. Passport Acquiring

1) Paper Passports: The process of acquiring a paper passport consists of the following steps:

- **Step 1:** User logs into the web-based system and requests a paper-based passport.[1]
- **Step 2:** System finds the associated UUID, generates a QR code containing that user's UUID, and prepares a PDF file which only displays that QR code.
- **Step 3:** User downloads and prints the PDF file with the QR code of their UUID. This is now the passport of the user.

2) Mobile Passports: Acquiring a mobile passport consists of the following steps:

- **Step 1:** User logs into the system through the application[1] and requests a passport (Fig. 4a). When using the online login method, login credentials are stored in the secure containers provided by the operating system for sensitive data and cryptographic keys.
- **Step 2:** System finds the associated UUID and sends it to the application (Fig. 4d).
- **Step 3:** Application stores the UUID in the aforementioned operating system provided secure containers. The QR code containing the UUID is generated and displayed by application. This is now the passport of the user.

Once the passport is acquired, the user does not have to have an internet connection. This is because BasGit stores the login credentials and UUID securely to allow the user to login to the mobile application and present their passport even while offline. Therefore, in both paper and mobile passport versions, BasGit only requires the traveller to be online during passport acquiring, but not during their travels.

[1]A secure login can be achieved through two-factor authentication [24], [25]. A more convenient secure solution can be implementing a single password authentication protocol [26]–[29]

C. Passport Verification

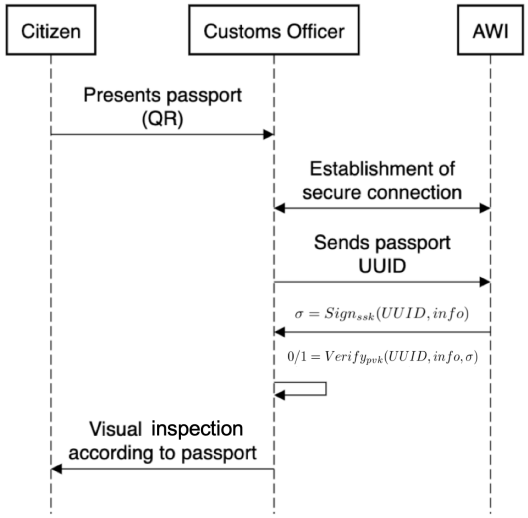


Figure 2. Sequence diagram showing the procedure of reading and verifying a passport.

In the BasGit system, the passports are verified using a smartphone application designed for the control officer. This mobile application must have internet connection to reach the central system to perform verification. Passport verification consists of these steps:

- **Step 1:** Officer logs into the system through the application[1] (Fig. 4e).
- **Step 2:** Reader application reads the QR and sends the UUID stored in the QR to AWI using a secure and authenticated connection.
- **Step 3:** AWI finds the associated passport information and sends it to the reader application along with the digital signature. Also, it logs the access time and reader's identity using a tamper-evident logging system [13]–[21].
- **Step 4:** Reader application verifies the digital signature and displays the passport information corresponding to the passport UUID (Fig. 4f).
- **Step 5:** Reader performs visual inspection to ensure that the passport holder is genuine.

As all the information related to the passport is retrieved when the passport is read by a reading authority. Step 4 can be altered to allow other ways of verification. For instance, it can be supported with biometric verification.

Mobile passports allow additional security measures for passport verification. A possible security measure against using the passport without holder's knowledge is adding support for two-factor authentication. The only drawback of this feature might be mobile network or internet connection constraints abroad. Providing secure wireless internet connection at the control points can be a solution to this.

D. Travel Visas

The visas granted to the ePassports are not stored within the contactless IC chip [30] as these chips cannot be written by multiple countries for security reasons. This separates the visa system from the passport system requiring multiple stages of verification, both for the passport and the visa [3].

The BasGit Passport Program enables a centralized online visa granting scheme using the aforementioned infrastructure.

Applying for a visa can be handled using online systems, which is already used in practice [31], [32]. BasGit does not propose any specific way of securely exchanging passport information between countries during the visa application process. Once the visa application is approved, the granting process occurs as follows:

- **Step 1:** A UUID is generated for each visa. The visa UUIDs are digitally signed by the visa granting country authority, using Equation 1 where $info$ is the visa information. This prevents attackers from scanning databases of different countries with one QR.
- **Step 2:** The system securely maps each UUID to the corresponding visa data and stores the UUID - visa information pair is stored in visa granting country's secure database.
- **Step 3:** The visa is digitally signed using Equation 1 and transmitted using any secure transmission method to the passport issuing country's system. It is securely mapped to the passport UUID of the individual.

Passport and visa UUIDs appear as separate QRs on the passport. Visa verification consists of only two steps:

- **Step 1:** Verifying the digital signature of the visa using Equation 2. As for the passport verification, an infrastructure similar to ICAO PKD can be used for data exchange for exchange of public key.
- **Step 2:** Verifying that the holder's passport has the visa UUID mapped to it.

Visa information obtained in the verification process can be used for confirming the visa type.

VI. Security Analysis and Comparison

A. An Overview of ePassport Security and Privacy Issues

The ePassport verification occurs when the customs officer reads the data stored in the contactless IC chip of a presented passport, after a series of steps for secure communication and authorized access [3]. The first step and the only mandatory step is Passive Authentication, which is basically using a PKI for checking if the chip is digitally signed by the issuing country [2]. Passive Authentication provides no protection against eavesdropping and skimming attacks [3].

The second step is the optional Basic Access Control (BAC). In essence, BAC aims to make sure that the first page of the e-passport that contains data is open as the reader tries to access the information in the IC chip. BAC system derives encryption and message authentication keys using the information stored in the Machine Readable Zone (MRZ) in order to establish secure communication for session key exchange. MRZ contains a maximum of 88 characters of information including name, surname, and date of birth of the owner, date of expiry, etc. [3], [33], [34]. Data stored in this area is usually easily guessable especially if the attacker knows the targeted passport holder. As a result, MRZ's entropy is not high enough to be immune to brute-force attacks [3], [33].

ICAO requires the IC chips used for ePassports to follow ISO 14443 standard [35]. Anticollision protocol of this standard requires the IC chips to emit a UID (Unique Identifier). This UID is fixed in some implementations and can be read by any reader device that complies with ISO 14443 protocol without any authorization. If the UID is fixed and unique to each chip, this protocol is prone to exposing the passport holder to be fraudulently tracked [5], [6], [33].

It is important to note that there are other optional security measures that ICAO proposes. One of these is Active Authentication, which intends to verify the authenticity of the contactless IC chip. Also, ICAO acknowledges that additional biometrics needs further protection and has proposed another optional security measure called Extended Access Control for this purpose. Even though Active Authentication aims to strengthen the security and privacy of the IC chips, it should be noted that if Active Authentication is used with RSA or Rabin-Williams signatures, the reader can acquire a value distinct to each chip. This way, the passport holder can be tracked without their knowledge [5].

B. Security Assessment of the BasGit Passport Program

The new passport design proposes to move all the personal information out of the passport itself and store it in central authorities. If a QR code for any passport is copied, at the inspection points this will be detected by the reader authorities who are performing visual inspection, biometric verification, or two-factor authentication in mobile passports. Also, the odds of an attacker generating a valid UUID at the time of inspection is negligible due to the random nature of the identifiers and their exponentially-large domain. In addition, the online verification obligation eliminates the risk of human error that may occur in border controls employing offline verification. Additionally, BasGit eliminates tracking attacks, since even though QR codes contain static UUIDs, they cannot be scanned unless they are visible to the reader.

The mobile application enables further security measures such as two-factor authentication and requiring login for preventing unauthorized access to the passport information. These measures are not necessities but opportunities.

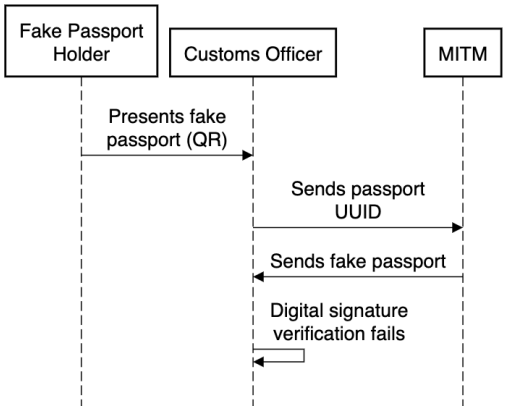


Figure 3. Sequence diagram showing an attack scenario where the attacker intercepts the connection between the reader and the central authority.

1) Man-in-the-middle Attacks: As the BasGit system is completely online, there is a considerable amount of network traffic between the readers and the central authorities. This traffic may be targeted by attackers (Fig. 3). Even though TLS connection makes it impractical, for this attack, we assume that the attacker can make the readers believe that they are connecting to the legitimate central authority. The attacker can achieve this by owning a fake certificate and performing DNS hijacking. If a malicious party intercepts the network traffic and replies to a reader with a fake passport, the reader will try to verify the digital signature of the sent passport.

Unless the malicious party can fake the digital signature of the central system, the verification will still fail. If the malicious party can indeed sign the fake passport, this means that the signing key of the central system is exposed, which is out of our scope.

2) Denial of Service (DoS) Attacks: The online systems of BasGit may be attacked with a denial of service attack to prevent the control points to reach the servers to authenticate the passport users, which will temporarily block travelers from crossing borders. A distributed system may be employed to prevent these types of attacks, which will increase the costs of implementing the program. However, this is necessary for the proper functioning as the availability of the system is crucial for international travel.

Observe that if the attacker can change the reader and put a different pvk and certificate into the reader application, then the attacker can have fake passports accepted or real passports denied. Unfortunately, such an attack cannot be prevented completely. But, we propose that a special passport QR entry can be hold at each border point, such that the officers can scan it before each shift starts to ensure that they are employing the correct certificate and signature verification key. For better security, this entry can be dynamically generated by the AWI.

3) Insider Attacks: The only foreseeable way to counterfeit a passport in the proposed system is an insider attack. People with high access levels may also alter the citizen records to create counterfeit passports with fake information to allow individuals to cross borders. However, insider attacks are nearly impossible to prevent as the access rights are given to ensure proper operation of the program. Logging activity done by the authorized personnel is the only way to prevent further damage by an insider attack as it is possible to find the attacker using the logs [13]–[21].

C. General Comparison of the Systems

ePassport and BasGit systems have advantages and disadvantages in terms of usability, security and privacy. BasGit is cheaper, easier to reissue and contains less information on the passport compared to ePassports. On the other hand, unlike BasGit ePassports allow some degree of offline verification and make producing fake passports difficult (Table II).

In addition to the broadly discussed security aspects of the two systems, a serious security risk for both is an attacker having reach to both ends of the validation structure. For BasGit, the attacker can validate a fake passport if they manage to change both pvk and ssk. Similarly, if the attacker can manipulate ICAO PKD as well as the private keys, they can achieve verifying counterfeit passports.

BasGit does not contain any personal information on the passport (the QR code), while ePassports expose private information such as the name, surname, date, and place of birth, details of travel history and in some cases profession and emergency contact information of the holder.

VII. Implementation

To demonstrate the usability and security of the proposed system, we have implemented a proof of concept system. The implementation consists of three main components. First component is the new passport design that is paper-based and does not require the complicated production procedures the ePassports use. Second component is the AWI which issues the passports, manages the readers, and allows citizens to acquire passports online. The third and the last component is a relay between the citizens and the central authority, the mobile application, which allows the users to access their passports from their smart phones.

Table II

Comparison of BasGit vs. ePassport			
BasGit		ePassport	
Pros	Cons	Pros	Cons
Much cheaper for the citizens to use.	Only allows online verification.	Allows for some degree of offline verification.	Production cost of a passport is much higher.
Passport is easy to obtain once issued.	Easy to create a fake passport (but it will not verify).	Hard to create a fake passport.	Issuing requires long bureaucratic process.
No identifying information on the passport (privacy-preserving).			Identifying information visible on the passport (prone to identity theft).

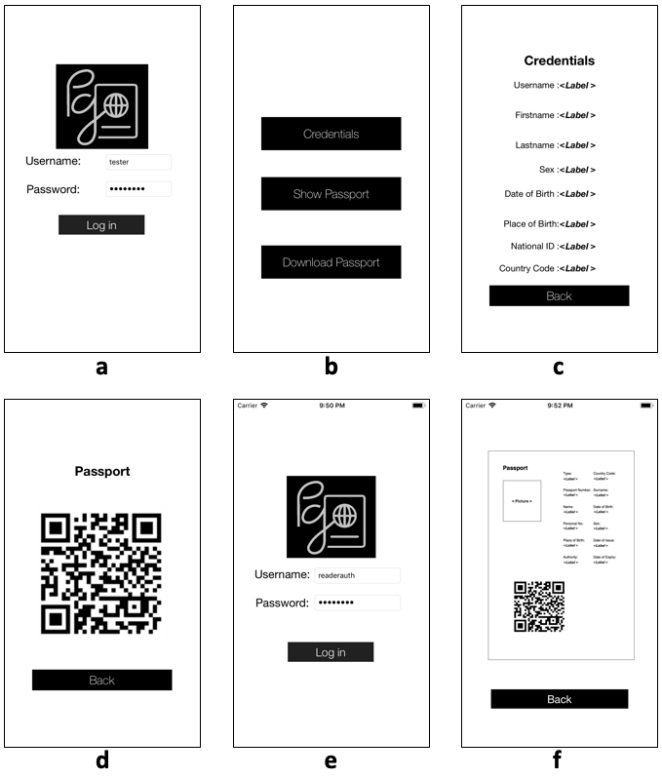


Figure 4. Figures a to d show screens for the traveller application. Figures e and f show screens for the reader application.

The proof-of concept system has been tested against vulnerabilities using open source tools [36], [37]. The main point of interest for the testing was the central authority as the other components of the system does not allow the attackers to alter user data permanently. Our implementation passed successfully from the tests against: Cross site scripting (XSS), Cross Site Request Forgery (CSRF), HTTP Strict Transport Security (HSTS), cookie vulnerabilities, SQL injections, Cross Origin Resource Sharing (CORS), session vulnerabilities, code injection and bypassing same origin policy.

VIII. Conclusions

The ePassports have some usability, security, and privacy problems. Many existing infrastructures, such as bank and government services requiring high levels of security, have been transformed into all-online systems to increase usability, security, and privacy. Therefore, it is realistic to anticipate that such an online passport system can be implemented as well.

Unlike the conventional ePassport systems, which require high levels of specialization in printing and material technology to print the physical travel documents, the proposed program offers passports to become printed at home or stored in smartphones. The proposed program lowers the cost and time for issuing, acquiring, canceling, and extending a passport. The BasGit program uses the physical passports to only link individuals with their information stored on a central system. This does not require the same level of physical protection on the documents as forging the document itself does not constitute a security risk as long as it will not be verified by the central system or the reader. Moreover, this system eliminates visa application processes withholding the holder from traveling.

Despite the requirement for a highly specialized central system, the governments already use such systems to verify national identities and check criminal records at checkpoints. It is possible to say that such systems can easily exist as similar ones do already [22]. The high, one-time cost of the central system will be compensated by the low operating cost. The eradicated cost of securing, developing, and printing passports will have a substantial financial effect.

To conclude, BasGit Passport Program may be developed with further research and field testing to become a more reliable and easier way of validating identity and crossing borders in the future. BasGit system currently does not offer a solution to the existing threat of insider attacks. An attacker can bribe or threaten passport issuing authority staff or an insider attacker can issue false passports [3]. What can be done to prevent this kind of attacks should be a part of future discussions. We plan to incorporate further cryptographic solutions as we learned via [38]. Also, considering the fact that passports are not only used as travel documents but also as identification documents, types of authorities with low-level access permissions can be employed, thanks to the role-based central system. The focused effort of ensuring security in only the digital medium compared to the currently divided attempts of trying to secure both the digital and the physical mediums will allow swifter and more stable progress in the field of international travel.

References

[1] Gemalto NV, "The electronic passport in 2018 and beyond," https://www.gemalto.com/govt/travel/electronic-passport-trends, [May. 26, 2019].

[2] ICAO, "Doc 9303, machine readable travel documents, part 3: Specifications common to all mrtds," 2015.

[3] G. S. Kc and P. A. Karger, "Ibm research report: Preventing security and privacy attacks on machine readable travel documents (mrtds)," 2005.

[4] V. Auletta, C. Blundo, A. De Caro, E. De Cristofaro, G. Persiano, and I. Visconti, "Increasing privacy threats in the cyberspace: The case of italian e-passports," in *FC*, R. Sion, R. Curtmola, S. Dietrich, A. Kiayias, J. M. Miret, K. Sako, and F. Sebé, Eds. Springer Berlin Heidelberg, 2010, pp. 94–104.

[5] A. Juels, D. Molnar, and D. Wagner, "Security and privacy issues in e-passports," in *SECURECOMM*, 2005, pp. 74–88.

[6] E. Kosta, M. Meints, M. Hansen, and M. Gasson, "An analysis of security and privacy issues relating to rfid enabled epassports," in *IFIPSEC*. Springer, 2007, pp. 467–472.

[7] W. E. F. S. I. on Shaping the Future of Mobility, "The known traveller: Unlocking the potential of digital identity for secure and seamless travel," 2018.

[8] F. A. C. A. David Bissessar, Maryam Hezaveh, "Mobile travel credentials," in *FPS*, 2018, pp. 46–58.

[9] A. M. Inc., "Mobile passport," https://mobilepassport.us/, [Sept. 3, 2019].

[10] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 281–308, 1988.

[11] D. McKenzie, "Paper walls are easier to tear down: passport costs and legal barriers to emigration." *World Development*, vol. 35, pp. 2026–2039, 2007.

[12] ICAO, "Security and facilitation: Public key directory," https://www.icao.int/Security/FAL/PKD/Pages, [May. 26, 2019].

[13] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," *ACM CCS*, 2009.

[14] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song, "Remote data checking using provable data possession," *ACM TISSEC*, vol. 14, no. 1, p. 1–34, 2011.

[15] D. S. W. Scott A. Crosby, "Efficient data structures for tamper-evident logging," in *SSYM*, 2009, pp. 317–334.

[16] D. Cash, A. Küpçü, and D. Wichs, "Dynamic proofs of retrievability via oblivious ram," *Journal of Cryptology*, vol. 30, no. 1, pp. 22–57, 2017.

[17] M. Etemad and A. Küpçü, "Generic efficient dynamic proofs of retrievability," in *ACM CCSW*, 2016.

[18] ——, "Transparent, distributed, and replicated dynamic provable data possession," in *ACNS*, 2013.

[19] E. Esiner, A. Kachkeev, S. Braunfeld, A. Küpçü, and Ö. Özkasap, "Flexdpdp: Flexlist-based optimized dynamic provable data possession," *ACM Transactions on Storage*, vol. 12, no. 4, 2016.

[20] E. Esiner, A. Küpçü, and Ö. Özkasap, "Analysis and optimization on flexdpdp: A practical solution for dynamic provable data possession," in *ICC*, 2014.

[21] A. Küpçü, "Official arbitration with secure cloud storage application," *The Computer Journal*, vol. 58, no. 4, pp. 831–852, 2015.

[22] "e-devlet kapısı devletin kısayolu," www.turkiye.gov.tr, [July. 17, 2019].

[23] R. S. P. Leach, M. Mealling, *A Universally Unique IDentifier (UUID) URN Namespace*, https://www.rfc-editor.org/info/rfc4122, 2005.

[24] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," in *AICCSA*, 2009.

[25] M. H. Eldefrawy, K. Alghathbar, and M. K. Khan, "Otp-based two-factor authentication using mobile phones," in *ITNG*, 2011, pp. 327–331.

[26] T. Acar, M. Belenkiy, and A. Küpçü, "Single password authentication," *Computer Networks*, vol. 57, no. 13, pp. 2597–2614, 2013.

[27] D. İşler and A. Küpçü, "Threshold single password authentication," in *ESORICS DPM*, 2017.

[28] D. İşler, A. Küpçü, and A. Coşkun, "User perceptions of security and usability of mobile-based single password authentication and two-factor authentication," in *ESORICS DPM*, 2019.

[29] D. İşler and A. Küpçü, "Distributed single password protocol framework," Cryptology ePrint Archive, Report 2018/976, 2018.

[30] ICAO, "Doc 9303, machine readable travel documents part 7: Machine readable visas," 2015.

[31] "Republic of turkey electronic visa application system," https://www.evisa.gov.tr/en/, [May. 26, 2019].

[32] "Authorized portal for visa application to india," https://indianvisaonline.gov.in/, [May. 26, 2019].

[33] Z. Říha, "An overview of electronic passport security features," in *The Future of Identity in the Information Society*, V. Matyáš, S. Fischer-Hübner, D. Cvrček, and P. Švenda, Eds. Springer Berlin Heidelberg, 2009, pp. 151–159.

[34] ICAO, "Doc 9303, machine readable travel documents, part 11: Security mechanisms for mrtds," 2015.

[35] ——, "Logical data structure (lds) for storage of biometrics and other data in the contactless integrated circuit (ic)," 2015.

[36] "arachni," https://www.arachni-scanner.com/, [July. 29, 2019].

[37] E. Torres, "Wmap using metasploit framework," https://www.metasploit.com/, [July. 29, 2019].

[38] A. Küpçü, "White paper on self study cryptography course," DOI: 10.13140/RG.2.2.13320.37124. [Online]. Available: https://sites.google.com/a/ku.edu.tr/self-crypto/

Kuantum Sonrası Güvenilir ABC Şifreleme Sisteminin Farklı Platformlardaki Uygulamaları

On the Implementations of Quantum Secure ABC Cryptosystem in Different Platforms

Sedat AKLEYLEK
Bilgisayar Mühendisliği Bölümüü
Ondokuz Mayıs Universitesi
Samsun, Türkiye
sedat.akleylek@bil.omu.edu.tr

Ramazan KOYUTURK
Bilgisayar Bilimleri
Ege Üniversitesi
Izmir, Türkiye
ramazankoyuturk@gmail.com

***Öz*—Bu çalışmada kuantum sonrası şifreleme sistemlerinden biri olan çok değişkenli polinom sistemlerine dayanan ABC sistemi anlatılmaktadır. ABC sisteminin teorik olarak yapısı hatırlatılmış ve buna bağlı olarak thread'siz ve thread'li bir uygulama gerçekleştirilmiştir. Her iki uygulamanın arasındaki farklar belirtilip karşılaştırılması yapılmıştır.**

Anahtar Sözcükler—kuantum sonrası kriptografi, çok değişkenli polinom sistemleri tabanlı şifreleme, paralel hesaplama.

***Abstract*—In this paper, ABC system based on multivariate polynomial systems which is one of the post-quantum encryption systems is explained. The theoretical structure of ABC system is recalled and implementations of ABC algorithm with no-thread and with thread are discussed. The differences between these two implementations are compared in terms of time complexity.**

Keywords—post-quantum cryptography, multivariate polynomial-based encryption, parallel computing.

I. GİRİŞ

Açık anahtarlı şifreleme sistemlerinin 1970'lerin sonunda geliştirilmesi ile modern şifrelemede köklü bir atılım oldu. O tarihlerden beri açık anahtarlı şifreleme sistemleri, iletişim ağlarının giderek artan bir şekilde, ayrılmaz bir parçası haline gelmiştir. Şifreleme teknikleri, modern toplumda iletişimin güvenliğini garanti altına almak için önemli bir araçtır. Son yıllarda internetin yaygınlaşması ile SSL (Secure Sockets Layer)'in de çalışma mantığında bulunan açık anahtarlı kriptosistem kullanımı oldukça artmıştır. Bilginin uçtan uça güvenli bir şekilde gönderimi, saklanması, insanların, şirketlerin ve devletlerin bu sistemi kullanmasını ve geliştirmesini sağlamıştır. Bununla birlikte kuantum bilgisayarların ortaya çıkmasıyla klasik açık anahtarlı şifreleme sistemleri güvenirliğini kaybedeceği düşünülmektedir. Bu sebeple kuantum bilgisayarlar tarafından gerçekleştirilecek ataklara karşı açık anahtarlı şifreleme sistemleri geliştirilmesi gerekmektedir. Ayrıca, günümüz işlemci mimarileri çok çekirdekli, kuantum sonrası güvenilir açık anahtarlı sistemlerin bunlara uygun bir şekilde uygulanmalarına ve geliştirilmelerine ihtiyaç vardır.

Günümüzde, internet ve diğer iletişim sistemleri temel olarak dijital imza algoritması (DSA), eliptik eğri DSA veya ilgili algoritmaları kullanan Diffie-Hellman anahtar değişimi, RSA şifrelemesi ve dijital imzalara dayanmaktadır [1]. Bu şifreleme sistemlerinin güvenliği, tam sayılı çarpanlara ayırma veya ayrık logaritma, eliptik eğri gibi belirli sayıdaki teorik problemlerin zorluğuna bağlıdır, ancak 1994 yılında Peter Shor, kuantum bilgisayarlarda bu problemlerin her birini polinom zamanda çözebileceğini göstermiştir [2]. Bu, kuantum bilgisayarların yaygınlaşmasıyla bir gerçeğe dönüşecek ve bu varsayımlara dayanan tüm şifreleme sistemleri güvensiz olacaktır.

Çok değişkenli polinom sistemleri tabanlı kriptosistemlerinin belirli koşullar altında kuantum hesaplama saldırılarına karşı dirençli olduğuna inanılmaktadır. Bunun nedeni, çok değişkenli açık anahtar şifreleme sistemlerinin NP-zor (NP-hard) bir problem olan sonlu bir cisim üzerinde çok değişkenli bir polinom sistemine dayanmasıdır [3, 4].

Günümüzde açık anahtarlı kriptografide imzalama, anahtar şifreleme, anahtar değişimi gibi işlemler için en çok tercih edilen algoritmalar RSA [1], Diffie-Hellman, DSA ve ECC'dir, ancak bu algoritmalar verinin güvenliğini sınırlı bir süre boyunca güvende tutabildiği için yeterince büyük kuantum bilgisayar geldiğinde bu gibi algoritmalar güvensiz hale gelecektir. Bu güvenlik sorununun sebebi, verileri elektriksel işaretleme ile değil de foton olarak adlandırılan ışık tanecikleri tanımlayıp bunları işleyebilen kuantum bilgisayarlardır. Bu bilgisayarlar üzerinde çarpanlara ayırma problemi ve ayrık logaritma problemini polinom zamanda çözen Shor [2] algoritması bulunmaktadır. Bu nedenle, kuantum bilgisayar saldırılarından etkilenmeyecek, matematiksel problemlere dayanan klasik şifreleme yöntemlerine alternatifler gerekir. Literatürde kuantum ataklarına karşı dirençli olduğu düşünülen beş ana sınıf bulunmaktadır: çok değişkenli polinom sistemleri, kafes, özet, kod ve izojeni tabanlı sistemlerdir. Bu çalışmada çok değişkenli polinom sistemlerini kullanan ABC kriptosistemi incelenecek ve farklı platformlardaki uygulamaları hakkında detaylar verilecektir.

Çok değişkenli polinom sistemleri tabanlı kriptosistemler kullandığı altyapı gereği oldukça hızlı ama anahtar boyutlarından dolayı genelde fazla bellek gereksinimine ihtiyaç duyar. Bu durum akıllı kartlar ve RFID [5] çipleri gibi

düşük maliyetli cihazlarda kullanım için onları çekici kılar. Bununla birlikte, birçok pratik çok değişkenli imza şeması [6] mevcut olsa da, verimli ve güvenli çok değişkenli şifreleme şemalarının sayısı sınırlıdır.

A. *Motivasyon ve Katkı*

Bilgilerin, iletilen mesajların korunması temel öncelik teşkil etmektedir. Verilerin güvenliğini sağlamak için gerek klasik bilgisayarlar gerekse kuantum bilgisayarlarda birçok şifreleme algoritmaları mevcuttur. Bunlardan biri ise çok değişkenli polinomlar temelli ABC şifreleme algoritmasıdır. Bu çalışmada kuantum bilgisayarlar sonrasında gerekli güvenliği sağlamak amacıyla ABC şifreleme sisteminin farklı platformlar için bir uygulaması geliştirilmiştir.

Açık kaynaklı kod geliştirilmesine ek olarak uygulamayı thread'li bir yapı kullanarak performans konusunda gelişmeler sağlanmıştır. Thread'li ve thread'siz uygulamanın performansları belirlenerek geliştirilmesi yapılmıştır ve algoritma stabil bir şekilde çalıştırılmıştır.

B. *Organizasyon*

Bu çalışma üç bölümden oluşmaktadır. Bölüm 2'de çok değişkenli polinom sistemleri nedir, ABC sistemi nasıl çalışır, algoritması nedir, uygulamak için hangi algoritmalar kullanılır sorularına cevaplar verilecektir. Bölüm 3'te ise standart ve paralel uygulama detayları anlatılacak ve bunların arasındaki farklar belirtilecektir. Son bölümde ise elde edilen sonuçlar hakkında özet bilgi sağlanacaktır.

II. ABC ALGORİTMASI

ABC, kuantum sonrası bilgisayarlar için öngörülen bir şifreleme yöntemidir. Son zamanlarda Tao et al [7] "basit matris şeması" veya "ABC" olarak adlandırılan matris çarpımına dayalı yeni bir basit ve verimli çok değişkenli açık anahtar şifreleme düzeni sunmuştur. Daha sonrasında, Ding, Petzoldt ve Wang [8] kübik polinomları gelişmiş bir ABC türevini önerdiler ve en azından rastgele ikinci dereceden bir denklem çözme kadar zor olan cebirsel saldırıları kullanarak bunu kırdıklarını gösterdiler. Çok yakın bir zamanda Tao, Xiang, Petzoldt ve Ding [9] ABC şemasını kare matris yerine kare olmayan matris kullanarak genelleştirdiler. Petzoldt, Ding ve Wang'ın ABC yapısında şifre çözme hatalarını ortadan kaldırmak için, matrislerin tensör çarpımını kullanan yeni bir ABC sürümünü önermiştir [10]. Bununla birlikte Hashimoto [11], bu türevin güvenliğinin ABC kökenli şemadan daha zayıf olduğunu göstermiştir. Daha sonra, Peng, Tang, Chen, Wu ve Zhang [12] verimliliği artırmak için modern x64 CPU'nun özelliklerinden yararlanarak ABC'nin uygulanmasını optimize etmiştir.

Verimlilik nedenleriyle, çok değişkenli polinom sistemleri genellikle K gibi q elemanlı bir sonlu cisim üzerinde birçok değişkene sahip ikinci dereceden polinom sistemidir.

$$p^{(1)}(x_1, \dots, x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(1)} x_i x_j + \sum_{i=1}^{n} p_i^{(1)} x_i + p_0^{(1)}$$

$$p^{(2)}(x_1, \dots, x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(2)} x_i x_j + \sum_{i=1}^{n} p_i^{(2)} x_i + p_0^{(2)}$$

$$\vdots$$

$$p^{(m)}(x_1, \dots, x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(m)} x_i x_j + \sum_{i=1}^{n} p_i^{(m)} x_i + p_0^{(m)}$$

DENKLEM 1

Çok değişkenli şifreleme sisteminin güvenliği, çok değişkenli ikinci dereceden polinom (MQ) problemine dayanır. Denklem 1'de gösterildiği gibi $p^{(1)}(x), \dots, p^{(m)}(x)$ olarak verilen m değişkenli ikinci dereceden polinomlar $p^{(1)}(\bar{x}) = 0, \dots, p^{(m)}(\bar{x}) = 0$ olacak şekilde bir $\bar{x} = (\bar{x}_1, \dots, \bar{x}_n)$ vektörü bulunur.

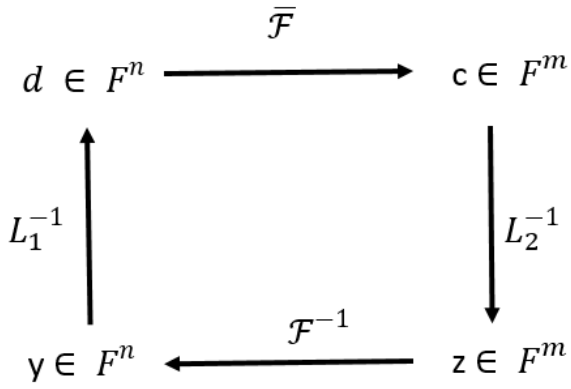
MQ problemi ($m \cong n$ için) $GF(2)$ cismi üzerindeki ikinci dereceden polinomlar için bile NP-zor problem olduğu kanıtlanmıştır [4].

MQ probleminin temelli bir açık anahtarlı kriptosistem oluşturmak için, kolayca tersi alınabilir bir ikinci dereceden $\mathcal{F} : F^n \rightarrow F^m$ polinomlar ile başlanır. Açık anahtarlıda $\mathcal{F}$'nin yapısını gizlemek için, iki tane tersi olan afin (veya lineer) $L_1 : F^n \rightarrow F^n$ ve $L_2 : F^m \rightarrow F^m$ yapısı oluşturulur.

Açık anahtarı oluşturacak yapı, $\overline{\mathcal{F}} = L_2 \, o \, F \, o \, L_1$.

Kapalı (Gizli) anahtar $L_1, \mathcal{F}$ ve L_2'den oluşur ve bu sayede açık anahtarın tersinin alınmasına olanak sağlar.

Çok değişkenli polinomlarda, şifreleme ve şifre çözme işlemlerinin çalışma süreci Şekil 1'de verilmiştir.



Şekil 1 ABC Sisteminin Şeması

Şifreleme: $d \in F^n$ şifrelemek için, tek bir basit hesaplama $c = \bar{\mathcal{F}}(d)$ yapılması yeterlidir. d mesajının şifrelenmiş hali $c \in F^m$'dir.

Şifre Çözme: $c \in F^m$ şifrelenmiş mesajı çözmek için, özyinelemeli olarak $z = L_2^{-1}(c), y = \mathcal{F}^{-1}(z)$ ve $d = L_1^{-1}(y)$ işlemleri yapılmalıdır. $d \in F^n$, şifrelenmiş olan c metnine karşılık gelen düz metindir.

Anahtar Üretimi: F, q elemana sahip sonlu bir cisim olarak ele alınır. $s \in S$ elemanı için, $n = s^2$ ve $m = 2n$ koşullarını oluşturur ve aşağıdaki gibi üç matris tanımlanır.

$$A = \begin{pmatrix} x_1 & \cdots & x_s \\ \vdots & \ddots & \vdots \\ x_{(s-1)(s+1)} & \cdots & x_n \end{pmatrix}, B = \begin{pmatrix} b_1 & \cdots & b_s \\ \vdots & \ddots & \vdots \\ b_{(s-1)(s+1)} & \cdots & b_n \end{pmatrix},$$

$$C = \begin{pmatrix} c_1 & \cdots & c_s \\ \vdots & \ddots & \vdots \\ c_{(s-1)(s+1)} & \cdots & c_n \end{pmatrix}$$

Burada $(x_1, \dots, x_n)$'ler $F[x_1, \dots, x_n]$ çok değişkenli polinomun lineer monomialidir. Ayrıca buradaki $(b_1, \dots, b_n)$ ve $(c_1, \dots, c_n)$'ler, $(x_1, \dots, x_n)$'in lineer birleşiminden rastgele seçilir.
$E_1 = AB$ ve $E_2 = AC$ çarpımlarından E_1 ve E_2 matrisleri elde edilir. Şemadaki $\bar{F}$, E_1 ve E_2'nin m bileşenlerinden oluşur.
Şemada açık anahtar, rastgele seçilmiş iki tersinir $L_2 : F^m \to F^m$ ve $L_1 : F^n \to F^n$ lineer denkleme sahip $\bar{F} = L_2 \, o \, F \, o \, L_1 : F^n \to F^m$ denkleminden meydana gelir. Kapalı anahtar ise B ve C matrislerinden ve L_1 ve L_2 lineer denklemlerinden meydana gelir.

Şifreleme: Bir $d \in F^n$ mesajını şifrelemek için tek bir hesaplama $c = \bar{F}(d) \in F^m$ yapılması yeterlidir.

Şifre Çözme: Şifrelenmiş $c \in F^m$ mesajını çözmek için aşağıdaki üç adımı takip edilir.

1. $z = L_2^{-1}(c)$'yi hesaplanır. $z \in F^n$ vektörünün elemanlarından aşağıdaki gibi $\overline{E_1}$ ve $\overline{E_2}$ matrisleri oluşturulur.

$$E_1 = \begin{pmatrix} z_1 & \cdots & z_s \\ \vdots & \ddots & \vdots \\ z_{(s-1)(s+1)} & \cdots & z_n \end{pmatrix}$$

$$E_2 = \begin{pmatrix} z_{n+1} & \cdots & z_{n+s} \\ \vdots & \ddots & \vdots \\ z_{n+(s-1)(s+1)} & \cdots & z_m \end{pmatrix}$$

2. İkinci adımda ise $y = (y_1, \dots, y_n)$ şeklinde $\mathcal{F}(y) = z$ koşulunu sağlayan bir vektör bulunur. Bunun yapılabilmesi için dört farklı koşul vardır.

   i) Eğer $\overline{E_1}$'in tersi varsa, $B\overline{E_1^{-1}}\overline{E_2} - C = 0$ denklemi düşünülür.
   ii) Eğer $\overline{E_1}$'in tersi yoksa ama $\overline{E_2}$'nin varsa, $C\overline{E_2^{-1}}\overline{E_1} - B = 0$ denklemi düşünülür.
   iii) Eğer ne $\overline{E_1}$ ne de $\overline{E_2}$'nin tersi yoksa ama $\bar{A} = \overline{A(y)}$'nın tersi varsa, $\overline{A^{-1}}\overline{E_1} - B = 0$ ve $\overline{A^{-1}}\overline{E_2} - C = 0$ denklemleri düşünülür.
   iv) Eğer $\overline{E_1}$, $\overline{E_2}$ ve $\bar{A}$'nın hiçbirinin tersi yoksa, şifre çözme başarısızdır.

3. Son olarak, çözümlenmiş mesajı bulmak için $d = L_1^{-1}(y_1, \dots, y_n)$ hesaplaması yapılır.

İkinci adımdaki şifre çözmede başarısızlık oranı $1/q$'dur. Şifre çözme işleminin ikinci basamağındaki lineer sistemlerin $y^{(1)}, \dots, y^{(l)}$ gibi birden fazla çözümü olabilir. Böyle bir durumda bir dizi olası şifresi çözülmüş mesaj elde etmek için (her bir dizi için) üçüncü adımın gerçekleştirilmesi gerekir. Daha sonrasında bu düz metinler teker teker şifrelenerek hangisinin verilen şifreli mesaja karşılık geldiği test edilir.
ABC şifreleme sisteminin uygulamasını yazmak için gerekli temel algoritmalar bulunmaktadır. Bunlar; GF(2^8) sonlu cismi üzerinde "toplama", "çıkarma", "çarpma" ve "bölme" işlemleri, GF(2^8)'deki bir elemanın "tersini alma", verilen herhangi bir kare matrisin "tersini" ve "transpozunu" alma, herhangi iki kare "matrisin çarpımını" bulma ve bir matrisin "Echelon matrisini" hesaplamadır.

III. ABC ALGORİTMASININ UYGULANMASI

Bu bölümde, ABC kriptosisteminin farklı platformlar için uygulama detayları verilmektedir. ABC sisteminin çalışmasında üç ana aşaması bulunmaktadır. Bunlar "anahtar üretimi", "şifreleme" ve "şifre çözme"dir. Programın gerek standart gerekse paralel uygulamasında parametre kümeleri Tablo I'de verilmiştir. Uygulama hem "Windows 8.1 x64" hem de "Kali Linux 64-Bit 2018.2" işletim sistemlerinde çalıştırılmıştır.

Tablo I'deki değerlerin boyutu 4-byte (32-bit) şeklindedir.

TABLO I Değerler Boyutu

S	8
N	64
M	128
CENTRAL_MAP_SIZE (Ortadaki Dönüşüm)	2080
PUBLIC_KEY_SIZE (Açık Anahtar Boyutu)	266240
SECRET_KEY_SIZE (Gizli Anahtar Boyutu)	294912

Performans iyileştirilmesinin en çok gerekli olduğu kısım anahtar üretim kısmıdır. Buradaki asimptotik karmaşıklık, iç içe dört kez "for" döngüsü kullanıldığından O(n^4)'dir.

A. Standart Uygulama

Standart uygulamada gerek ön tanımlı (define) gerekse "Main()" fonksiyonu içinde tanımlamalar yapıldıktan sonra sırasıyla "anahtar üretimi", "şifreleme" ve "şifre çözme" için yazılan fonksiyonları çağırarak uygulama gerçekleşmektedir. Bölüm II'de adlandırılan gerekli algoritmaların bu üç kısımda (anahtar üretimi, şifreleme, şifre çözme) kaç kez çağrıldığı Tablo II'de gösterilmiştir. Çağrılma sayıları, her bir fonksiyon için genel (generic) olarak tanımlanan bir değişkenin fonksiyon içinde arttırılması ile elde edilmiştir.

TABLO II Fonksiyonların Çağırılma Sayısı

	Anahtar Üretimi	Şifreleme	Şifre Çözme	Toplam
Toplama	4452352	0	286720	4739072
Çıkarma	0	0	2064512	2064512
Çarpma	107740992	532480	2617792	110891264
Bölme	0	0	16256	16256
Tersini Alma	193	0	1	194
Matris Tersi	2	0	0	2
Matris Çarpımı	257	0	0	257
Matris Trans.	1	0	0	1
Denk. Kats. He.	128	0	0	128
Echelon	0	0	1	1

B. Paralel Uygulama

Matris çarpımının performansını arttırmak için kod optimize edilebilir ya da thread mantığı ile paralel hesaplama seçenekleri kullanılabilir. Standart C fonksiyonları 1970'li yıllarda tasarlandığı için birden fazla thread ile kullanılabilecek biçimde tasarlanmamıştır. Standart C kütüphanelerinin tek thread için (single threaded) ve çok thread için (multi threaded) iki versiyonu vardır ancak kütüphane, UNIX ortamında (dolayısıyla LINUX ortamında da) POSIX kütüphanesi olarak geçmektedir ve bu kütüphanenin baş harfi olan P harfi ile thread kelimesinin birleşmesinden türemiştir (pthread).

Bir thread başlatıldıktan sonra, hazır durumuna geçer. Zamanlama algoritmasına (scheduling algorithm) [13] bağlı olarak, çalışır duruma geçer. Çalışır durumdayken bir sebeple bekleme durumuna geçebilir. Örneğin farklı bir thread'i bekleyebilir veya bir sistem kaynağına erişmek isteyebilir veya belirli bir süre için uyutulmuş olabilir. Durma sebebi ortadan kalktıktan sonra, hazır duruma geri geçer ve hazır sırasında (ready queue) beklemeye başlar.

ABC algoritmasının öncelikle anahtar üretimi fonksiyonu içinde gerekli olan matrislerin üretimi ve değerlerinin yazılması işlemlerinde kullanılır. https://gitlab.com/ramcho/abc adresinden erişilebilen uygulama kodlarında tanımlama bloğunda kullanılan;

```
WORD S[VARIABLE*VARIABLE];
WORD INVS[VARIABLE*VARIABLE];
WORD INVT[EQUATION*EQUATION];
WORD T[EQUATION*EQUATION];
```

matrisleri genel tanımlama için "abc.h" isimli header dosyasının içine eklenmiştir. Böylelikle bağımsız olarak hem threadler'de kullanılırken hem de fonksiyonlarda işlemlere girdiğinde işlenmiş değerler kaybolmamaktadır.

Buradaki "S, INVS, T ve INVT" matrisleri ABC sisteminin gerçekleşmesi için gerekli olan L_1 ve L_2 matrislerini oluşturulmasında (tekil olmadığı kontrol edilip) S ile lineer dönüşümü başlatılmasında ve T^{-1} hesaplamasında kullanılmaktadır. Daha sonrasında anahtar üretimi fonksiyonunun içinde aşağıdaki kod eklemesi yapılır.

```
pthread_t thread_id;
void *thread_result;
pthread_create( &thread_id, NULL, thread_routine, NULL );
pthread_join( thread_id, &thread_result);
```

Burada öncelikle "thread_id" isimli bir thread tanımlanır. Benzer şekilde tipi "void" olan "thread_result" isimli bir işaretçi tanımlanır. Pthread kütüphanesinde ön tanımlı olan "pthread_create" fonksiyonu ile oluşturulan thread algoritmaya tanıtılır ve hangi fonksiyonu çağırması gerektiği parametre olarak verilmektedir. En son satırda ise thread'i çağırma işlemi yapılmaktadır.

```
void *thread_routine(void* arg){
        int eof = 0, i, j;
        while (eof == 0) {
                for (i = 0; i < VARIABLE; i++) {
                        for (j = 0; j < VARIABLE; j++) {
                                INVS[i * VARIABLE + j]
= S[i * VARIABLE + j] =rand() % FIELD;
                        }}
                eof = matrixinv(INVS, VARIABLE);
        }
        eof=0;
        while (eof == 0) {
                for (i = 0; i < EQUATION; i++) {
                        for (j = 0; j < EQUATION; j++) {
                                INVT[i * EQUATION + j]
= T[i * EQUATION + j] = rand() % FIELD;
                }}
        eof = matrixinv(INVT, EQUATION);
}}
```

"*thread_routine" isimli fonksiyon "abc.c" isimli dosyada main dışında herhangi bir yere eklenir. Bu kod bloğu çalıştığında "S, INVS, T ve INVT" isimli matrislere rastgele değerler üretilip ataması yapılmıştır.

C. Karşılaştırma

ABC kriptosistemi için hazırlanan uygulama iki farklı bilgisayarda üç farklı ide ortamında hem thread'siz hem de pthread kütüphanesi ile denenmiştir. Tablo III'te kullanılan bilgisayar özellikleri, derleme ortamı ve işletim sistemi bilgileri özetlenmiştir.

TABLO III Programın Çalışma Ortamı

İndeks	Bilgisayar Özellikleri	Ram	Derleme Ortamı	İşletim Sistemi
1	Intel(R) Core(TM) i7-4500U CPU @ 1.80GHz	12 Gb	Visual Studio, 2013	Windows 8.1
2	Intel(R) Core(TM) i7-4500U CPU @ 1.80GHz	12 Gb	Dev C++, 5.6.1	Windows 8.1
3	Intel(R) Core(TM) i3-4000M CPU @ 2.40GHz	8 Gb	GCC, 8.3.0	Kali Linux

Tablo IV'te ABC kriptosistemi için hazırlanan uygulamanın hem thread'li hem de thread'siz olarak üç farklı ortamdaki toplam çalışma süreleri mikro saniye (µs) cinsinden verilmiştir.

TABLO IV Programın Tamamının Çalışma Süreleri

	Thread'siz	Thread'li
İndeks 1	4336000 µs	3637000 µs
İndeks 2	1171000 µs	1125000 µs
İndeks 3	1460734 µs	1440778 µs

Tablo V'de ABC kriptosistemi için hazırlanan uygulamanın "şifreleme" ve "şifre çözme" fonksiyonlarının çalışma süreleri üç farklı ortam için hem thread'li hem de thread'siz olarak mikro saniye cinsinden verilmiştir.

TABLO V Şifreleme ve Şifre Çözme Fonksiyonlarının Çalışma Süreleri

	Thread'siz		Thread'li	
	Şifreleme	Şifre Çözme	Şifreleme	Şifre Çözme
İndeks 1	16000 µs	132000 µs	12000 µs	128000 µs
İndeks 2	8000 µs	28000 µs	4000 µs	24000 µs
İndeks 3	5458 µs	30872 µs	5428 µs	30620 µs

Uygulamanın çalıştırılması sonucunda elde edilen süreler ve "Tablo II"de ayrıntılı olarak gösterilen ABC yapısı için gerekli olan fonksiyonların "anahtar üretimi", "şifreleme" ve "şifre çözme"de kaç defa çağrıldığını ve kullanıldığı sayılarak değerlendirilmiştir. Thread'li veya thread'siz olarak çalıştırılan kodda, fonksiyonların çağrılma işlemlerinde çok az bir fark vardır, ancak süre bazında gelişme sağlanmıştır. Süre ölçümü ise Tablo IV'te her iki kodda da "anahtar üretimi"nden önce başlayıp "şifre çözme"nin tamamlanmasıyla bitirilmiştir. Tablo V'de ise şifreleme ve şifre çözme olarak thread'li ve thread'siz olarak ölçülmüştür. Her üç ortamda da GF(2^8)'de bir elemanın tersini alma fonksiyonu thread'siz yapıda 194 kez çağırılırken thread'li yapıda 193 kez çağrılmıştır.

İndeks numarası 1 olan derleyici ve bilgisayarda thread'siz kodun çalışması sonucu 4336000 mikro saniyelik bir sonuç elde edilmiştir. Thread'li yapıda ise 3637000 mikro saniyelik bir sonuç elde edilmiştir. Burada thread'li yapı sayesinde %16'lık bir zaman kazanımı sağlanmıştır.

İndeks numarası 2 olan derleyici ve bilgisayarda thread'siz kodun çalışması sonucu 1171000 mikro saniyelik bir sonuç elde edilmiştir. Thread'li yapıda ise 1125000 mikro saniyelik bir sonuç elde edilmiştir. Burada thread'li yapı sayesinde %4'lük bir zaman kazanımı sağlanmıştır.

İndeks numarası 3 olan derleyici ve bilgisayarda thread'siz kodun çalışması sonucu 1460734 mikro saniyelik bir sonuç elde edilmiştir. Thread'li yapıda ise 1440778 mikro saniyelik bir sonuç elde edilmiştir. Burada thread'li yapı sayesinde %1'lik bir zaman kazanımı sağlanmıştır.

Uygulamaların çalışma ortamları fark etmeksizin, paralel uygulamalar, performans olarak standart olanlarına göre daha iyidir. ABC kriptosisteminin şifre çözme aşamasında kullanılan L_1, L_2 lineer dönüşümlerinin tanımlandığı aşama bu farkı oluşturur. ABC kriptosisteminin uygulamasında bu aşama "anahtar üretimi" fonksiyonu içinde gerçekleşmektedir. Paralel uygulamada L_1, L_2 ve L_1^{-1}, L_2^{-1} dönüşümlerinin matris tanımlaması ve rastgele oluşturulan elemanlarının atama işlemleri thread yöntemi ile yapılmaktadır. Bu sayede 3 farklı ortam için ortalama %7'lik bir performans gelişimi sağlanmıştır.

Performans gelişimiyle veriler daha güvenli, daha hızlı şifrelenip iletilmekte ve çözülmektedir. Bu sayede veriler daha verimli şekilde kullanılıp zaman kaybı azaltılmaktadır. Zaman kaybının azaltılması, yüksek verimlilik ve güvenlik uygulamanın amacıdır.

Farklı ortamlarda farklı süreler elde edilmesini nedeni öncelikle işletim sistemi farklılığıdır. İndeks numarası 3 olan bilgisayarda Unix tabanlı "Kali Linux" işletim sistemi bulunmaktadır. İndeks numarası 1 ve 2 olan bilgisayarlarda ise "Windows" işletim sistemi bulunmaktadır. İşletim sistemleri farklılığına ek olarak CPU mimarisi farklılığı (Tablo III'te ayrıntılı olarak verilmiştir) süre değişkenliğini etkilemiştir.

Aynı bilgisayar üzerinde çalışan İndeks 1 ve İndeks 2 numaralı ortamlarda ise süre farkının oluşmasının temel sebebi; paralel programlamadır. Paralel uygulama çalışmaya başladığında main içerisinde "anahtar üretimi" fonksiyonu çağrıldığında aynı anda bir thread oluşmaktadır. Bu thread programın ana akışından farklı bir paralel yol izlemekte ve yapması gereken işlemleri tamamlayıp tekrar ana akışa dönmektedir. Bu sayede "anahtar üretimi" fonksiyonu içerisinde fazladan tanımlama ve özyinelemeli fonksiyon çağırımı yapılmamış olur. Bir diğer sebep ise farklı ide'ler kullanılmasıdır. Visual Studio, Dev-C++'a göre daha kompleks bir ide olduğundan çalışma süresinde farklılığa sebep olmuştur. "Anahtar Üretimi" fonksiyonunda kullanılan matrislerin thread yapısı ile değer atanması sonucu Tablo IV'te ayrıntılı olarak verilen süreler elde edilmiştir.

IV. SONUÇ

Çok değişkenli açık anahtar şifreleme sistemlerinden biri olan ABC sisteminin, kuantum hesaplama saldırılarına karşı direnç gösterebileceğine inanılmaktadır. Bu çalışmada elde edilen sonuçlar neticesinde bilgisayarların çalışma ortamı fark etmeksizin thread'li bir yapı ile geliştirilmiş uygulama, süre bazında daha iyi sonuçlar vermektedir. Bunun sebebi uygulamada kullanılan thread sayesinde uygulamayı zaman konusunda yoran fonksiyon ve matris işlemlerinin paralel olarak hesaplanmasıdır. Süre bazında geliştirilmesi için thread yapısını sadece ön tanımlı değişkenler için değil, uygulamanın geneline entegre edilmesi daha iyi sonuçlar elde edilmesine olanak sağlamıştır.

Daha sonraki çalışmalar için, temel ABC sistemi algoritmasının performans artışının sağlanması, asimtotik karmaşıklığın azaltılması, farklı diller için yazılımının yapılması ve en son olarak da herhangi bir projede kullanılabilir hale getirilerek kullanılması amaçlanmaktadır.

TEŞEKKUR

Bu çalışma EEEAG-116E279 proje numarası ile TÜBİTAK tarafından desteklenmiştir.

KAYNAKLAR

[1] R.L. Rivest, A. Shamir, L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Commun. ACM 21(2), 120–126 (1978)

[2] P. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM J. Computing, vol. 26, no. 5, 1997, pp. 1484–1509

[3] J.A. Buchmann, D. Butin, Post-Quantum Cryptography: State of the Art. The New Codebreakers, LNCS 9100, 2016, pp.88-108.

[4] M.R. Garey, D.S. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness. W.H. Freeman and Company, New York (1979).

[5] J. Landt, The history of RFID, IEEE Potentials(Volume: 24, Issue: 4, Oct.-Nov. 2005), pp. 8–11.

[6] J. Ding, D. Schmidt, Rainbow, a new multivariable polynomial signature scheme. In: Ioannidis, J. Keromytis, A.D. Yung, M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 164–175. Springer, Heidelberg (2005)

[7] C. Tao, A. Diene, S. Tang, J. Ding, Simple matrix scheme for encryption, PQCrypto 2013, LNCS 7932 (2013), pp. 231-242.

[8] C. Tao, H. Xiang, A. Petzoldt, J. Ding, Simple Matrix - a multivariate public key cryptosystem (MPKC) for encryption, Finite Fields and Their Applications 35 (2015), pp. 352-368.

[9] J. Ding, A. Petzoldt, L.C. Wang, The cubic simple matrix encryption scheme, PQCrypto 2014, LNCS 8772 (2014), pp. 76-87.

[10] A. Petzoldt, J. Ding, L.C. Wang, Eliminating decryption failures from the simple matrix encryption scheme, http://eprint.iacr.org/2016/010, 2016.

[11] Y. Hashimoto, A note on tensor simple matrix encryption scheme, http://eprint.iacr.org/2016/065.

[12] Z. Peng, S. Tang, J. Chen, C. Wu and X. Zhang, Fast Implementation of Simple Matrix Encryption Scheme on Modern x64 CPU, ISPEC 2016, LNCS 10060, pp. 151-166, 2016.

[13] H. Cho, B. Ravindran, E. D. Jensen, An Optimal Real-Time Scheduling Algorithm for Multiprocessors. 19 December 2006.

Docker Konteyner Teknolojisi Üzerine Yapılan Güvenlik Çalışmalarının İncelemesi

A review on security studies of Docker container technology

Tamer Say
Bilgi Güvenliği Mühendisliği
Gazi Üniversitesi
Ankara, Türkiye
tamer.say@gazi.edu.tr

Mustafa Alkan
Elektrik-Elektronik Mühendisliği
Teknoloji Fakültesi, Gazi Üniversitesi
Ankara, Türkiye
makan@gazi.edu.tr

Murat Dörterler
Bilgisayar Mühendisliği
Teknoloji Fakültesi, Gazi Üniversitesi
Ankara, Türkiye
dorterler@gazi.edu.tr

İbrahim Alper Doğru
Bilgisayar Mühendisliği
Teknoloji Fakültesi, Gazi Üniversitesi
Ankara, Türkiye
iadogru@gazi.edu.tr

***Özet* – Docker konteyner teknolojisi son yıllarda kullanıcılar tarafından çok hızlı şekilde kabul gören yazılım teknolojilerinden birisidir. Yıllardır benimsenen sanal makine kullanımına çeşitli alanlarda üstün gelerek hızla yaygınlaşmıştır. Yüksek başarım ve portatif olma özellikleriyle oldukça kullanışlı olmasına karşın konak işletim sisteminin çekirdeğini kullanması nedeniyle birçok güvenlik riskini bünyesinde barındırmaktadır. İşletim sisteminden farklı olarak kullanıcılar kendi imajlarını kolayca oluşturabilmektedir. Temel alınan imajlarda oluşabilecek güvenlik problemleri ve hatalı yapılandırmalar gibi çeşitli sebeplerle Docker imajları ve Docker'ın aktif sistemlerde kullanımı birçok tehdite karşı açık kapılar bırakmaktadır. Docker konak işletim sistemi üzerindeki tehditler, Docker mimarisindeki potansiyel riskler ve Docker imajlarının analizi üzerine gerçekleştirilen güvenlik çalışmaları araştırılarak araçlar ve yöntemler incelenmiş; sonuçları değerlendirilmiştir.**

***Anahtar Kelimeler* – docker güvenliği, konteyner güvenliği, devops, docker statik analizi.**

***Abstract* – Docker container technology is one of the most rapidly adapted software technologies in recent years. Containers have swiftly become widespread use in many areas by overcoming virtual machine usage. Despite it's performance and portability features, usage of containers may be a high security risk since containers use kernel of the host operations system. Regardless of the host operation system, users are able to create their own Docker images. These images can be created by predetermined Docker base images thus, any security issue on base image is directly inherited to newly created image. Misconfiguration of docker images during creation or usage of misconfigured docker containers on production systems may lead to severe security threats. In this research, security threats on host systems, potential risks of Docker architecture and static analysis of Docker images are investigated, tools and methods which are used on studies are examined and results discussed.**

***Keywords* – docker security, container security, static analysis of docker images.**

I. GİRİŞ

Konteyner teknolojisi yazılım sürümlerini oluşturma, dağıtım olarak çıkartma ve farklı konak işletim sistemleri üzerinde çalışması özellikleri nedeniyle birçok alanda değişime yol açmıştır. Yazılım süreçlerini kolaylaştırması, performans kaybını minimize etmesi, kolay taşınabilirliği, çoklu bulut altyapılarına olanak sağlaması ve sunucu kaynaklarını paylaşımlı kullanabilmesi gibi özellikleriyle oldukça geniş bir çevre tarafından benimsenmekte ve kullanılmaktadır [1][2]. Konteynerlerin bir standart hale gelmesiyle açık kaynak dünyasındaki önde gelen vakıflar ve kuruluşlar bu teknolojiyi destekleme kararı almıştır [2][3]. Konteyner teknolojisinin en önemli iki özelliği; konak makinenin çekirdiğini kullanması ve aynı konak makine üzerinde çalıştırılan farklı konteynerler arasında yalıtım sağlamasıdır. Bu sayede konak ile konteynerler arasında ve konteynerlerin birbirleri arasında yalıtım sağlanarak saldırı yüzeyi daraltılmış olur. Tüm bu özelliklerine rağmen konteyner teknolojisi güvenlik açısından sanal makine kullanımına göre daha büyük riskleri bünyesinde barındırmaktadır. Konteyner imajlarındaki potansiyel güvenlik problemleri ve konak makine üzerindeki bir konteynerin ihlal edilmesi ile oluşabilecek tehditler bu risklerin başlıcaları olarak göze çarpmaktadır.

Bu çalışmada Docker konteyner teknolojisi üzerine yapılan güvenlik çalışmaları incelenerek konteyner mimarisindeki temel problemler araştırılmıştır. Docker kullanımının konak makineye karşı potansiyel tehditleri, hatalı yapılandırmalar sonucu oluşabilecek riskler ve konteyner imajlarındaki zafiyetlerin statik analizi incelenerek değerlendirilmiş; Docker kullanımı üzerine öneriler sonulmuştur.

Çalışmanın ikinci bölümünde konteynerlerin tarihi ve Docker mimarisinin tasarımı verilmiştir. Üçüncü bölümünde konak işletim sistemindeki potansiyel güvenlik tehditleri belirtilmiş ve konak işletim sistemindeki güvenlik sıkılaştırmalarına değinilmiştir. Dördüncü bölümde Docker

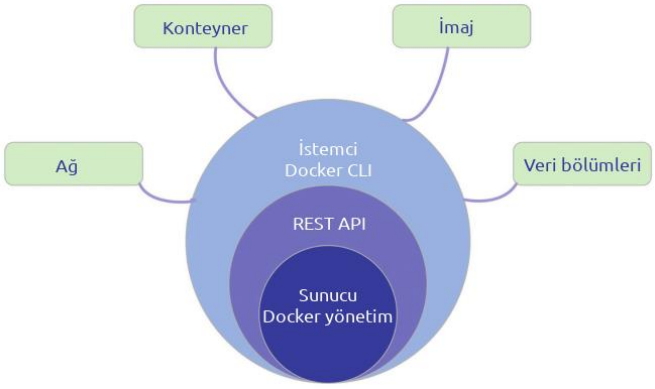
mimarisindeki kusurlar üzerine gerçekleştirilen çalışmalara yer verilmiştir. Beşinci bölümde Docker imajları üzerinde gerçekleştirilen statik imaj analizi çalışmaları incelenmiştir. Altıncı bölümde incelenen çalışmalar hakkında değerlendirmeler yapılmıştır.

II. KONTEYNERLERİN TARİHİ VE DOCKER MİMARİ YAPISI

Konteynerler, Linux işletim sistemi ile çekirdeği sayesinde daha basit ve doğrudan sanallaştırma imkânı sunarak yüksek başarım kazancı ve kolay kullanım olanağı sağlamaktadır. Konaktan bağımsız çalışan konteynerler farklı ortamlara taşınabilmekte veya kaynak ihtiyacının değişmesi durumlarına göre hızlı adaptasyon sağlayabilmektedir. Konteynerlerin ilk ilkel örnekleri 2000 yılındaki SELinux'a dayanmaktadır [4]. Daha sonra çıkan LXC teknolojisi ile süren bu gelişim 2014 yılında ilk kararlı sürümü yayınlanan Docker ile pekişmiştir. Devam eden süreçte ilgili kuruluşlar tarafından açık kaynak olarak desteklenerek gelişimini sürdürmektedir. Docker, 0.9 sürümüne kadar LXC teknolojisini temel almakta ve varsayılan sürücüsü olarak LXC'yi kullanmaktaydı [5]. Tespit edilen güvenlik ihlalleri nedeniyle bu altyapı değiştirilmiştir.

Docker konteynerleri LXC konteynerlerine benzer bir yapıda çalışmaktadır. Docker kütüphane olarak libcontainer kullanırken; LXC, liblxc kullanmaktadır [5-7]. Çekirdek bağımlılıkları aynı iken Docker, konak çerkideğinde 3.10 ve üzeri sürümlerde çalışabilmektedir. Diğer yazılım bağımlılıkları açısından Docker, LXC'den farklı olarak iptables, perl, AppArmor ve sqlite gerektirmektedir [7].

Docker mimarisi çeşitli bileşenlerden oluşmaktadır. Bunlar, Docker istemcisi, Docker Daemon (yönetim) uygulaması ve Docker kayıt bileşenleridir. İstemci sayesinde kullanıcılar Docker motoru ile etkileşime geçebilmektedir. Bu iletişim Docker Daemon aracılığıyla bir HTTP protokolü kullanan RESTful API kullanılarak gerçekleştirilmektedir. RESTfull API sayesinde bu iletişim aynı makine üzerinde veya uzak bağlantı kurulan bir makinede gerçekleştirilebilir. Docker kayıt bileşeni imajların saklandığı bileşen olarak görev almaktadır. Docker iç yapısı ve bileşenleri Şekil 1'de gösterilmektedir.



Şekil 1. Docker motoru yapısı [4]

Docker çevresel elemanlarından ağ yapısı, konteynerler, imajlar ve veri depolama bölümleri kullanıcı tarafından Docker yönetim birimi aracılığıyla yönetilmektedir [4].

Konteynerler, bir veya birden fazla Docker imajı kullanarak oluşturulabilirler. Dockerfile isimli yönergeler içeren dosya ile imajlar konteyner haline dönüşerek çalışır bir servis haline getirilebilmektedir. Kullanıcılar kendi imajlarını oluşturabildiği gibi Docker firması tarafından yönetilen DockerHub üzerindeki resmi imajlar veya diğer kullanıcılar tarafından oluşturulan imajlar kullanılarakta imaj veya konteyner oluşturulabilir.

III. SAVUNMANIN İLK HATTI KONAK İŞLETİM SİSTEMİ

Docker konteynerlerin oluşturulduğu, çalıştırıldığı ve birbirleri ile iletişime geçtikleri makineye konak işletim sistemi denilmektedir. Genellikle Linux işletim sistemi ve çekirdeği üzerinde çalışan konterynerler çeşitli yöntemler ile MAC ve Windows tabanlı işletim sistemlerinde de çalışabilmektedir [8].

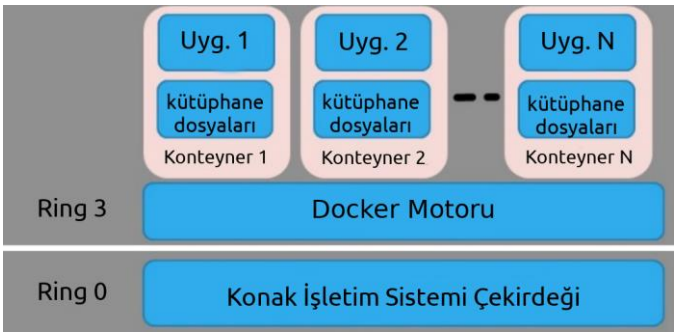
Konteynerlerin iç güvenliğini sağlamadan önce konteynerlere tam erişime sahip konak makinenin güvenliğini sağlamak daha büyük öneme sahiptir.

Atılacak ilk adımlardan birisi Docker Daemon biriminin iletişim bağlantıları şifrelenerek daha güvenli iletişim kurulmasıdır. Docker firması tarafından geliştirilen konak ortamlarını oluşturmakla birlikte iletişimi sağlayan Docker Machine uygulaması açık kaynak olarak sunulan bir araçtır. Docker Machine ile konak ortamları güvenli bir şekilde oluşturulabilmekte ve süregelen iletişim trafiği TLS mekanizması ile şifrelenebilmektedir [8][9]. Bu sayede kurulan bağlantıya ekstra bir güvenlik katmanı sağlanmaktadır.

Konak işletim sistemleri olarak özünde sanallaştırmada ve sanal makine olarak kullanılan Debian, Ubuntu, Redhat ve CentOS dağıtımları kullanılmaktadır. Bu işletim sistemleri çok amaçlı kullanılabilirlik özellikleri nedeniyle bünyelerinde yüzlerce paket barındırmaktadır. Docker konak olarak kullanılması düşünülen işletim sistemi bu paketlerin birçoğuna ihtiyaç duymaz. İhtiyaç duyulmayan paketlerde zamanla doğacak güvenlik tehditleri bütün sistemi tehlikeye atacak risk taşımaktadır. Bu nedenle Docker konak işletim sistemi olarak kullanılmak üzere CoreOS ve Alpine Linux işletim sistemleri doğmuştur [1]. Bu dağıtımlardaki daha asgari paket sayısı ile gerekli işlemler ve süreçler eksiksiz gerçekleştirilebilmektedir. Bu işletim sistemleri geliştirilirken canlı yama [8] yapabilecek şekilde geliştirilmiştir. Bu sayede otomatik güncelleme mekanizmalarıyla güvenlik tehditlerine karşı hızlı tedbir alınmasına olanak sağlanmıştır.

A. Linux Çekirdeği Güvenliği

Docker motoru mimarisi gereği Linux işletim sistemi üzerinde çekirdeğe en uzak katman olan Ring 3'te çalıştırılmaktadır [1][10]. Fakat çekirdek kullanımı ve kabiliyetleri konak işletim sistemi seviyesinde çalışması gerekliliği nedeniyle Ring 0 seviyesinde çalışır ve bu seviye tüm haklara sahiptir. Docker çalışma seviyesi ve konak işletim sistemi ile bağlantısı Şekil 2'de gösterilmektedir. Yapılan araştırmalara göre bu seviyedeki çalışma yetkinliği nedeniyle konteynerler ile konak işletim sistemi arasındaki trafiğin dinlenebileceği belirtilmiştir [10].



Şekil 2. Docker çalışma seviyesi [10]

Docker motorunun Ring 3 seviyesinde çalışması aynı seviyede çalışan diğer uygulamalar tarafından da etkilenebileceği anlamına gelmektedir. Konak üzerindeki herhangi bir uygulamanın konteynerin çalışan işlemini manüpele etmesi söz konusudur.

Ring 0 seviyesindeki çekirdeği kullanması nedeniyle konteynerler üzerinden hafızanın (memory) manipüle edilmesi yöntemiyle konak makine üzerine geçiş yapılabilmesi saldırıları Docker güvenlik çalışmaları tarafından en tehlikeli görülen yöntemlerden birisidir [10]. Çeşitli kaynaklarda bu durumun olası riskler arasında en kritik olarak değerlendirilen olduğu belirtilmektedir. Docker ve Docker kütüphanesi olan libcontainer'i ilgilendiren 11 farklı güvenlik açığı tespit edilebilmiştir [12]. Docker 1.10 sürümü ile konteyner içerisindeki işlem (process) ile konak üzerindeki işlem ayrılarak farklı isim-uzayında (namespace) çalıştırılmaktadır [13]. Bu da konteyner – konak yalıtımı için önemli bir güvenlik mekanizması sunmaktadır. Docker çalışma mantığı gereği işlemler arası yalıtım da sağlamaktadır. Her bir konteyner sadece kendi işlemi dahilinde yazma ve okuma süreçlerini gerçekleştirebilmektedir. Bunun için Linux çekirdediğinde her konteyner için ayrı işlem; her işlem için ayrı isim-uzayı oluşturur bu sayede işlemler arası yalıtım sağlanmış olur. Konteynerlerin birbirleri ile iletişim kurma ihtiyaçları doğması halinde arası belirli kurallar çerçevesinde işlemler-arası iletişim (inter-process communication) gerçekleşebilir [12].

Çekirdek seviyesinde güvenlik için çeşitli yamalar ve uygulamalar geliştirilmektedir. Çalışma ortamı için geliştirilen bu uygulamalardan SELinux, AppArmor, LoadPin, Smack, TOMOYO, YAMA güvenlik mekanizmalarının uygulanması önerilmektedir [8, 14-16].

Intel firması kendi üretimi olan işlemciler üzerinde çalışan konteynerlerin işlemlerini dış tehditlere karşı yalıtımını sağlamak için SGX mekanizmasını geliştirmiştir [16]. SGX mekanizması farklı seviyelerde çalışan uygulamalar için ekstra bir katman getirmektedir [17]. İşlemci seviyesinde gerçekleşen ve bir kapsülleme mekanizması gibi çalışan bu yöntem ile az da olsa performans kaybı yaşanmakta iken saldırı yüzeyi konak işletim sistemi ve Hypervisor olan saldırılara karşı etkili olmadığı belirtilmektedir [1][18].

IV. DOCKER MİMARİSİ GÜVENLİĞİ

Docker bileşenleri açık kaynak ekosistemi sayesinde oldukça gelişmiş ve çeşitli güvenlik mekanizmaları bu süreçte standart haline gelmiştir. Docker kurulumu mimarisindeki konteyner yalıtımı gereği bir sıkılaştırma uygulanmadığı takdirde dahi belirli bir çerçevede güvenlik önlemini kendi bünyesinde barındırmaktadır. Varsayılan olarak uygulamaları kendi dosya sistemlerinde çalıştırması, farklı uygulamalar için farklı kullanıcılar ataması ve Linux'un kabiliyetlerinden olan chgroups ve isim-uzayı kullanması güvenlik açısından Docker'ı bir adım öteye taşımaktadır [8][10][12][14][19].

Docker, TUF (The Update Framework) mekanizmasını kullanarak uygulamaların son güncel sürümünün elde edildiğini doğrular. Bu mekanizma kullanılan içeriklerin güvenilir kaynaklardan elde edildiğinden emin olunmasını sağlamaktadır. Notary (noter) aracı bu uygulamalardan bir tanesidir. Açık kaynak bir uygulama olan Notary ile kullanıcılar kendi anahtarlarını kullanarak imzalama işlemleri gerçekleştirebilmekte ve imaj sahteciliğinin önüne geçilebilmektedir [8][13][20]. DockerHub veya başka bir Docker imaj deposu için bu anahtar-imza mekanizması kullanılarak doğrulama süreci ile bütünlük sağlanabilmektedir.

Varsayılan olarak bir konak üzerindeki tüm konteynerler birbirleri ile iletişime geçebilecek şekilde ağ yapılandırmasına sahiptirler. Tüm konteynerler için bu tür bir gereksinim bulunmaması halinde bu yapılandırma değiştirilebilmektedir. Test için eklenmiş ve unutulmuş konteynerler bu konuda önemli bir risk teşkil etmektedir.

Docker konteynerleri varsayılan olarak okuma, yazma ve çalıştırma haklarına sahip bir şekilde içindeki uygulamaları kullanıma sunmaktadırlar. Bu da konteynerlerin çalışma anında içeriğinin değişebileceği anlamına gelmektedir. Bir konteynerin çalışma anında işlediği verileri konteyner içerisinde bir alana kaydetmesi bu verilerin kaybolması riskini doğurmaktadır. Diğer bir açıdan ele geçirilenbir konteynere zararlı içerik yüklenilmesi durumunda bu konteynerler bünyesindeki zararlı içerikle birlikte kapatılacak, açılacak veya taşınarak çalıştırılmaya devam edecektir. Bu durum konak, diğer konteynerler ve zararlı bulaştırılan konteyner için oldukça tehlikelidir. Docker bu tür risklere karşı sadece-okuma (--read-only) modu geliştirmiştir [1,7-8,13]. Fakat, bazı uygulamalar çalışma anında okuma-yazma işlemine ihtiyaç duyduklarından sadece-okuma izni verilerek çalıştırılmak istenilen konteynerler çalışmayacak veya işlemleri yerine getiremeyecektir. Bu durum için de konak işletim sistemi ile geçici okuma yazma ihtiyacı olan konteynerler arasında paylaşımlı bir dizin kullanıma sunulabilmektedir. Kalıcı olması gereken veriler içinde benzer bir yöntem uygulanabilmektedir. Bunun sonucunda ise konteyner üzerinden konak işletim sistemine geçiş kolay hale gelerek ortaya yeni bir risk çıkacaktır. Bu riski önlemek için ise konak üzerindeki paylaşımlı klasörün Linux geçici veri tutan klasörlerlerinden birisi olarak ayarlanması önem arz etmektedir.

Docker konteyner dizin yönetiminde olduğu gibi ağ iletişiminde de benzer bir yöntem kullanılmakta ve çeşitli güvenlik problemleri yer almaktadır. Docker ağ bağlantısını varsayılan olarak sanal ethernet köprüsü (virtual ethernet bridge) olarak atamaktadır [21]. Her konteyner için ayrı bir ağ katmanı oluşturmakta ve her bir konteynere ayrı IP adresi, ayrı yönlendirme tablosu ve ağ aygıtı atamaktadır. Bu sayede konteynerler birbirleri arasında ağ arayüzlerine bağlanarak

iletişim kurabilmektedir. Varsayılan olarak atanan bu ağ arayüzleri "ortadaki adam" ve ARP sahtekarlığı (spoofing) saldırılarına karşı konteynerleri savunmasız bırakmaktadır [22][23]. Bu tür saldırılara karşı savunma sunan çözümler ve mekanizmalar bulunmaktadır. Docker ağ bağlantısı yöntemi değiştirilebileceği gibi Cilium, Calico ve AppArmor gibi çeşitli harici araçlar ile bu güvenlik mekanizmasının sağlanabildiği belirtilmektedir [24]. Cilium bu işlemi BPF ismi verilen bir yöntem ile gerçkleştirirken bu kabiliyeti ancak Linux çekirdeğinin 4.8.0 versiyonundan sonraki dağıtımlarda sağlayabilmektedir. Calico ise bu süreçleri bir güvenlik duvarı gibi çalışarak ve erişim kontrol listeleri tutarak gerçekleştirebilmektedir [25].

V. İMAJLARIN STATİK ANALİZİ

Docker imajlarının içeriğindeki paketlerin ve uygulamaların üstverilerinin (metadata) elde edilerek bilinen açıklıklar veritabanında (CVE) karşılaştırılması ile imajların sahip olduğu açıkların bilgisinin elde edilmesi işlemine imajların statik analiz denilmektedir. Daha sonra bu açıklıklar sayılarına ve kritiklik seviyelerine göre incelenerek imajlar üzerinde değerlendirmeler yapılmaktadır. İmajların statik analizi için en yaygın kullanılan açık kaynak uygulamalar; Clair, OpenSCAP, Falco, Dagda, BanyanOps Collector, Dockscan, Anchore ve hub-detect-ws uygulamalarıdır.

Docker firması tarafından sunulan imaj deposu olan DockerHub üzerinde Temmuz 2019 itibariyle yaklaşık 2.5 milyon Docker imajı yer almaktadır [26]. Bu imajlardan bir kısmı Resmi Otorite imajı, bir kısmı Docker firması tarafından onaylı üreticisi firma tarafından derlenen imajlardır. Geriye kalan tüm imajlar kullanıcılar tarafından oluşturup gönderilmiş imajlardır. Örnek olarak Nginx web sunucusu imajı 46 bin imaj isminde geçmektedir. Fakat bunlardan sadece 2 tanesi onaylanmış firma tarafından gönderilmiş, 1 tanesi de Nginx ürünü sahibi firma tarafından yüklenmiş imajdır. Kalan tüm diğer imajlar kullanıcıların paylaştığı imajlardır.

Kullanıcılar tarafından kullanılabilen DockerHub, resmi imajlar ve kullanıcılar tarafından oluşturulmuş imajların yanı sıra "zehirlenmiş imajlar" [7][8][11][13] da içermektedir. Yapılan çalışmalara göre kullanıcılar tarafından gönderilen bazı imajların belirtilen amacı gerçekleştirmesinin yanı sıra zararlı içerik yayma amacıyla oluşturulduğu tespit edilmiştir. Docker firmasının ücretsiz olarak sunduğu hizmet ile ticari imaj depolarındaki imajlar bilinen zafiyetlere karşı sürekli olarak taranmaktadır. Tüm kullanıcılara açık imajlar için bu mekanizma sunulmamaktadır.

Statik kod analizi gerçekleştirilerek yapılan çalışmalar en sık kullanılan resmi imajlarda dahi birçok zafiyetin ve bilinen açıklıkların yer aldığını göstermektedir. Duarte ve arkadaşları tarafından yapılan bir çalışmaya göre her imajda bir tanesi kritik seviyeli açıklık olmak üzere toplamda ortalama 70 adet açıklığın yer aldığını göstermektedir [9].

BanyanOps aracı kullanılarak gerçekleştirilen bir çalışmaya göre ise resmi imajların %30'unda kritik seviyede açıklık bulunduğu sonucu elde edilmiştir [27].

Statik zafiyet analizi gerçekleştirilen farklı bir çalışmada ise OpenSCAP uygulaması ve Vulners çevrimiçi uygulaması değerlendirilmiş fakat OpenSCAP uygulamasının sadece RedHat tabanlı imajları desteklemesi; Vulners uygulamasının ise Alpine Linux tabanlı imajları desteklememesi nedeniyle bu uygulamaların kullanılamadığı belirtilmiştir [28]. Outpost24 isimli ticari bir araç kullanılarak en popüler 1000 imaj arasından işletim sistemi desteklenen 831 adet imajın statik analizi gerçekleştirilmiştir. İşletim sistemleri arasında %35 oran ile en çok tercih edilen işletim sisteminin Ubuntu olduğu belirtilmiştir. 169 imaja ait işletim sistemi üstverisinin bilgisinin elde edilemediği; 44 imajın işletim sisteminin ise bu uygulama tarafından desteklendiği belirtilmiştir.

TABLE I. OUTPOST24 ARACI İLE TARANAN İŞLETIM SISTEMLERI [28]

Dağıtım	Sayısı
Ubuntu	289
Alpine Linux	239
Debian	225
CentOS	34
Diğer	44
Toplam	*831*

Taranan 1000 imaj üzerinden tespit edilebilen değerler

Taranan 787 imaj üzerinden oran olarak en çok açıklık bulunan işletim sisteminin Debian olduğu tespit edilmiştir [28]. Tespit edilen açıklıklara dair bilinan açıklıklar veritabanındanki kritiklik seviyesi göz önünde bulundurularak derecelendirme yapılmıştır. Uzaktan kod çalıştırılmasına olanak sağlayan açıklıklar için en kritik açıklık değerlendirilmesi yapılmaktadır. Tespit edilebilen açıklıkların işletim sistemlerine ve açıklıkların kritiklik seviyelerine göre dağılımı Tablo 2'de gösterilmektedir.

TABLE II. AÇIKLIKLARIN İŞLETIM SISTEMINE GÖRE DAĞILIMI [28]

Dağıtım	Elde Edilen İstatistik	
	Toplam açıklık	***En kritik açıklıkların oranı***
Ubuntu	65 314	%78
Debian	46 667	%83
CentOS	774	%29
Alpine Linux	283	%0
Toplam	113 038	%54

Elde edilen değerlerin ve istatistiklerin doğrulaması ayrıca bir zafiyetli işletim sistemi imajı oluşturarak test edilmiş ve doğrulanmıştır [28]. İstatistiklere göre imajların %70'inin yüksek seviye; %54'ünün ise kritik seviye güvenlik açığına sahip olduğu belirtilmektedir [28]. Bu değerlerin BanyanOps kullanılarak gerçekleştirilen çalışmadaki istatistiklerden daha yüksek olduğu karşılaştırması çıkartılmaktadır. Değerlere göre Alpine Linux işletim sisteminin diğer işletim sistemlerine göre daha güvenli olduğu vurgulanmıştır.

Tak ve arkadaşları tarafından gerçekleştirilen çalışmada imaj oluşturmada kullanılan işletim sistemlerinin içerdiği paketlere göre zafiyet sayıları ve oranları tespit edilmiştir [29].

Taranan toplam 10.000 imajın işletim sistemlerine göre dağılımı daha önceki çalışmalara göre yüksek oranda farklılık göstermiştir. Bunun sebebi olarak ilk 1000 imajın yoğunlukla resmi üreticiler tarafından oluşturulan imajlar olması sebebiyle kaynaklandığı düşünülmektedir. 10.000 imajın işletim sistemlerine göre dağılımı Tablo 3'te gösterilmektedir.

TABLE III. DOCKERHUB ÜZERINDEKI EN POPÜLER 10.000 İMAJIN İŞLETIM SISTEMLERI [29]

Dağıtım	Sayısı	Oranı
Debian	3189	%31.7
Alpine Linux	2896	%28.8
Ubuntu	2634	%26.1
CentOS	766	%7.6

Taranan 10.000 imaj üzerinden tespit edilebilen değerler

Alpine Linux, Debian ve Ubuntu işletim sistemlerinin 10.000 imaj arasından toplamda %87'lik bir paya sahip olduğu kaydedilmiştir. Taranan 10.000 imaj içerisindeki zafiyete sebep olan en çok 10 paketin listesi elde edilmiştir. Buna göre açıklığa sebep olan Perl yazılım paketinin ilk 10.000 imaj arasında en yoğun kullanılan paket olduğu tespit edilmiştir [29]. En sık kullanılan ilk 10 zafiyetli paket Tablo 5'te gösterilmektedir.

TABLE IV. EN SIK KULLANILAN İLK 10 ZAFIYETLI PAKET LISTESI [29]

Paket	Bulunduğu İmaj Sayısı	Oranı
perl	3122	%47.4
sensible-utils	3007	%45.6
openssl	2845	%43.2
libssl1.0.0	2400	%36.4
curl	2385	%36.2
libxml2	2064	%31.3
libtasn1-6	1947	%29.5
gnupg	1926	%29.2
libgrypt20	1867	%28.3
wget	1845	%27.8

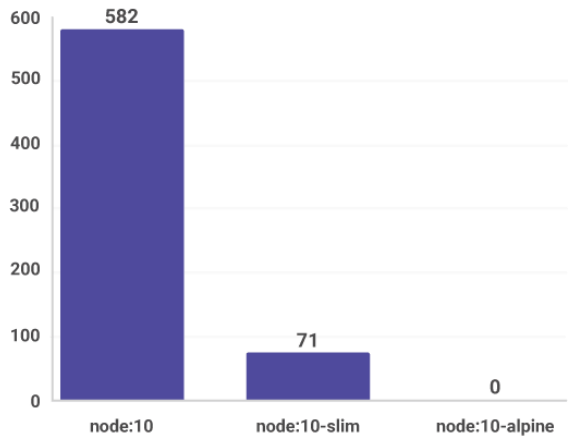
Paketlerin işletim sistemine göre dağılımı incelendiğinde Ubuntu'nun libssl1.0.0, Debian'ın openssl ve CentOS'un libstdc++ paketleri nedeniyle genellikle zafiyetli olarak işaretlendiği görülmüştür. Taranan 10.000 imajın arasından %99'unun en az beş Docker uyumluluk kuralına uymadığı; tüm imajlardan %92'sinin ortalama 10 zafiyeti bünyesinde barındırdığı tespit edilmiştir [29].

Zerouali ve arkadaşları tarafından gerçekleştirilen Debian tabanlı imajların statik analizi yapılarak üzerlerindeki hatalı paket ve kod parçacığı içeren imajlar hakkında çıkartımlar gerçekleştirilmiştir. Elde edilen tespite göre 7380 en popüler imajın tamamında en az bir kritik seviye zafiyet olduğu belirtilmiştir [30]. Bu durumun sebebi olarak Debian'ın son sürümü olan Stretch dağıtımını kullanan imajların dahi eski sürüm paketler içerdiği ve bu paketlerin güncellenmemesi nedeniyle bu yönde bir sonuç elde edildiği kaydedilmiştir. Ek olarak hatalı kod parçacığı içeren paketlerin çözümünün henüz paket üreticisi tarafından giderilmediği bilgisi belirtilmektedir.

Özel bir yöntem geliştirilerek statik imaj analizi gerçekleştirilen farklı bir çalışmada 85000 imajın farklı versiyonlarıyla birlikte 356000 dağıtımı analiz edilmiştir [31]. DIVA ismi verilen bu yöntem olarak DockerHub üzerindeki imajları keşfetmekte, indirmekte ve analiz etmektedir [31]. Clair tarama uygulaması 1.0 sürümü ve veritabanı olarak PostgreSQL Docker imajı tercih edildiği belirtilmiştir. Clair, imajın içeriğindeki paket sürümleri ve işletim sistemi üstverisini dikkate alarak zafiyet veritabanlarından eşleştirme yöntemi ile çıktı vermektedir. Çalışmada belirtildiği kadarıyla Ubuntu CVE, Debian ve RedHat Güvenlik Takip sistemini kullanarak eşleştirmeler gerçekleştirmiştir. İmajlardaki açıklıklara en çok sebep olan paketlerin; glibc, util-linux, shadow ve perl olduğu tespit edilmiştir. Çalışmada güvenlik açıklıkları ile imajların güncellenme sıklıkları arasındaki ilişkiye değinilmiş ve çıktılar yorumlanmıştır.

- İmajların tüm sürümleri göz önünde bulundurulduğunda dağıtım başına ortalama 180 açıklık görülmektedir.
- İmajların %50'si son 200 gün, %30'u son 400 gün içerisinde bir güncelleme almamıştır.
- Çoğu açıklık imajın oluşturulduğu temel imajdan kaynaklanmaktadır.

Gerçekleştirilen farklı bir statik analiz çalışmasında imajların sürümleri arasında açıklık olarak çok fazla farklılıklar olabileceği görülmüştür [32]. Bu durumun sebebi ise uygulamaların bazı sürümlerinin henüz geliştirme aşamasında olduğu ve aktif kullanım için uygun olmadığı belirtilmektedir. Node isimli programlama dili uygulamasının farklı sürümleri arasındaki açıklıklık sayıları dağılımı Şekil 3'de gösterilmektedir [32].



Şekil 3. Node uygulamasının farklı sürümlerindeki açıklık sayıları [32]

Node uygulaması DockerHub sayfası üzerinde ilgili uygulamayı kullanacaklar için 10-alpine etiketli sürümün kullanması uyarısı yer almaktadır. Diğer sürümlerin henüz geliştirme aşamasında olduğunu düşünülerek tercih edilmemesi güvenlik açısından öneme sahiptir.

A. Docker Mimarisi Statik Kod Analizi

Docker mimarisi içeriğinde 2014-2019 yılları arasında 20 adet zafiyet tespit edilmiştir [33]. Bu zafiyetlerden iki tanesi en üst seviye olan 10 seviyesi açıklık; dört tanesi ise yedi seviyesi açıklık olarak kayda geçmiştir.

Go programlama dili ile yazılmış olan Docker mimarisinin kodlarının statik analizinin gerçekleştirildiği çalışmaya göre kod mimarisinde bir güvenlik problemi bulunamadığı belirtilmiştir [9]. Buna karşın kod yapısında çeşitli boşlukların olduğu ve buna ek olarak statik kod analizi gerçekleştiren Go Meta Linter ve Go Reporter uygulamalarının yeterince başarılı olmadıkları sonucuna ulaşılmıştır [9].

VI. SONUÇ VE DEĞERLENDİRME

Yapılan araştırmalar sonucunda Docker konteyner uygulamasını üzerine gerçekleştirilen güvenlik çalışmaları incelenerek tespit edilen güvenlik tehditleri ve riskler incelenmiştir.

Konak işletim sisteminin güvenliğinin sağlanması üzerine yapılan çalışmalarda genellikle çekirdek sıkılaştırma mekanizmaları üzerinde durulduğu görülmektedir. Konteynerlerin üzerlerinde bulundukları konak işletim sistemi çekirdeğini kullanması performans açısından büyük katkı sağlasa da güvenlik açısından daha büyük riskler taşımaktadır.

Docker'ın kod mimarisi üzerine gerçekleştirilen çalışmalara göre ilk kararlı sürümü üzerinden beş yıl geçmesine rağmen henüz boşlukların yer aldığı belirtilmektedir. Güncel sürümünde aktif çalışmasını etkileyecek bir sorun veya tehdit yer almadığı belirtilse sıfırıncı gün açıkları için önleyici çözümlerin geliştirilmeye çalışıldığı görülmektedir.

Docker üzerine gerçekleştirilen güvenlik çalışmalarının yoğunlukla imajların statik analizi üzerine olduğu kaydedilmiştir. Ticari ve açık kaynak olmak üzere çeşitli uygulamaların geliştirildiği görülmüştür. Konteyner uygulamalarındaki farklılıklar nedeniyle belirli testlerin uygulanamaması kullanıcıları imaj bilgilerinden elde edilen veriler sonucunda bilgi edinmeye götürmüştür. İmajların içeriğindeki paketlerin ve uygulamaların üstverileri ile işletim sistemi bilgileri incelenerek bilinen açıklıklar veritabanlarından elde edilen karşılaştırmalar ile sonuçlar elde edilebilmektedir.

Elde edilen istatistikler Docker teknolojisindeki en büyük riskin güvenilir kaynaklardan elde edilmeyen imajlar olduğunu açık bir şekilde göstermektedir. İmajların güncel tutulması ve derlenmeleri sırasında Docker uyumluluk kurallarına uyularak derlenmesi önerilmektedir.

Gerçekleştirilen çalışmalar Docker firmasının güvenlik açısından üzerine düşen gereklilikleri sağladığı fakat konak işletim sistemi, konteyner içerisindeki yazılım kütüphaneleri gibi Docker harici faktörlerin güvenlik konusunda büyük riskler teşkil ettiği tespit edilmiştir. Kullanıcıların Docker kullanımı konusunda bilinçli bir şekilde gerekli yapılandırmaları sağlaması, konak güvenliği ve imaj güvenilirliği konusunda dikkatli olması durumunda güvenliğin belli bir seviyede sağlanabileceği söylenebilmektedir.

İleri çalışmalarda Docker imajlarını statik olarak analiz etme işlemi için incelenen çalışmalardaki üstveri bilgisi kullanımından farklı bir metod geliştirilmesi düşünülmektedir.

REFERANSLAR

[1] Mavridis, I., & Karatza, H. (2019). Combining containers and virtual machines to enhance isolation and extend functionality on cloud computing. Future Generation Computer Systems, 94, 674-696.

[2] *İnternet: https://www.opencontainers.org/about/members Son Erişim Tarihi: 31.07.2019.*

[3] *İnternet: https://www.linuxfoundation.org/projects/cloud/ Son Erişim Tarihi: 31.07.2019.*

[4] Pittenger, M. (2016). Addressing the security challenges of using containers. Network Security, 2016(12), 5-8.

[5] Bui, T. (2015). Analysis of docker security. arXiv preprint arXiv:1501.02967.

[6] Rad, B. B., Bhatti, H. J., & Ahmadi, M. (2017). An introduction to docker and analysis of its performance. International Journal of Computer Science and Network Security (IJCSNS), 17(3), 228.

[7] Martin, A., Raponi, S., Combe, T., & Di Pietro, R. (2018). Docker ecosystem–vulnerability analysis. Computer Communications, 122, 30-43.

[8] Gallagher, S. (2016). Securing Docker. Birmingham, United Kingdom. Packt Publishing Ltd.

[9] *Duarte, A. F. S. (2018). Security Assessment and Analysis in Docker Environments (Yüksek Lisans Tezi).*

[10] *De Lucia, M. J. (2017). A survey on security isolation of virtualization, containers, and unikernels (No. ARL-TR-8029). US Army Research Laboratory Aberdeen Proving Ground United States.*

[11] Lin, X., Lei, L., Wang, Y., Jing, J., Sun, K., & Zhou, Q. (2018, December). A measurement study on linux container security: Attacks and countermeasures. In Proceedings of the 34th Annual Computer Security Applications Conference (pp. 418-429). ACM.

[12] Jian, Z., & Chen, L. (2017, March). A defense method against docker escape attack. In Proceedings of the 2017 International Conference on Cryptography, Security and Privacy (pp. 142-146). ACM.

[13] Upadhya, S., Shetty, J., Raja Rajeshwari, H. S., & Shobha, D. G. (2016). A State-of-Art Review of Docker Container Security Issues and Solutions. American International Journal of Research in Science, Technology, Engineering & Mathematics, ISSN (Print), 2328-3491.

[14] Manu, A. R., Patel, J. K., Akhtar, S., Agrawal, V. K., & Murthy, K. B. S. (2016, March). A study, analysis and deep dive on cloud PAAS security in terms of Docker container security. In 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT) (pp. 1-13). IEEE.

[15] MP, A. R., Kumar, A., Pai, S. J., & Gopal, A. (2016, July). Enhancing security of docker using linux hardening techniques. In 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT) (pp. 94-99). IEEE.

[16] Sultan, S., Ahmad, I., & Dimitriou, T. (2019). Container Security: Issues, Challenges, and the Road Ahead. IEEE Access, 7, 52976-52996.

[17] Arnautov, S., Trach, B., Gregor, F., Knauth, T., Martin, A., Priebe, C., Goltzsche, D. (2016). {SCONE}: Secure Linux Containers with Intel {SGX}. In 12th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI} 16) (pp. 689-703).

[18] Truyen, E., Van Landuyt, D., Preuveneers, D., Lagaisse, B., & Joosen, W. (2019). A comprehensive feature comparison study of open-source container orchestration frameworks. Applied Sciences, 9(5), 931.

[19] Dua, R., Raja, A. R., & Kakadia, D. (2014, March). Virtualization vs containerization to support paas. In 2014 IEEE International Conference on Cloud Engineering (pp. 610-614). IEEE.

[20] *İnternet: https://docs.docker.com/notary/service_architecture/ Son Erişim Tarihi: 31.07.2019.*

[21] Catuogno, L., & Galdi, C. (2016, December). On the evaluation of security properties of containerized systems. In 2016 15th International Conference on Ubiquitous Computing and Communications and 2016 International Symposium on Cyberspace and Security (IUCC-CSS) (pp. 69-76). IEEE.

[22] Yasrab, R. (2018). Mitigating docker security issues. arXiv preprint arXiv:1804.05039.

[23] Chelladhurai, J., Chelliah, P. R., & Kumar, S. A. (2016, June). Securing docker containers from denial of service (dos) attacks. In 2016 IEEE International Conference on Services Computing (SCC) (pp. 856-859). IEEE.

[24] Ranjbar, A., Komu, M., Salmela, P., & Aura, T. (2017, May). Synaptic: Secure and persistent connectivity for containers. In 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID) (pp. 262-267). IEEE.

[25] *İnternet: https://sysdig.com/blog/20-docker-security-tools/ Son Erişim Tarihi: 31.07.2019.*

[26] *İnternet: https://hub.docker.com/ Son Erişim Tarihi: 31.07.2019.*

[27] *İnternet: https://www.infoq.com/news/2015/05/Docker-Image-Vulnerabilities/ Son Erişim Tarihi: 31.07.2019.*

[28] *Henriksson, O., & Falk, M. (2017). Static vulnerability analysis of docker images. Blekinge Institute of Technology, Karlskrona, Sweden. (Yüksek Lisans Tezi).*

[29] Tak, B., Kim, H., Suneja, S., Isci, C., & Kudva, P. (2018, June). Security Analysis of Container Images Using Cloud Analytics Framework. In International Conference on Web Services (pp. 116-133). Springer, Cham.

[30] Zerouali, A., Mens, T., Robles, G., & Gonzalez-Barahona, J. M. (2019, February). On the Relation between Outdated Docker Containers, Severity Vulnerabilities, and Bugs. In 2019 IEEE 26th International Conference on Software Analysis, Evolution and Reengineering (SANER) (pp. 491-501). IEEE.

[31] Shu, R., Gu, X., & Enck, W. (2017, March). A study of security vulnerabilities on docker hub. In Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy (pp. 269-280). ACM.

[32] *İnternet: https://snyk.io/blog/top-ten-most-popular-docker-images-each-contain-at-least-30-vulnerabilities/ Son Erişim Tarihi: 31.07.2019.*

[33] *İnternet: https://www.cvedetails.com/vulnerability-list/vendor_id-13534/product_id-28125/Docker-Docker.html Son Erişim Tarihi: 31.07.2019.*

Improving PKI, BGP, and DNS Using Blockchain: A Systematic Review

Parça Zinciri ile PKI, BGP ve DNS İyileştirmeleri: Sistematik Bir İnceleme

Faizan Safdar Ali, Alptekin Küpçü
Computer Science and Engineering, Koç University, İstanbul, TURKEY
{fali18,akupcu}@ku.edu.tr

***Abstract*—The Internet has many backbone components on top of which the whole world is connected. It is important to make these components, like Border Gateway Protocol (BGP), Domain Name System (DNS), and Public Key Infrastructure (PKI), secure and work without any interruption. All of the aforementioned components have vulnerabilities, mainly because of their dependence on the centralized parties, that should be resolved.**

Blockchain is revolutionizing the concept of today's Internet, primarily because of its degree of decentralization and security properties. In this paper, we discuss how blockchain provides nearly complete solutions to the open challenges for these network backbone components.

***Keywords*—Blockchain, Internet, BGP, DNS, PKI.**

***Öz*—Dünya çapında bağlantı sağlayan İnternet çeşitli omurga bileşenlere sahiptir. Sınır Geçidi Protokolü (BGP), Alan Adı Sistemi (DNS) ve Açık Anahtar Altyapısı (PKI) gibi bileşenlerin güvenli hale getirilerek ve kesintisiz çalışmalarının sağlanması. Bu bileşenlerin özellikle merkezi otoritelere olan bağımlılıkları nedeniyle çözülmesi gereken zayıf noktaları vardır.**

Parça zinciri dağıtık çalışma ve güvenlik özellikleri nedeniyle günümüzün İnternet kavramında devrim yaratan bir yapıdır. Bu makalede, parça zincirinin belirtilen omurga bileşenlerdeki sıkıntılara nasıl neredeyse bütüncül çözümler sunduğunu tartışıyoruz.

***Anahtar Sözcükler*—Parça Zinciri, Blokzincir, İnternet, BGP, DNS, PKI.**

I. Introduction

The first design of the Internet was presented as a centralized single entity. With time, the Internet was divided into subsystems (e.g., DNS, BGP, PKI). Still, these components were built on a centralized architecture. This introduces security, privacy, and performance issues such as a single point of failure, trust issues, high latencies, and storage [1]. This results in these centralized services getting hacked frequently. Efforts were put in to make the services distributed [2]. These improved the Internet by solving the above-mentioned challenges but introduced new types of issues like scheduling, resource allocation, coordination, device management, scalability, security, trust, and multiple weak points of contact for attackers [2]. The overall performance was decreased because of the replication of work, backups, and the communication of distributed parts of the overall system [2]. Recently, blockchain-based solutions were introduced, with the goal being improving security while keeping the speed, cost and correctness comparable to the legacy components presented in Table I. We can see that the current protocols take less time and cost (as most of the vendors have already implemented them) and achieve the desired (correct) results. For example, DNS protocol will always give the IP (Internet Protocol) address of the domain name, unless it malfunctions or is attacked. But the security of these components is vulnerable to the attacks and should be improved as described in sections III to V.

Table I: Legacy Protocol Performance

Protocol	Time per query	Security	Correctness	Cost
DNS	0.048s [1]	Needs improvement	High	Low
BGP	38s for 100% propagation [2]	Needs improvement	High	Low
PKI	Within few milliseconds [3]	Needs improvement	High	Low

A blockchain is a public distributed ledger that can record transactions that are connected using a cryptographic hash function [3]. The basic functionality provided by a blockchain is a secure mechanism for storing and obtaining data, ordered by the timestamp of each record in the data, in a publicly verifiable and immutable manner. For that reason, in most of the system architectures, blockchain provides a storage mechanism for data collection and consensus among participants. In general, blockchain can help in (1) decentralization, (2) provenance and immutability of data, (3) security, and (4) heterogeneity and programmability.

Our contributions: In this paper, we first overview the blockchain technology, then provide a discussion of three widely-employed Internet components (PKI, BGP, DNS) and their security vulnerabilities, afterward showing a detailed explanation of the available blockchain-based solutions, and conclude with a summary and open issues.

II. Blockchain Technology

A blockchain is a decentralized, distributed, and public digital ledger that records data in the form of transactions across multiple devices to enforce immutability, except with a very

[1] https://wp-rocket.me/blog/test-dns-server-response-time-troubleshoot-site-speed

[2] http://www.circleid.com/posts/how_a_routing_prefix_travels_through_the_internet

[3] https://blogs.technet.microsoft.com/option_explicit/2012/04/19/validating-a-certificate/

small probability of the adversary controlling a large fraction of the processing power, stake, etc. A blockchain can be split into *network*, *consensus*, *storage*, *view*, and *side* planes [4], enabling researchers to work on a single idea while improving the overall blockchain infrastructure.

Hash Function: Blockchain is built upon collision-resistant deterministic hash functions that map an arbitrary-length input to a fixed-length n-bit output. The hash function should have the property of collision resistance, meaning that an adversary cannot find two different inputs mapping to the same output in polynomial time. This property is important for the integrity and immutability of blockchain.

Transactions and Blocks: The 'transaction' term was first used by Bitcoin [3], where a transaction contains the amount of Bitcoin value transferred between entities and information of the sender and the receiver. Generally, a transaction is data or information of the variant type and can be created by any participant.

Blocks are created by the verifiers (miners). A block is a set of approved transactions, along with a timestamp and a hash pointer to the previous block. The first block of a blockchain is called the Genesis Block. The genesis block is almost always hardcoded with a verifiable universal fact and does not refer to a previous block. As shown in Figure 1 hashes of all transactions are kept in a Merkle tree for efficient memory management [5]. For example *Hash0* is the hash of transaction *Tx0*, *Hash1* is the hash of transaction *Tx1*, *Hash01* is the hash of *Hash0* and *Hash1*, and eventually we have the Merkle root hash *Tx_Root*. The block also contains the hash of the previous block (*prev_hash*). Thus, it is computationally infeasible to modify or tamper with the contents of the previous blocks, as this would require finding the hash of all of the remaining blocks to keep the chain connected.

Types of Blockchains. In a blockchain, entities can be readers or writers (writers can be of two types, data owners, who create transactions, and verifiers, who create blocks). Depending on the permissions of these entities, a blockchain can be divided into two groups. In **Permissionless Blockchain**, an entity does not require permission to become a reader or writer like Bitcoin [3] and Zerocash [6]. Whereas in **Permissioned Blockchain**, a centralized entity grants permission to the users to be the readers or writers (e.g., Hyperledger [7]).

Consensus Protocols. Blockchain presents a solution for the environment where the parties do not have to trust each other and collaborate. As there is no universal trusted third party, each blockchain has to have a consensus protocol for reliability and consistent state of the network.

Proof of Work (PoW): In PoW, a node can get its block accepted if it can solve a cryptographic puzzle (hash) and spend some computational resources in the process. It was first implemented by Bitcoin [3].

Proof of Stake (PoS): A node is randomly selected depending upon the stake/resources (ether in Etherium [8]) she has. Then its block is accepted to be appended to the chain.

Byzantine Fault Tolerance (BFT): In Practical BFT (PBFT) [9], there is a leader election (where each entity participates) to elect an entity that has authority to add a new transaction in

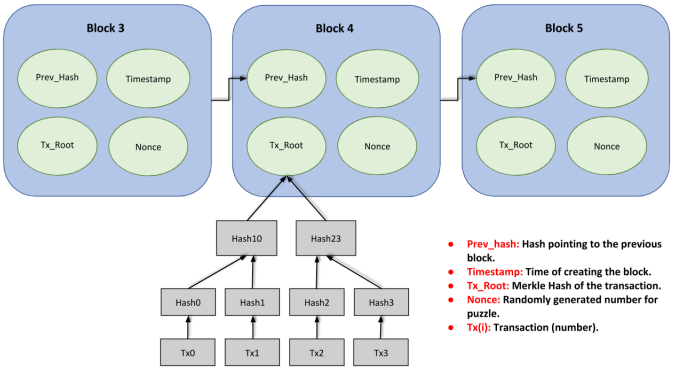


Figure 1: Sample blockchain blocks and transactions.

the chain. This protocol assumes that there more than 2/3 of the honest participants. In Delegated BFT (DBFT) [10], participants, by voting, pick the delegate they support. The selected delegates, through the BFT algorithm, reach a consensus and generate new blocks.

Problems. Blockchain presents a new perspective on Internet security, but the traditional Bitcoin blockchain (which is used as the solutions discussed in the upcoming sections show) still has issues regarding huge power, energy, storage, and communication requirements [11] (current Bitcoin blockchain is around 200 GB). Moreover, the Bitcoin blockchain is secure assuming that more than 50% of the hashing power belongs to the honest parties in the system. There are further attacks on the incentive mechanism, such as selfish mining [12].

III. PKI

Earlier, anyone could pretend to be anybody over the Internet as none of the Internet layers verifies the identity of the entity over the network. This created privacy and trust issues. As a solution, Secure Socket Layer (SSL) and Transport Layer Security (TLS) were introduced. The concept is to provide data integrity, confidentiality, and authenticity using a public/private key pair. But these keys can be compromised. Then another idea was introduced to create cryptographic identities known as digital certificates. Digital certificates contain the identity and public keys of the entity to be used for encryption and authentication. The problem remained that it is very easy to create a digital certificate by self-signing it. There was a need of having a trusted third party that can provide these certificates, now known as a Certificate Authority (CA). CA is a trusted entity that issues digital certificates that verify a digital entity's identity over the Internet. The infrastructure to manage, store and distribute these certificates is called the Public Key Infrastructure (PKI).

A CA signs a certificate to bind the public key of a server to its identity. Then SSL/TLS uses these certificates to authenticate the web-server. Trusting the CA, the browser obtains the server's public key to establish a secure connection. There are two types of certificate authorities **ROOT-CA** and **SUB-CA**. The certificate is trusted if it is signed by ROOT-CA. The browsers or operating systems come with many ROOT-CA public keys stored in their databases. As ROOT-CAs might

be limited in number and become bottle-neck when there is a lot of demand, there are SUB-CAs that can sign the certificates. PKI works on *Chain of Trust*. To authenticate a certificate, the browser (or any other entity) checks whether or not the certificate is signed by a valid ROOT-CA. If the signer is a SUB-CA, the validation continues in a chain up to the ROOT-CA. Recent research indicates that CAs can be dishonest, get attacked, or can be using faulty or outdated cryptographic algorithms [13]. Which effects the security of PKI.

Currently, there are two types of approaches for the security of PKI. **Log Based PKI:** Highly available servers are appointed for publishing and secure monitoring of the certificates to ensure that CAs do not behave maliciously. Still, there are issues with log-based solutions like revocation explained in [14]. **Web of Trust (WoT):** is a decentralized approach. Users can put their trust in another entity by signing their certificate. Then each trusted entity keeps a certificate that contains signatures of the users that trusted it, in addition to its public key.

Limitations of PKI security and the advantages of using blockchain to enhance the security and efficacy of PKI is given by [15]. The architecture assumes the existence of blockchain-backed PKI and uses it to secure the critical (rich) credentials. A privacy-aware PKI system based on blockchain was presented by [16]. The paper claims that there are many instances (like anonymous social forums), where the entity does not want to reveal its identity. Current PKI leaks this information by knowing which key is used in the protocol. The paper uses blockchain to have online and offline keys and encryption to hide the identity of the user. [17] proposes Etherium-based blockchain technology to build secure PKI systems, resolving the issues of log-based PKI and the WoT approaches. Blockchain resolves the single point of failure issue and the need for a newcomer to prove its trustworthiness.

Certificate Transparency (CT) was introduced by [18], using an append-only public log, to improve the accountability of CAs. As certificates are publicly recorded in the log servers, a fraudulent certificate can be detected, and the countermeasures can be taken to handle the potential attack. Though this removes the central authenticating entity [18], considering the increasingly huge number of current certificates, it may introduce computation and communication burden on both clients and servers [19]. Moreover, it is shown that *split-world* attack can be performed on CT [20], where the attacker presents different views of the log to successfully impersonate as the victim. Another issue with CT is that it is not a privacy-preserving scheme [21]. Certificate Revocation is another phenomenon that reduces the efficacy of these solutions as stale certificates can be used by attackers [20].

[22] gives an approach to detect the man-in-the-middle (MITM) attack happened/happening to a victim client. The concept of notary nodes is used, where the server connects and requests the observation of its certificate. In [23] public notaries are used by the client, hence replacing the dependence on the web browsers/operating systems to validate the certificates. In [22], the MITM can be detected but cannot be prevented, and in [23], the users still have to rely on the notaries (which can all be compromised).

[13] proposes a blockchain-based solution to construct certificate transparency. The certificates are published as transactions in a global blockchain by the web servers, which is downloaded by browsers. To verify a certificate, the browser just has to see if the certificate is in the blockchain. As the certificates of the authorities are also published, the CAs are also publicly accountable. This creates more trust and decreases the possibility of having a fraudulent CA. Each certificate has a period of validity and can be revoked at will by omitting it from the next block and hence putting into a certificate revocation list (CRL).m In this solution, compromised CA can be detected two ways. One is that other CAs will not approve of its transactions. Secondly, the target server will only publish the certificates from valid CAs and the fraudulent certificates will not be appended to the global chain. As the attacker fails to impersonate the target server, a wrong certificate will not be publicized even if the Publishing Key Pair is compromised. In the case both PK and CA are compromised, the countermeasures are taken within a period before the certifiers certify the change. Still, the attacker may prevent the browser from obtaining the blockchain, which is difficult in such a distributed setting. Second, there can be forks introduced but unless more than 1/3 of the certifiers are malicious, then this is not possible either [13]. However, this scheme has the following drawbacks identified in [20]:

1) An adversary can use unexpired transactions of the revoked certificate to impersonate the victim server; this is a type of a man-in-the-middle attack.
2) The proposal is inefficient in terms of storage and has large headers.
3) The proposal depends on the CAs to publish revocation information of the certificate to the blockchain but the compromised CA might not issue Certificate Revocation information to the public.

CertLedger [20] provides a solution that is resilient to split-world attacks, does not depend on CA for the certificate revocation, and preserves the privacy of the clients.

Open Issues: There are still some issues like what is the incentive for the certifiers? What if honest nodes are compromised after joining? What happens when the key pair of the server is compromised?

IV. Border Gateway Protocol (BGP)

Autonomous Systems (AS) are responsible for the routing among their network typologies. Typically, an AS represents a collection of IP prefixes to which data is routed [24]. Sometimes these ASes require a flow of data among themselves to reach the destination not present within individual networks. This data flow is peer-to-peer (P2P) in its nature, and is done through the Border Gateway Protocol (BGP) [25]. In BGP, an AS announces the IP prefix of all the IPs reachable through itself, together with path delay metrics. All the other Internet Service Providers (ISPs) behind ASes update their routing tables according to the BGP announcement. Although efficient in practice, ASes assume that their neighboring ASes behave honestly and propagate correct routing information (without having the global knowledge). However, the interests of ASes

may conflict, and this weak notion of trust can be breached by malicious ASes (e.g. *prefix hijacking* [24]).

Previous efforts have developed many solutions like Secure BGP (S-BGP) [26], Secure Origin BGP (SoBGP) [27], Inter-domain Route Validation (IRV) [28] and Path-End Validation [29]. Each of them depends upon a central trusted entry, which has a huge cost of management and is complex. Also, these solutions depend upon the PKI, which has the vulnerabilities described in the previous section. Another problem is the lack of adoption of these protocols as they introduce costly additional infrastructure for their operation. To avoid the cost of adoption, ASes and ISPs are reluctant to migrate towards these solutions despite the known security threats and their clear benefits.

BGP is open to different kinds of attacks. In **BGP route manipulation** attack, an adversary manages to change the BGP table to disrupt the traffic of the Internet. Whereas in **BGP route hijacking**, an attacker AS announces the prefixes belonging to the victim. As a result, the traffic is re-routed to or through the attacker AS. An attacker can also send malicious or faulty BGP traffic to a victim. The victim exhausts its resources to handle the traffic and is left incapable of processing valid BGP traffic. In **Route Leak**, as the result of a potential attack or the AS malfunction, an AS issues incorrect information about the IP addresses on their network. This results in inefficient routing and failures for the traffic.

BGP route hijacking is most dangerous and can be classified into two types: partial attack and complete attack [30]. The partial attack occurs when an adversarial AS announces an identical IP prefix as that of the victim AS. Attack on Youtube in 2008 [24] is an example of partial hijacking. In a complete attack, the adversary AS announces more specific prefixes than the target AS. Since the default forwarding is based on the longest prefix matching, ASes switch to more specific prefixes and start sending the packet through that route. [30]. Figure 2 explains the difference between the attacks. In the partial attack, an attacker would announce the 208.65.153.0/24, which is already announced by AS1. Since the two announcements are the same, when any other AS receives the announcement, it can either switch to it or continue with the old routing path. In the complete attack, an attacker would announce 208.65.153.128/25. This IP has a longer prefix match than 208.65.153.0/24 in the respective finger (for example see finger table of AS3 in Fig. 2b) tables so other ASes would switch to this route. Interestingly, Youtube used the same concept as a legitimate way to get back the traffic in the 2008 attack [30]. Some BGP attack examples include a global route leak in November 2017, a country-wide Internet outage in Japan due to BGP issues in August 2017, and possible financial traffic re-routing in April 2017.[4]

Blockchain-based Solutions: One effort towards securing BGP was to use the PKI presented by IANA [31] to sign the routes. This scheme is problematic as to effectively use PKI, ASes set up a route assigning authority called Routing Origin Authorization (ROA) which is very costly to implement. Also, as we constructed that PKI infrastructure has security

[4]https://securityintelligence.com/bgp-internet-routing-what-are-the-threats/

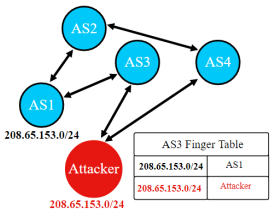


Fig. 2a: Partial Attack

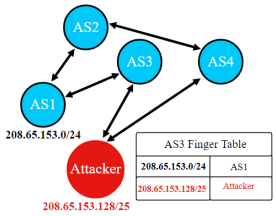


Fig. 2b: Complete Attack

Figure 2: Difference between prefix high-jack attacks

vulnerabilities (section III), signed BGP update messages based on PKI signatures in BGPSec do not result in a secure path verification protocol.

Considering the mentioned problems and the properties of blockchain discussed in Section II, [31] gives a structure of a system that uses blockchain for the better security and performance of BGP. Blockchain helps in the following ways:

1) All transactions occur between peers without any intermediary (like ROA). Also, there is no need for a third party to authentication, eliminating the possibility of tampering or spoofing by a malicious entity.
2) Provides announcement immutability and re-traceability of the chain of BGP routes. Also, a route is validated by multiple parties and is more trustworthy.
3) The authors argue that the blockchain should be different from the Bitcoin blockchain and its properties should depend upon the nature of the use case.

The paper does not provide an implementation and do not discuss the possible attacks and the prevention.

The authors in [24] present a clique-based BGP architecture, RouteChain, to secure BGP against both complete and partial attacks. The method distributes the ASes into subgroups. The system has a global blockchain, and each subgroup has its own private-permissioned blockchain. The main purpose of this sharding is to reduce the storage overhead of having only one global chain and to decrease the transaction validation which is critical for the timely detection of a potential attack. The ASes are grouped based on their geographical proximity for low delays. All groups select a leader to randomly to announce the local routes to the global chain. They use local collaboration among ASes to prevent the complete attack. Whenever there is an update, all the ASes in the group check if their path changes with the update. If it does, they observe the original path and its corresponding prefix. Next, they locate the true owner of the prefix through the global blockchain. If the new update does not belong to the true owner, then the update is discarded. The paper claims that the consensus in the partial attack scenario is achieved in 200 milliseconds, and it is 54.23 seconds for the complete attack. Comparing this timing with the attack on Youtube hijacking incident (in which within 20 minutes, 97 ASes were hijacked) RouteChain asserts that the system will notify the ASes about the attack while it is in its initial stages [24]. The protocol runs on top of the current BGP architecture, which makes it adaptable and economical.

Open Issues: In BGP, different ASes have different policies

for sharing the route with the other AS or not. For example, if AS1 does not want its traffic to go through AS2, then AS1 will advertise the path that does not include AS2 even if the resultant path is longer. How can blockchain solutions cater to these policies? Can different blockchain architectures be used to solve the BGP security issues?

V. Domain Name System (DNS)

The domain name system is used for the resolution of the global domain names. It has a distributed hierarchical design with one root server and 13 specialized servers operated by agencies within a few parts of the world. This design made the system simple, scalable, and flexible. The (in)security of DNS leads to many advanced attacks on DNS including DNS spoofing/cache poisoning, DNS hijacking, and DNS rebinding. A DNS DDoS attack in October 2016 brought down many of the websites including Netflix, Twitter, and CNN [39].

DNSSec is crucial for providing origin authentication and message integrity to communication between the user and the name server. In DNSSec, the root server sends the certificate containing the public key of the next name server along with the IP address of the next server and the hash of the entire message (for data integrity). The next server does the same until the IP address for the domain name is found. This protocol solves the problem of authentication and integrity but still suffers from various attacks namely IP fragmentation and DDoS. The most major problem is its slow adoption.

Blockchain-based DNS Alternatives: Namecoin [34] was built with the motivation of removing managing domains to avoid trust in a single entity. Namecoin uses different prefixes to store and map other types of name-value pairs. For example, the "d/" prefix is used for domain names and "id/" is used to register identities. It further uses the virtual .bit top-level domain name that is not officially registered in the current DNS system. This means Namecoin is isolated from the DNS system and users have to install additional resolving software for resolution of the .bit domain names. Just like DNS, Namecoin provides complete functionalities for registering, renewing, and transferring a domain. The developers modified Bitcoin blockchain to store name-value data like transactions, still utilizing the PoW-based mining mechanism for consensus. Namecoin has shown to have some security flaws: for instance, it was found that a single miner consistently had more than 51% of the total computing power on the Namecoin network [33]. In another instance, a Namecoin bug allowed people to steal names from anyone [33]. Performance-vise, [33] experienced a latency spike and throughput drop due to software issues of Namecoin.

Blockstack [33] combines a DNS system with PKI and purely works with the Bitcoin blockchain. To improve the efficiency of the Bitcoin blockchain for handling a large amount of name-value pairs, a separate logical layer, namely virtual chain, is proposed that works on top of the blockchain to maintain the naming system while the underlying blockchain is only used for achieving consensus on the state of the DNS (or any naming system in general) and the integrity of the name-value data records. Blockstack has significant improvements over Namecoin as it increases the data storage capacity considerably and the virtual chain improves the maintenance of the system.

In [39], authors use blockchain to improve the security and performance of DNSSec. The solution decreases the number of keys needed for DNSSec for easy key management and reduction in DNSSec response size. They use the X509 Cloud blockchain network that is used to store X.509 certificates. This allows us to speed up the verification process.

DecDNS [35] gives a blockchain based data storage model for DNS. They also build multiple DNS nodes for further decentralization and addressing single-point-of-failure in DNS resolution. They report 0.006025s response for parallel domain name resolution, which satisfies the DNS performance requirements and shows the potential of using the architecture in the real network for domain name resolutions.

Open Issues: There should be compatibility between the traditional and the blockchain-based DNS architectures for the systems using the conventional methods for DNS, as this leaves performance and security concerns. For example, a query from the blockchain-backed DNS system can be misinterpreted or discarded by a system using a legacy DNS mechanism. How can blockchain-based and traditional DNS mechanisms inter-operate and integrate? This area of the combination of blockchain-based and traditional decentralization mechanisms for name resolution requires more research.

VI. Comparison

We finish with an analysis of the mentioned blockchain-based solutions using three main parameters. **Security:** The level of integrity, confidentiality, and availability introduced by the proposed solutions. **Performance:** The performance of these solutions compared to the legacy solutions. **Resource Constraints:** The speed, storage, and cost constraints involved. Table IIa gives an overview of the proposed solutions per-protocol regarding the analysis parameters.

In Table IIb, we identified the key security aspects between blockchain in general and the currently deployed protocols. Blockchain provides Data integrity by the use of hashing in block construction backed by the public key cryptography (as discussed in Section II) to create trust between trustless entities under the same system.. The blockchain excels in availability as the ledger is distributed globally on different nodes offering robustness against the *single point of failure* problem. Further, blockchain provides fault tolerance, i.e., even if some participants leave the system, fail, or get attacked, the blockchain system is not affected as each participant has (more or less) the same copy of the ledger.

Looking at the drawbacks, we can see that the contents of the records in blockchain are transparent and costs confidentiality to the users considering to opt for blockchain solutions. Furthermore, as discussed in [11], blockchain requires lots of storage and computational resources, which come at a high cost and decreased scalability. Furthermore, the blockchain can be attacked (for example using selfish mining [12]). With the ever-increasing use of the Internet, this issue needs to be solved using better optimizations of currently available blockchain systems, such as LightChain [42].

Table II: Overall analysis of blockchain based solutions

Protocol	Solutions	Hashed Data	Security	Performance	Resources Constraints
PKI	[32], [33], [34], [35], [20]	TLS Certificates	Improved	Comparable	Storage and computational costs
DNS	[36], [37], [38], [39]	Domain Names	Improved	Comparable	Same as of blockchain
BGP	[40], [31], [41]	Domain Routes	Improved	Comparable	Storage and speed

a: Blockchain based solutions summary

Security Features	Blockchain	Legacy Systems
Integrity	High	Medium
Availability	High	Medium
Confidentiality	Low	Medium
Fault Tolerance	HIgh	High
No. of Trustless Nodes	High	Low

b: Security Comparison

VII. Conclusion

Blockchain is an emerging solution for improving the security of the overall structure of the Internet to ensure the interruption-free performance of the network. In this paper, we presented blockchain-based solutions for three core network components and systems: PKI, BGP, and DNS, and identified open problems. We plan to further extend our cryptographic discussion with the knowledge we gained from [43].

Acknowledgements

The authors acknowledge TÜBİTAK (the Scientific and Technological Research Council of Turkey) 119E088 grant.

References

[1] Ö. Ulusoy, "Research issues in peer-to-peer data management," in *IEEE ISCIS*, 2007, pp. 1–8.
[2] K. S. Mishra and A. K. Tripathi, "Some issues, challenges and problems of distributed software system," *International Journal of Computer Science and Information Technologies*, 2014.
[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[4] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer *et al.*, "On scaling decentralized blockchains," in *FC*. Springer, 2016, pp. 106–125.
[5] R. C. Merkle, "Protocols for public key cryptosystems," in *IEEE Symposium on Security and Privacy*, 1980, pp. 122–122.
[6] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *IEEE Symposium on Security and Privacy*, 2014.
[7] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *ACM EuroSys*, 2018.
[8] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, 2014.
[9] M. Castro, B. Liskov *et al.*, "Practical byzantine fault tolerance," in *OSDI*, 1999, pp. 173–186.
[10] I. M. Coelho, V. N. Coelho, P. Lin, and E. Zhang, "Community yellow paper: A technical specification for neo blockchain," 2019.
[11] A. De Vries, "Bitcoin's growing energy problem," *Joule*, vol. 2, no. 5, pp. 801–805, 2018.
[12] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Communications of the ACM*, 2018.
[13] Z. Wang, J. Lin, Q. Cai, Q. Wang, J. Jing, and D. Zha, "Blockchain-based certificate transparency and revocation transparency," in *FC*. Springer, 2018, pp. 144–162.
[14] S. Matsumoto and R. M. Reischuk, "IKP: Turning a PKI around with blockchains." *IACR Cryptology ePrint Archive, Report 2016/1018*, 2016.
[15] K. Lewison and F. Corella, "Backing rich credentials with a blockchain PKI," 2016.
[16] L. Axon and M. Goldsmith, "PB-PKI: A privacy-aware blockchain-based PKI," in *SECRYPT*, 2017.
[17] A. Yakubov, W. Shbair, A. Wallbom, D. Sanda *et al.*, "A blockchain-based pki management framework," in *IEEE/IFIP Man2Block*, 2018.
[18] B. Laurie, A. Langley, and E. Kasper, "Certificate transparency," *ACM Queue*, vol. 12, no. 8, pp. 10–19, 2014.
[19] M. Etemad and A. Küpçü, "Efficient key authentication service for secure end-to-end communications," in *Provable Security*. Springer, 2015, pp. 183–197.
[20] M. Y. Kubilay, M. S. Kiraz, and H. A. Mantar, "Certledger: A new pki model with certificate transparency based on blockchain," *Computers & Security*, vol. 85, pp. 333–352, 2019.
[21] S. Eskandarian, E. Messeri, J. Bonneau, and D. Boneh, "Certificate transparency with privacy," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 4, pp. 329–344, 2017.
[22] E. Yüce and A. A. Selçuk, "Server notaries: a complementary approach to the web pki trust model," *IET Information Security*, vol. 12, 2018.
[23] E. Alnatsheh, "The efficient use of a list of trusted certificate authorities," *International Journal of Engineering Technology and Sciences*, vol. 5, no. 3, pp. 118–131, 2018.
[24] M. Saad, A. Anwar, A. Ahmad, H. Alasmary, M. Yuksel, and A. Mohaisen, "Routechain: Towards blockchain-based secure and efficient bgp routing," in *IEEE ICBC*, 2019, pp. 210–218.
[25] Y. Rekhter, T. Li, and S. Hares, "A border gateway protocol 4 (bgp-4)," *IETF RFC 4271*, 2006.
[26] S. T. Kent, "Securing the border gateway protocol," *The Internet Protocol Journal*, vol. 6, no. 3, pp. 2–14, 2003.
[27] R. White, "Securing bgp through secure origin bgp (sobgp)," *Business Communications Review*, vol. 33, no. 5, pp. 47–53, 2003.
[28] G. Goodell, W. Aiello, T. Griffin, J. Ioannidis, P. D. McDaniel, and A. D. Rubin, "Working around bgp: An incremental approach to improving security and accuracy in interdomain routing." in *NDSS*, 2003.
[29] C.-N. Chuah, S. Bhattacharyya, and C. Diot, "Measuring i-bgp updates and their impact on traffic," Sprint ATL Technical Report TR02-ATL-051099, Tech. Rep., 2002.
[30] "Bgp hijacking overview. routing incidents prevention and defense mechanisms," https://www.noction.com/blog/bgp-hijacking.
[31] A. Hari and T. Lakshman, "The internet blockchain: A distributed, tamper-resistant transaction framework for the internet," in *ACM HotNets*, 2016.
[32] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, "Consortium blockchain-based malware detection in mobile devices," *IEEE Access*, vol. 6, pp. 12 118–12 128, 2018.
[33] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains," in {*USENIX*}, 2016, pp. 181–194.
[34] "Namecoin," https://namecoin.org/.
[35] J. Liu, B. Li, L. Chen, M. Hou, F. Xiang, and P. Wang, "A data storage method based on blockchain for decentralization dns," in *IEEE DSC*, 2018, pp. 189–196.
[36] D. Basin, C. Cremers, T. H.-J. Kim, A. Perrig, R. Sasse, and P. Szalachowski, "Design, analysis, and implementation of arpki: an attack-resilient public-key infrastructure," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 3, pp. 393–408, 2016.
[37] R. Oppliger, "Certification authorities under attack: A plea for certificate legitimation," *IEEE Internet Computing*, vol. 18, no. 1, pp. 40–47, 2013.
[38] M. Ali, R. Shea, J. Nelson, and M. J. Freedman, "Blockstack: A new decentralized internet," *Whitepaper, May*, 2017.
[39] S. Gourley and H. Tewari, "Blockchain backed dnssec," in *International Conference on Business Information Systems*. Springer, 2018.
[40] A. d. L. R. Gómez-Arevalillo and P. Papadimitratos, "Blockchain-based public key infrastructure for inter-domain secure routing," in *IFIP INET-SEC*, 2017.
[41] Q. Xing, B. Wang, and X. Wang, "Bgpcoin: Blockchain-based internet number resource authority and bgp security solution," *Symmetry*, vol. 10, no. 9, p. 408, 2018.
[42] Y. Hassanzadeh-Nazarabadi, A. Küpçü, and Ö. Özkasap, "Lightchain: A dht-based blockchain for resource constrained environments," *arXiv preprint arXiv:1904.00375*, 2019.
[43] A. Küpçü, "White paper on self study cryptography course," DOI: 10.13140/RG.2.2.13320.37124. [Online]. Available: https://sites.google.com/a/ku.edu.tr/self-crypto/

Büyük Veri Analitiği Kullanan Bir SIEM Yazılımı Geliştirilmesi

Burak ÇAYIR
Bilgisayar Mühendisliği , Teknoloji Fakültesi
Gazi Üniversitesi
Ankara , Türkiye
burak.cayir@gazi.edu.tr

Bünyamin CİYLAN
Bilgisayar Mühendisliği , Teknoloji Fakültesi
Gazi Üniversitesi
Ankara , Türkiye
bciylan@havelsan.com.tr

***Öz*---Siber tehditlerin oldukça arttığı günümüzde yazılımların ürettiği loglar siber tehditlerin tespit edilebilmesi için büyük önem arz etmektedir. Bu sebepten dolayı "log yönetimi" büyük önem kazanmıştır. Çünkü loglar üzerinde yapılan incelemeler sonucunda gerçek zamanlı veya geçmiş zamanda yapılan siber saldırılar tespit edilebilmekte ve izlenebilmektedir. Ayrıca gerçekleşmek üzere olan ve/veya hazırlık aşamasında olan siber saldırılarda tespit edilebilmektedir. Bu çalışmada yazılımlardan toplanan loglar aracılığı ile siber saldırılara karşı etkin bir savunma yöntemi geliştirilmesi amaçlanmıştır. Araştırma ve geliştirme yapılırken "büyük veri" teknolojilerinden yararlanılmıştır. Büyük veri teknolojisi ile loglar gerçek zamanlı olarak izlenebilmekte ve gerçek zamanlı siber savunma sağlama amacı gerçekleştirilebilmektedir. Araştırma gerçekleştirilirken açık kaynak yazılımlardan yararlanılmıştır. Bu açık kaynak yazılımlar sayesinde amaca uygun etkin bir sistem inşa edilmiştir. Bu çalışmada bir sanal makine logları toplayan sunucu, diğer 2 makine ise logları gönderen bilgisayarlar olarak ayarlanmıştır. Logları toplayan sunucuda açık kaynak yazılımlar aracılığı ile log toplama, anlamlandırma, korele etme ve alarm üretme amaçlanmıştır. Logları gönderen bilgisayarların ise yazılımlar aracılığıyla logları etkin ve hızlı şekilde sunucuya göndermesi amaçlanmıştır. Sunucuya gönderilen loglar anlamlandırıldıktan sonra korele edilmiştir. Bu korelasyon işlemlerinden sonra kullanıcının oluşturduğu kurallara uyan bir işlem gerçekleştirdiği takdirde alarm üretilmesi sağlanmıştır.**

Anahtar Sözcükler---Bilgi Güvenliği , Olay Yönetimi, Büyük Veri

***Abstract*---Cyber threats are increasing day by day and the logs produced by the software are of great importance for the detection of cyber threats. For this reason, log management has gained importance. Because, as a result of investigations on the logs, cyber attacks in real time or in the past can be detected and monitored. It can also be detected in cyber attacks that are about to take place and / or are in preparation. In this study, it is aimed to develop an effective defense method against cyber attacks through the logs collected from the software. Research and development is done by using "big data" technologies. With big data technology, logs can be monitored in real time and real-time cyber defense can be achieved. Open source software was used during the research. Thanks to these open source software, an effective system has been built for the purpose. In this study, a virtual machine is set as the server that collects the logs and the other 2 as the computers that send the logs. It is aimed to generate logging, interpretation, correlation and alarming by means of open source software on the server that collects the logs. The computers that send the logs are intended to send the logs to the server effectively and quickly through the software. Logs sent to the server are correlated after they are meaningful. After this correlation process, if the user complies with the rules created by the user, the alarm is generated.**

Index Terms—Security Information, Event Management, Big Data

I. GIRIŞ

Bilgi ve iletişim teknolojilerinde çeşitli uygulamaların artarak kişilerin günlük yaşantılarının vazgeçilmez bir parçası haline gelmesi, internet gibi zaman ve coğrafi sınırlılıkların kalkarak anlık iletişim ve bilgi paylaşımının bulunduğu ortamlarla birlikte siber güvenlik ile ilgili farklı bir ihtiyaç türü oluşmaya başlamıştır. Oluşan bu ihtiyaçlar kurum ve kuruluşlar tarafından değerlendirilmekte, giderilmeleri için çeşitli yöntemler ve çözümler ele alınmaktadır. Bunun yanı sıra siber güvenlik şirketleri oluşan ihtiyaçlar için kendi değerlendirmeleri ve müşterilerinin isteklerine uygun çözümler sunan yazılım ve donanım ürünleri üretmeye çalışmaktadırlar.

Dünya genelinde çeşitli siber güvenlik ihtiyaçlarına yönelik geliştirilmiş birçok ürün bulunmaktadır. Bu ürünlere Firewall, WAF, DAF, IPS, IDS, DLP gibi çözümler örnek verilebilir. Kurum ve kuruluşlarca kullanılan bu sistemler kritik görevler yapmaktadırlar. Bu sistemler ne kadar başarılı görev yaparlarsa yapsınlar, organize ve motivasyonu yüksek yeni nesil saldırgan grupların saldırılarına karşı her zaman başarılı koruma sağlayamamaktadırlar.

APT saldırılarına karşı etkin bir önlem sistemi üretmek isteyen Siber Güvenlik şirketleri ve araştırmacılar büyük araştırmalar ve geliştirmeler sonucu SIEM sistemlerini tasarlamış ve üretmeyi başarmışlardır.

Yapılan araştırma ve geliştirme sonucu geliştirilmiş SIEM izleme, anlamlandırma, korele etme ve uyarı verme gibi işlevlere sahiptir. Bu işlevler sayesinde alınabilecek önlemlerin etkinliği artırılabilir ve engelleme sistemlerine erken uyarı sağlanabilmektedir. Önceki çalışmalara ek olarak geliştirilmiş olan SIEM'in uyarı sistemi çeşitli platformlara uyumlu olduğundan kullanıcının istediği platforma alarmlar yönlendirilebilmektedir. Ayrıca geliştirilmiş olan grafik arayüzlü log yönlendirme ajanı ile kullanıcıların kolaylıkla SIEM sunucusuna log yönlendirme yapabilmesi sağlanmıştır.

II. Literatur Değerlendirilmesi

SIEM Güvenlik Bilgi Yönetimi (SIM) ve Güvenlik Olay Yönetimi (SEM) sistemlerinin birleşik halidir. SIM, günlük verilerin ve uzun vadeli depolanan verilerin analizine ve raporlanmasına, SEM ise gerçek zamanlı olay izlemeye ve bildirimlere odaklanır. SIEM bunları birleştirir ve gerçek zamanlı analiz ve korelasyon içerir[1].

Bir SIEM ürününden beklenen hedeflenen saldırıların ve veri ihlallerinin erken tespiti için olay verilerini gerçek zamanlı olarak analiz etmesi ve olaya tepki üretimi, adli tıp ve yasal düzenlemelere uyum için günlük verileri toplamak, depolamak, araştırmak ve raporlamaktır.

David Swift adlı araştırmacı tarafından yazılan "A Practical Application of SIM/SEM/SIEM Automating Threat Identification" adlı makalesi SIEM hakkındaki ilk bilimsel makale olarak kabul edilmektedir[2].

Siber saldırılara karşı küçük ve orta ölçekli işletmelerin kullanabileceği SIEM sistemleri ile alakalı Alan Mercer adlı araştırmacının "Security Information and Event Management for Small and Medium-Sized Enterprises" isimli tezinde işletmelerin siber saldırılara karşı SIEM sistemleri ile nasıl önlemler alabileceği ele alınmıştır[3].

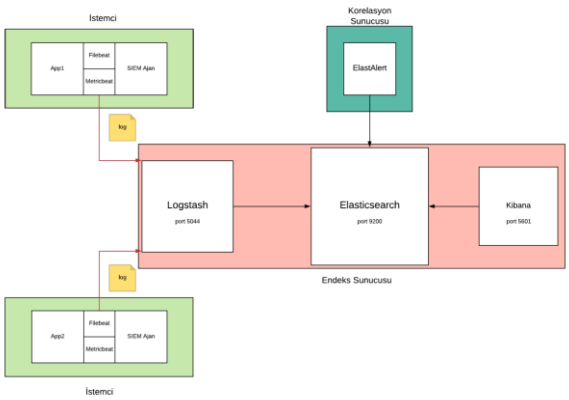
SIEM sistemleri için saldırı modellemesi ve analizi ile alakalı Igor Kotenko ve Andrey Chechulin adlı araştırmacıların "Common Framework for Attack Modeling and Security Evaluation in SIEM Systems" isimli makalelerinde SIEM sistemlerinde saldırı modellemesi ve güvenlik değerlendirmesi için bir çerçeve önerilmektedir[4].

Bu araştırma artarak gerçekleşmekte olan siber saldırılara ve veri sızıntılarına karşı etkin önlemler alınması ve var olan SIEM sistemlerinde var olmayan siber güvenlik önlemleri eklenmesi amacıyla gerçekleştirilmiştir.

Çalışma 6 temel başlık altında ele alınmıştır. Bunlar; Giriş, Literatür Değerlendirmesi, Materyal ve Metotlar, Siber Saldırılar, SIEM, Örnek Tehdit Senaryolarına Karşı SIEM İle Alınabilecek Önlemler, Sonuç ve Öneriler'dir.

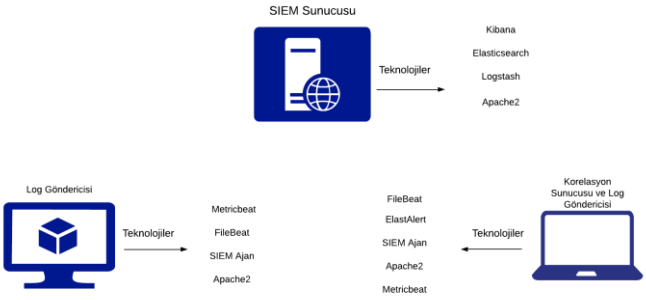
III.Materyaller ve Metotlar

Bu çalışma esnasında birçok sanal makine kullanılmış, kullanılan bu sanal makinalar için en optimal özellikler belirlenmiştir. Yapılan testler sonucu 2 sanal makine bir normal makine kullanılmasına karar verilmiştir. Geliştirilen SIEM'in topolojisi Şekil 3.1'de gösterilmiştir.



Şekil 3.1 SIEM Topolojisi

Kullanılan makinaların temel işlevleri Şekil 3.2 üzerinde gösterilmiştir.



Şekil 3.2 SIEM Yazılımı Topolojisi

A. *SIEM İşlevleri Ve Kabiliyetleri*

Üzerinde çalışılmış olan SIEM yazılımının işlevleri ve kabiliyetleri siber saldırıların potansiyel zararlarını önleme amacıyla belirlenmiştir. Bu işlevlere ve kabiliyetlere giriş yapmadan önce geliştirilen SIEM'deki büyük veri teknolojisine ve kurulan açık kaynak yazılımların işlevleri belirtilmiştir.

1) Büyük Veri :

Big Data(Büyük Veri) olarak isimlendirdiğimiz bu olgu, diskte çok fazla yer kaplayan veri çağrışımı yapsada aslında tam olarak böyle değil. Big Data, sosyal medya paylaşımları, fotoğraf arşivlerimiz, sürekli kayıt aldığımız 'log' dosyaları gibi farklı kaynaklardan elde ettiğimiz tüm bu verilerin anlamlı ve işlenebilir hale dönüştürülmüş biçimidir.

2) SIEM Kabiliyetleri :

Geliştirilmiş olan SIEM sisteminin kabiliyetleri;

- Ajanlar Tarafından Gönderilen Logları Toplama
- Ayrıştırılan Logların Elasticsearch'e Gönderilmesi ve Endekslenmesi
- Logların Kibana Arayüzü Üzerinden İzlenebilmesi
- ElastAlert Yazılımı Sayesinde Korelasyon Oluşturulabilmesi ve Oluşturulan Korelasyonlara Uyan Logların Oluşması Durumunda Alarm Üretilmesi

a) Ajanlar Tarafından Gönderilen Logları Toplama :

Aynı ağda bulunan bilgisayarlardan ajan aracılığıyla toplanan loglar SIEM sunucusundaki Logstash yazılımı tarafından toplanmaktadır. Toplanan bu loglar filtrelerden geçirilerek ayrıştırılır. Anlamlı hale getirilir.

b) Ayrıştırılan Logların Elasticsearch'e Gönderilmesi ve Endekslenmesi :

Loglar anlamlandırıldıktan ve ayrıştırıldıktan sonra Endeks sunucusu olan Elasticsearch'e Logstash aracılığıyla gönderilir. Gönderilen bu loglar Endeks sunucusu tarafından endekslenir. Endekslenen bu loglara Elasticsearch'ün sağladığı tam metin arama teknolojisiyle çok hızlı şekilde ulaşım sağlanmaktadır.

c) Logların Kibana Arayüzü Üzerinden İzlenebilmesi :

Elasticsearch endekslerinde tutulan loglar Kibana yazılımı aracılığıyla <sunucuip:5601> adresi ile web tarayıcı aracılığıyla izlenebilir. Kibana kişinin ihtiyaçlarına uygun şekilde göstergeler oluşturulmasını sağlar. Ayrıca Kibana kendi üzerinde bulunan filtreleme özelliği sayesinde kullanıcının filtreleme isteklerine arayüz üzerinden imkan tanır ve filtrelere göre sonuçlar üretir.

d) ElastAlert Yazılımı Sayesinde Korelasyon Oluşturulabilmesi ve Oluşturulan Korelasyonlara Uyan Logların Oluşması Durumunda Alarm Üretilmesi :

Elastalert yazılımı aracılığıyla çalışan korelasyon sunucusu konfigürasyon sonucu oluşturulan soket aracılığıyla sürekli Endeks sunucusu ile iletişim halindedir. Elastalert yazılımı içerisinde kural oluşturulabilmektedir. Oluşturulan bu kurallar endekslerdeki loglarla karşılaştırılır. Karşılaştırma sonucunda eşleşme oluşursa alarm tetiklenir ve kullanıcı uyarılır.

IV. Siber Saldırılar

Siber saldırganların motivasyonu gün geçtikçe artmaktadır. Hackerlar gün geçtikçe daha agresif daha egoist ve daha organize hale gelmektedir. Bundan dolayı kurum ve kuruluşlara yönelik siber tehditler zamanla daha da tehlikeli hale gelmektedir.

Siber tehditlerin ortaya çıkmasına neden olan üç boyut bulunmaktadır[5]:

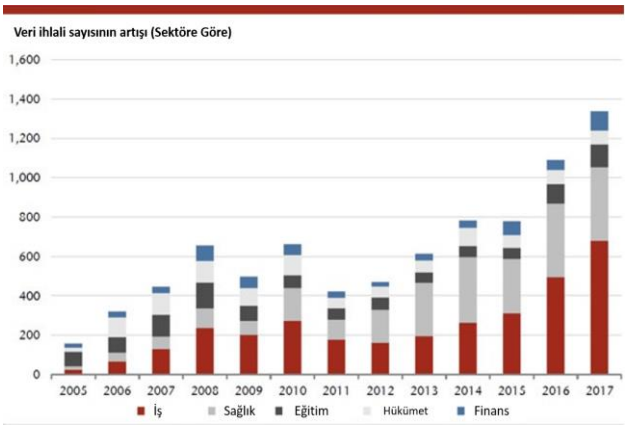
- Internet tasarımındaki zafiyetler (adresleme sistemi, yönetim eksikliği, internetin çalışmasını sağlayan sistemlerin çoğunun açık ve şifresiz olması, zararlı yazılımları dağıtma kabiliyeti ve internetin merkezî olmayan büyük bir ağ olması)
- Donanım ile yazılımlardaki hatalar
- Kritik sistemlere çevrim içi erişim imkânı

Günümüz siber ortamında saldırılara ağırlıklı olarak kurum ve şirketler maruz kalmaktadır. Kurum ve şirketlere yönelik bu saldırıların giderek artan bir çizgide ilerlemesine ve saldırı riskinin artmasına:

- Siber ortamda saldırı için gerekli yazılım ve bilginin ucuz ve kolay elde edilebilir olması,
- Dünyanın herhangi bir yerinden herhangi bir zamanda kişi veya sistemlerin kasıtlı ya da kasıtsız olarak bu saldırılara katılmalarının mümkün olması,
- Siber uzayın bütüncül ve kesintisiz iletişime açık yapısı nedeniyle kötücül yazılım ve benzeri tehditler ile yapılan saldırılar yoluyla sistemlerin birbirine zarar vermesi,
- Çok geniş kitlelere ulaşan kritik hizmet ve servislerin artarak bilişim sistemleri tarafından veriliyor olması,
- Birçok kurum ve şirketin kritik altyapılarının internete bağlı olması,
- İnternet kullanıcılarının çoğunun siber güvenlik bilincinin yetersiz olması,

gibi etmenler sebep olmaktadır[6].

Bilgisayar dünyası ve internet teknolojisinin popülerleşmeye başladığı 2000'li yıllardaki siber saldırılara nazaran günümüz yıllara yakın süreçte ortaya çıkan APT saldırıları ve zararlı yazılımlar kurum ve kuruluşların kullandığı sistemler için büyük tehlikeler oluşturmaktadır[7]. Artık saldırganlar daha organize hale gelmiş, hedefleri maddi ve manevi bakımdan daha da büyümüştür. Yıllar geçtikçe gerçekleşen saldırıların etkisi artmış, daha büyük veri sızıntıları gerçekleşmeye başlamıştır. 2005 ve 2017 yılları arasındaki veri sızıntıları trendi Şekil 4.1'de gösterilmiştir.



Şekil 4.1 2005-2017 Yılları Arasında Gerçekleşen Veri Sızıntılarının Yıllık Trendi[8]

STM'nin 2018 Yılında yayınlanan "Ocak-Mart Siber Tehdit Durum Raporu" adlı makalesinde siber saldırıların etki artışı konusuna şöyle dikkat çekilmiştir[9];

- Siber suçların küresel ekonomiye maliyeti 2014'te yapılan araştırmada 445 milyar ABD Doları iken geçtiğimiz yıl itibarı ile 600 milyar ABD Dolarına yaklaşmış durumda.
- Mülkiyet hakları ve mahrem iş bilgilerinin çalınmasına yönelik suçların siber suçların sebep olduğu maliyetin tüm siber suçların maliyeti içindeki payı en az %25 ve bu hırsızlık askeri teknolojiye ait ise milli güvenliği de tehdit ediyor.

- Bankalar siber suçluların en gözde hedefleri haline gelmiştir.
- Rusya, Kuzey Kore ve İran finansal kurumlara saldırılarda, Çin ise siber casusluk alanında en aktif ülkeler. Siber suçlarda Rusya ilk sırada Kuzey Kore ikinci sırada yer alıyor.
- Fidye yazılımları 6 bini aşkın çevrimiçi pazar ve hizmeti olarak sunulabilir hale geldiğinden en hızlı büyüyen siber suç aracı.
- İstismar araçları, sipariş usulü zararlı yazılımlar ve kiralık Botnet'ler gibi çok çeşitli araç ve servisler sunan ve büyüyen pazarlarıyla hizmet olarak sunulabilir hale gelen siber suç, gittikçe daha karmaşık bir hale gelmiş durumda.
- Tor ve Bitcoin gibi kripto para birimlerinin anonim olmaları, suç aktörlerinin tanımlanmalarını zorlaştırıyor.

Siber güvenlik yıllar geçtikçe artan şekilde stratejik ve ekonomik önem arz eden bir kavram haline gelmiştir. Ağır saldırılar sadece büyük şirketler ve devlet teşkilatlanmaları için değil, halka açık ve halka kapalı varlıklar içinde büyük tehlike arz eder olmuştur ve hiçbir azalma eğilimi göstermemiştir. Halka açıklanan siber saldırı hedefleri arasında büyük finansal şirketler, eğlence şirketleri, siber güvenlik şirketleri, ABD Savunma Bakanlığı, ABD Senatosu, Brezilya ve Malezya hükümetleri de dahil olmak üzere ABD ve yabancı devlet teşkilatlanmaları bulunmaktadır[10]. Buradan şu çıkarıma varılmaktadır. Siber saldırılar yalnızca kurum ve kuruluşları hedeflememekte, devlet destekli hackerlar veya hacker organizasyonları aracılığıyla devletleri de hedef almaktadır.

Savaş devletlerin, aralarındaki ekonomik ve siyasal anlaşmazlıklar vb. nedeniyle, siyasal ilişkilerini keserek, birbirlerine karşı ordularıyla giriştikleri silahlı eylem olarak tanımlanmaktadır.

Siber savaşı konvansiyonel savaştan ayıran en önemli faktörler:

- İnsan kayıp oranının az olması,
- Yatırım maliyetinin daha düşük olması,
- Oluşturulan silahların birçok hedefe karşı geniş zaman aralığında defalarca kullanılabilmesi,
- Stratejik ve politik olayları etkileyebilmesi,
- Saldırıların maskelenebilmesi,
- Tek taraflı saldırı yapılabilmesi.

Siber savaşlar artık konvansiyonel savaşların öncüsü olmuş hatta siber savaşlar konvansiyel savaşların önüne geçtiği değerlendirilmektedir.

A. Siber Saldırılara Karşı Alınabilecek Kurumsal Önlemler

Siber saldırıların hazırlanışı kadar siber saldırılardan korunma yöntemleri de karmaşık ve meşakkatli işlemlerdir. Bu yöntemlerin profesyonellerce tasarlanması, sistemlere entegre edilmesi ve yönetilmesi gerekmektedir. Ancak unutulmamalıdır ki en zayıf halka insandır. Her ne kadar yazılım ve donanım güvenliği sağlansa da insan faktörü asla göz ardı edilmemelidir. Bu konuda kurumlar ve kuruluşlar çalışanlarını bilinçlendirmeli ve siber güvenlik farkındalığını en kısa sürede kazandırmalıdırlar.

Kurumların siber saldırılardan korunma amaçlı birçok önlem alması gerekmektedir. Bu önlemlerin önceden planlanması, test edilmesi, kurum sistemleriyle uyumluluğunun sağlanması ve entegre edilmesi çok kritiktir.

Alınabilecek kurumsal önlemler;

a) Tehditlerin Tanımlanması
b) Siber Suç Farkındalığı
c) Çalışanların Kurum İçerisinde Gözlemlenmesi
d) Verilerin Önem Derecesine Göre Korunması

1) Tehditlerin Tanımlanması :

Tehdit geleceğe ilişkin olarak, gerçekleşmesi failin iradesine bağlı olarak, haksız ve ağır bir zarara uğrayacağını mağdura hissettirmek suretiyle, iç hürriyetin kısıtlanması, iç huzur ve güvenlik hissinin zedelenmesidir.

Çoğu şirket, sızdırılmışsa şirket için maddi ve manevi kayıplar oluşturabilecek çok hassas bilgiler içerir. Bu nedenle kurum içerisinde var olan tehditler belirlenmeli ve gerekli önlemler derhal alınmalıdır.

2) Siber Suç Farkındalığı :

Daima siber suçlulara karşı temkinli olunmalıdır ve saldırı bekleniyormuş gibi çalışılmalıdır. Bu, kurumların her zaman gerekli stratejiler ve planlarla korunduğundan emin olunmasını sağlayacaktır. Hangi bilgilerin suçlular için dikkat çekici olduğu ve hangilerinin olmadığı daima tetkik ve takip edilmelidir. ,

3) Çalışanların Kurum İçerisinde Gözlemlenmesi :

Tutarlı bir bilgi güvenliği süreci oluşturmak ve bu sürecin sürdürülebilirliğini sağlamak, ancak çalışanların tamamının katılımı ile sağlanabilir. Bilgi teknolojileri ve sistemlerini kullanan tüm çalışanlara siber güvenlik kavramları, tehditleri ve korunma yöntemleri ile ilgili farkındalık kazandırmak temel amaç olmalıdır. Ayrıca kurum içinde çalışan tüm çalışanlara bilgi güvenliği farkındalığı kazandırılmalı, siber saldırıların ve sosyal mühendislik tehdidinin kurumu nasıl ve hangi yollarla hedef alabileceği bilinci kazandırılmalıdır.

Kurum çalışanlarının bilgi güvenliği sağlanması amacıyla uyması gereken yasal zorunluluklar bulunmaktadır. 5651 numaralı kanun maddesi buna örnek verilebilir. 5651 numaralı kanun maddesine göre internet erişimi kontrol altına alınmalıdır. 5651 Sayılı Kanunda açıkça belirtilen ve yasanın gerekliliklerini yerine getirmeyen işletme ve kuruluşlar için maddi ve idari para cezaları bulunmaktadır. Yasa gereği olarak işletmeler log tutma ve sundukları hizmetin kimler tarafından hangi zaman dilimlerinde kullanıldığını geçmişe dönük olarak belgeleyebilmek zorundadırlar.

Kurum olarak çalışanlar düzenli olarak denetlenmeli ve düzenli siber farkındalık eğitimleri düzenlenmelidir.

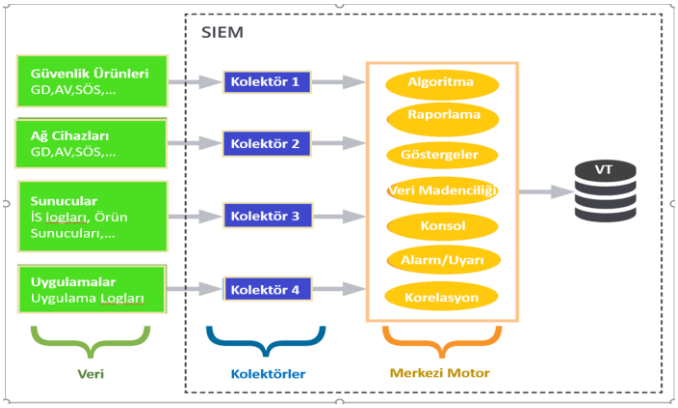
4) Verilerin Önem Derecesine Göre Korunması :

Kurumlar için en hassas bilgileri korumak birinci öncelik olmalıdır. Bu veriler hackerlar tarafından ilk hedeflenen varlıklardandır. Bu verilere personelin nasıl eriştiği daima

kontrol edilmeli ve verilerin saklandığı sunucular güvenlik kameraları ve ses kayıt cihazları gözetimindeki, ancak yetkili ve sorumlu personelin ulaşabileceği çift doğrulama sistemi kullanarak giriş yapılabilen ortamlarda saklanmalıdır. Veriler yedekleme yazılımlarıyla ve donanımlarıyla sürekli olarak yedeklenmeli ve felaket senaryolarına karşı hazır olunmalıdır. Ayrıca bu yedekleme yazılımları ve donanımlarının çalışması düzenli olarak takip edilmelidir[11].

V.SIEM

SIEM Güvenlik Bilgi Yönetimi (SIM) ve Güvenlik Olay Yönetimi (SEM) sistemlerinin birleşik halidir. SIM, günlük verilerin ve uzun vadeli depolanan verilerin analizine ve raporlanmasına, SEM ise gerçek zamanlı olay izlemeye ve bildirimlere odaklanır. SIEM bunları birleştirir ve gerçek zamanlı analiz ve korelasyon içerir[12]. SIEM yazılımının çalışma sistemi Şekil 5.1'de gösterilmiştir.



Şekil 5.1 SIEM yazılımının çalışma sistemi[13]

A. SIEM İşlevleri

Yapılan bu araştırma sonucunda bir SIEM sisteminde bulunması gereken özellikler belirlenmiştir.

3) Veri Toplama :

SIEM çözümleri, eksik kritik olayların önlenmesine yardımcı olmak için izlenen verileri birleştirme yeteneği sağlayan, ağ, güvenlik, sunucular, veritabanları, uygulamalar dahil olmak üzere birçok kaynaktan gelen verileri toplar[14].

4) Korelasyon (Bağıntı) :

Bu teknoloji, verileri yararlı bilgilere dönüştürmek için farklı kaynakları entegre ederek çeşitli korelasyon teknikleri gerçekleştirme yeteneği sağlar.

5) Alarm Üretimi :

SIEM, kullanıcı tarafından girilen kurallara takılan olayların ortaya çıkması durumunda bu olayları alıcılarına bildirmek için, uyarıların üretimini sağlar ve kullanıcıyı bilgilendirir.

4) Veri Saklama :

SIEM çözümleri, verilerin zaman içinde korelasyonunu kolaylaştırmak ve uyumluluk gereklilikleri için uzun vadeli tarihsel verilerin depolanmasını sağlamak için kullanır[15].

VI.ÖRNEK TEHDİT SENARYOLARINA KARŞI SIEM İLE ALINABİLECEK ÖNLEMLER

Bu bölümde hazırlanmış olan SIEM'in kullanımı ve örnek tehdit senaryolarına karşı nasıl kullanılabileceği anlatılmıştır.

Öncelikle SIEM sunucusunun düzgün şekilde başlatıldığından emin olunmalıdır. Elasticsearch, Kibana, Apache2 uygulamaları otomatik olarak başlayacaktır. Logstash yazılımı ise elle başlatılacaktır.

A. Örnek Tehdit Senaryosuna Karşı SIEM Ile Önlem Alma

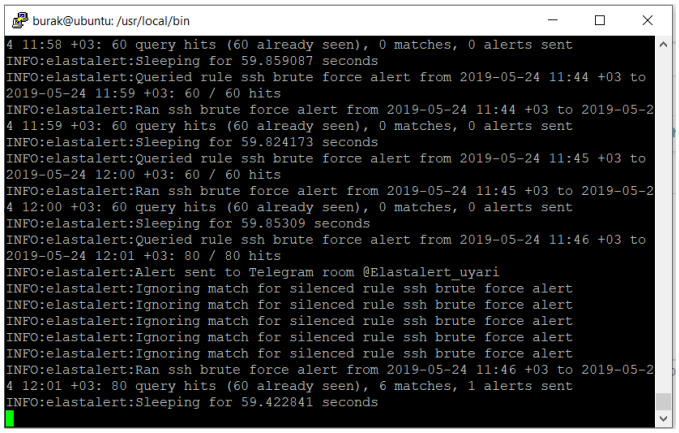
Bu bölümde örnek bir tehdit senaryosuna karşı SIEM'le alınabilecek önlem anlatılmıştır.

1)SSH Brute Force Alarmı :

SSH uzaktan terminal erişimine izin veren güvenli bir protokol olarak kabul edilmektedir. Ancak saldırganlar brute force (kaba kuvvet) yöntemleriyle kullanıcı bilgilerini tahmin ederek terminallere izinsiz şekilde giriş yapmaya çalışmaktadırlar. SIEM aracılığıyla bu tip bir saldırıyı başlangıç esnasında tespit edebilir, alarm ürettirebiliriz.

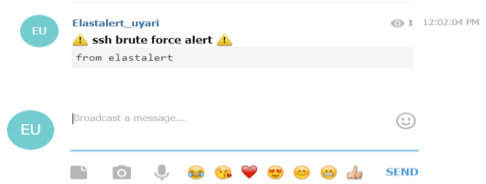
Bu alarmı üretebilmemiz için Elastalert yazılımı içerisinde bir kural yazmamız gerekmektedir. Kuralın temeli şudur; Eğer gelen loglar içerisindeki message kolonunda "Failed password" uyarısı ve fileset.name kolonunda "auth" kelimesi 1 saat içerisinde 10 kere gelirse alarm tetiklenecektir.

Korelasyon sunucusuna çeşitli kurallar girilmiştir ve bu kurallar tetiklenerek uyarı üretilmiştir. Şekil 6.1'de ssh_bruteforce kuralının tetiklenmesi görülmüştür.



Şekil 6.1 Korelasyon sunucusunda ssh_brute_force kuralının tetiklenmesi ve alarm gönderilmesi

Şekil 6.2'de tetiklenen ssh_brute_force kuralının Telegram kanalına gönderildiği görülmüştür.



Şekil 6.2 Gönderilen alarmın Telegram kanalında görülmesi

B. Genel SIEM Korelasyon Testleri

Korelasyon sunucusuna çeşitli kurallar girilmiştir ve bu kuralları tetikleyecek aktivitelerde bulunulmuştur. Kuralların üreteceği alarmlar çeşitli platformlara yönlendirilmiştir. Yapılan bu çalışmanın sonuçları Çizelge 6.3'de görülebilir.

Kural	Tetikleme	Alarm'ı Mail'e Yönlendirme	Alarmı Telegram'a Yönlendirme	Alarmı Komut Satırında Görebilme
SSH_Brute_Force	Başarılı	Başarılı	Başarılı	Başarılı
Tek Kullanıcının 2 Farklı Ip'den Giriş Yapması	Başarılı	Başarılı	Başarılı	Başarılı
Web Sitesinin 1 Saat Boyunca Başarılı Yanıt Verememesi	Başarılı	Başarılı	Başarılı	Başarılı
URI'ye yapılan isteğin 1 haftadır 10 saniye üzerinde Cevap Veriyor Olması	Başarılı	Başarılı	Başarılı	Başarılı
Hata loglarının toplandığı dosyadaki log sayısı bir saat içerisinde 2 katına ulaşması	Başarılı	Başarılı	Başarılı	Başarılı
Hata dosyasında yeni bir hata türü görülmesi	Başarılı	Başarılı	Başarılı	Başarılı
İşlemcinin Uzun Süre Boyunca Yüksek Kapasite Çalışması	Başarısız	-	-	-

Şekil 6.3 Test Sonuçları

Bu çalışmada log verileri ile korelasyonlar oluşturulabilmekte fakat metrik verileriyle korelasyon oluşturulurken sıkıntılar meydana gelmektedir. Bunun nedeninin metrik endeksleriyle ElastAlert yazılımı arasındaki iletişim problemi olduğu anlaşılmıştır.

Log verileri sayesinde detaylı senaryolar oluşturulabilmiş ve istenilen sonuçlar alınabilmiştir. Günümüz siber saldırılarının adımları simüle edilmiştir. Simüle edilen bu saldırılara saldırgan bakış açısıyla bakılıp hangi tip davranışlar ile tespit edileceği belirlenmiştir. Bu davranışları temsilen kurallar eklenmiş ve davranışlar gerçekleştiğinde gerekli uyarılar elde edilmiştir.

VII. SONUÇ VE ÖNERİLER

Bu çalışmada günümüzde gerçekleştirilen organize ve motivasyonu yüksek siber saldırıların nasıl gerçekleştiğini, saldırıların arkasındaki güçlerin kimler olduğu, bu saldırılara karşı kurumların, kuruluşların ve hatta devletlerin nasıl önlemler aldığı ve alması gerektiği, SIEM sistemlerinin alınacak bu önlemler arasında rolünün ne olduğu ve nasıl kullanılması gerektiği, açık kaynak yazılımlarla oluşturduğum SIEM'in kabiliyetleri ve kullanımı ele alınmıştır.

Yeni nesil siber saldırıların karakteristikleri ve kabiliyetleri araştırılmış ve elde edilen sonuçlar analiz edilmiştir. Bu analiz sonucunda ne gibi önlemler alınacağı kararlaştırılmış ve oluşturulan SIEM sistemiyle elde edilen loglar izlenerek ve incelenerek önlemler hayata geçirilmiştir. Sistemsel ve yazılımsal logların saldırıların tespitindeki rolünün önemi anlaşılmıştır.

Çalışma sonucunda SIEM sistemlerinin sahip oldukları büyük kabiliyetlere rağmen kurum ve kuruluşlar için tek başına güvenlik sağlamayacağı anlaşılmıştır. SIEM kullanımının yanı sıra diğer siber güvenlik sistemleri de kurum ve kuruluşlarda ele alınmalı, SIEM'le entegre edilip profesyonel kişilerce kullanılmalıdır. Bu sistemlerin profesyoneller tarafından değil de bilgisiz kişiler tarafından kullanılması halinde kabiliyetlerden yararlanmak imkansıza yakındır. Bu sebepten ötürü çalışanlara farkındalık ve siber güvenlik bilgisi kazandırmak veya siber güvenlik profesyonelleri istihdam etmek hayati bir önem arz etmektedir.

Çalışma sonucunda mevcut SIEM sistemlerine kullanıcıya kolaylık ve hız sağlamak amacıyla bazı ek özellikler eklenebileceği gözlemlenmiştir. Bundan sonra geliştirilecek olan SIEM'ler de ek olarak arayüze entegre edilmiş alarm yönetim sistemi eklenebilir. Kullanıcılar bu arayüz üzerinden korelasyon kuralı girebilir ve alarmları buradan görebilir. Bir diğer eklenebilecek sistem ise makine öğrenmesi kullanılarak loglarda anomali tespit edebilen sistemdir. Böylece loglar canlı olarak akarken zararlı aktiviteler yapay zeka teknolojisi ile tespit edilebilir. Ayrıca işletim sisteminden gelen metrik değerlerini işleyebilecek motorlar geliştirilebilir ve metrik korelasyonları oluşturulabilir.

1) REFERANSLAR

[1] DORIGO Sander "Security Information and Event Management", Radboud University Nijmegen, 2012, s. İx

[2] SWIFT David "A Practical Application of SIM/SEM/SIEM Automating Threat Identification", Information Security Reading Room, 2007

[3] MERCER Alan, "Security Information and Event Management for Small and Medium-Sized Enterprises", Luleå University of Technology Department of Computer science, Electrical and Space engineering, 2013

[4] KOTENKO Igor ve CHECHULIN Andrey, "Common Framework for Attack Modeling and Security Evaluation in SIEM Systems", 2012 IEEE International Conference on Green Computing and Communications, 2012, s. 91-101

[5] R. A. Clarke ve R.K. Knake, "Cyber War-The Next Threat to National Security and What to Do About It", New York: HarperCollins Publishers, 2010, s.74-85 16

[6] YAŞAR Hakan ve ÇAKIR Hüseyin, "Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri", Düzce Üniversitesi Bilim ve Teknoloji Dergisi, S:3 (2015), s.489.

[7] YAŞAR Hakan ve ÇAKIR Hüseyin, "Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri", Düzce Üniversitesi Bilim ve Teknoloji Dergisi, S:3 (2015), s.489.

[8] İnternet:https://www.marketwatch.com/story/how-the-number-of-data-breaches-issoaring-in-one-chart-2018-02-26 "How the number of data breaches is soaring" Son Erişim Tarihi: 16.05.2019

[9] İnternet: https://www.stm.com.tr/documents/file/Pdf/siber-tehdit-durum-raporuocak-mart-2018.pdf "2018 OCAK-MART DÖNEMİ SİBER TEHDİT DURUM RAPORU" Son Erişim Tarihi: 17.05.2019

[10] CARR Jeffrey Inside Cyber Warfare: Mapping the Cyber Underworld O'Reilly Media, Inc. (syf: xi) (2012)

[11] İnternet: https://www.itproportal.com/features/10-essential-steps-for-preventingcyber-attacks-on-your-company/ "10 essential steps for preventing cyber attacks on your company" Son Erişim Tarihi: 17.05.2019

[12] DORIGO Sander "Security Information and Event Management", Radboud University Nijmegen, 2012, s. İx

[13] İnternet: https://www.recordedfuture.com/siem-threat-intelligence-part-1/ "Threat Intelligence and SIEM (Part 1) — Reactive Security", Son Erişim Tarihi: 18.05.2019

[14] DEBAR H., WESPI A,. Aggregation and correlation of intrusion-detection alerts,in: Recent Advances in Intrusion Detection, Springer, 2001, s.85–103

[15] Guillermo Suarez-Tangil, Esther Palomar, Arturo Ribagorda, Ivan Sanz Providing, SIEM systems with self-adaptation Providing SIEM systems with self-adaptation, Information Fusion, 2015, s.145-158

Enhanced AES with Arnold's CAT Map

Arnold's CAT Map ile Güçlendirilmiş AES

1st Hakan Bostan
Computer Engineering Dept.
Middle East Technical University
Ankara, Turkey
hbostan@ceng.metu.edu.tr

2nd Atila Bostan
Ankara, Turkey
atilabostan@hotmail.com

***Abstract*—Advanced Encryption Standard (AES) is one of the widely used block encryption algorithm. On the other hand, Chaotic functions are better tools to foster complexity in calculation. In this study, AES algorithm is modified to include Arnold's CAT Map chaotic function in order to enhance algorithm complexity. The encryption power of the modified AES is compared by means of plaintext and key avalanche effect measures. The results indicate modified AES is not worse than genuine one in avalanche effect measurements, where as there are strong evidences pointing the modified one could yield better results.**

***Index Terms*—Advanced Encryption Standard, Chaotic Encryption, Avalanche Effect**

***Öz*—Advanced Encryption Standard (AES) yaygın olarak kullanılan blok şifreleme algoritmalarından biridir. Diğer yandan Kaotik fonksiyonlar hesaplamada karmaşıklığı arttıran iyi yöntemlerdir. Bu çalışmada, şifreleme algoritması karmaşıklığını arttırmak amacıyla, AES algoritması Arnold's CAT Map kaotik fonksiyonunu içerecek şekilde değiştirilmiştir. Değiştirilen AES algoritmasının şifreleme gücü açık metin ve şifreleme anahtarı çığ etkisi (avalanche effect) ölçütü ile karşılaştırılmıştır. Sonuçlar, değiştirilmiş AES algoritmasının çığ etkisi ölçütünde orijinalden daha kötü olmadığını göstermekle beraber daha iyi bir şifreleme için güçlü kanıtlara işaret etmektedir.**

***Anahtar Sözcükler*—Advanced Encryption Standard, Kaotik Şifreleme, Çığ Etkisi**

I. Introduction

Due to high computation cost and convenience in sharing the public-key on open environments, asymmetric encryption is typically preferred in sharing a symmetric-session key between the communicating peers. Furthermore, block encryption alternatives are in common use in the security domain. Internal Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), Carlisle Adams Stafford Tavares (CAST), Rivest Cipher (RC-2,4,5,6), Data Encryption Standard (DES) and Triple-DES (TDES or 3DES) are the most widespread ones in sector [1]. Practically, all the symmetric encryption alternatives consist of two essential functions, namely substitution and permutation [2]. In that, replacement of a specific byte pattern with some other one is called substitution and changing the order of bytes in the block is called permutation. In a characteristic symmetric-key block encryption, those two functions are deemed essential. With the intention to increase the complexity they are typically executed many times and in altered order. Generic to the block encryption algorithms, repeated sequence of operations is called a round. Minimum number of rounds in a block encryption algorithm is a function of key-length in use. Inevitably, a round-key that is derived from the initial-key is the important parameter in round operations and generally used to substitute the block bytes with some others. Usually round key is XOR'ed with the block state [2].

On the other hand, there are chaotic mathematical functions called Continuous Automorphism of Torus (CAT) [3], [4]. This type of functions return back to the initial state after several iterations when applied to a given state. Number of iterations required to return back to the initial state is chaotic and fixed for a given set of function parameters. In Figure 1 a visual description of such a torus function is given [5].

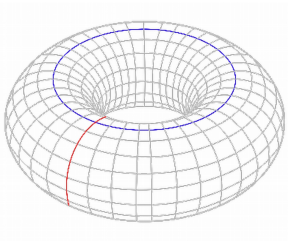


Fig. 1. Schematic description of a continuous automorphism of the torus

When a CAT function is applied to a vectorial data, such as a digital picture, it is called CAT-MAP. Although there are several CAT-MAP functions in the literature, Arnold's CAT-MAP and Henon CAT-MAP are the most known ones [6]. CAT-MAP functions are commonly named as chaotic maps. Chaotic map functions are widely studied in the field of cryptology. However, due to their strong connection with the vectorial data chaotic-map functions were mainly studied in digital image encryption [7]–[10]. Shuffling the image bytes in a chaotic pattern yields an imperceptible output. Nevertheless, CAT-MAP functions are permuting-only operations, they lack in substitution process. Their distinctive characteristic is the guaranteed return back to initial-state following a number of iterations [11]–[13]. In the literature there are significant number of studies using chaotic maps in encryption [14]–[17]. Unfortunately, all the earlier studies are focused on encrypting images but not on other data types.

In this study we have combined classical block encryption algorithm "AES" with chaotic map "Arnold's CAT-MAP" function in order to enhance the AES with the power of chaotic computation.

In Section II, background information on AES and Arnold's CAT Map are given. In Section III, the proposed encryption scheme is explained. In Section IV, our results are presented and in Section V closing remarks are made.

II. Background

A. Advanced Encryption Standard

Block encryption algorithm, Advanced Encryption Standard (AES) has three distinct modes of usage, namely AES-128, AES-192 and AES-256 with respect to the functional key sizes 128, 192 or 256 bits [18]. AES inputs the plaintext in 128 bits blocks (16 bytes). It uses a 4 byte by 4 byte matrix data structure for the block and call it as state. When encrypting the plaintext with AES, the input block is subject to a byte substitution with the help of predefined s-boxes. Later, on the output of s-box substitution, row-wise shuffling, named as "shift-rows" and a second substitution (but this time related with the other bytes on the same column), named as "mix-columns" are executed. In last step of the round operations the sate matrix is XORed with the round key which is derived from the initial key. In relation with the AES mode (with the initial key size as well) above mentioned round operations are repeated 10, 12 or 14 times in AES-128, AES-192 and AES-256 respectively. Round-key generation out of initial key is a spate operation AES. Round-key is referred as sub-key in some other literature. For the clarity in understanding the round operations schematic flow of execution is shown in Figure-2. Additionally, the process of round-key generation out of initial key is shown in Figure-3 for initial key size of 128 bits. Round-key generation for other key sizes are very similar to the one shown in Figure-3.

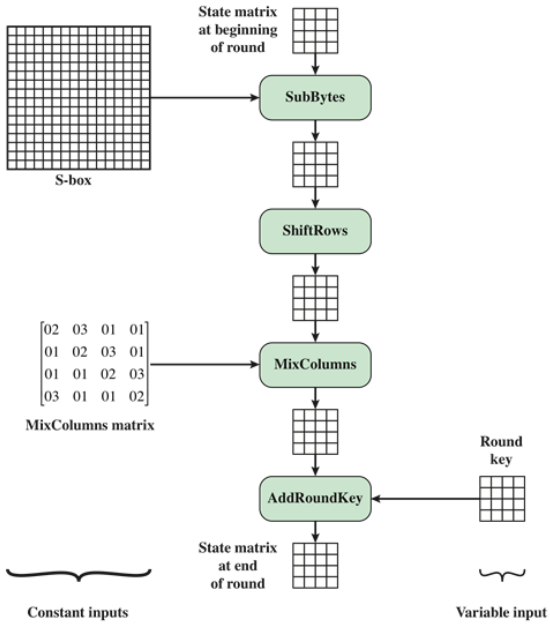


Fig. 2. Four processes in one round of AES encryption.

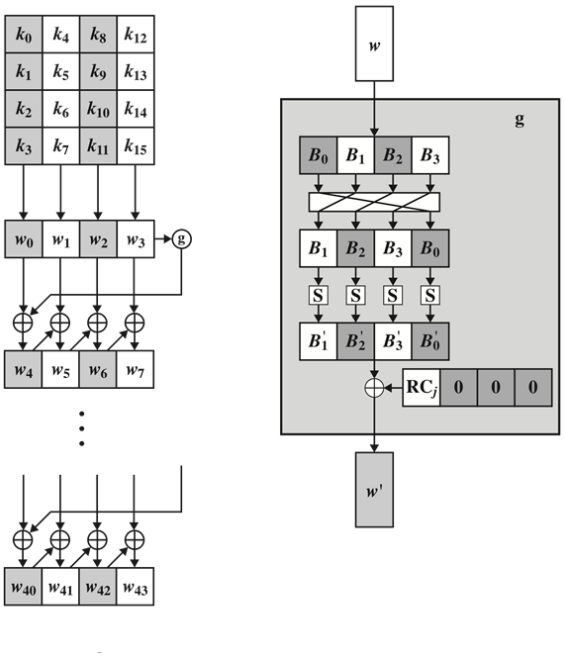


Fig. 3. Sub-key generation (a) overall algorithm (b) function g

B. Arnold's CAT Map

Arnold's CAT MAP (ACM) function is essentially a matrix permutation operation [19]. In ACM, the coordinates of a cell (typically pixel when applied on the digital image) in a two dimensional NxN size plane are mapped to new ones where no overlapping is observed. Mathematically, two-member vector of X and Y coordinates for a given cell is multiplied with a special 2x2 matrix under mode N where N is the dimension of plane. The output is a two-member vector consists of new coordinates in the plane for a given cell. It is guaranteed that no two different cell coordinates map into identical new ones. Generic mathematical representation of ACM is shown in equation (1) where X, Y and X', Y' represent the old and new coordinate vectors respectively. Special multiplication matrix is formed with two integer numbers, P and Q. Multiplicand-matrix cell at coordinates $[1,1]$ should always have the value 1. Whereby, cells at coordinates $[1,2]$ and $[2,1]$ should have P and Q integer values of choice and in any order. Finally the last cell at coordinates $[2,2]$ should hold the result of $P \times Q + 1$. This definition of multiplicand matrix guarantees the determinant is always 1, so the multiplicand has a real inverse matrix. See equation (2) for the definition of inverse of the multiplicand matrix.

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \left\{ \begin{bmatrix} 1 & P \\ Q & P \times Q + 1 \end{bmatrix} \times \begin{bmatrix} X \\ Y \end{bmatrix} \right\} mod N \tag{1}$$

$$\begin{bmatrix} P \times Q + 1 & -P \\ -Q & 1 \end{bmatrix} \tag{2}$$

Iterative execution of ACM calculation with identical parameters (P,Q,N) assure that the initial state will ever be reached without any information loss. In Figure-4 ACM iterations with parameters $P = 1$, $Q = 1$ and $N = 144$ are shown. With the given parameters the iteration count for full cycle is observed as 11. Picture returns back to initial state after 11 iterations [20]. Iteration order in Figure-4 is row-wise.

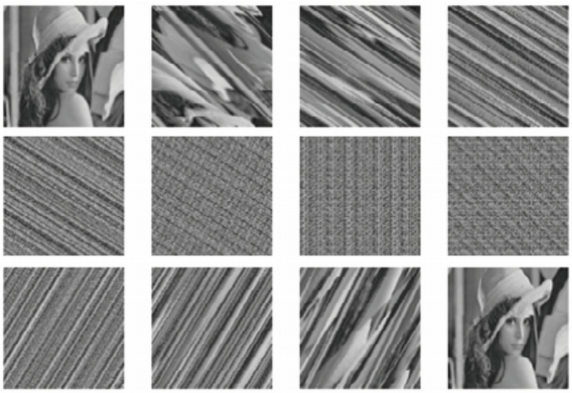


Fig. 4. Arnold's CAT Map period of Lena picture (144x144) with P=1,Q=1. Sequence is row-wise

As it can easily be observed in Figure-4, the most imperceptible state is normally achieved about the half of the full cycle iterations count. In Figure-4 it is 5 or 6.

III. Methodology

Our proposed encryption scheme removes the shift-rows step of the AES encryption algorithm and instead introduces a new permutation step using Arnold's CAT Map. Since proposed scheme works by modifying AES slightly, we call it modified AES (mAES).

In the modified algorithm shift-rows step is discarded, while other three steps, namely AddRoundKey, SubBytes and MixColumns, are left untouched. Instead of the removed shift-rows step we introduce a new step arnold-mix. In the arnold-mix step, state matrix is permutated with the help of ACM. Order of the steps remain same as AES, but instead of shift-rows, arnold-mix step is performed.

To perform arnold-mix, P, Q values and the number of iterations are needed to be known. Since in AES 16-byte block is mapped into a 4x4 matrix N is fixed as 4. P and Q are selected to be the first and second byte of the current round-key. Moreover, ACM periods of unique (P, Q) pairs can be pre-calculated for later use as a look-up table.

Arnold-mix step works as follows. First, P and Q values are selected as the first and second byte of the current round-key, respectively. Then a look-up is performed to find the period from pre-calculated values with given P and Q. State matrix is then permuted period/2 times using ACM permuation algorithm.

TABLE I
Avalanche Effects of AES and mAES

Round No	AES Plaintext	mAES Plaintext	AES Key	mAES Key
0	1	1	1	1
1	20	20	22	60
2	58	34	58	69
3	59	37	67	58
4	61	32	63	68
5	68	35	81	58
6	64	66	70	58
7	67	70	74	69
8	65	68	67	65
9	61	53	59	64
10	58	67	53	60

In each round, unlike shift-rows, applied permutation would be different since P and Q values are selected from the round-key.

IV. Results

In our evaluation we used avalanche effect to measure the effectivness of mAES compared to standard AES-128. We performed two types of experiments. In one type of experiment we used the same key to encrypt two plaintexts which differ only by one bit and measured the number of different bits between the corresponding chiphertexts. In the other type of experiment we encrypted the same plaintext using two keys, which differ only by one bit and again measured the number of different bits between the resulting ciphertexts. We performed each type of experiment with both AES-128 and mAES.

For the first type of experiment we encrpyted two plaintexts which only differ at 8th bit with a key, first using AES-128 and then using mAES. We recorded the number of different bits at reach round during the encryption proces.

For the second type of experiment, we encrypted a plaintext, with two different keys differing only at 8th bit, first using AES-128 then using mAES. We then measured the avalanche effect caused by the single bit change in two different encryption schemes.

Encrypted plaintexts and ciphertexts at each round along with the number of different bits between two plaintexts can be seen on Tables 2-5. First row of the tables show the initial plaintexts. Note that plaintexts start same on Tables 4 and 5 but since we use different keys ciphertexts differ.

Results of our experiments can be seen on Table 1 and Figure 5. Number of different bits observed becomes quite close to eachother after round 6. At the end of 10 rounds there is no significant difference between different approaches.

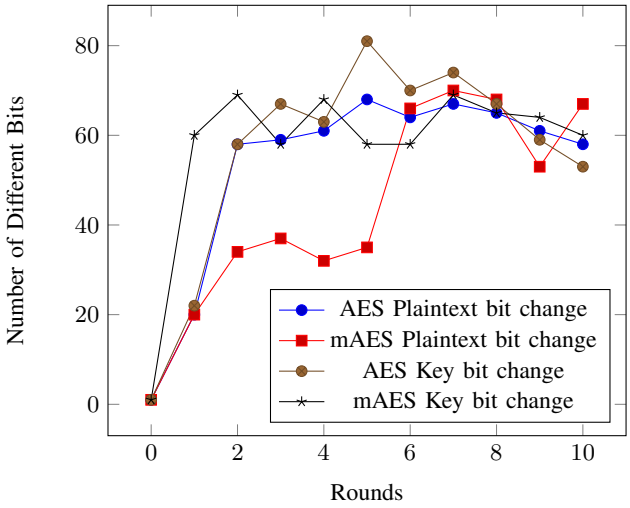


Fig. 5. Avalanche effect in AES and mAES

TABLE II
AVALANCHE EFFECT IN AES WITH PLAINTEXT BIT CHANGE

Round No	Ciphertexts	# of Different Bits
	0123456789abcdeffedcba9876543210 0023456789abcdeffedcba9876543210	1
0	0e3634aece7225b6f26b174ed92b5588 0f3634aece7225b6f26b174ed92b5588	1
1	657470750fc7ff3fc0e8e8ca4dd02a9c c4a9ad090fc7ff3fc0e8e8ca4dd02a9c	20
2	5c7bb49a6b72349b05a2317ff46d1294 fe2ae569f7ee8bb8c1f5a2bb37ef53d5	58
3	7115262448dc747e5cdac7227da9bd9c ec093dfb7c45343d689017507d485e62	59
4	f867aee8b437a5210c24c1974cffeabc 43efdb697244df808e8d9364ee0ae6f5	61
5	721eb200ba06206dcbd4bce704fa654e 7b28a5d5ed643287e006c099bb375302	68
6	0ad9d85689f9f77bc1c5f71185e5fb14 3bc2d8b6798d8ac4fe36a1d891ac181a	64
7	db18a8ffa16d30d5f88b08d777ba4eaa 9fb8b5452023c70280e5c4bb9e555a4b	67
8	f91b4fbfe934c9bf8f2f85812b084989 20264e1126b219aef7feb3f9b2d6de40	65
9	cca104a13e678500ff59025f3bafaa34 b56a0341b2290ba7dfdfbddcd8578205	61
10	ff0b844a0853bf7c6934ab4364148fb9 612b89398d0600cde116227ce72433f0	58

V. CONCLUSION

In this study we present a new encryption scheme merging chaos based encryption and standard AES algorithm. Our intention is to increase complexity and diffusion by having a chaotic calculation to each encryption round. Byte permutation performed in ACM would meet the fuctionality of ShiftRows step in a more complex way, since ShiftRows operation is fixed at each round but ACM permutation changes each round depending on the round keys.

TABLE III
AVALANCHE EFFECT IN MAES WITH PLAINTEXT BIT CHANGE

Round No	Ciphertexts	# of Different Bits
	0123456789abcdeffedcba9876543210 0023456789abcdeffedcba9876543210	1
0	0e3634aece7225b6f26b174ed92b5588 0f3634aece7225b6f26b174ed92b5588	1
1	d8f7520cc8358ebe808eb36555283d19 d8f7520cc8358ebe808eb36588f541b8	20
2	698dd616461d410f8cf8472504f80fca bd42bdfa461d410f59ff469c04f80fca	34
3	764ea61cbabb495894839398b4344b7f 764ea61c241cbc7794839398307bfc17	37
4	b414c474c5ca9876f0a5bf46997d05f7 4a7718a4c5ca9876a061ecf4997d05f7	32
5	9ae903b09030e602db2ece77fff5faab 8bcf496b9030e6028d7530bafff5faab	35
6	89587a312d52d18e77c42ee222e15e17 92c675b132d5a65553a0597184d3c981	66
7	19b58aa8bd2bee9944696270872c8491 17a03d21828678f4b710595aaca60b1f	70
8	4645d060d6bbf1bc5bf9bf807ae0d7e5 749821984c598fcd632a519ce2898d41	68
9	5bcbfd8018b20a9cc210b635b9a31665 b349bd51d49a38be134994ebfec25a02	53
10	9144bdc4ec92540346520ded2b117fa8 c9b5d1bb01bdad39127623f1ce9e1fd8	67

TABLE IV
AVALANCHE EFFECT IN AES WITH KEY BIT CHANGE

Round No	Ciphertexts	# of Different Bits
	0123456789abcdeffedcba9876543210 0123456789abcdeffedcba9876543210	0
0	0e3634aece7225b6f26b174ed92b5588 0f3634aece7225b6f26b174ed92b5588	1
1	657470750fc7ff3fc0e8e8ca4dd02a9c c5a9ad090ec7ff3fc1e8e8ca4cd02a9c	22
2	5c7bb49a6b72349b05a2317ff46d1294 90905fa9563356d15f3760f3b8259985	58
3	7115262448dc747e5cdac7227da9bd9c 18aeb7aa794b3b66629448d575c7cebf	67
4	f867aee8b437a5210c24c1974cffeabc f81015f993c978a876ae017cb49e7eec	63
5	721eb200ba06206dcbd4bce704fa654e 5955c91b4e769f3cb4a94768e98d5267	81
6	0ad9d85689f9f77bc1c5f71185e5fb14 dc60a24d137662181e45b8d3726b2920	70
7	db18a8ffa16d30d5f88b08d777ba4eaa fe8343b8f88bef66cab7e977d005a03c	74
8	f91b4fbfe934c9bf8f2f85812b084989 da7dad581d1725c5b72fa0f9d9d1366a	67
9	cca104a13e678500ff59025f3bafaa34 0ccb4c66bbfd912f4b511d72996345e0	59
10	ff0b844a0853bf7c6934ab4364148fb9 fc8923ee501a7d207ab670686839996b	53

TABLE V
AVALANCHE EFFECT IN MAES WITH KEY BIT CHANGE

Round No	Ciphertexts	# of Different Bits
	0123456789abcdeffedcba9876543210 0123456789abcdeffedcba9876543210	0
0	0e3634aece7225b6f26b174ed92b5588 0f3634aece7225b6f26b174ed92b5588	1
1	d8f7520cc8358ebe808eb36555283d19 53b0e1248cd32abec7c1494a001bacbf	60
2	698dd616461d410f8cf8472504f80fca f285798b211ddd60bfbdca9df84a9215	69
3	764ea61cbabb495894839398b4344b7f 79a7ce1c78ff5c65258de6dfa7d6fe87	58
4	b414c474c5ca9876f0a5bf46997d05f7 a52e4b57240eff59b07d603b10132888	68
5	9ae903b09030e602db2ece77fff5faab a20e43c0e7641d17bf25052ff9e8ce22	58
6	89587a312d52d18e77c42ee222e15e17 e27bf8ad11ccd55e2d957f207407bc20	58
7	19b58aa8bd2bee9944696270872c8491 5489468b94df22780b078f1e4f8f78e9	69
8	4645d060d6bbf1bc5bf9bf807ae0d7e5 80decd43c8f34b1124fadd6844377ba1	65
9	5bcbfd8018b20a9cc210b635b9a31665 90d8e89af7df09989bb24a664053d087	64
10	9144bdc4ec92540346520ded2b117fa8 310bb01bfcca8d7b71d6381d9156f522	60

Our results show that the avalance effect of mAES is closer to ideal than standard AES. In the experiment where the bit change occurs in the plaintext, avalanche effect of proposed algorithm was observed as 67 bits, while that of standard AES' was observed as 58 bits at the end of encrpytion process. Furthermore, in the experiment where the bit change occurs in the key, avalance effect of proposed scheme was observed as 60 bits, while that of standard AES' was observed as 53 bits at the end of encrpytion process. In both cases average avalanche effect of proposed scheme is recorded to be closer to 64 bits (i.e. half of block size) than standard AES. Although, more tests should be conducted, the findings in the study suggest a better strength in encrpytion. Such that chaos enhanced AES (mAES) may provide better grounds for increased security.

We plan to extend this study with the following future works.

- Specific and average effect of each bit position in both key and data block on avalanche effect calculation.
- Replace the substution steps with Arnold's CAT Map algorithm as well.
- Conduct comparative tests on randomness of the ciphertext.
- Implement comparative tests on timing of the algoritm.

REFERENCES

[1] L. Kocarev and S. Lian, *Chaos-based Cryptography: Theory, Algorithms and Applications*, ser. Studies in Computational Intelligence. Springer Berlin Heidelberg, 2011. [Online]. Available: https://books.google.com.tr/books?id=GyNwXgkCUMIC

[2] W. Stallings, *Cryptography and Network Security: Principles and Practice, Global Edition*. Pearson Education, 2016. [Online]. Available: https://books.google.com.tr/books?id=mYDbAQAACAAJ

[3] R. Adler and R. Palais, "Homeomorphic conjugacy of automorphisms on the torus," *Proceedings of the American Mathematical Society*, vol. 16, no. 6, pp. 1222–1225, 1965.

[4] P. R. Halmos, "On automorphisms of compact groups," *Bulletin of the American Mathematical Society*, vol. 49, no. 8, pp. 619–624, 1943.

[5] A. Borel and N. R. Wallach, *Continuous cohomology, discrete subgroups, and representations of reductive groups*. American Mathematical Soc., 2013, vol. 67.

[6] A. Soleymani, M. J. Nordin, and E. Sundararajan, "A chaotic cryptosystem for images based on henon and arnold cat map," *The Scientific World Journal*, vol. 2014, 2014.

[7] L. Shujun, M. Xuanqin, and C. Yuanlong, "Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography," in *International Conference on Cryptology in India*. Springer, 2001, pp. 316–329.

[8] Y. Zhang, P. Xu, and L. Xiang, "Research of image encryption algorithm based on chaotic magic square," in *Advances in Electronic Commerce, Web Application and Communication*. Springer, 2012, pp. 103–109.

[9] Z.-H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Physics Letters A*, vol. 346, pp. 153–157, 10 2005.

[10] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2191–2199, 2009.

[11] J. Keating, "Asymptotic properties of the periodic orbits of the cat maps," *Nonlinearity*, vol. 4, no. 2, p. 277, 1991.

[12] C. Fu, B.-b. Lin, Y.-s. Miao, X. Liu, and J.-j. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Optics communications*, vol. 284, no. 23, pp. 5415–5423, 2011.

[13] H. Liu, Z. Zhu, H. Jiang, and B. Wang, "A novel image encryption algorithm based on improved 3d chaotic cat map," in *2008 The 9th International Conference for Young Computer Scientists*. IEEE, 2008, pp. 3016–3021.

[14] K. Suneja, S. Dua, and M. Dua, "A review of chaos based image encryption," in *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*. IEEE, 2019, pp. 693–698.

[15] M. Talbi, "Speech signal embedding into digital images using encryption and watermarking techniques," in *International conference on the Sciences of Electronics, Technologies of Information and Telecommunications*. Springer, 2018, pp. 3–13.

[16] E. Pawan and K. Kaharuddin, "Kombinasi arnold cat map dan modifikasi hill cipher menggunakan kode bunyi beep bios phoenix," *SISFOTENIKA*, vol. 9, no. 2, pp. 159–168, 2019.

[17] J. Thiyagarajan, B. Murugan, and N. G. A. Gounden, "A chaotic image encryption scheme with complex diffusion matrix for plain image sensitivity," *Serbian Journal of Electrical Engineering*, vol. 16, no. 2, pp. 247–265, 2019.

[18] R. A. E. B. L. Knudsen, "Serpent: A proposal for the advanced encryption standard," in *First Advanced Encryption Standard (AES) Conference, Ventura, CA*, 1998.

[19] C. Cokal and E. Solak, "Cryptanalysis of a chaos-based image encryption algorithm," *Physics Letters A*, vol. 373, no. 15, pp. 1357–1360, 2009.

[20] D. Elmacı and N. B. Catak, "An efficient image encryption algorithm for the period of arnold's cat map," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 6, no. 1, pp. 80–84, 2018.

Bazı Kod Tabanlı Kuantum Sonrası Algoritmaların Performans Analizleri

Performance Analysis of Some Code Based Post Quantum Algorithms

Zülfükar SAYGI
Matematik Bölümü
TOBB Ekonomi ve Teknoloji Üniversitesi
Ankara, Türkiye
zsaygi@etu.edu.tr

Burcu Ecem YILMAZ
Matematik Bölümü
TOBB Ekonomi ve Teknoloji Üniversitesi
Ankara, Türkiye
burcuecemyilmaz@gmail.com

***Özet*—Bu çalışmada NIST'in Kuantum Sonrası Kriptografi Standartlaştırma çağrısı kapsamında anahtar kapsülleme mekanizması olarak önerilen sekiz farklı kod tabanlı algoritmanın performansları karşılaştırılmıştır. Bu algoritmalar uzun yıllardır literatürde bulunan klasik McEliece sisteminin farklı kodlar kullanılarak değiştirilmiş ve iyileştirilmiş versiyonlarıdır. Performans ölçümleri 128-bit, 192-bit ve 256-bit güvenlik seviyeleri için dört farklı bilgisayar ortamında çalıştırılarak yapılmıştır.**

Anahtar Kelimeler—Kuantum sonrası kriptografi, kod tabanlı kriptografi, McEliece.

***Abstract*—In this work, the performances of eight different code-based algorithms proposed as key encapsulation mechanism within the scope of NIST post-quantum cryptography standardization call are compared. These algorithms are the modified and improved versions of the classic McEliece system, which has been in the literature for many years, using different codes. Performance measurements were carried out in four different computer environments for 128-bit, 192-bit and 256-bit security levels.**

Keywords—Post-quantum cryptography, code-based cryptography, McEliece.

I. GİRİŞ

Günümüzde yaygın olarak kullanılan açık anahtarlı kriptografi sistemler, güvenilirlikleri çarpanlara ayırma problemine dayalı RSA, ayrık logaritma problemine dayalı Diffie-Hellman anahtar değişimi ve DSA imza algoritması, eliptik eğri ayrık logaritma problemine dayalı ECCDSA algoritmalarıdır. Ancak yeterince güçlü kuantum bilgisayarların kullanılmaya başlanması durumunda bu algoritmaların polinom zamanda kırılabileceği Shor algoritması [1] ile mümkündür.

Kuantum sonrası kriptografi, kuantum ve klasik bilgisayarlarla yapılan ataklara karşı güvenli olan kriptografik sistemlerin geliştirilmesini amaçlamaktadır. Kuantum bilgisayarlar üzerine yapılan çalışmaların son yıllarda artmasıyla 2016 yılında NIST tarafından Kuantum Sonrası Kriptografi Standartlaştırma çağrısı [2] yapılmıştır. 2017 yılında bu kapsamda toplam 69 adet olmak üzere kafes tabanlı, kod tabanlı, özet fonksiyonları tabanlı, çok değişkenli polinom tabanlı ve diğer bazı özel algoritmalar standartlaşma süreci için birinci turda aday olarak sunulmuştur. 2019 ocak ayında ise ikinci tura toplam 26 algoritmanın kaldığı açıklanmıştır [3]. Eksilen 43 algoritma arasında süreçten çekilen, kriptografik olarak zafiyetleri ortaya çıkarılan ve benzer özellikler taşımasından dolayı birleşerek sürece devam eden algoritmalar mevcuttur.

II. KOD TABANLI KRİPTOGRAFİ

Kod tabanlı kriptografi, kuantum bilgisayarla yapılan ataklara karşı dayanıklı açık anahtarlı kriptosistemlerin oluşturulmasında kullanılan ve temel olarak kodlama teorisindeki bazı özel kodların kod çözme işleminin matematiksel zorluğunu temel alan yöntemlerden biridir. İlk kod tabanlı kriptosistem 1978 yılında Robert McEliece tarafından önerilmiştir [4]. Günümüzde önerilen birçok kod tabanlı sistem McEliece sisteminin iyileştirilmiş ve değiştirilmiş versiyonları olarak düşünülebilir. McEliece sisteminin detayları için bazı kodlama teorisi bilgilerini takip eden bölümde vereceğiz. Detaylı ve genel bilgiler için [5] incelenebilir.

A. Lineer Kodlar

Bu bölümde lineer kodların anlaşılması için gerekli bazı temel bilgiler verilecektir. F_q, q elemanlı cisim ve F_q üzerindeki n boyutlu vektör uzayı F_q^n olsun.

F_q^n vektör uzayının k boyutlu bir $\mathcal{C}$ alt uzayına, uzunluğu n ve boyutu k olan *lineer kod* denir ve $[n, k]$ şeklinde gösterilir. $\mathcal{C}$ uzayının her bir elemanı kod kelimesi olarak adlandırılır. $\boldsymbol{x} \in F_q^n$ vektörünün sıfırdan farklı bileşenlerinin sayısına bu vektörün *Hamming ağırlığı* denir ve $\mathrm{wt}(\boldsymbol{x})$ ile gösterilir. $\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}$ olmak üzere, bu iki kod kelimesinin *Hamming uzaklığı* $d(\boldsymbol{x}, \boldsymbol{y})$ birbirlerinden farklı koordinatlarının sayısıdır. Özel olarak $d(\boldsymbol{x}, \boldsymbol{y}) = wt(\boldsymbol{x} - \boldsymbol{y})$ eşitliği sağlanır. Bir $\mathcal{C}$ lineer kodunun *minimum uzaklığı* bu kod içerisindeki birbirinden farklı tüm kod kelimeleri arasındaki uzaklıkların en küçük değeri olarak tanımlanır. Özel olarak bu uzaklık lineer kodlarda minimum ağırlığa sahip kod kelimesinin ağırlığına eşittir. Minimum uzaklığı d olan bir $\mathcal{C}$ lineer kodu ile en fazla $d-1$ tane hata tespit edebilir ve en fazla $\left\lfloor \frac{d-1}{2} \right\rfloor$ tane hata düzeltebilir.

Satırları $\mathcal{C}$ kodunun bir bazını oluşturan $k \times n$ boyutlarındaki G matrisine $\mathcal{C}$ - $[n,k]$ lineer kodunun *üreteç matrisi* denir ve bu durumda $\mathcal{C} = \{\boldsymbol{m}G \mid \boldsymbol{m} \in F_q^k\}$ olarak yazılabilir. $\mathcal{C}$ kodunun ortogonal tümleyeni olan $\mathcal{C}^{\perp} = \{\boldsymbol{x} \in F_q^n : \forall \boldsymbol{y} \in \mathcal{C}, \boldsymbol{x} \cdot \boldsymbol{y} = \boldsymbol{0}\}$ kümesi *dual kod* olarak adlandırılır ve bu durumda $\mathcal{C}^{\perp}$ - $[n, n-k]$ lineer kod olur. $\mathcal{C}^{\perp}$ kodunun $(n-k) \times n$ boyutlarındaki H üreteç matrisi $\mathcal{C}$ kodunun *eşlik-denetim matrisi* olarak adlandırılır ve burada $\mathcal{C} = \{\boldsymbol{c} \in F_q^n \mid H\boldsymbol{c}^{\boldsymbol{T}} = 0\}$ olur.

B. McEliece Kriptosistemi

McEliece algoritmasının genel fikri hata düzeltebilen lineer kod ailesinden seçilen ve rastgele hata eklenmiş bir kod kelimesini şifreli metin olarak kullanmaktır. Açık anahtar olarak kodun üreteç matrisi kullanılır. Kod ailesi için gizli, hızlı kod çözen algoritmayı bilen kullanıcılar şifreli metinden hataları uzaklaştırarak açık metne ulaşabilirler [6].

Literatüre ilk sunulan McEliece kriptosisteminde hızlı kod çözme algoritmasına sahip olan Goppa kodlarının kullanılması önerilmiştir. Ancak iyi kod çözme algoritmasına sahip olan herhangi bir kod ailesi de kullanılabilir. McEliece kriptosistemi anahtar üretimi, şifreleme ve şifre çözme olmak üzere üç adımdan oluşur. F_2 üzerinde en fazla t hata düzeltebilen bir $[n,k]$ ikili lineer kodu verilsin.

Anahtar üretme:

1. Lineer kodun $k \times n$ boyutunda G üreteç matrisi üretilir.
2. $\det(S) \neq 0$ olmak üzere $k \times k$ boyutunda S matrisi ve $n \times n$ boyutunda P permütasyon matrisi oluşturulur.
3. $G' = SGP$ hesaplanır.
4. G' açık anahtar ve S, G, P gizli anahtarları oluşturulur.

Şifreleme:

1. Mesaj k bitlik bloklar olarak kodlanır. $Mesaj = m_1 m_2$ ... olsun.
2. Uzunluğu n ve ağırlığı t olan rastgele e vektörü üretilir.
3. Her bir blok için $c_i = m_i G' + e$ şifreli metin blokları üretilir ve karşı tarafa gönderilir.

Şifre çözme:

1. Her bir blok c_i için $c_i' = c_i P^{-1}$ hesaplanır.
2. Kod çözme algoritması kullanılarak her bir blok için c_i' vektörlerinden m_i' vektörleri elde edilir.
3. Her bir blok için $m_i = m_i' S^{-1}$ hesaplanarak mesaj elde edilir.

McEliece, ilk olarak $\mathrm{n} = 1024,\ \mathrm{k} = 524,\ \mathrm{t} = 50$ parametreleri ile önerilmiştir [4]. Bu durumda açık anahtar uzunluğu yaklaşık olarak $524(1024 - 524) = 262000$-bit olduğundan sistem yeterli ilgiyi görmemiştir. Fakat yeterli güvenlik seviyelerine ulaşmak için bu parametrelerin yeterli olmayacağı gösterilmiş ve 80-bit güvenlik için standart cebirsel kod çözme algoritmaları kullanıldığında $\mathrm{n} = 2048,\ \mathrm{k} = 1751,\ \mathrm{t} = 27$ parametreleri, Goppa kodları için liste kod çözme algoritmaları kullanıldığında $\mathrm{n} = 1632,\ \mathrm{k} = 1269,\ \mathrm{t} = 34$ parametreleri önerilmiştir [7]. Kuantum bilgisayarlara dayanıklı olabilmesi için Goppa kodlarının $\mathrm{n} = 6960,\ \mathrm{k} = 5413,\ \mathrm{t} = 119$ parametreleri ile kullanılabileceği önerilmiştir [8]. Bu durumda ise açık anahtar boyutu yaklaşık olarak $8\mathrm{x}10^6$-bit olmaktadır. NIST'in çağrısına sunulan kod tabanlı algoritmalar, klasik McEliece algoritmasının değiştirilmiş ve iyileştirilmiş versiyonları olarak düşünülebilir.

III. Anahtar Kapsülleme Mekanizması

Anahtar kapsülleme mekanizmaları, asimetrik (açık anahtarlı) kriptosistemleri kullanarak simetrik kriptosistemler için ortak gizli anahtar oluşturmayı hedeflemektedir. Bu mekanizma aşağıdaki gibi üç adımda gerçekleşmektedir:

1. *Anahtar Üretme*: Kapsülleme ve kapsülden çıkarma işlemi için açık ve gizli anahtar üretir.
2. *Kapsülleme*: Açık anahtarı ve rastgele üretilen başka değerleri kullanarak bir şifreli metin ve K anahtarını oluşturur.
3. *Kapsülden Çıkarma*: Şifreli metni ve gizli anahtarı kullanarak K anahtarına ulaşır.

Bu çalışmada NIST'in Kuantum Sonrası Kriptografi Standartlaştırma çağrısı kapsamında anahtar kapsülleme mekanizması olarak önerilen ve birinci turu geçebilen 8 farklı kod tabanlı algoritmanın performansları karşılaştırılmıştır. Bu algoritmalar uzun yıllardır literatürde bulunan klasik McEliece sisteminin farklı kodlar kullanılarak değiştirilmiş versiyonlarıdır. Dolayısıyla güvenilirlikleri McEliece algoritmasında olduğu gibi kod çözmenin zorluğuna dayanmaktadır. Algoritmalar kod çözmenin zorluğu problemini kullandıkları kod ailelerine göre uyarlamışlardır.

Performans ölçümleri 128-bit, 192-bit ve 256-bit güvenlik seviyeleri için 4 farklı bilgisayar ortamında çalıştırılarak yapılmıştır. Çalışmada kullanılan bilgisayarların özellikleri aşağıdaki gibidir:

- **SERVER** – POWER8 (architected), altivec supported CPU@4116.000000MHz, 107GB SCSI Disk, Linux 64-bit,
- **ASUS** – Intel® Core™ i7-6500u CPU @ 3.16GHz, 512 GB SSD, Ubuntu 64-bit,
- **FUJITSU** – Intel® Core™ i5-3230M CPU @ 2.60GHz, Ubuntu 64-bit,
- **MAC** – Intel® Core™ i5-5257U CPU @ 2.70GHz, Ubuntu 64-bit.

128-bit güvenlik seviyesi için tüm algoritmalarda 10 anahtar üretimi, 10 anahtar kapsülleme ve 10 kapsülden çıkarma işlemi yapılarak çalışma süreleri milisaniye cinsinden ölçülmüştür. Bu sürelerin ortalama değerleri alınarak anahtar üretimi için Tablo I'de, anahtar kapsülleme işlemi için Tablo II'de ve kapsülden çıkarma için Tablo III'te verilmiştir.

Tablo I incelendiğinde, 128-bit güvenlik seviyesi için dört bilgisayarda da en hızlı anahtar üretimi yapan algoritmanın BIKE olduğu görülmektedir. BIKE algoritmasını sırasıyla Ouroboros-R, HQC ve LAKE algoritmaları takip etmektedir. LEDAkem diğerlerine göre daha yavaştır. BIG QUAKE ve RLCE ise en yavaş anahtar üretimi yapan algoritmalardır.

Tablo II'den 128-bit güvenlik seviyesi için dört bilgisayarda da en hızlı kapsülleme işlemini gerçekleştiren algoritmanın anahtar üretiminde olduğu gibi yine BIKE olduğu görülmektedir. BIKE algoritmasını sırasıyla LAKE, LOCKER Ouroboros-R ve HQC algoritmaları takip etmektedir.

Kapsülleme aşaması için BIG QUAKE, LEDAkem ve RLCE daha yavaşlardır ancak diğer algoritmalarla aralarında anahtar üretiminde olduğu gibi büyük bir fark yoktur.

TABLO I. 128-BİT GÜVENLİK SEVİYESİ İÇİN ANAHTAR ÜRETME SÜRELERİ (ms)

Algoritma		Server	Asus	Fujitsu	Mac
BIG QUAKE		556,059	346,654	423,731	353,484
BIKE	BIKE-1	1,873	0,113	0,355	0,148
	BIKE-2	4,357	2,399	2,942	2,569
	BIKE-3	0,238	0,086	0,232	0,147
HQC	HQC-I	0,388	1,231	0,557	1,539
	HQC-II	0,405	1,349	0,378	1,547
	HQC-III	0,427	1,575	0,808	1,731
LAKE		2,320	1,079	2,324	1,321
LEDAkem			50,165	59,831	53,078
LOCKER	LOCKER I	4,720	1,732	4,688	1,921
	LOCKER IV	6,620	11,477	7,468	12,015
	LOCKER VII	14,880	19,096	15,457	23,509
Ouroboros-R		0,431	0,262	0,670	0,298
RLCE	RLCE-A	611,140	216,439	249,944	219,541
	RLCE-B	1263,650	457,284	581,987	510,340

TABLO II. 128-BİT GÜVENLİK SEVİYESİ İÇİN ANAHTAR KAPSÜLLEME SÜRELERİ (ms)

Algoritma		Server	Asus	Fujitsu	Mac
BIG QUAKE		2,314	1,509	1,801	1,609
BIKE	BIKE-1	1,936	0,117	0,409	0,159
	BIKE-2	0,382	0,081	0,158	0,122
	BIKE-3	0,439	0,123	0,351	0,138
HQC	HQC-I	0,674	1,371	1,111	1,609
	HQC-II	0,689	1,386	0,792	1,980
	HQC-III	0,716	1,565	1,259	1,727
LAKE		0,359	0,197	0,441	0,253
LEDAkem			2, 172	3,706	3,260
LOCKER	LOCKER I	0,651	0,349	0,590	0,432
	LOCKER IV	0,860	1,904	0,770	2,194
	LOCKER VII	1,598	1,733	0,933	2,094
Ouroboros-R		0,654	0,334	0,946	0,320
RLCE	RLCE-A	3,548	1,182	3,376	1,341
	RLCE-B	5,516	1,872	5,337	2,301

TABLO III. 128-BİT GÜVENLİK SEVİYESİ İÇİN KAPSÜLDEN ÇIKARMA SÜRELERİ (ms)

Algoritma		Server	Asus	Fujitsu	Mac
BIG QUAKE		2,879	1,745	2,259	1,745
BIKE	BIKE-1	13,659	1,507	2,476	1,693
	BIKE-2	3,358	1,531	2,279	1,642
	BIKE-3	2,612	1,780	2,870	1,812
HQC	HQC-I	1,367	0,920	1,770	1,301
	HQC-II	1,437	0,813	1,369	1,091
	HQC-III	1,379	0,900	1,944	1,019
LAKE		1,183	0,829	0,862	0,903
LEDAkem			2071,975	20,624	2932,986
LOCKER	LOCKER I	2,480	1,658	2,411	1,983
	LOCKER IV	2,884	7,612	1,911	9,521
	LOCKER VII	4,952	5,454	3,155	5,998
Ouroboros-R		1,029	0,711	1,782	0,699
RLCE	RLCE-A	7,319	2,705	334,215	3,405
	RLCE-B	10,892	4,010	528,394	5,399

Tablo III'te 128-bit güvenlik seviyesinde dört bilgisayarda da kapsülden çıkarma işlemi için öne çıkan algoritmanın Ouroboros-R olduğu görülmektedir. Ardından sırasıyla LAKE, HQC, BIKE ve BIG QUAKE algoritmaları gelmektedir. En yavaş olanlar ise RLCE ve LEDAkem algoritmalarıdır.

192-bit güvenlik seviyesi için de 10'ar kere anahtar üretimi, anahtar kapsülleme ve kapsülden çıkarma işlemi yapılarak çalışma süreleri milisaniye cinsinden ölçülmüştür. Bu sürelerin ortalama değerleri anahtar üretimi için Tablo IV'te, anahtar kapsülleme işlemi için Tablo V'te ve kapsülden çıkarma için Tablo VI'da verilmiştir.

TABLO IV. 192-BİT GÜVENLİK SEVİYESİ İÇİN ANAHTAR ÜRETME SÜRELERİ (ms)

Algoritma		Server	Asus	Fujitsu	Mac
BIG QUAKE		4829,134	3081,125	3829,313	3423,600
BIKE	BIKE-1	23,451	0,214	0,892	0,294
	BIKE-2	15,225	3,095	11,281	3,154
	BIKE-3	0,603	0,242	0,552	0,318
HQC	HQC-I	0,750	2,616	1,066	3,198
	HQC-II	0,776	2,867	1,098	2,980
	HQC-III	0,840	1,945	1,293	2,345
LAKE		2,929	1,176	4,604	1,261
LEDAkem			209,324	251,610	400,031
LOCKER	LOCKER II	5,566	2,177	3,324	3,201
	LOCKER V	7,238	13,011	7,753	13,948
	LOCKER VIII	16,309	22,162	13,621	29,806
Ouroboros-R		0,489	0,266	0,655	0,271
RLCE	RLCE-A	2454,471	861,411	1126,866	893,012
	RLCE-B	4971,158	1982,791	2188,167	2004,059

Tablo IV incelendiğinde 192-bit güvenlik seviyesi için tüm bilgisayarlarda anahtar üretimini en hızlı yapan algoritmaların Ouroboros-R ve BIKE olduğu görülmektedir. Bu iki algoritmadan sonra ise HQC, LAKE ve LOCKER gelmektedir. LEDAkem, RLCE algoritmaları diğerlerine göre oldukça yavaş kalmışlardır ancak en yavaş algoritmanın BIG QUAKE olduğu görülmektedir.

TABLO V. 192-BİT GÜVENLİK SEVİYESİ İÇİN ANAHTAR KAPSÜLLEME SÜRELERİ (ms)

Algoritma		Server	Asus	Fujitsu	Mac
BIG QUAKE		5,107	3,738	4,324	5,734
BIKE	BIKE-1	1,014	0,226	1,064	0,278
	BIKE-2	0,951	0,128	0,453	0,152
	BIKE-3	1,161	0,227	0,915	0,259
HQC	HQC-I	1,324	1,461	1,673	1,810
	HQC-II	1,462	1,312	2,335	1,791
	HQC-III	1,514	1,395	2,774	1,792
LAKE		0,404	0,189	0,549	0,221
LEDAkem			7,928	14,612	8,301
LOCKER	LOCKER II	0,686	0,375	0,505	0,428
	LOCKER V	0,938	2,482	0,612	3,491
	LOCKER VIII	1,646	1,579	0,923	1,971
Ouroboros-R		0,773	0,344	0,827	0,339
RLCE	RLCE-A	8,413	2,804	8,131	3,500
	RLCE-B	12,943	4,777	11,909	5,317

Tablo V'te 192-bit güvenlik seviyesi için tüm bilgisayarlarda anahtar kapsülleme işlemini en hızlı yapan LAKE algoritmasıdır. Ardından sırasıyla Ouroboros-R,

LOCKER, BIKE, HQC ve BIG QUAKE algoritmaları gelmektedir. Bu sürecin en yavaş algoritmalarıysa RLCE ve LEDAkem olduğu görülebilir.

TABLO VI. 192-BİT GÜVENLİK SEVİYESİ İÇİN KAPSÜLDEN ÇIKARMA SÜRELERİ (ms)

Algoritma		Server	Asus	Fujitsu	Mac
BIG QUAKE		11,211	12,187	22,382	14,133
BIKE	BIKE-1	12,723	3,573	6,024	4,201
	BIKE-2	9,127	3,288	6,251	4,009
	BIKE-3	5,685	3,662	6,249	4,267
HQC	HQC-I	2,463	1,650	1,730	2,750
	HQC-II	2,490	1,687	3,418	2,135
	HQC-III	2,538	1,857	3,948	2,272
LAKE		1,918	1,206	1,341	1,529
LEDAkem			5863,974	59,055	5953,342
LOCKER	LOCKER II	2,638	1,685	2,093	2,193
	LOCKER V	3,900	0,189	2,573	0,311
	LOCKER VIII	5,087	4,530	3,009	4,870
Ouroboros-R		1,865	1,188	2,950	0,990
RLCE	RLCE-A	16,099	5,828	804,940	6,318
	RLCE-B	24,228	9,618	1178,949	9,977

Tablo VI'ya bakıldığında 192-bit güvenlik seviyesi için dört bilgisayarda da kapsülden çıkarma işlemini en hızlı gerçekleştiren algoritmaların Ouroboros-R ve LAKE olduğu görülmektedir. Bu iki algoritmadan sonra ise HQC, LOCKER, LAKE ve BIG QUAKE gelmektedir. LEDAkem ve RLCE ise en yavaş algoritmalardır.

Diğer güvenlik seviyelerinde olduğu gibi 256-bit güvenlik seviyesi için de 10'ar kere anahtar üretimi, anahtar kapsülleme ve kapsülden çıkarma işlemi yapılarak çalışma süreleri milisaniye cinsinden ölçülmüştür. Bu sürelerin ortalama değerleri anahtar üretimi için Tablo VII'de, anahtar kapsülleme işlemi için Tablo VIII'de ve kapsülden çıkarma için Tablo IX'da verilmiştir.

TABLO VII. 256-BİT GÜVENLİK SEVİYESİ İÇİN ANAHTAR ÜRETME SÜRELERİ (ms)

Algoritma		Server	Asus	Fujitsu	Mac
BIG QUAKE		8733,030	6027,456	6742,165	6587,916
BIKE	BIKE-1	1,334	0,315	1,633	0,389
	BIKE-2	23,450	6,970	25,391	7,090
	BIKE-3	1,334	0,329	1,256	0,329
HQC	HQC-I	1,170	3,024	1,853	3,753
	HQC-II	1,270	2,876	2,114	4,201
	HQC-III	1,342	3,626	2,080	4,114
	HQC-IV	1,389	6,379	2,196	6,920
LAKE		3,015	1,200	4,104	2,298
LEDAkem			642,918	817,088	697,170
LOCKER	LOCKER III	6,235	11,756	6,352	13,860
	LOCKER VI	8,103	2,551	9,929	2,832
	LOCKER IX	18,118	6,524	18,738	6,901
Ouroboros-R		0,597	0,355	1,163	0,402
RLCE	RLCE-A	5900,639	2379,420	2788,513	3003,130
	RLCE-B	11682,897	4723,123	5107,598	5099,072

Tablo VII'ye göre 256-bit güvenlik seviyesi için dört bilgisayarda da anahtar üretimini en hızlı yapan algoritmaların Ouroboros-R ve BIKE olduğu görülmektedir. Bu iki algoritmadan sonra ise HQC, LAKE, LOCKER ve LEDAkem gelmektedir. BIG QUAKE ve RLCE ise en yavaş algoritmalardır.

TABLO VIII. 256-BİT GÜVENLİK SEVİYESİ İÇİN ANAHTAR KAPSÜLLEME SÜRELERİ (ms)

Algoritma		Server	Asus	Fujitsu	Mac
BIG QUAKE		7,156	5,340	5,844	6,241
BIKE	BIKE-1	2,595	0,332	1,566	0,402
	BIKE-2	1,015	0,178	0,600	0,199
	BIKE-3	2,592	0,502	1,801	0,704
HQC	HQC-I	2,248	1,732	3,981	2,108
	HQC-II	2,409	2,336	4,518	3,431
	HQC-III	2,619	2,539	4,114	3,021
	HQC-IV	2,690	9,420	4,662	9,812
LAKE		0,446	0,222	0,614	0,281
LEDAkem			21,954	44,102	28,910
LOCKER	LOCKER III	0,783	1,788	0,419	1,901
	LOCKER VI	0,935	0,413	0,513	0,510
	LOCKER IX	1,822	0,858	1,248	1,078
Ouroboros-R		0,951	0,568	1,491	0,570
RLCE	RLCE-A	24,730	7,598	24,800	7,999
	RLCE-B	40,834	12,565	36,413	13,932

Tablo VIII ise 192-bit güvenlik seviyesi için tüm bilgisayarlarda anahtar kapsülleme işlemini en hızlı yapan algoritmanın LAKE olduğunu göstermektedir. Bu algoritmayı sırasıyla LOCKER, Ouroboros-R, BIKE, HQC ve BIG QUAKE takip etmektedir. En yavaş olanlar ise RLCE ve LEDAkem algoritmalarıdır.

TABLO IX. 256-BİT GÜVENLİK SEVİYESİ İÇİN KAPSÜLDEN ÇIKARMA SÜRELERİ (ms)

Algoritma		Server	Asus	Fujitsu	Mac
BIG QUAKE		16,618	16,618	24,873	19,315
BIKE	BIKE-1	13,611	7,806	14,110	7,931
	BIKE-2	12,724	7,889	12,867	9,230
	BIKE-3	13,608	9,606	15,690	10,021
HQC	HQC-I	3,745	2,641	3,481	2,729
	HQC-II	3,877	2,927	2,841	3,921
	HQC-III	4,190	3,741	3,974	4,250
	HQC-IV	4,417	7,311	4,477	8,021
LAKE		2,512	1,751	2,013	2,790
LEDAkem			11140,809	116,214	11998,120
LOCKER	LOCKER III	3,653	7,942	2,545	8,492
	LOCKER VI	3,980	2,133	2,559	2,392
	LOCKER IX	6,490	3,855	4,889	5,908
Ouroboros-R		2,597	2,062	1,885	2,001
RLCE	RLCE-A	48,427	17,528	2455,193	19,420
	RLCE-B	76,103	28,202	3604,934	31,000

Son olarak Tablo IX'da ise 192-bit güvenlik seviyesi için tüm bilgisayarlarda kapsülden çıkarma işlemini en hızlı yapan algoritmaların LAKE ve Ouroboros-R olduğu görülmektedir. Bu algoritmayı sırasıyla HQC, LOCKER, BIKE ve BIG QUAKE takip etmektedir. Anahtar kapsüllemede olduğu gibi

RLCE ve LEDAkem kapsülleme işlemini en yavaş yapan algoritmalardır.

IV. Analiz Sonuçları

Performans analizlerinin sonuçları, anahtar kapsülleme mekanizmasının üç adımı için ortak değerlendirildiğinde Tablo X ortaya çıkmaktadır. Bu tabloya göre BIKE algoritması 128 bit güvenlik seviyesindeki en hızlı algoritmalardandır. 192-bit ve 256-bit güvenlik seviyeleri için kapsülden çıkarma adımında diğer algoritmadan bir adım geride olduğundan tabloda yer almamıştır. HQC algoritması, 128-bit güvenlik seviyesindeki durumunun aksine 192-bit ve 256-bit güvenlik seviyelerinde kapsülleme adımında diğer algoritmalara göre daha yavaş olduğundan tabloda işaretlenmemiştir. LOCKER algoritması da BIKE ve HQC algoritmalarının aksine yalnızca 128-bit güvenlik seviyesinde özellikle anahtar üretimi adımında yavaş kalmıştır. Tüm güvenlik seviyeleri için sekiz anahtar kapsülleme mekanizması arasında en hızlı algoritmalar LAKE ve Ouroroboros-R bulunmuştur.

Ayrıca algoritmaların süreleri incelendiğinde anahtar kapsülleme adımının kapsülden çıkarma ve anahtar üretmeye göre çok daha hızlı olduğu görülmüştür.

TABLO X. Çalışma Sürelerine Göre Öne Çıkan Algoritmalar

Algoritma	128-bit	192-bit	256-bit
BIKE	✓		
HQC	✓		
LAKE	✓	✓	✓
LOCKER		✓	✓
Ouroboros-R	✓	✓	✓

V. Sonuç

Bu çalışma sonucunda NIST'in Kuantum Sonrası Kriptografi Standartlaştırma çağrısı kapsamında aday olan birinci turdaki kod tabanlı algoritmalardan 8 adet anahtar kapsülleme mekanizmasının performans analizleri yapılarak algoritmaların hızları ölçülmüştür. Bu kapsamda en hızlı algoritmalar BIKE, HQC, LAKE, LOCKER ve Ouroboros-R, en yavaş algoritmalar ise LEDAkem ve RLCE olmuştur.

Çalıştırılan algoritmalardan önce çıkan LAKE, LOCKER ve Ouroboros-R algoritmaları birleşerek ROLLO adı altında ikinci turda yer almışlardır. Aynı şekilde BIKE ve HQC algoritmaları ikinci turdaki aday algoritmalar arasındadır. Son olarak LEDAkem algoritması da LEDApkc şifreleme-şifre çözme algoritması ile birleşerek LEDAcrypt ismiyle ikinci tura geçmiştir.

Kaynaklar

[1] P.W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE Comput. Soc. Press. doi:10.1109/sfcs.1994.365700.

[2] Post Quantum Cryptography, Round 1 Submission, https://csrc.nist.gov/Projects/Post-QuantumCryptography/Round-1-Submissions. (Erişim tarihi 31 Temmuz 2019.)

[3] Post Quantum Cryptography, Round 2 Submission, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/round-2-submissions. (Erişim tarihi 31 Temmuz 2019.)

[4] R.J. McEliece, "A public-key cryptosystem based on algebraic coding theory", Deep Space Network progress report, Jet Propulsion Lab., California Inst. Technology, Jan. 1978, pp. 114–116.

[5] S.A. Vanstone, P.C. Van Oorschot, An Introduction to Error Correcting Codes with Applications, Vol. 71, Springer Science & Business Media, 2013.

[6] N. Sendrier, "Code-based cryptography: State of the art and perspectives", IEEE Security & Privacy, 15.4, 2017, pp. 44-50

[7] D.J. Bernstein, T. Lange, C. Peters, "Attacking and defending the McEliece cryptosystem", Proc. 2nd International Workshop on Post-Quantum Cryptography, Lecture Notes in Computer Science, 5299, pp. 31–46, Aug. 2008.

[8] A. Daniel, et al. "Initial recommendations of long-term secure post-quantum systems", PQCRYPTO: Post-Quantum Cryptography for Long-Term Security, https://pqcrypto.eu.org/docs/initial-recommendations.pdf (Erişim tarihi 31 Temmuz 2019.)

Analyzing NIST 2nd-round Lattice-based Post-quantum KEM Algorithms

NIST 2. Tur Kafes Tabanlı Quantum Sonrası Anahtar Kapsülleme Mekanizmalarının Analizi

Berkin AKSOY*, Yusuf Alper BİLGİN*, Murat CENK†,
Murat Burhan İLTER*, Neşe KOÇAK* and Yunus Emre YILMAZ*
*ASELSAN Inc.
Ankara, TURKEY
Email:*{berkinaksoy, yabilgin, mbilter, nesekocak, yeyilmaz}@aselsan.com.tr*
†Institute of Applied Mathematics, METU
Ankara, TURKEY
Email: *mcenk@metu.edu.tr*

***Abstract*—National Institute of Standards and Technology (NIST) in the USA started a post-quantum standardization process in November 2017 and the first evaluation stage was completed in the beginning of 2019. It is expected that one or more algorithms for the public key cryptography will be selected by NIST in a few years. This paper analyzes the second round key encapsulation mechanisms (KEM) based on lattices. To this end, the classification of those algorithms in terms of their types is made and their security, sizes, and performance are discussed. In addition, two types of lattice-based systems namely the ring learning with errors (RLWE) and the module learning with errors (MLWE) are compared and the similarities are highlighted in order to make them simple to understand.**

***Keywords*—Post-quantum cryptography, lattice-based cryptography, key encapsulation mechanism, encryption**

***Öz*—ABD'deki Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) Kasım 2017'de kuantum sonrası standardizasyon sürecini başlattı ve ilk değerlendirme aşaması 2019'un başında tamamlandı. Önümüzdeki birkaç yıl içerisinde NIST tarafından açık anahtarlı kriptografi için bir veya daha fazla algoritmanın seçilmesi bekleniyor. Bu makale, ikinci tura kalan kafes tabanlı anahtar kapsülleme mekanizmalarını (KEM) analiz etmektedir. Bu amaçla, bu tür algoritmaların dayandıkları probleme göre sınıflandırılması yapıldı ve algoritmaların güvenliği, boyutları ve performansları incelendi. Ayrıca, kafes tabanlı iki sistem olan hata ile öğrenme probleminin halka versiyonu (RLWE) ve modül versiyonu (MLWE)'nun karşılaştırılması yapıldı ve bu sistemleri daha anlaşılabilir kılmak için benzerlikleri vurgulandı.**

***Anahtar Sözcükler*—Quantum sonrası kriptografi, Kafes-tabanlı kriptografi, anahtar kapsülleme mekanizması, şifreleme**

I. Introduction

When the large scale quantum computers are built, they will break currently used public key cryptographic systems such as RSA, DSA, or ECC since such computers solve in polynomial time the intractable problems, integer factorization problem and discrete logarithm problem, that ensures the security of those systems against classical computers. Many scientists believe that such computers will be built in the near future while some are suspicious about the establishment of them. In 2015, Michele Mosca from University of Waterloo says [1] that "I estimate a 1/7 chance of breaking RSA-2048 by 2026 and a 1/2 chance by 2031". Some big companies such as Google, Intel, and IBM announce the developments of their research on the quantum computers. Therefore, a great amount of work have been devoted to the replacement of currently used public key cryptographic algorithms with the algorithms that are resistant to attacks done by both classical and quantum computers, called post-quantum cryptography. There are basically five types of post-quantum cryptography. These are lattice-based, multivariate, hash-based, code-based, and supersingular elliptic curve isogeny-based cryptography. There are plenty of public key proposals based on those systems. Some of them such as lattice-based have been studied for more than 20 years but some of them like supersingular elliptic curve isogeny-based are relatively newer than the others.

Due to those developments, National Institute of Standards and Technology (NIST) started the post-quantum cryptography standardization process at the end of 2017. In the beginning of 2019, 17 encryption/KEM (Key Encapsulation Mechanism) and 9 signature algorithms were selected as the second round candidates. There are three types of KEM algorithms selected for the second round; lattice-based, code-based, and isogeny-based and majority of the algorithms are lattice-based type.

In this paper, we analyze lattice-based post-quantum algorithms that were selected as the second round candidates in the NIST post-quantum standardization process. We classify them in terms of the intractable problems that the security is based on. In addition, we compare the security, key and data sizes, and performance of those systems. In order to compare the performances fairly, we run all implementations on the same platform and measure their running times. Furthermore, in order to see the relations deeply, the similarities and differences of the algorithms based on the ring learning with errors and the module learning with errors are discussed and the case they are equivalent is emphasized.

The rest of the paper is organized as follows: NIST PQC (Post Quantum Cryptography) 2nd-round lattice based KEM algorithms are classified regarding the problems their security are based on and key generation, encapsulation and decapsulation algorithms are given in Section II. In Section III, we compare algorithms in terms of performance, security and size. Similarities and differences between module learning with errors (MLWE) and ring learning with errors (RLWE)

based algorithms are emphasized in Section IV and finally we conclude in Section V.

II. Classification of NIST PQC 2nd round lattice-based KEM algorithms

In this section, we classify NIST PQC 2nd round lattice-based KEM algorithms according to the problems they are based on.

Security properties for KEMs are:

- IND-CPA (Indistinguishability under Chosen Plaintext Attack): The adversary may call enryption oracle or other operations for a polynomial bounded time. Then, the adversary selects two message with the same length and send them to challanger. Given a public key, the ciphertext of one of the two possible plaintext, it is infeasible to decide whether the ciphertext is the result of the encryption of the first message or the second one. The adversary may call encryption oracle or other operations for a polynomial bounded of time after receiving ciphertext.
- IND-CCA (Indistinguishability under Chosen Ciphertext Attack): It is similar to IND-CPA, but this time the adversary may call both encryption and decryption oracles. In non-adaptive case, the decryption oracle may only be called before obtaining the challanged ciphertext. On the other hand, in adaptive case it may be called even after obtaining the challange but may not submit the received ciphertext.

A. Learning with Errors (LWE)

LWE [2] problem is constructed by adding noise to the system of linear equation with respect to an error distribution. This problem can be defined as given in [3]. For a given dimension $n \geq 1$, modulus $q \geq 2$ and error probability distribution χ on Z_q, samples of the LWE distribution in normal-form are constructed as

$$(\mathbf{a}, b = \frac{1}{q}\langle \mathbf{a}, \mathbf{s} \rangle + e \bmod 1)$$

by choosing a vector $a \in Z_q^n$ uniformly at random and all components of the secret $s \in Z_q^n$ and e from the distribution χ.

FrodoKEM:

FrodoKEM [4] is designed to satisfy IND-CCA security level, and FrodoPKE is ensured IND-CPA security level. There are three versions of FrodoKEM corresponding to different security levels: Frodo-640 (Level 1), Frodo-976 (Level 3), and Frodo-1344 (Level 5). Apart from generating the matrices, the main operation on KEM and PKE (Public Key Encryption) is matrix-vector product.

For the pseudorandom matrix generation $\mathbf{A}$, both AES-128 or SHAKE-128 algorithm can be used . The error distribution χ on integers is rounded continuous Gaussian Distribution with standard deviation $\sigma \geq 1.4$. In the key generation part, by using generated matrix $\mathbf{A}$ and sampling error matrices from $\mathbf{E}$ and $\mathbf{S}$, the matrix $\mathbf{B}$ can be computed:

$$B = AS + E.$$

Operations are done in modulus $q = 2^D$, where $D \leq 16$. Details of FrodoKEM algorithm can be examined in [4].

B. Ring Learning with Errors (RLWE)

RLWE problem was introduced in [5]. It is a special case of LWE problem where polynomials defined in $\mathcal{R}_q$ are used instead of vectors whose coefficients are defined in $\mathbb{Z}_q$. The problem is defined as follows:

Let χ be a distribution function, and $e \xleftarrow{\$} \chi$ denotes e is sampled following the distribution χ. a is selected as a random but publicly known polynomial in $\mathcal{R}_q$. s and e are small and private polynomials, and selected as $s \xleftarrow{\$} \chi$ and $e \xleftarrow{\$} \chi$. Given a polynomial pair $(a \in \mathcal{R}_q, b \in \mathcal{R}_q)$, while the decision problem is to decide whether the polynomial b is constructed as $b = (a \cdot s + e)$ or it is generated randomly in $\mathcal{R}_q$, the search problem is to find the private polynomial s.

NewHope:

NewHope [6] is one of the fastest and most promising NIST post-quantum standardization candidates. Its security relies on decision version of RLWE problem.

NewHope cryptosystem includes two KEMs which are NewHope-CPA-KEM and NewHope-CCA-KEM. Both schemes are constructed by using NewHope-Simple [7] scheme which is referred as NewHope-CPA-PKE. This is not a part of the specification. It is only used to construct NewHope-CPA-KEM and NewHope-CCA-KEM. The pseudocodes for these algorithms may be examined in [6]. Some important parts of NewHope-CPA-PKE algorithm are given below. Please refer to [6] for more detailed information.

Secret term s and error term e of NewHope are distributed by using centered binomial distribution ψ_k of parameter $k = 8$. Moreover, the parameters of NewHope are selected such that a fast and efficient NTT (Number Theoretic Transform) can be performed for polynomial multiplication. Therefore, NTT is one of the most important part of NewHope.

C. Module Learning with Errors (MLWE)

MLWE problem [8], [9] is an interpolation between LWE and RLWE and was proposed to point out imperfections in both problems. Standard LWE-based cryptosystems has the advantage of easy scalability, but suffers from efficiency. On the other hand, RLWE-based schemes are efficient in terms of both speed and size, but their additional structure might make them more vulnerable to attacks. MLWE offers trade-offs between these two. The MLWE problem can be informally viewed as taking the RLWE problem and replacing the ring elements a and s with module elements over the same ring. With this perspective, RLWE can be seen as MLWE with module rank 1.

A formal definition for MLWE can be given as follows. Let χ be a distribution function, and $e \xleftarrow{\$} \chi$ denotes e is sampled following the distribution $\chi \in \mathcal{R}_q$. a is selected uniformly random in $(\mathcal{R}_q)^d$, where d is the rank of the module. All components of the secret $s \in (\mathcal{R}_q)^d$ and e are chosen from the distribution χ. Given some uniform random $a \in (\mathcal{R}_q)^d$, the decision problem is to decide whether the polynomial b is constructed as $b = a \cdot s + e$ or it is generated randomly in $\mathcal{R}_q$ and the search problem is to find the secret polynomial s.

CRYSTALS-KYBER:

KYBER [10] is an IND-CCA2-secure KEM whose security relies on the hardness of MLWE problem. Different from the usual definition of MLWE, in KYBER b is constructed as $b = A \cdot s + e$, where A is a matrix over $(\mathcal{R}_q)^{d \times d}$

(with a small rank, like 3). KYBER has three versions namely, KYBER512, KYBER768 and KYBER1024 leading to different security levels.
In KYBER, NTT is used only in the sampling of $\mathbf{A}$ and the public key. KYBER uses a deterministic approach to sample elements in $\mathcal{R}_q$ which are statistically close to a uniformly random distribution. For noise sampling, a centered binomial distribution is used. Symmetric primitives used in KYBER are SHAKE-128, SHA3-256, SHA3-512 and SHAKE-256. An interested reader may refer to [11] for a more comprehensive view of the algorithm.

D. Module Learning with Rounding (MLWR)

LWE based schemes use samples from noise distributions which requires randomness. However, schemes based on Learning with Rounding (LWR) obtain noise deterministically by reducing from modulus q to modulus p, where $p|q$. Module versions of LWE/LWR problems decrease computational complexity and bandwidth. Also, modules are used to prevent attacks on the ring structure of Ring-LWE/LWR.

SABER:

SABER.KEM [12] is an IND-CCA secure KEM. SABER's security is based on the hardness of the MLWR problem. SABER has three versions, namely LightSaber, Saber and FireSaber.

SHAKE-128 algorithm is used to generate a pseudorandom matrix $A \in {\mathcal{R}_q}^{l \times l}$ from a seed. Also, SHA3-256 and SHA3-512 are used in the protocol. The coefficient vectors of the secret vectors are sampled according to a centered binomial distribution. In SABER, all integer moduli are powers of 2. Therefore, NTT cannot be applied to speed up polynomial multiplication. As multiplication algorithms, Toom-Cook and Karatsuba are used. For more specific information one can see [12].

E. Integer Module Learning With Errors (I-MLWE)

In order to understand I-MLWE, in the first place MLWE must be understood and MLWE is explained briefly in Section II-C. In I-MLWE, instead of reducing each coefficient of the polynomial $mod\ q$, the polynomial is reduced by setting $x = q$. As the result of this, the ring is isomorphic to $\mathbb{Z}/N$, where $N = \phi(q)$ is a generalized Mersenne number. Hence, the noise, encoding and decoding functions for polynomial LWE still work, with the substitution $x = q$.

ThreeBears:

THREEBEARS [13] is a post-quantum KEM which has CCA-secure and CPA-secure variants. THREEBEARS is based on I-MLWE problem and uses the approaches of NEWHOPE [6] and KYBER [10] algorithms.
Due to I-MLWE implementation in THREEBEARS, it follows this pattern of LWE with some small variations, which is to take $x = q = 2^{10}$ and $\phi(x) = x^{312} - x^{156} - 1$.
The encryption system does not work well in the practical applications and hence, some practical improvements are implemented in the algorithm.
For key generation, encapsulation and decapsulation of THREEBEARS algorithm, please refer to [13] for more detailed information.

F. Polynomial-Learning with Errors (PLWE)

PLWE problem was introduced in [14]. It is a special case of RLWE problem.

Let $P := Z[x]/f(x)$, $P_q := P/qP$. $\overline{h} \in P_q$ shows its equivalence class for $h \in P$. Let $\overline{s} \in P_q$ is secret term, PLWE problem involves ℓ PLWE samples $(a_i, a_i \cdot s + e_i)$ for $1 \leq i \leq \ell$ where $a_i \in P_q$ is randomly chosen and publicly known, e_i is sampled from a distribution χ. While the decision problem is to decide whether the polynomial $b_i \in P_q$ is constructed as $b_i = (a_i \cdot s + e_i)$ or it is generated randomly in P_q, the search problem is to find the private polynomial s_i.

LAC:

LAC [15] is a public key cryptographic primitive based on PLWE problem. It is the first instantiation to the RLWE based primitives where the modulus is at a byte level.

LAC consists of four primitives which are a CPA secure public key encryption scheme (LAC.CPA), a CCA secure key encapsulation mechanism (LAC.CCA), a passively secure key exchange protocol (LAC.KE), and an authenticated key exchange protocol (LAC.AKE). LAC.CPA is the main foundation of all these primitives. The main subroutines of LAC.CPA may be found in [15].

This cryptosystem samples secret and error terms from centered binomial distribution. Moreover, the polynomial operations are much more easier than the other NIST candidates since the modulus is at byte level. Therefore, the modular reduction can be performed by simple bitwise operators. The multiplication with s and r can also be implemented by bitwise operators since they are selected from $\{-1, 0, 1\}$. However, using a byte level modulus increases the decryption failures. The designers decided to use BCH error correcting code in order to handle the decryption failure.

G. General Learning with Rounding (GLWR)

GLWR problem is defined in such a way that schemes relying on this problem can be instantiated as relying on LWR or RLWR depending on the parameter set. LWR problem and RLWR problem are similar to LWE and RLWE recpectively. In LWE and RLWE, noise and secret terms are sampled from a distribution. This requires random data and a sampling function. On the other hand, schemes relying on LWR and RLWR obtain the error term by modulus switching which does not require any random data. Therefore, the computation complexity is also decreased.

ROUND5:

ROUND5 [16] proposes both a key encapsulation mechanism and a public key encryption scheme. It is the merger of the submissions Round2 and HILA5. The security relies on GLWR problem. In other words, the security relies on both LWR and RLWR problems in a unified way so that ROUND5 can be instantiated LWR or RLWR depending on the input parameters. There are 18 different parameter sets of ROUND5 which include six ring parameter sets with error correction, six ring parameter sets without error correction, and six non-ring parameter sets. Each of these six parameter sets contain three CPA secure KEM and three CCA secure PKE that achieve security level 1, 3 and 5.

The ring instantiate of ROUND5 uses NTRU ring $\mathbb{Z}_q/(x^{n+1} - 1)$ to improve performance. They also choose p and q as powers of two. Therefore, the rounding function and modular computation can be simply realized by ignoring some bits. Moreover, ROUND5 uses XE error correcting code to decrease the failure rate. XE codes are resistant to timing attacks since they avoid table look-ups and conditions.

H. NTRU

NTRU is public key cryptosystem that use lattice based cryptography to encrypt and decrypt data. Security is based on shortest vector problem (SVP).

CLASSICAL NTRU:

CLASSICAL NTRU [17] proposes quantum resistant key encapsulation mechanism (KEM) that uses lattice based cryptography and recommends two parameter sets referred as NTRU-HPS and NTRU-HRSS. While NTRU-HPS uses fixed-weight sample spaces and allows several choices of q for each n, NTRU-HRSS parameter set uses arbitrary weight sample spaces and fixes q as a function of n. NTRU is a merged version of NTRUEncrypt and NTRU-HRSS-KEM submission in the first round of NIST PQC standardization process. Merged NTRU submission is based on Saito, Xagava and Yamakawa [18] variant of NTRU-HRSS-KEM proposes different variant of NTRU-HRSS-KEM that eliminates the length-preserving message confirmation hash and expensive part of decapsulation routine without impact on security.

NTRU PRIME:

NTRU PRIME [19] provides two key encapsulation mechanisms: "STREAMLINED NTRU PRIME " and "NTRU LPRIME ". Their security are based on shortest vector problem. Both algorithms are designed for the standard goal of IND-CCA2 security.

STREAMLINED NTRU PRIME is optimized from an implementation perspective.

NTRU LPRIME is a variant offering different tradeoffs.

In lattice-based cryptography, attack surface of NTRU PRIME can be significantly reduced with only a minor loss of efficiency. Two cryptosystems in NTRU PRIME are introduced as the smallest and fastest lattice-based cryptosystems. Moreover, some recent attacks based on homomorphisms against lattice-based cryptosystems can be eliminated thanks to NTRU PRIME ring structure. NTRU PRIME uses a prime degree field with a large Galois group and an invert modulus to minimize the number of ring homomorphism available to the attacker.

III. COMPARISON OF ALGORITHMS

In this section, we compare NIST 2nd round lattice-based KEM algorithms in terms of their performance, cost and security levels.

A. Performance

Benchmark tests for all schemes are performed on an Intel Core i7-6500U Skylake processor running at 2500 MHz with Turbo Boost and Hyperthreading disabled. The operating system is Ubuntu 18.04.2 LTS with Linux Kernel 4.15.0, and all softwares are compiled with gcc-7.4.0. The benchmark results for 2nd round lattice-based KEM candidates of NIST post-quantum project are given in Table I. We have taken IND-CCA secure optimized implementations of all given schemes in Table I except for ROUND5 which provides IND-CPA secure KEM. Transformation from IND-CPA to IND-CCA causes some performance loss in all three parts of a scheme which are key pair, encapsulation and decapsulation but mostly in decapsulation operation. Therefore, comparing ROUND5 with the other schemes directly is not appropriate.

B. Security and Size

Key and data size comparison of algorithms together with their security levels is shown in Table II. As can be seen from Table II, among the algorithms having security type IND-CCA and security level 1, LAC has the smallest public key and private key sizes while CLASSICAL NTRU-HPS has the smallest data size. Actually, for level 1 LAC, CLASSICAL NTRU-HPS and SABER are very close regarding the public key, private key and ciphertext sizes. For level 5, LAC has the minimum public key size, THREEBEARS has the minimum private key size and CLASSICAL NTRU-HPS has the minimum data size. On the other hand, FRODOKEM has the largest size values for security levels 1, 3 and 5. The reason why ROUND5 has very small public, private key and data size is it has IND-CPA security type.

IV. COMPARISON OF MLWE AND RLWE

NEWHOPE relies on the hardness of RLWE problem while KYBER relies on the hardness of MLWE problem. Although these two problems are different, one can see RLWE problem as a MLWE problem with module rank 1. The main advantage of MLWE over RLWE is that the dimension of the ring is smaller and it is the same for different security levels. Therefore, changing the security level of a scheme relies on MLWE only requires changing the modulus rank. However, for RLWE, it requires changing the dimension of the ring. Consequently, some security levels may not be reachable for RLWE schemes since the most efficient way to implement RLWE scheme is to choose the dimension as powers of two which does not allow for intermediate security levels. KYBER is defined over the ring $\mathcal{R}_{3329}/(x^{256}+1)$ and NEWHOPE is defined over $\mathcal{R}_{12289}/(x^{512}+1)$ or $\mathcal{R}_{12289}/(x^{1024}+1)$. While KYBER achieves the NIST security levels 1,3 and 5 by adjusting the modulus rank as 2, 3 and 4 respectively, NEWHOPE only achieves the security level 1 and 5 with the rings $\mathcal{R}_{12289}/(x^{512}+1)$ and $\mathcal{R}_{12289}/(x^{1024}+1)$. Recently, [20] proposes a variant of NEWHOPE that achieves the security level 3 over the ring $\mathcal{R}_{3457}/(x^{768}-x^{384}+1)$. Moreover, this variant of NEWHOPE also decreases the modulus q to 3329 for $(n = 512)$ and $(n = 1024)$ by changing the definition of NTT. These recent advances on NTT enable RLWE based schemes to achieve intermediate security levels. An advantage of RLWE over MLWE is that the public parameter $\mathbf{a}$ can be generated by less entendable output function (such as SHAKE-128) call which saves a lot of time.

V. CONCLUSION

Before the arrival of quantum computers, we should be prepared for the new era with quantum-secure algorithms. Therefore, NIST post-quantum standardization process has drawn much attention of both academic and industrial community. After the second round of this process, out of 17 encryption/KEM algorithms, 9 of them are lattice-based.

In this paper, we analyzed NIST PQC 2nd-round lattice-based KEM candidate algorithms. We classified the algorithms according to the hard problems which they are built on. We sketched the most important structures of these algorithms. We also performed the benchmark tests for all schemes and compared them according to their performance. In order to evaluate all algorithms with respect to their sizes, a comparison table showing public key, private key and data

Tablo I
CYCLE COUNTS OF NIST 2ND ROUND LATTICE-BASED KEM CANDIDATES. THE GIVEN CYCLE COUNTS SHOW THE PERFORMANCE OF FULLY OPTIMIZED IMPLEMENTATIONS.

Algorithm	Security Level	Key Pair	Encapsulation	Decapsulation	Total
FRODOKEM	1	1454267	1907695	1848336	5210298
	3	3078807	3697066	3545744	10321617
	5	5239676	6206283	6011942	17457901
KYBER	1	33982	48726	38380	121088
	3	62316	80754	66964	210034
	5	86998	113448	96634	297080
LAC	1	68100	104789	125442	298331
	3	161806	232959	355986	750751
	5	198054	320323	436708	955085
NEWHOPE	1	71946	113364	115976	301286
	5	131845	212306	215136	558927
CLASSICAL NTRU-HPS	1	236118	105342	49630	391090
	3	379971	143316	72792	596079
	5	Not provided			
CLASSICAL NTRU-HRSS	3	381528	90817	76894	549239
STREAMLINED NTRU PRIME	2	1199982	82297	103518	1385797
	3	1580275	90852	109608	1780735
	4	1998035	109806	145072	2252913
NTRU LPRIME	2	68218	111862	134485	314565
	3	74544	118078	140032	332654
	4	93190	152730	186682	432602
ROUND5.nd.5d	1	78186	130968	76929	286083
	3	128308	220761	132231	481300
	5	235368	384159	228650	848177
ROUND5.nd.0d	1	57834	96937	53488	208259
	3	211638	336708	193735	742081
	5	247747	410033	235592	893372
ROUND5.n1.0d	1	571830	658812	291278	1521920
	3	968702	1162340	393356	2524398
	5	2510717	2777599	1531123	6819439
SABER	1	69012	85536	81545	236093
	3	120878	146332	141156	408366
	5	183963	216522	214389	614874
THREEBEARS	2	82891	126590	208841	418322
	4	176460	204989	322912	704361
	5	253365	305334	447359	1006058

sizes was given. Moreover, we discussed the difference of MLWE and RLWE.

REFERENCES

[1] M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?" Cryptology ePrint Archive, Report 2015/1075, 2015, https://eprint.iacr.org/2015/1075.

[2] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing*, ser. STOC '05. New York, NY, USA: ACM, 2005, pp. 84–93.

[3] M. R. Albrecht and A. Deo, "Large modulus ring-lwe $\geq$ module-lwe," Cryptology ePrint Archive, Report 2017/612, 2017, https://eprint.iacr.org/2017/612.

[4] E. Alkim, J. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, C. Peikert, A. Raghunathan, D. Stebila *et al.*, "Frodokem: Learning with errors key encapsulation," *URL: https://csrc. nist. gov/projects/post-quantum-cryptography/round-2-submissions. Citations in this document*, vol. 1, no. 1.3, pp. 1–3, 2019.

[5] V. Lyubashevsky, C. Peikert, , and O. Regev, "On ideal lattices and learning with errors over rings. in henri gilbert, editor, eurocrypt 2010, volume 6110 of lncs," May / June, 2010. [Online]. Available: doi:10.1007/978-3-642-13190-5_1

[6] E. Alkim, R. Avanzi, J. Bos, L. Ducas, A. de la Piedra, T. Poppelmann, P. Schwabe, and D. Stebila, "Newhope - algorithm specifications and supporting documentation (version 1.02)," NIST Post-Quantum Cryptography Standardization Process, 2019, https://newhopecrypto.org/.

[7] E. Alkim, L. Ducas, T. Poppelmann, and P. Schwabe, "Newhope without reconciliation," Cryptology ePrint Archive, Report 2016/1157, 2016, https://eprint.iacr.org/2016/1157.

[8] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(leveled) fully homomorphic encryption without bootstrapping," in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, ser. ITCS '12. New York, NY, USA: ACM, 2012, pp. 309–325. [Online]. Available: http://doi.acm.org/10.1145/2090236.2090262

[9] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," *Des. Codes Cryptography*, vol. 75, no. 3, pp. 565–599, Jun. 2015. [Online]. Available: http://dx.doi.org/10.1007/s10623-014-9938-4

[10] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals-kyber: a cca-secure module-lattice-based kem," in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2018, pp. 353–367.

[11] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "Cyrystals-kyber - algorithm specifications and supporting documentation (version 2.0)," NIST Post-Quantum Cryptography Standardization Process, 2019, https://pq-crystals.org/kyber/.

[12] J.-P. D'Anvers, A. Karmakar, S. S. Roy, and F. Vercauteren, "Saber: Module-lwr based key exchange, cpa-secure encryption and cca-secure kem," in *International Conference on Cryptology in Africa*. Springer, 2018, pp. 282–305.

[13] M. Hamburg, "Post-quantum cryptography proposal: THREEBEARS," 25 March, 2019. [Online]. Available: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions

[14] Z. Brakerski and V. Vaikuntanathan, "Fully homomorphic encryption from ring-lwe and security for key dependent messages," in *Advances in Cryptology – CRYPTO 2011*, P. Rogaway, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 505–524.

[15] Y. Liu, D. Jia, H. Xue, Z. Zhang, Z. Liu, H. Yang, B. Li, and K. Wang, "Lac lattice-based cryptosystems - algorithm specifications and supporting documentation (version 2)," NIST Post-Quantum Cryptography Standardization Process, 2019.

[16] H. Baan, S. Bhattacharya, S. Fluhrer, O. Garcia-Morchon, T. Laarhoven, R. Rietman, M.-J. O. Saarinen, L. Tolhuizen, and Z. Zhang, "Round5: Compact and fast post-quantum public-key encryption," Cryptology ePrint Archive, Report 2019/090, 2019, https://eprint.iacr.org/2019/090.

Tablo II
COMPARISON OF ALGORITHMS IN TERMS OF SECURITY AND SIZE

Algorithm	Security Level	Public Key (bytes)	Private Key (bytes)	Data (bytes)	Security Type
FRODOKEM	1	9616	19888	9720	IND-CCA
	3	15632	31296	15744	
	5	21520	43088	21632	
KYBER	1	800	1632	736	IND-CCA
	3	1184	2400	1088	
	5	1568	3168	1568	
LAC	1	544	512	712	IND-CCA
	3	1056	1024	1188	
	5	1056	1024	1424	
NEWHOPE	1	928	1888	1120	IND-CCA
	5	1824	3680	2208	
CLASSICAL NTRU-HPS	1	699	935	699	IND-CCA
	3	931	1235	931	
	5	1230	1592	1230	
CLASSICAL NTRU-HRSS	3	1138	1452	1138	IND-CCA
STREAMLINED NTRU PRIME	2	994	1518	897	IND-CCA
	3	1158	1763	1039	
	4	1322	1999	1184	
NTRU LPRIME	2	897	1125	1025	IND-CCA
	3	1039	1294	1167	
	4	1184	1463	1312	
ROUND5.nd.5d	1	445	16	549	IND-CPA
	3	780	24	859	
	5	972	32	1063	
ROUND5.nd.0d	1	634	16	682	IND-CPA
	3	909	24	981	
	5	1178	32	1274	
ROUND5.n1.0d	1	5214	16	5236	IND-CPA
	3	8834	24	8866	
	5	14264	32	14288	
SABER	1	672	832	736	IND-CCA
	3	992	1248	1088	
	5	1312	1664	1472	
THREEBEARS	2	804	40	917	IND-CCA
	4	1194	40	1307	
	5	1584	40	1697	

[17] C. Chen, Q. Danba, J. Hoffstein, A. Hülsing, J. Rijneveld, J. M.Schanck, P. Schwabe, W. Whyte, and Z. Zhang, "Algorithm specifications and supporting documentatiton (version 2)," NIST Post-Quantum Cryptography Standardization Process, 2019.

[18] T. Saito, K. Xagawa, and T. Yamakawa, "Tightly-secure key-encapsulation mechanism in the quantum random oracle model," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2018, pp. 520–551.

[19] D. J. Bernstein, C. Chuengsatiansup, T. Lange, and C. Van Vredendaal, "Ntru prime," *IACR Cryptology ePrint Archive*, vol. 2016, p. 461, 2016.

[20] E. Alkim, Y. A. Bilgin, and M. Cenk, "Compact and simple RLWE based key encapsulation mechanism," in *Progress in Cryptology - LATINCRYPT 2019 - 6th International Conference on Cryptology and Information Security in Latin America*, 2019, To appear.

POSTER PRESENTATIONS / POSTER SUNUMLAR

Comparing PRESENT and LBlock block ciphers over IoT Platform

PRESENT ve LBlock şifreleme algoritmaları IoT Platform üzerinde karşılaştırmak

Pejman Panahi
Department of Computer Engineering
Sakarya University
Sakarya, Turkey
panahi.pejman@gmail.com

Cüneyt Bayılmış
Department of Computer Engineering
Sakarya University
Sakarya, Turkey
cbayilmis@sakarya.edu.tr

Unal Çavuşoğlu
Department of Computer Engineering
Sakarya University
Sakarya, Turkey
unalc@sakarya.edu.tr

Sezgin Kaçar
Departmrnt of Electrical ve Electronic Engineering
Sakarya University
Sakarya, Turkey
skacar@sakarya.edu.tr

Öz—Son yıllarda, Nesnelerin İnterneti (IoT), sanayi, sağlık, akıllı şehirler gibi farklı sektörler kullanılmaktadır. Basitçe, IoT, çoğunlukla WiFi, Bluetooth gibi kablosuz teknolojilerle bağlanan aralarında very akışı olan bir grup düğümdür. IoT üyeleri arasında büyük veri aktarımı göz önüne alındığında, verilere yetkisiz erişimi önlemek için güvenlik mekanizmalara ihtiyaç duyuluyor. IoT cihazlarında bazı zorluklardan örneğin sınırlı depolama ve işlem gücünden dolayı klasik şifreleme algoritmalarını kullanamayız, bu nedenle Hafif Bloklu şifreler bu amaç için iyi adaylar. Literatürde araştırma yapılırken, düşük kısıtlı IoT cihazları için bir çok Hafif Blok şifrelerinin algoritmalar geliştirilmiş ve kullanmaktadır. Bu bildiri, LBlock ve PRESENT blok şifreleme algoritmaların performanslarını Raspberry pi 3 kullanarak ölçmektedir. Çeşitli senaryolar için, bellek, enerji tüketimi, throughput ve yürütme süresi karşılaştırılarak farklı veri yükleri incelenmiş ve sonuçlar elde edilmiştir.

Anahtar Sözcükler — PRESENT algoritması, LBlock algoritması, IoT, Güvenlik, Raspberry Pi 3, Hafif blok şifreleme.

Abstract— Over the last couple of years, the Internet of Things (IoT) has been used exceedingly for several sectors including industry, health, smart cities, etc. Simply, IoT is a group of nodes that are connected mainly through wireless infrastructure. Considering enormous data transfer among IoT members, security is a concept that reveals automatically to avoid unauthorized access to data sent by IoT network members. There are some major challenges for IoT devices like restricted processing power, and storage so we can't use classic encryption algorithms, therefore, Lightweight Block ciphers are good nominates for the goal. Many works include developing and measuring Lightweight Block ciphers for low restricted IoT devices has been done while searching the literature. Consecutively, in this paper, we are evaluating LBlock and PRESENT block ciphers performance over Raspberry pi 3 as a popular IoT gadget. Several scenarios were examined and results were compared focusing on memory, energy consumption, throughput, and execution time for various payloads.

Keywords — PRESENT algorithm, LBlock algorithm, IoT, Security, Raspberry P 3i, Lightweight Block ciphers.

I. INTRODUCTION

Internet of things (IoT) ecosystem contains smart nodes equipped with sensors and telecommunication facilities, and these nodes have limited resources including process and storage units. They can share data, and interact with each other and therefore, we can see less dependency on human intervention. IoT is widely used ranging from smart houses, wearable health sector to different benefits over the industry internet. The large volume of data interacted among IoT devices especially for particular scenarios must be protected against attacks and misuses. There are many security challenges for current IoT devices. Some of them are: Lack of authentication, using the public key, device updates, constrained hardware resources, etc. For the reason, enciphering the data is a good solution and since IoT devices have constrained resources, we cannot apply traditional encryption methods. Consequently, Lightweight Block ciphers can provide satisfaction for end to end security [1-3]. In this paper, we evaluate PRESENT and LBlock algorithms performance concerning on energy, throughput, execution time, and RAM consumption and Raspberry Pi 3 is our testbed. The rest of the paper has been organized as follows: Sector II is about Lightweight Block ciphers. Section III, represents testbed and performance evaluation and finally section IV is about conclusion and future works.

II. LIGHTWEIGHT BLOCK CIPHERS

Table I shows some of the most important Lightweight Block Ciphers. The comparison has been done due to Key,

and Block size and round number of related algorithms [4-17].

TABLE I. Lightweight Block Ciphers

Algorithm	Key Size (Bit)	Blok Size (Bit)	Round
DES	56	64	16
3DES	168, 112, 56	64	48
DESL	56	64	16
DESX	184	64	16
DESXL	184	64	16
Blowfish	448	64	16
Twofish	128, 192, 256	128	16
Threefish	256, 512, 1024	256, 512, 1024	72
TEA	128	64	64
XTEA	128	64	Variable
MISTY	128	64	8, 12
Cast 5	40 -128	64	12-16
Cast 6	128	128,160,192,224,256	48
Skipjack	80	64	32
Camellia	128,192, 256	128	24
Kasumi	128	64	24
Seed	128	128	16
Sea	6*n	6*n	NR/2
Hight	128	64	32
Clefia	128, 192 256	128	18,22,26
MIBS	64, 80	64	32
LBlock	80	64	32
PRESENT	80, 128	64	31
Piccolo	80, 128	64	25, 31
LEA	128, 192,256	128	24,28,32
Twine	80, 128	64	32
Khudra	80	64	18
SIMECK	64, 96, 128	32, 48, 64	32,36,44
RoadRunneR	80, 128	64	10, 20
KAMAR	128, 192, 256	128	16,20,32
QTL	64, 128	64	25, 31
LILIPUT	80	64	30
NASE	Variable	Variable	Variable

III. Testbed And Performance Evaluation

In order to evaluate two algorithms (block size is 64 bits and key size is 80 bits in both algorithms) we chose Raspberry Pi 3 [18]. Fig. I shows a hardware view of our testbed system. Raspberry Pi 3 is connected to a monitor and for measuring energy consumption, a USB meter is between Raspberry Pi 3 and the power source. The power source could be an external battery pack or power adaptor. All codes have been written in C and compiled by GCC compiler. Different scenarios for encryption and decryption were examined using several payloads (at least 5 iterations for each payload). The code receives every 8 bytes as plaintext, encrypt it and store it inside a file. On a destination, decryption code reads contents of the file and start to decrypt ciphertext 8 bytes by 8 bytes.

For calculating the energy consumption, we used the following equations:

$$\text{Current Stream(A)} * \text{Time(Second)} = \text{Charge(C)} \quad (1)$$

$$\text{Charge(C)} * \text{Voltage(V)} = \text{Energy(Joule)} \quad (2)$$

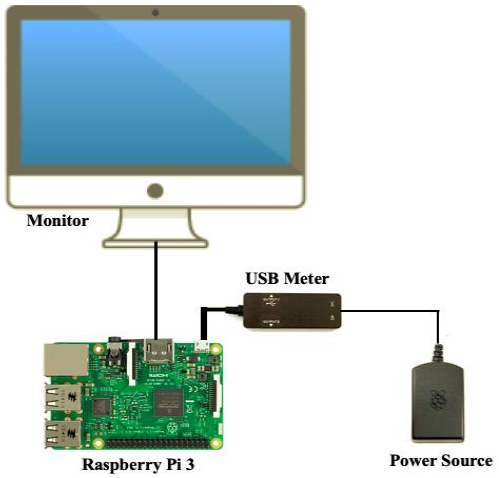


Fig. I. Testbed system used for experiments

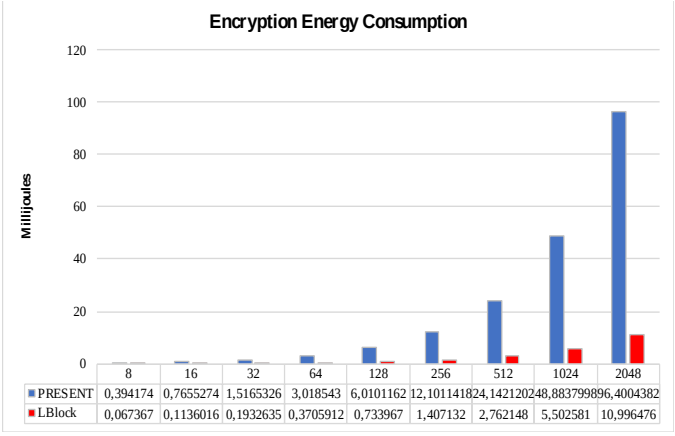


Fig. II. Energy consumption for Encryption

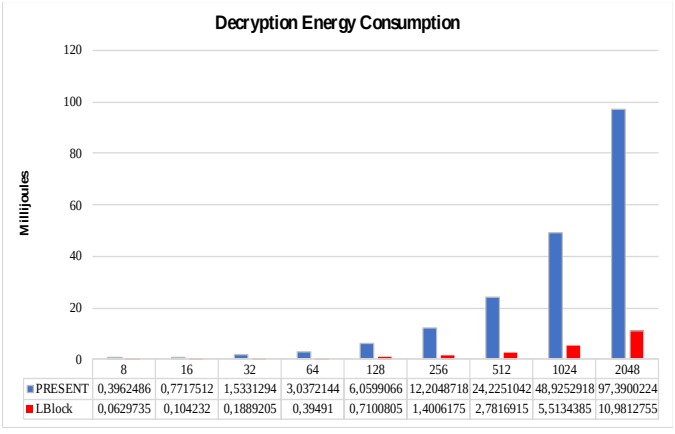


Fig. III. Energy consumption for Decryption

As we can see in Fig. II and Fig III, for both encryption and decryption operations, the Raspberry Pi 3, consumes considerably more energy for PRESENT block cipher comparing to LBlock. Here, the difference mainly starts from 32 bytes and continues till 2048 bytes. In order to calculate Throughput, we used the equation 3:

$$Throughput = \frac{Number\ of\ Bytes}{End\ Time - Start\ Time} \quad (3)$$

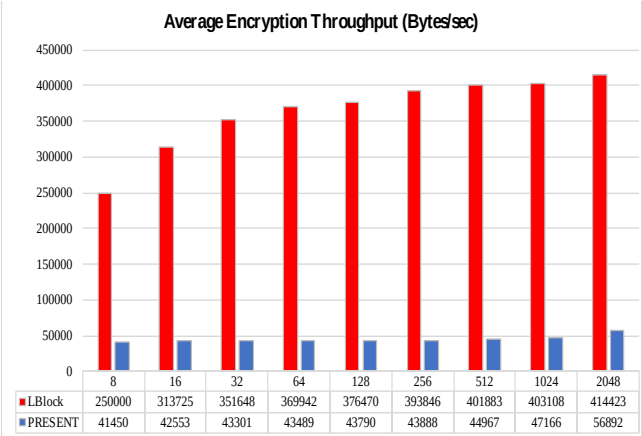


Fig. IV. Average Throughput for Encryption

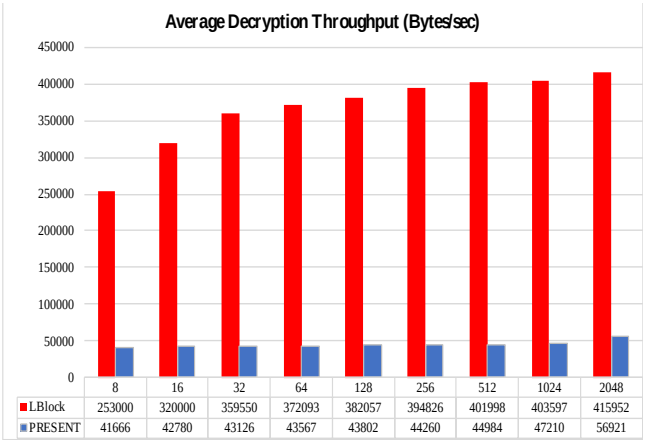


Fig. V. Average Throughput for Decryption

Fig. IV and Fig. V illustrate average throughput values for both encryption and decryption functions. Unlike energy consumption, LBlock shows higher rates than PRESENT. For PRESENT, values except 2048 bytes are growing gradually but for LBlock from the beginning, we can see a regular increase for values.

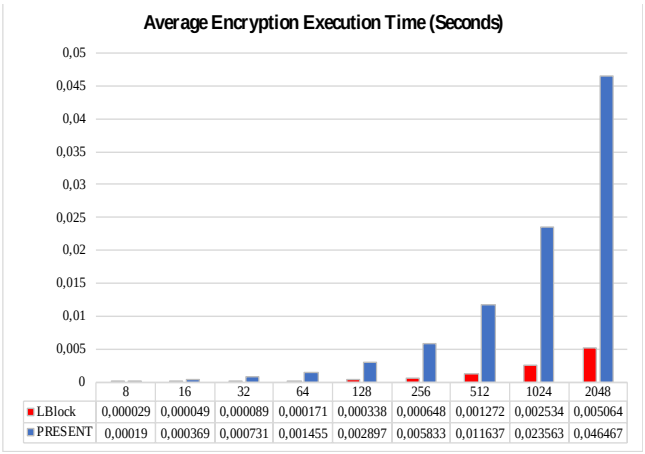


Fig. VI. Encryption average Execution time

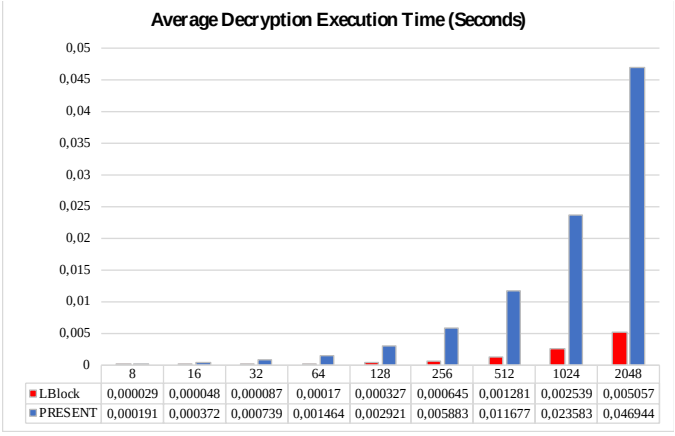


Fig. VII. Decryption average Execution time

Looking at Fig. VI and Fig VII, the average execution time growing logically for LBlock but for the same payloads in PRESENT we can see erratically climb especially for 1024 and 2048 bytes in both encryption and decryption modes.

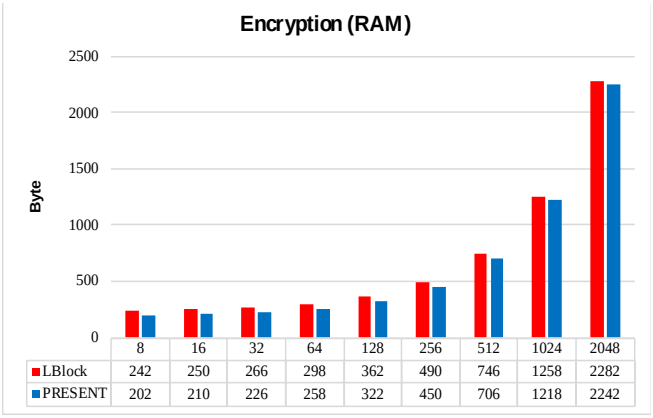


Fig. VIII. RAM measurement for Encryption

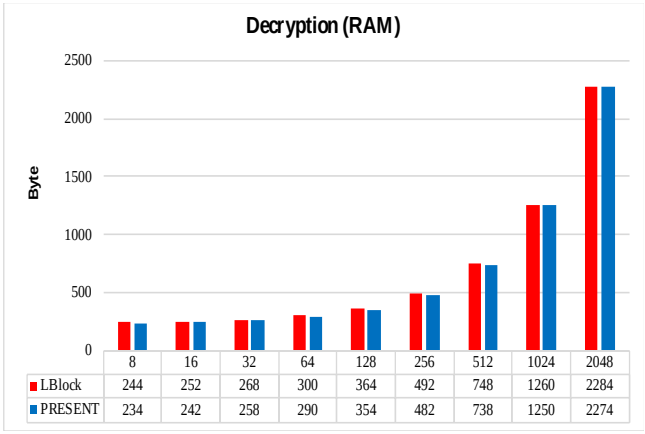
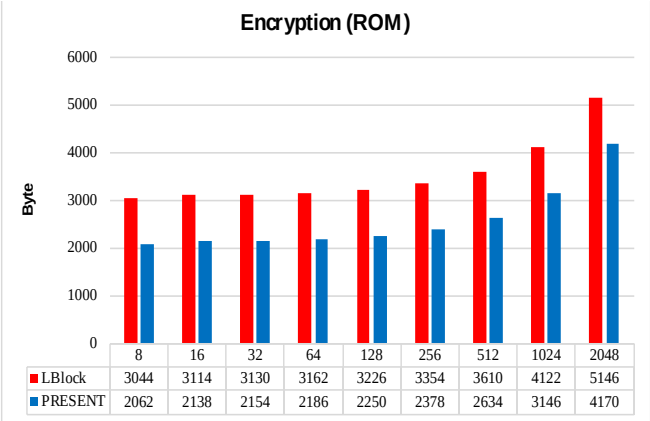


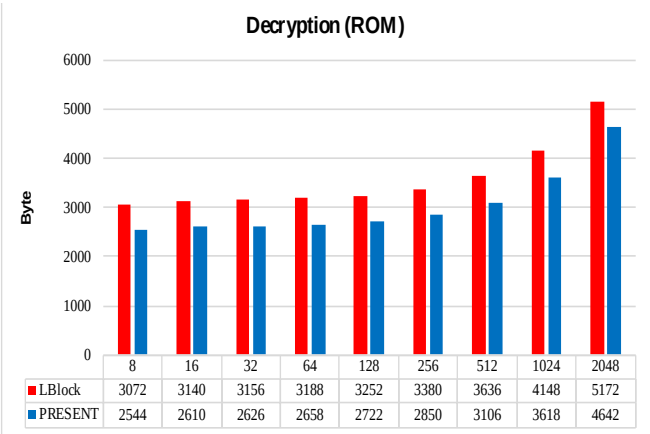
Fig. IX. RAM measurement for Decryption

Focusing on RAM consumption, Fig. VIII and Fig. IX represent measured values for encryption and decryption functions. Analyzing two graphs present a similar behavior. They both grow as expected regarding increase in the number of bytes. LBlock has a bit higher rate comparing to PRESENT but measured amounts are still close.



	8	16	32	64	128	256	512	1024	2048
LBlock	3044	3114	3130	3162	3226	3354	3610	4122	5146
PRESENT	2062	2138	2154	2186	2250	2378	2634	3146	4170

Fig. X. ROM measurement for Encryption



	8	16	32	64	128	256	512	1024	2048
LBlock	3072	3140	3156	3188	3252	3380	3636	4148	5172
PRESENT	2544	2610	2626	2658	2722	2850	3106	3618	4642

Fig. XI. ROM measurement for Decryption

Fig. X and Fig. XI reveal ROM measurements for two block ciphers in each of encryption or decryption modes. The measured ROM for both encryption and decryption operations has an upward trend but all the evidence supports that LBlock has higher ROM consumption.

IV. Conclusion and Future Works

In limited resources IoT devices, the use of lightweight cryptographic algorithms with a light processing load is very advantageous in order to ensure secure communication. Speed, safety and more efficient data communication can be achieved with algorithms that have less processing load and complexity. In particular, lightweight algorithms are preferred because of the low amount of memory and processing power of IoT devices. Due to the limited energy resources in terms of energy consumption, low energy consumption is of vital importance in these applications. In this paper, we compared PRESENT and LBlock algorithms performance using the Raspberry Pi 3 platform. Different metrics were evaluated like energy consumption, throughput, execution time, and memory measurements. Focusing on Energy and execution time, PRESENT shows higher values and LBlock has higher rates for average throughput, RAM and ROM consumptions (both encrypting and decrypting scenarios). Implementing experiments over other IoT devices and comparing results with other block ciphers can be part of the future work.

References

[1] Seongtaek Chee, Sangjin Lee, Choonsik Park and Soo Hak Sung, "Developments in generalised Feistel networks," in Electronics Letters, vol. 35, no. 9, pp. 707-708, 29 April 1999.

[2] S. B. Sadkhan and A. O. Salman, "A survey on lightweight-cryptography status and future challenges," 2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA), Wasit, 2018, pp. 105-108.

[3] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann and L. Uhsadel, "A Survey of Lightweight-Cryptography Implementations," in IEEE Design & Test of Computers, vol. 24, no. 6, pp. 522-533, Nov.-Dec. 2007.

[4] T. P. Berger, J. Francq, M. Minier and G. Thomas, "Extended Generalized Feistel Networks Using Matrix RePRESENTation to Propose a New Lightweight Block Cipher: "Lilliput" in IEEE Transactions on Computers, vol. 65, no. 7, pp. 2074-2089, 1 July 2016.

[5] Bogdanov A. et al. (2007) PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier P., Verbauwhede I. (eds) Cryptographic Hardware and Embedded Systems - CHES 2007. CHES 2007. Lecture Notes in Computer Science, vol 4727. Springer, Berlin, Heidelberg.

[6] Wu W., Zhang L. (2011) LBlock: A Lightweight Block Cipher. In: Lopez J., Tsudik G. (eds) Applied Cryptography and Network Security. ACNS 2011. Lecture Notes in Computer Science, vol 6715. Springer, Berlin, Heidelberg.

[7] Lang Li, Botao Liu, Hui Wang, QTL: A new ultra-lightweight block cipher, Microprocessors and Microsystems, Volume 45, Part A, 2016, Pages 45-55.

[8] Baysal A., Şahin S. (2016) RoadRunneR: A Small and Fast Bitslice Block Cipher for Low Cost 8-Bit Processors. In: Güneysu T., Leander G., Moradi A. (eds) Lightweight Cryptography for Security and Privacy. LightSec 2015. Lecture Notes in Computer Science, vol 9542. Springer.

[9] Yang G., Zhu B., Suder V., Aagaard M.D., Gong G. (2015) The Simeck Family of Lightweight Block Ciphers. In: Güneysu T., Handschuh H. (eds) Cryptographic Hardware and Embedded Systems, CHES 2015. Lecture Notes in Computer Science, vol 9293. Springer.

[10] Kolay S., Mukhopadhyay D. (2014) Khudra: A New Lightweight Block Cipher for FPGAs. In: Chakraborty R.S., Matyas V., Schaumont P. (eds) Security, Privacy, and Applied Cryptography Engineering. SPACE 2014. Lecture Notes in Computer Science, vol 8804. Springer.

[11] Hong D., Lee JK., Kim DC., Kwon D., Ryu K.H., Lee DG. (2014) LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors. In: Kim Y., Lee H., Perrig A. (eds) Information Security Applications. WISA 2013. Lecture Notes in Computer Science, vol 8267. Springer.

[12] Bassam Jamil Mohd, Thaier Hayajneh, Khalil M. Ahmad Yousef, Zaid Abu Khalaf, Md Zakirul Alam Bhuiyan, Hardware design and modeling of lightweight block ciphers for secure communications, Future Generation Computer Systems, Volume 83, 2018, Pages 510-521, ISSN 0167-739X.

[13] Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I. et al.A review of Lightweight Block ciphers, J Cryptogr Eng (2018) 8: 141.

[14] B. J. Mohd and T. Hayajneh, "Lightweight Block Ciphers for IoT: Energy Optimization and Survivability Techniques," in *IEEE Access*, vol. 6, pp. 35966-35978, 2018.

[15] T. P. Berger, J. Francq, M. Minier and G. Thomas, "Extended Generalized Feistel Networks Using Matrix RePRESENTation to Propose a New Lightweight Block Cipher: "Lilliput" in IEEE Transactions on Computers, vol. 65, no. 7, pp. 2074-2089, 1 July 2016.

[16] Jeyaprakash, J., Seka, J. and Villayutham, K. (2016) KAMAR: A Lightweight Feistel Block Cipher Using Cellular Automata. Circuits and Systems, 7, 222-230.

[17] Lang Li, Botao Liu, Hui Wang, QTL: A new ultra-lightweight block cipher, Microprocessors and Microsystems, Volume 45, Part A, 2016, Pages 45-55.

[18] https://www.raspberrypi.org/products/raspberry-pi-3-model-b/

BLE Teknolojisi ve Güvenliği

BLE Technology and Security

Bengü Tacettin
Bilgisayar Mühendisliği
İstanbul Üniversitesi - Cerrahpaşa
İstanbul, Türkiye
btacettin@ogr.iu.edu.tr

Muhammed Ali Aydın
Bilgisayar Mühendisliği
İstanbul Üniversitesi - Cerrahpaşa
İstanbul, Türkiye
aydinali@istanbul.edu.tr

***Özet*— Nesnelerin İnterneti (IoT – Internet of Thing) ekosisteminde enerji tüketimi, nesnelerin mimari tasarımlarında önemli bir kriterdir. Bu sebeple nesneler arası iletişimde, enerji tasarrufu sağlayan haberleşme protokolleri kullanımı artmaktadır. Bluetooth Low Energy (BLE) de bu protokollerden biridir. Kullanımı akıllı nesnelerde yaygındır ancak akıllı nesnelerin enerji tüketimi gibi kaynak kısıtları, diğer haberleşme protokollerinde olduğu gibi BLE teknolojisinde de güvenlik zafiyetlerini beraberinde getirmiştir. Bu zafiyetler ise saldırganlar tarafından kolayca istismar edilebilecek boyutlardadır.**

Bu makalede, BLE teknolojisinin genel özellikleri ile birlikte, saldırı çeşitleri, saldırı araçları ve BLE güvenliği hakkında yapılan çalışmalar incelenmiştir.

Anahtar Sözcükler — Bluetooth Low Energy, Nesnelerin İnterneti, Siber Güvenlik, Bluetooth.

***Abstract*— Energy consumption in the Internet of Thing ecosystem is an important criterion in the architectural design of objects. Therefore, the use of energy-saving communication protocols is increasing in the communication between objects. Bluetooth Low Energy (BLE) is one of these protocols. Its use is common in smart objects, but resource constraints such as energy consumption of smart objects have brought security weaknesses in BLE technology as in other communication protocols. These weaknesses are easily exploited by attackers.**

In this article, general characteristics of BLE technology, types of attacks, attack tools and studies on BLE security are examined.

Keywords — Bluetooth Low Energy, Internet of Things, Cyber Security, Bluetooth.

I. GİRİŞ

BLE teknolojisi, akıllı nesnelerin günlük hayatta kullanımı ile birlikte yaygınlaşmaktadır. Bluetooth muhtemelen en popüler kablosuz kısa menzilli iletişim protokolüdür. Öncelikle cep telefonu, kulaklık, dizüstü bilgisayar, araba ve giyilebilir cihazlar olarak birçok tüketici dağıtımında kısa mesafeli radyo frekansı (RF) iletişiminde kullanılmaktadır. İlk sürümden en son sürüme kadar, Bluetooth'un güvenlik özellikleri, veri iletişiminde çeşitli güvenlik yöntemlerinin geliştirilmesine iyileştirmeler sağlamıştır. Ancak tüm bunların yanı sıra BLE cihazlarında genel (Gizli Dinleme, Ortadaki Adam saldırısı, Hizmet Reddi ve özel olarak tasarlanmış tehditlere karşı bazı güvenlik zafiyetleri bulunmaktadır [1].

Bu makalede BLE teknolojisi genel olarak pek çok açıdan ele alınmaktadır. Makale kapsamında BLE teknolojisinin genel özellikleri, BLE saldırı çeşitleri, BLE güvenliği hakkında yapılan çalışmalar incelenmiştir.

II. BLE HAKKINDA TEMEL BİLGİLER

BLE protokolü Bluetooth SIG tarafından geliştirilmektedir. Bluetooth ile karşılaştırıldığında (Bluetooh Classic)'e göre BLE daha az güç tüketir, cihazları eşleştirmek daha az zaman ve efor gerektirir. Bluetooth Classic'e göre daha düşük bir bağlantı hızı sağlar. Önemli derecede küçük ve ucuzdur. Bluetooth kullanan cihazlara kıyasla %70 oranında daha ucuza üretilebilmektedir. IoT, Sağlık, Akıllı Ev Otomasyonları, Akıllı Enerji, Reklam sektörlerinde kullanılmaktadır.

BLE, Bluetooth 4.0 teknolojisinin bir parçasıdır. Kablosuz olarak düşük enerji kullanarak veri iletmek ve almak için uygun bir teknolojidir Kısa periyotlarda az veri aktarımı sağlamaktadır. 2.4 GHz radyo frekansını kullanmaktadır. 10 ile 100 metre aralıklarındaki mesafeler de sağlıklı çalışmaktadır. CCM Encryption ile birlikte 128 bit AES şifreleme kullanmaktadır. IoT cihazlarına ve uygulamalarına kolaylıkla uygulanabilmektedir. Master – Slave ilişkisi kullanmaktadır [2].

III. BLE MİMARİ

BLE katmanları yukarıdan aşağıya Uygulama (Application), Host (Ana Bilgisayar), Denetleyici (Controller) olmak üzere 3 ana katmandan oluşmaktadır. Ayrıca bu katmanların belirli rolleri yerine getiren alt kategorileri vardır.

A. GAP (Generic Attribute Profile)

GAP, BLE Stack'i üzerindeki genel topolojiyi tanımlar. Bluetooth cihazların birbiri ile iletişime geçebilmesi için iki adet mekanizma vardır. Bunlar: Yayın yapmak veya Bağlanmak. GAP bu iki mekanizmayı tanımlamaktadır. Bir cihaz aşağıdaki GAP rollerinden birini kabul ederek Bluetooth ağına dahil olur [3]. İki mekanizma aşağıda belirtilmiştir:

1) *Yayın Yapmak (Broadcasting):* Bu rolde bir cihaza veri aktarmak için bağlantıya gerek yoktur [3]. Rolleri şu şekildedir:

   a) *Yayın Yapan (Broadcaster):* Bu rolde verilerin aktarılması için cihazların açıkça birbirine bağlı olması gerekmez [3].

   b) *Observer:* Bu roldeki bir cihaz yayın yapan cihazdan gelen verileri dinler. Cihazların birbiri ile bağlı olmasına gerek yoktur [3].

2) *Bağlanmak (Connecting):* Bu rolde veri transferi için cihazların bağlı olması gerekmektedir. Bu rol Yayın Yapma (Broadcasting) rolüne göre daha fazla kullanılmaktadır [3]. Rolleri şu şekildedir:

   a) *Çevresel cihaz (Peripheral Device):* Merkezi cihazlar (Central Devices) ile bağlantı kurabilir. Bağlantı kurulduktan sonra herhangi bir veri yayınlamaz. Dinleyici modda kalırlar [3].

   b) *Merkezi cihaz (Central Device):* Çevresel cihaz ile bağlantıyı sağlayan cihazdır. Bir merkezi cihaz birden fazla çevresel cihaza bağlanabilir. Bağlantı için çevresel cihaza bir istek gönderir ve çevresel cihaz bunu kabul ederse bağlantı sağlanmış olur [3].

Çevresel cihazlar ve merkezi cihazların bağlantıları birçok sebeple kopabilir fakat cihazlar kendi bağlantılarını da sonlandırabilirler [3].

B. GATT

GATT, Cihazların birbiri ile iletişime geçebilmesi için bazı roller tanımlayan bir protokoldür. Verinin iki cihaz arasında nasıl gidip geleceğini tanımlar [2]. GATT'in cihazların etkileşime geçebilmesi için kabul edebileceği/benimseyebileceği roller bulunmaktadır. Bunlar:

1) İstemci: Sunucu (Server) üzerindeki parametreleri okuyabilir veya parametre yazabilir [3].

2) Sunucu: Sunucunun ana rollerinden birisi parametreleri saklamaktır. İstemci bir istekte bulunduğunda sunucu bu parametre/özellikleri kullanılabilir hale getirmek zorundadır [3].

IV. BLE CİHAZLARI ARASINDAKİ EŞLEŞME

BLE destekli bir cihazın bağlanma isteğinde genel süreç aşağıdaki gibi ilerleyecektir:

1. Bu süreçte, ortamda iki cihaz bulunmaktadır. Bunlardan birisi hizmet veren cihaz (Peripheral), diğeri ise bu hizmetten faydalanacak cihazdır [2].
2. Hizmet verecek olan cihaz, etrafa sürekli kendini tanıtan paketler (Advertising) yollar (*Cihaza bağlı birisi varken, BLE destekli cihaz advertising paketleri göndermeyi keser).* Hizmeti alacak cihaz, bu yayınları görür ve kendisine uygun olduğunu düşünürse, bu cihaza bağlanmak için bir bağlantı talebi yollar [2].
3. Bir eşleşme mekanizması seçilerek cihazlar arasında ilişkilendirme yapılır ve cihazlar birbirine bağlanır [2].
4. Eşleştirme tamamlandıktan sonra artık cihazlar arasında bir veri yolu açılır ve veri akışı başlar [2].

3. Maddede geçen eşleşme yöntemlerinin özellikleri aşağıda belirtilmiştir:

1) *Just Works (JW):* Eşleşme için herhangi bir şey sormadan arka planda varsayılan bir değerle eşleşmeyi sağlar (Örneğin telefon kulaklığı) [2]. Pasif dinlemeye karşı koruma sağlar ancak MITM saldırısına karşı koruma sağlamaz.

2) *Numeric Comparison (Sayısal Karşılaştırma):* Her iki cihaz ekranında bir eşleşme numarası çıkarılır ve «EVET-HAYIR» gibi bir soru ile eşleşme isteği sorulur. Çoğu cihazda kullanılmaktadır [2]. PIN değerlerinin bilinmesi iki cihaz arasında paylaşılan şifreli verilerin şifresinin çözülmesine bir fayda sağlamaz.

3) *Passkey (Parola):* 6 rakamdan oluşan bir anahtar kullanılır. Bir cihazın giriş kapasitesine sahip olduğu ancak 6 basamağı gösterme yeteneğinin olmadığı ve diğer cihazın çıkış kapasitesine sahip olduğu senaryo için tasarlanmıştır (Örneğin Klavye - PC). Kaba kuvvet (Brute Force) saldırılarına karşı dayanıksızdır [2].

4) *Farklı bir kanaldan paylaşım:* OOB yöntemi, eşleştirme bilgisi alışverişinde bulunmak için Bluetooth dışında bir arayüz kullanır. Bu yöntem, geçiş kodu girişinden daha güvenlidir ve yalnızca yöntemlerle çalışır. Ancak, her iki cihazın da birbirleriyle uyumlu olması için bir arabirimi olması gerekir [4]. Cihazlar eşleşme için gerekli PIN değerini NFC gibi bir yöntem ile gönderebilirler [2].

V. BLE SALDIRI ÇEŞİTLERİ

Günlük hayatta araba anahtarlarından bulaşık makinelerine kadar pek çok alanda kullanılan BLE teknolojisi, diğer birçok kablosuz iletişim protokolünde olduğu gibi güvenlik riskleri barındırmaktadır. BLE teknolojisinin kısıtlı kaynaklara sahip ürünlerde, düşük enerji harcama amaçlı kullanımlarda, güçlü şifreleme ve güçlü güvenlik koruması göz ardı edilebilmektedir. Bunun sonucunda ise BLE cihazlar, Tekrarlama Saldırısı, Cihaz Spoofing, Komut Fuzzing, Dinleme, Ortadaki Adam Saldırısı, Firmware Dump, Hizmet Dışı Bırakma gibi kablosuz saldırılara maruz kalabilmektedir. Saldırı yöntemleri eşleşme mekanizmalarına bağımlı olarak farklılık gösterecektir. Eşleşme mekanizması saldırı öncesi bilinmelidir. Saldırı çeşitlerinden aşağıda bahsedilmektedir.

1) *Tekrarlama Saldırısı (Replay Attack):* Bir tekrarlama saldırısı, bir saldırgan bir dizi komut kaydettiğinde ve daha sonra yetkisiz erişim sağlamak için onları tekrar hedef cihaza ilettiğinde gerçekleşir [5].

2) *Cihaz Spoofing (Device Spoofing):* Bir saldırganın bağlantıyı ele geçirmesine izin veren ciddi bir problemdir. Bununla birlikte, BlueID gibi araçlar, Bluetooth cihazlarının clock'ları tarafından yazdırılmasını sağlar ve bir cihazın geçerliliğini belirlemek için kullanılır [5].

3) *Komut Fuzzing (Command Fuzzing):* Saldırgan bir cihazın hatalı biçimlendirilmiş verilerini programlamadaki kritik hatalara beslemek için command fuzzing kullanır [5].

4) *Dinleme (Sniffing):* Şifreleme (encryption) yapmış cihazlara karşı kullanılmaktadır. BLE iletişimi dinlenir ve bilgi toplanır [6].

5) *Ortadaki Adam Saldırısı (Man in The Middle (MITM) Attack):* BLE Bağlantı katmanında şifreleme (encryption) kullanmayan cihazlara karşı kullanılmaktadır [6]. Saldırganın birbiri ile doğrudan iletişim kuran iki taraf arasındaki iletişimi gizlice ilettiği veya değiştirdiği saldırı türüdür. Kullanıcının hedef cihaza bağlandığını düşünerek saldırganın kurduğu sahte cihaza bağlanması temeline dayanır [5].

6) *Firmware Dump:* Hedef cihazın kullandığı özellikle gizli, dökümante edilmemiş özel kodlar dahil tüm kodların bulunması temeline dayanır [6].

7) *Hizmet Dışı Bırakma (Denial Of Service (DOS*)): Protokol seviyesinde gerçekleştirilen bu saldırıda Slave cihazların Master cihaza bağlanması engellenmektedir [5].

VI. BLE SALDIRI ARAÇLARI

BLE cihazın eşleşme mekanizması, kullanım alanı gibi farklılıklara göre V. Bölümde bahsedilen saldırı türlerinden hangisi/hangileri uygunsa cihaz üzerinde o saldırı/saldırılar gerçekleştirilecektir. Bu saldırıları yaparken de bazı araçlar kullanılmaktadır. Araçlardan bazıları aşağıda verilmektedir.

1) *Ubertooth:* Pasif BLE ve BTC bağlantılarını kesebilen kablosuz bir geliştirme platformudur. Ubertooth belirli bir donanım alıcısı gerektirir, bu nedenle emtia USB adaptörleriyle uyumlu değildir [5].

2) *Crackle:* Geçici bir anahtarın kaba kuvvet (brute forcing) saldırısına izin veren BLE eşleştirme sürecinde kullanılır. Saldırgan, geçici anahtarı (TK - Temporary Key) ve eşleştirme işlemindeki bilgileri kullanarak uzun vadeli anahtarı (LTK - Long Term Key) kırabilir. Saldırganın uzun vadeli bir anahtarı olduğunda, cihazlar arasındaki tüm iletişimin şifresini çözmek mümkündür. Bu araç eşleştirme işleminin bilinmesini ve bir Ubertooth gerektirir [5].

3) *BTLEJuice:* Etkileşimli bir arayüz içeren MITM çerçevesidir (framework) [5].

4) *Gattacker:* Ortadaki adam saldırısı (MITM) için kullanılan bir uygulamadır [5].

5) *Blue Hydra:* Bluez kütüphanesinin üstüne kurulu bir Bluetooth cihaz bulma servisidir. Blue Hydra, kullanılabilir olduğunda Ubertooth'tan yararlanır ve zamanla BTC ve BLE cihazlarını izlemeye çalışır. Kullanıcıya cihaz adı, Bluetooth sürümü, RSS, üretici ve tahmini cihaz mesafesi sağlar [5].

6) *Hcitool:* BLE cihazlarındaki değişiklikleri iletmek/ okumak / yazmak için bir dizüstü bilgisayardaki ana bilgisayar denetleyicisi arabirimini kullanır. hcitool, bu nedenle, reklamı (advertise) yapan mevcut kurban BLE cihazını bulmakta ve ardından bağlantıdan sonra değerleri değiştirmekte kullanışlıdır. Değerler/veriler ancak verinin geldiği hizmeti ve karakteristiği bilen biriyle değiştirilebilir. İlgili hizmet ve özellikleri bulmak için, gatttool aracı kullanılabilir [7].

7) *Gatttool:* gatttool, mevcut bir BLE cihazının hizmetlerini ve özelliklerini bulmada yardımcı olur, böylece kurbanın verileri saldırgana göre okunabilir/yazılabilir [7].

8) *Bleah:* Bleah bir BLE tarayıcısıdır. Bluepy python kütüphanesine dayanıyor [7].

9) *nRF Connect for Mobile:* Herhangi bir root/jailbreak işlemine gerek kalmadan Android ve IOS üzerinde bilgi toplama ve komut göndermeye yarayan bir uygulamadır. Spectrum dağılımı, uygulamaların hangilerinin bağlanabilir olduğu, yayın güçleri – mesafe, cihazların servis ve karakteristik bilgisi gibi keşif bilgileri toplayabilmektedir. Mobil uygulama üzerinden cihaza komutlar göndermek mümkündür [2].

VII. BLE GÜVENLİĞİ HAKKINDA ÇALIŞMALAR

Bu bölümde BLE cihazlarının güvenliği hakkında yapılan bazı çalışmalar incelenmiştir.

2007'de "Security Evaluation And Exploitatin Of Bluetooth Low Energy Devices" isimli tez çalışmasının amacı bluetooth erişim kontrol cihazlarının çoğunun istismara açık olduğu ancak korunabileceğidir. 13 BLE erişim kontrol cihazı için 8 ayrı istismar geliştirilmiştir. 17 güvenlik cihazının 13'ünde, çeşitli çözümler kullanılarak azaltılabilecek bir veya daha fazla güvenlik açığı içerdiği ortaya çıkarılmıştır [5].

2013 yılında "Bluetooth: With low energy comes low security" isimli çalışmada BLE gizlice dinlenerek paket

izleme ve paket enjekte yöntemleri anlatılmakta ve uygulanmaktadır. Herhangi bir BLE bağlantısının şifrelemesini etkili bir şekilde yararsız hale getirebileceği gösterilmektedir [8].

2015 yılındaki "Exploiting Bluetooth Low Energy Pairing Vulnerability in Telemedicine" isimli bir başka BLE çalışmasında, tıbbi telemetri uygulamalarında kullanılan HealthCare cihazları için Bluetooth Düşük Enerjideki (Bluetooth Smart) eşleştirme güvenlik zafiyetinden yararlanma ve güvenliğin telemetride oynadığı kilit rolü gösterilmektedir. Klasik BTLE eşleşmesinin mevcut açık kaynak araçları kullanılarak ne kadar kolay kırılabileceğini göstermekte ve bu saldırının Teletıp'taki yaklaşmakta olan tıbbi cihazlara etkisini vurgulamaktadır. Veriyi ele geçirmenin mümkün olduğu belirtilmiştir [9].

2016 IEEE ICCE-Asia etkinliği kapsamında sunulan "Bluetooth low energy security vulnerability and improvement method" isimli yayınlanan makalede BLE teknolojisinde bulunan bir açık sunulmuş ve çözümü için geliştirilmiş bir güvenlik yöntemi önerilmiştir. BLE'nin güvenlik açığı, şifreleme anahtarını oluşturmak için TK uzunluğunun çok kısa olmasıdır. Geleneksel BLE protokolünde, TK sadece 6 basamaktır. Önerilen yöntemde, TK'yi tekrar tekrar girerek TK'nin boyutunu (12, 18 ve 24 haneye) artırarak güvenlik açığını çözmenin mümkün olduğu belirtilmiştir. Önerilen yöntemin güvenli bir veri iletişimi sağladığı anlamına geldiği savunulmuştur [4].

2016 IEEE'nin 3 ayrı konferansında yer alan "Assessing vulnerabilities in Bluetooth low energy (BLE) wireless network based IoT systems" isimli IEEE'de yer alan makalede, BLE kablosuz ağ özellikli IoT sistemlerinin kırılganlığını doğru bir şekilde değerlendirmek için, National Infrastructure Advisory Council tarafından önerilen Common Vulnerability Scoring System (CVSS) v2 geleneksel temel puan denklemlerinde kullanılan değişkenler olan kimlik doğrulaması için hesaplama formülünü genişletmek için yeni bir yaklaşım önerilmektedir [10].

2017 yılındaki IEEE 41. Annual COMPSAC konferansında "Cybersecurity Of Wearable Devices: An Experiment Al analysis And A Vulnerability Assessment Method" isimli bir makale yayınlanmıştır. Deneysel bir kampanyayla, bir yöntem, bir akıllı telefon ile iletişim kuran giyilebilir cihazlar üzerinde bir güvenlik zafiyeti değerlendirmesi (VA) ortaya koyulmaktadır. Bu tür bir analizin giyilebilir bir cihazın kırılganlıklarını tespit etmek ve nihayetinde onları düzeltmek için nasıl yararlı olduğunu vurgulamak için üç farklı vaka çalışması gösterilmektedir [1].

2018 ICIRCA konferansında sunulan "Bluetooth Low Energy (BLE) crackdown using IoT" isimli IEEE'de yayınlanan makalede BLE protokolü kullanan Akıllı Ampul'ün gerçek zamanlı olarak ele geçirilmesi sunulmaktadır. Diğer cihazlar ile iletişim kurmak için BLE protokolünü kullanan bir IoT cihazına gerçek zamanlı sızma testi yapılmaktadır [11].

Son olarak, 2019 yılında ICEIC konferansında sunulan "Analyzing the Security of Bluetooth Low Energy" isimli IEEE de yayınlanan makalenin amacı BLE güvenlik standartlarını test etmektir. Güvenlik zafiyetlerinden yararlanmaya çalışılarak bu standardın gerçekten ne kadar güvenli olduğu ölçülmektedir. Açık kaynaklı donanım ve yazılım kullanarak BLE cihazlarının güvenliğini analiz etmek için adımlar sunulmaktadır. Makalede sonuç olarak BLE'nin en ciddi güvenlik açığının TK olduğu belirtilmektedir [12].

VIII. SONUÇ

BLE teknolojisi kullanımı ile birlikte artan güvenlik risklerine dikkat çekilen bu makalede, BLE teknolojisi hakkında temel bilgiler verilmiş, uygulanabilecek saldırı çeşitleri, saldırılarda kullanılabilecek araçlar ve BLE güvenliği hakkında yapılan çalışmalar incelenmiştir. Çalışmada açık kaynak yazılım ve donanımlar kullanılarak kolayca BLE cihazlarına saldırı gerçekleştirilebileceği belirtildi. İncelenen çalışmalar göstermektedir ki BLE protokolünün kullanıldığı IOT cihazları risk altındadır. BLE, küçük cihazlar için kullanışlı bir protokoldür ancak kritik görev sistemlerinde veya hassas verilerle kullanılabilmesi için veri iletişiminde çeşitli güvenlik yöntemleri geliştirilmelidir.

KAYNAKÇA

[1] Langone, Matteo, Roberto Setola, and Javier Lopez. "Cybersecurity of wearable devices: an experimental analysis and a vulnerability assessment method." 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC). Vol. 2. IEEE, 2017.

[2] B. Altınok, Kablosuz Ağ Güvenliği (Saldırı – Savunma - Analiz) Kitabı, Abaküs Yayınları, 2018.

[3] E. Ergün, Bluetooth Low Energy Nedir? [Online], https://canyoupwn.me/tr-bluetooth-low-energy-nedir/, 2018.

[4] Kwon, Giwon, et al. "Bluetooth low energy security vulnerability and improvement method." 2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia). IEEE, 2016.

[5] Rose, Anthony J. Security Evaluation and Exploitation of Bluetooth Low Energy Devices. No. AFIT-ENG-MS-l 7-M-066. AIR FORCE INSTITUTE OF TECHNOLOGY WRIGHT-PATTERSON AFB OH WRIGHT-PATTERSON AFB United States, 2017.

[6] A. Bilal Can, "BLE'nin ABCsi: 2 – MITM"[Online], https://eybisi.run/BLE-nin-ABCsi-2-MITM/ , 2018.

[7] Vaibhav Bedi, The Practical Guide to Hacking Bluetooth Low Energy [Online], https://blog.attify.com/the-practical-guide-to-hacking-bluetooth-low-energy/ , 2018.

[8] Ryan, Mike. "Bluetooth: With low energy comes low security." Presented as part of the 7th {USENIX} Workshop on Offensive Technologies. 2013.

[9] Zegeye, Wondimu K. "Exploiting Bluetooth low energy pairing vulnerability in telemedicine." International Foundation for Telemetering, 2015.

[10] Qu, Yanzhen, and Philip Chan. "Assessing vulnerabilities in Bluetooth low energy (BLE) wireless network based IoT systems." 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS). IEEE, 2016.

[11] Chandan, Abhishek R., and Vaishali D. Khairnar. "Bluetooth Low Energy (BLE) Crackdown Using IoT." 2018 International Conference on Inventive Research in Computing Applications (ICIRCA). IEEE, 2018.

[12] Sevier, Seth, and Ali Tekeoglu. "Analyzing the Security of Bluetooth Low Energy." 2019 International Conference on Electronics, Information, and Communication (ICEIC). IEEE, 2019.

Hassas Verilerin Korunmasında Klasik ve Kuantum Kriptoloji Yöntemleri Üzerine Bir Araştırma

A Research on Classical and Quantum Cryptology Methods for Protecting Sensitive Data

Ömer KASIM
Simav Teknoloji Fakültesi Elektrik Elektronik Mühendisliği
Kütahya Dumlupınar Üniversitesi
Kütahya, Türkiye
omer.kasim@dpu.edu.tr

Esmanur COŞKUN
Bilgisayar Programcılığı
İstanbul Şehir Üniversitesi
İstanbul, Türkiye
coskun-nur@hotmail.com

***Özet*— Hassas veriler kişiye özel ve kişinin isteği dışında paylaşılmaması gereken verilerdir. Bu verilerin iletilmesi, saklanması ve paylaşılmasında farklı servis sağlayıcılar ve sosyal medya kullanılmaktadır. Bu sistemlerde erişim denetimi olsa da hassas verilerin iletilmesinde şifreleme yöntemlerinin kullanılması verilerin elde edilmesi ve çeşitli saldırılara karşı önlem alma noktasında en önemli unsur olarak günümüzde kullanılmaktadır. Klasik şifreleme yöntemlerinin yanı sıra son zamanlarda Qbit'ler ile işlem yapabilme yetisinde olan çeşitli kuantum şifreleme algoritmaları geliştirilmiştir. Bu çalışmada hem klasik kriptoloji yöntemleri hem de kuantum kriptoloji yöntemlerinde kullanılan algoritmalar ve bu algoritmaların uyarlandığı çeşitli çalışmalar incelenmiştir. Bu çalışmalar ile kriptoloji yöntemlerinin avantajlı ve problemli olduğu durumlar irdelenmiştir. Özellikle Shor algoritmasının klasik kriptoloji şifre çözme yöntemleri üzerinde etkin olduğu ve güvenlik için kuantum şifrelemenin mutlaka kullanılması gerektiği sonucuna varılmıştır.**

***Anahtar Kelimeler*— Kriptoloji, Hassas Veri, Kuantum Kriptoloji, Veri Güvenliği**

***Abstract*— Sensitive data is personal and should not be shared against the will of the person. Different service providers and social media are used to transmit, store and share this data. Although there is access control in these systems, the use of encryption methods in transmitting sensitive data is used as the most important element in obtaining data and taking precautions against various attacks. In addition to classical encryption methods, several quantum encryption algorithms capable of processing with Qbits have recently been developed. In this study, the algorithms used in both classical cryptology methods and quantum cryptology methods and various studies adapting these algorithms are examined. With these studies, the situations where cryptology methods are advantageous and problematic are examined. In particular, the Shor algorithm is effective on classical cryptology decryption methods and the use of quantum encryption for security is absolutely essential.**

***Index Terms*— Cryptology, Sensitive Data, Quantum Cryptology, Data Security**

I. GİRİŞ

Son yıllarda üretilen veri miktarı bir önceki yıl üretilen veri miktarını neredeyse ikiye katlamaktadır. Veri miktarındaki bu artış eğilimi verilerin bulut ortamında saklanmasını gerekli kılmaktadır. Bulut ortamında saklanan veriler kişisel veriler, hassas veriler, e-posta işlemleri, kişisel tercihler, çerezler, web aramaları vb. olarak sıralanmaktadır. Bu tür veriler kişiden bağımsız olarak web ortamı, depolama alanları, sosyal medya hizmet sağlayıcıları ve internet servis sağlayıcılarında saklanmaktadır. Verilerin saklandığı bu hizmet sağlayıcılardaki verilerin çeşitliliği, miktarı ve önemi göz önüne alındığında, kişisel verilerin güvenliğine yönelik güvenlik endişesi ortaya çıkmaktadır [1].

Hassas veri olarak isimlendirilen kişisel veriler, e-posta içeriklerinde yer alan veriler, web aramaları, sosyal medya verileri ve kişisel verilerin depolandığı hizmet sağlayıcılardaki farklı türde dosyaları içermektedir. Güvenlik açısından bakıldığında bu tür verilere erişim sadece kişiye özel belirtilen kişi ve kurumlarca sağlanabilmelidir. Ayrıca erişilen bu veriler kullanıcının belirlediği rollere göre diğer kullanıcının erişimine açılabilmelidir. Bu problemin çözümünde kriptoloji algoritmaları kullanılabilir. Kişi farklı türdeki gizlenmesini istediği verileri şifreleyerek iletme ve saklama yoluna gittiğinde veriye istem dışı erişim sağlayacak kullanıcıların hassas veriler görmesi engellenebilecektir. Bu çalışmada hassas verilerin güvenli olarak şifrelenebileceği yöntemler ele alınmış olup bir araştırma metodolojisi sunulmuştur.

II. KRİPTOLOJİ

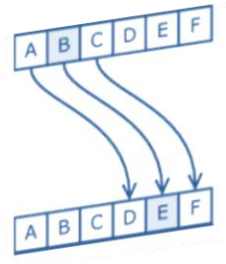
Gönderici alıcıya elektronik ortamda veri göndermek istemektedir. Bu durumda iletinin üçüncü kişiler tarafından erişilip mesajın değiştirilmesini ya da iletişim kanalını dinlemesini önlemek gerekmektedir [2]. Kriptoloji algoritmaları kullanılarak verinin şifrelenmesi ve şifreli verilerin çözülmesi prensibiyle verinin üçüncü kişilere karşı korunmasını sağlamaktadır [3]. DES kriptolojide kullanılan şifreleme standardıdır. Yer değiştirme ve yayılma tekniğini kullanan DES standardının en büyük dezavantajı 56 bitlik anahtar kullanmasıdır. Bu nedenle DES gelişen teknoloji ve işlem hızı artan bilgisayarlara karşı 3 boyutlu DES (3D-DES) geliştirilmiştir. 3D-DES, 3 tane 56 bitlik olmak üzere 168 bitlik şifreleme gücüne erişilmektedir. Fakat şifreleme ve şifre çözme işlemleri için 3 kat fazla işlemci çevrimi gerektirmektedir [4]. DES iki girdi ile işlem yapmaktadır. Bunlar şifrelenecek olan 64 bit uzunlukta düzyazı ve 56 bit uzunluktaki anahtardır [5].

Şifreleme ve şifre çözme işlemi gerçekleştiren anahtarlar farklı uzunluk ve boyutlarda olabilmektedir [6].

A. Kriptolojide Kullanılan Algoritmalar

1) Sezar Şifreleme Algoritması

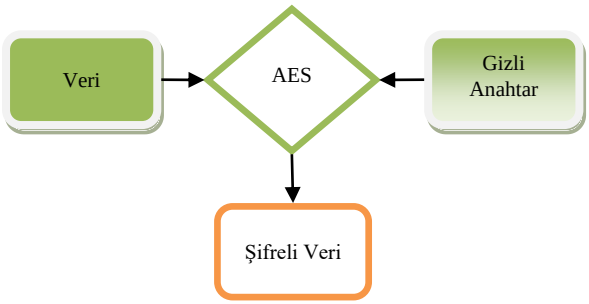
Kriptoloji tarihinin bilinen en eski şifreleme algoritması Sezar Şifreleme Algoritmasında alfabedeki harflere göre şifreleme işlemi yapmaktadır. Açık metindeki harfler kendinden 3 harf sonraki harflerle şifrelenmektedir. Şekil 1 'de örnek bir uygulama gösterilmiştir.



Şekil 1. Sezar Şifreleme Algoritmasının Çalışma Prensibi

2) AES Simetrik Şifreleme Algoritması

AES simetrik şifreleme algoritmasında verinin şifrelenmesinde kullanılan anahtar bilgisi ile verinin şifrelerinin çözümünde kullanılan anahtar bilgisi tektir. Gönderici şifreli veriyi alıcıya gönderirken bu anahtar bilgisini de güvenli bir şekilde göndermelidir [5]. Şekil 2'de Alıcının kriptolu metinden açık metine ulaşması için anahtar bilgisine sahip olması gerekmektedir. Tek bir anahtar olması şifreleme ve şifre çözme işlemlerinin hızlıca yapılmasını sağlamaktadır. AES, 128 bitlik veri bloklarını 128, 192, 256 bitlik anahtarlarla şifrelemektedir. 128 bitlik uzunluktaki verileri 4x4'lük durum matrislerine bölünmektedir.

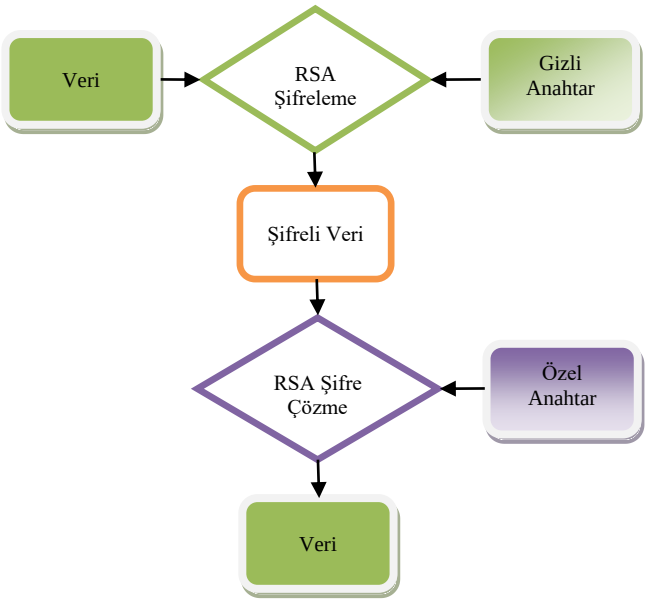


Şekil 2. AES Şifreleme Algoritmasının Çalışma Prensibi

AES anahtar uzunluğuna göre döngü sayısına karar vermektedir. Döngünün artması verinin güvenliğini arttırmaktadır. Ancak döngünün artması işlem sayısını ve bellek hafızasını artırmaktadır. Bu nedenle 256 bitlik anahtar kullanıldığında hız problemi yaşanmaktadır [7]. Şifreleme işlemi için dört adım gereklidir. Bunlar alt bayt, satır değiştir, sütunları karıştır, anahtarın yuvarlanmış halinin eklenmesidir [8].

3) RSA Asimetrik Şifreli Algoritması

RSA algoritmasında şekil 3'de görüldüğü gibi biri özel diğeri açık olmak üzere iki anahtar kullanılmaktadır. Şifreleme işlemi herkesin erişebildiği açık anahtarla yapılmaktadır. Kullanıcının açık anahtarına herkes ulaşılabilirken özel anahtarı kullanıcı tarafından gizli tutulmaktadır. Gönderici mesaj göndermek için, alıcının açık anahtarıyla gönderilecek metni şifreler ve kriptolu mesajı alıcıya göndermektedir. Alıcı kriptolu metni kendi özel anahtarı ile açık metin haline getirir. Kullanıcının açık anahtarı ile şifrelenmiş metni sadece o kullanıcının özel anahtarı ile açabilmektedir. Açık anahtar herkese dağıtılabilir fakat anahtarın kime ait olduğunu doğrulamak için sertifika bilgisine ihtiyaç bulunmaktadır [9]. RSA'nın güvenliği çok büyük asal sayıların çarpımına dayanmaktadır. Açık Anahtarlı Sistemlerin en çok kullanılan algoritmasıdır. RSA, şifrelemenin yanı sıra e-imza gibi alanlarda da kullanılmaktadır. RSA algoritmasında kullanıcıların anahtar oluşturması için iki tane farklı, rastgele ve yaklaşık aynı uzunlukta olan p ve q asal sayılar seçilmektedir.



Şekil 3.RSA Şifreleme Algoritmasının Çalışma Prensibi

$$n = pq \text{ ve } Ø = (p-1)(q-1) \quad (1)$$

n değeri eşitlik 1 ile hesaplanır. $1 < e < Ø$ ve gcd (e; Ø) = 1 olacak şekilde rastgele bir e sayısı seçilir. Öklid algoritmasını kullanarak, eşitlik 2'deki koşulu sağlayan d sayısı hesaplanır.

$$1 < d < Ø \text{ ve } e.d = 1 \ (\text{mod } Ø) \quad (2)$$

Kullanıcının açık anahtarı (n; e) ve kullanıcının gizli anahtarı ise d olur [10]. Bu bilgilere dayanarak örnek bir şifreleme işlemi için; gönderici açık şifre olan (n,e) değerlerini yayınlamaktadır. Alıcı bu şifreyi almakta ve mesajı eşitlik 3'ü kullanarak şifrelemektedir.

$$c = m.e \bmod n \quad (3)$$

Eşitlik 3'te m şifrelenecek olan metin, e ve n açık anahtarı ifade etmektedir [11]. Şifre çözme işlemi için; alıcı göndericiden gelen mesajı açmak için eşitlik 4'ü kullanmaktadır.

$$m = c.d \bmod n \quad (4)$$

Eşitlik 4'de c şifrelenmiş metin, d alıcının gizli anahtarı, n taban değeridir [11]. Sistemin kırılma süresinin uzunluğu, şifreleme ve şifre çözme işlemlerinde algoritmanın hızı, bu işlemler için ihtiyaç duyulan bellek hafızası ve algoritmanın kurulacak sisteme olan uygunluğu şifreleme algoritmalarının gücünü belirlemektedir [12].

B. Kriptolojinin güvenlikte kullanımı

Erişim kontrolünün güvenilir olması hassas ve kişisel verilerin gizliliğini koruyarak saklanması için önemli bir unsurdur. Bulut tabanlı sistemler için kriptoloji erişim kontrol modelleri en bilinen ve güvenli yapılardır. Kriptoloji teknikleri bir arada kullanılarak ince taneli erişim kontrol modelleri geliştirilebilmektedir. Buna örnek olarak bulut sistemleri için öznitelik tabanlı şifreleme, vekil yeniden şifreleme, hiyerarşik kimlik tabanlı şifreleme ve şifre metni özniteliğine dayalı şifreleme gibi kriptoloji teknikleri kullanılabilmektedir. Veri Sızıntısına Karşı Önlemlerde bölümleme, sayısal imzalar ve şifreleme yöntemleri kullanılmaktadır. Bölümleme ve gereğinden fazla dağıtım yönteminde veriler anlamsız parçalara bölünür ve dağıtık sistemin çeşitli taraflarına dağıtılır. Parçaların her biri kendi içinde bir anlam taşımamalıdır. Sayısal İmzalar, sanal ortamda veriler aktarılırken sayısal imza ile güvenliği sağlanabilmektedir. Bu işlemi yapabilmek güçlü algoritmalara ihtiyaç vardır. Bu algoritmalara örnek olarak RSA, AES ve Diffie Hellman anahtar değişimi algoritması örnek verilebilir. Şifreleme teknikleri ise veriyi korumak için kullanılan yöntemlerden biridir. Bulut sistemlerinde, verilerin şifreli halinin saklanması veya verinin şifreli yapıda gönderilmesi veri güvenliğini sağlamaktadır. Bu şifreleme işlemleri için kullanılan algoritmaların AES gibi güçlü ve hızlı algoritmalar olması gerekmektedir [13].

Homomorfik şifreleme ile istemci için gerekli hesaplamalar şifreli olmayan veriler yerine kriptolu veriler üzerinde gerçekleştirilmektedir. Bu yöntemle, açık metin ile yapılan hesaplamalarla aynı sonucu verecek şekilde şifre çözme yapılmadan ve özel anahtar bilinmeden şifreli veriler üzerinde çeşitli işlemler yapılabilmektedir. Böylece hassas ve kişisel verilerin gizliliği korunmaktadır. Homomorfik şifrelemede, sadece tek bir işlem yapılabilmektedir. Toplama veya çıkarma işlemlerinin yalnızca birini yapabilecek şekilde kısıtlandırılmıştır. Vekil (Proxy) Yeniden Şifrelemede herhangi bir kullanıcının genel anahtarı ile şifrelenen veriyi yine herhangi bir kullanıcının özel anahtarıyla şifre çözme işlemini yapabilecek şekle dönüştürülmesini sağlanmaktadır. Kullanıcıları ya da kimlik niteliklerini ve prensip değişikliklerini ekleme, iptal etme gibi işlemleri yeterli ölçüde yapmasını bu yöntem sağlamaktadır. Veriler birden fazla kopyalanıp saklandığı için yüksek hesaplama maliyetlerine sebep olmaktadır. Özellik tabanlı şifrelemede açık anahtarlı şifreleme sistemleri temel alınmaktadır. Verilerin kullanıcı özniteliğine göre şifrelenip şifre çözme işlemleri gerçekleştirilmektedir. Sistem kullanıcıları için belirleyici nitelik sınıflarıyla, şifreleme anahtarları veya kriptolu veriler etiketlenmektedir. Belirlenen kullanıcı bu özel anahtarıyla eşleşen kriptolu veriyi çözebilmektedir. Bu yöntemle şifrelenen verilere, yalnızca anahtarları belirlenen niteliklere uyumlu olan kullanıcılar ulaşabilmektedir [13].

Steganografi ve filigran tekniği bir arada kullanılarak ses, video, görüntü gibi verilerin saldırganlardan korunması sağlanmaktadır. Bulut ortamına görüntü yüklenmesi durumunda, istemci görüntüyü RSA ile şifreleyip depolama işlemini gerçekleştirmektedir. Kriptolu görüntü, veri gizleme mesajı ve filigranlı verinin kriptolu yapıda çakışmasını engellemek için iki parçaya ayrılmaktadır. İlk parçada görüntü LSB ve RGB yöntemiyle Steganografi saklama işlemi gerçekleştirilmektedir. İkinci parçaya ise Eliptik Eğri Kripto sistemi (EEK) kullanılarak filigran yapıya çevrilmektedir. Kriptolu görüntü buluttan çekildiğinde kullanıcı doğrudan şifre çözme işlemini yapabilmektedir.

Geliştirilen SregAD yönteminde Steganografi saldırılarına karşı sistemi korumak için Rs ve SADi bileşenleri kullanılmaktadır. Rs bileşeninin kullanılması şüpheli ses Steganografi dosyalarının tespitini kolaylaştırmaktadır. SADi ise şüpheli dosyaların gizlenebileceği alanlardaki verileri engellemektedir.

III. KUANTUM KRİPTOGRAFİ

Kuantum kriptolojinin gücü klasik kriptoloji algoritmalarının aksine fizik bilimine dayanmaktadır. Kuantum kriptoloji, kuantum mekaniğinin yasalarını kullanmaktadır. Bu sayede daha güçlü kriptoloji sistemlerinin elde edilmesi mümkün olmaktadır. Şekil 4'de görüldüğü gibi Kuantum kriptolojide birbiriyle iletişim kurmak isteyen alıcı ve gönderici rastgele üretilecek olan ortak bir bit dizisinde anlaşmaktadır. Bu bit dizisini yalnızca iletişimi kuracak tarafların bilmesi gerekmektedir. Üretilen bit dizisi verinin şifrelenmesi ve şifrenin çözülmesi işlemlerinde kullanılmaktadır. Haberleşme anında iletişime üçüncü bir kişi dahil olmaya çalıştığında gönderici ve alıcı bu kişiden haberdar olmaktadır. Böyle bir durumda iletişimin güvenliği için bit dizisi yeniden oluşturulur. Saldırganın Man In the Middle (MIM) gibi bir yöntemle veriyi elde etmek amacıyla ortamı dinlemesi için öncelikle tarafların kullandığı bit dizisi anahtarını ölçümlemesi gerekmektedir. Böyle bir durumda işlemin gerçekleşmesi sistemde bozulmalara sebep olmaktadır. Üçüncü kişinin güvenli bir anahtar üretmesi için gizli dinleme seviyesinin belli değerlerin altında olması gerekmektedir. Bu durum oluşmadığında iletişim durdurulmaktadır [14]. Kuantum kriptolojide haberleşmeyi sağlamak için fotonlar kullanılmaktadır. Bit dizisini anahtar olarak temsilen fotonların polarizasyon özelliğinden faydalanılmaktadır [2]. Kuantum kriptolojide anahtar dağıtım protokolleri BB84 ve BB95'tir.

Bit Sırası	0	1	2	3	4	5
Gönderici Mantık Sırası	0	0	1	1	1	1
Polarizasyon Filtresi	↑	↖		→	↗	↗
Alıcı Polarizasyon Durumu	↑	↖	↖	→	↑	↗
Alıcı-Verici durum testi	d	d	x	d	x	d
Kuantum Anahtarı	↑	↖	x	→	x	↗

Şekil 4. Kuantum Kriptografi Çalışma Prensibi

BB84 protokolünde anahtar dağıtımı için gönderici, fotonları dört polarizasyondan rastgele seçilen birinde göndermektedir. Alıcı, göndericinin yolladığı fotonlardan her biri için ölçüm türünü rastgele seçerek kenarsal veya köşegensel ölçüm sonuçlarını kaydetmektedir. Alıcı ölçüm türünü x veya + olarak belirlemektedir. Fakat gönderici ölçüm türlerinden hangilerinin doğru olduğunu alıcıya söylemelidir. Her iki taraf da doğru belirlenen ölçüm türlerini ve ölçüm sonuçlarını saklamalıdır. Bu ölçüm sonuçlarına göre bitler 0 ve 1 olarak belirlendikten sonra anahtar elde edilmektedir [15].

B92 protokolünde ise bitler 00 ve 450 polarizasyonla kodlanmaktadır. "0" biti (Qbit) 00 polarizasyona sahip fotonlarla kodlanırken "1" biti (Qbit) 450 polarizasyona sahip fotonlarla kodlanmaktadır. BB84 protokolündeki gibi + ve x filtreleri uygulanmaktadır. Fakat B92 protokolü 00 ve 450 polarizasyondaki fotonları eleyerek 900 ve 1350 açıdaki fotonları anahtara dâhil etmektedir [16].

BB84 protokolünde iletişimi sağlayan alıcı ve gönderici tarafların aynı tip filtre kullanamaması sonucunda fotonların onaylanma ihtimali %50 iken bu durum B92 protokolünde %33' e kadar inmektedir. Bu bakımdan anahtar oluşturabilme süresi B92 protokolünde daha uzun sürmektedir. Her ne kadar hız konusunda dezavantaja sahip olsa da saldırı anında dinleme tespit oranının yüksek olmasıyla güvenlik konusunda avantaja sahip olmaktadır. BB84 protokolünde saldırı tespit oranı %40 iken B92 protokolünde %50'dir [16].

A. Kuantum Kriptolojide Saldırının Tespit Edilmesi

Anahtar belirlenirken üçünü bir kişinin ortamı dinlemesi ölçüm sonuçlarında değişikliklere ve bozulmalara sebep olabilmektedir [15]. Ortamın üçüncü kişi tarafından dinlenmesi durumunda göndericinin gönderdiği fotonlara önce saldırgan erişmektedir. Saldırgan yaptığı ölçümlerinin sonunda bir bit dizisi oluşturmaktadır. Kopyalanamazlık ilkesi gereği saldırgan fotonları birebir kopyalayamaz. Bu durumda fotonları yeniden oluşturmalıdır. Oluşturduğu yeni fotonları alıcıya göndermelidir [17]. Anahtar belirlenirken alıcı ve gönderici hattaki üçüncü bir kişinin varlığını polarizasyon tabanları ve bitlerin değerlerini karşılaştırarak öğrenebilmektedir [17].

B. Kuantum Kriptografi Algoritmaları

1) Deutsch Algoritması

Kuantum kriptoloji algoritmaların ilk geliştirilen modelidir. Tek bir Qbit üzerinde işlem yapabilmektedir. Algoritma zamanla geliştirilerek n Qbitli işlem yapılabilir hale gelmiştir [18]. Deutsch Algoritması, çözümsüz olan bir sorunun çözülmesinden ziyade kuantum yasalarını kullanarak sorunun daha kısa zamanda çözülebileceğini göstermektedir [19].

2) Shor Algoritması

Shor Algoritmasının bulunmasıyla güvenliği asal sayıların çarpanlara ayırma zorluğuna dayanan klasik kriptoloji algoritmalarından olan RSA Algoritmasının kırılmasına neden olabilmektedir [20]. Shor algoritmasının Qbit tabanlı çarpanlara ayırma algoritması, klasik bilgisayarlar ile çözümü yıllar sürebilecek asal sayıları dakikalar içinde çözebilmektedir [21]. Qbitler aynı anda farklı bilgiler saklayabilmektedir. Qbitler, 0 veya 1 durumunda iken sonucun alabileceği değerleri algoritma tek bir işlemle çözümleyebilmektedir ve tek bir işlemle bütün sayıları çarpıp muhtemel sonuçları bulabilmektedir. Ayrıca Shor algoritması da kuantum paralelliğini kullanmaktadır [19].

3) Grover Algoritması

Grover Algoritması, veritabanı üzerinde arama yaparak belirlenen değerin bu veritabanında olup olmadığını kontrol etmektedir. Veritabanındaki verilerin alan göre alfabetik ya da belirli bir kurala göre sıralanması arama süresini etkilemektedir. Sıralanmış bir tablodaki arama süresi oldukça kısayken sıralı olmayan bir alan gönderilecek arama işleminde sırasıyla satırlar taranacaktır [19]. Böyle bir durumda Grover Algoritması temel olarak üç adımla bu işlemi gerçekleştirmektedir. İlk adımda başlangıç durumunu tüm durumların eşiti bulunduğu duruma getirmektedir. Bu işleme Süper pozisyon ismi verilmektedir. İkinci adımda aranan değer işaretlemekte ve veriyi bulma olasılığı arttırılmaktadır. Son adım olan ölçme işlemidir Veriye erişim süresi ölçülerek performans belirlenir [19].

C. Kuantum Protokollerinin Kullanıldığı Çalışmalar

Kuantum kriptolojide gönderilen foton sayısının, gürültüsüz ortamda elde edilen anahtar uzunluğuna etkisi için yapılan çalışmada Tguid kütüphanesi kullanılmıştır. Bu kütüphanedeki rastsal sayı üretimine dayalı, BB84 protokolü de baz alınarak bir simülasyon oluşturulmuştur. Oluşturulan simülasyon iki aşamalı olarak çalışmaktadır. İlk aşamada gürültüsüz ortamda anahtar dağıtımı yapılırken arada bir saldırgan olmadığı düşünülerek fotonlar gönderilmiştir. Gönderilen foton sayısına göre alıcının rastgele seçtiği filtreler kullanılarak elde edilen ham anahtar uzunlukları ölçülmüştür. İkinci aşamada arada saldırgan olması durumu göz önüne alınarak iletişimdeki etkisi ölçümlenmiştir [22].

Bu ölçümlerin sonuçları veritabanında iki farklı tablo olacak şekilde kaydedilmiştir. Bu veriler ölçüm sonuçlarına göre tablo haline getirilerek analizi yapılmış ve çeşitli bulgular elde edilmiştir.

Gürültüsüz ortamda saldırı olmadığı sürece anahtar uzunluğu gönderilen foton sayısının yarısı kadar olmaktadır. Gürültüsüz ortamda saldırganın ham anahtar uzunluğuna etkisi bulunmamaktadır. Gürültüsüz ortamda saldırganın anahtar üzerinde sebep olduğu bozulmalar (bitler) foton sayısının %30'u kadardır. Gürültüsüz ortamda saldırganın olması halinde gönderilen foton sayısı ile hatalı bitlerin oranı eşit miktarda artmaktadır. Gürültüsüz ortamda saldırganın bulunması halinde gönderilen foton sayısı artarken polarizasyonu değişen fotonların oranında değişim olmamaktadır. Gürültüsüz ortamda saldırgan bulunması halinde gönderilen foton sayısı artarken bit değeri değişen fotonların oranında değişim bulunmamaktadır. Gürültüsüz ortamda saldırgan bulunması durumunda gönderilen foton sayısındaki artış miktarı saldırganın doğru olarak yakaladığı bitlerin oranında değişikliğe sebep olmamaktadır [22].

Kuantum kriptoloji benzetim ve eğitim uygulaması çalışmasında kuantum kriptoloji benzetim ve eğitim uygulaması adı verilen eğitimcilerin ve öğrencilerin faydalanabileceği animasyon destekli bir yazılım geliştirilmiştir. Bu uygulamada BB84 protokolünün benzetimi yapılmıştır. Uygulamada eğitsellik ve sayıtsallık üzerinde

durulmaktadır. Eğitsellik, görsel nesnelerin ön planda olduğu bir ara yüz sunarken sayıtsallık daha çok istatistiksel kullanım için hazırlanmış bir ara yüz modudur. Eğitsellik modunda uygulama yavaş ve dar değer aralıklarıyla çalışmaktadır. Sayıtsallık modunda istatistiksellik ön planda olduğu için görsellik az tutulmuştur. Uygulama bu modayken daha hızlı ve geniş değer aralıklarıyla çalıştığı çalışmada tespit edilmiştir. Geliştirilen uygulamada kullanıcı dört farklı rapor alabilmektedir. Son yapılan denemenin raporu, uygulama içinde şimdiye kadar yapılan simülasyonların genel raporu, genel raporun ayrıntılı raporu ve özet rapor. Kullanıcı ayarlar bölümünden hangi modda eğitsel veya sayıtsal işlem yapacağını tercih edebilmektedir. Uygulama içinde benzetimler, saldırgan olması durumunda kuantum kriptoloji benzetimi ve saldırgan olmadığı durumlarda kuantum kriptoloji benzetimi olmak üzere kullanıcı tarafından tercih edilebilmektedir. Yapılan bu çalışmayla kuantum kriptolojinin temel kavramlarının anlaşılması hedeflenmiştir [23].

RSA ve AES algoritmaları kullanılarak yapılan çalışma olan güvenli elektronik posta sisteminin FPGA üzerinde tasarımı ve gerçeklenmesi çalışmasında günümüz iletişim araçlarının herkesin erişimine açık olması nedeniyle verilerde güvenlik zafiyeti oluşmaması adına kriptoloji yöntemleri kullanılmaktadır. Pretty Good Privacy (PGP) ile veriler önce imzalanır, sıkıştırılır, şifrelenir ve son aşama olan iletim sağlanmaktadır. Bu yöntem e-posta güvenliği için kullanılmaktadır. Bu çalışmada PGP'de kullanılan Message-Digest Algorithm 5 (MD5), RSA ve International Data Encryption Algorithm (IDEA) algoritmalarından IDEA algoritması yerine AES şifreleme algoritması kullanılmaktadır. Veriler önce MD5 sonra RSA ve AES algoritmalarından geçerek şifrelenmesi sağlanmıştır [24]. PGP, kriptoloji algoritması olarak açık anahtar şifreleme algoritmalarını kullanmaktadır. Anahtar yönetiminde sayısal imza olan RSA kullanırken veri şifreleme için özel anahtar kriptoloji (IDEA) ve sayısal imza için tek yönlü özet fonksiyon (MD5 ve RSA) kullanmaktadır. PGP'nin Field Programmable Gate Array (FPGA) üzerinde gerçekleşmesinde IDEA algoritması yerine AES şifreleme algoritması kullanılmıştır. PGP mesajları gönderici tarafından sayısal olarak imzalanabilmektedir. PGP imzası, alıcının göndericiyi belirlemesi ve veride değişiklik olup olmadığını doğrulaması için kullanılmaktadır. PGP'nin Oluşturulması: Modülün oluşması için öncelikle MD5, RSA ve AES algoritmalarının sırasıyla bağlanması gerekmektedir. PGP'nin çalışma mantığı ve sıralaması gereği bu işlem yapılmaktadır.

MD5 algoritmasının girdisi 800 bitken alınan çıktı 128 bittir. RSA ve AES algoritmalarının girdi ve çıktıları 1024 bittir. MD5 algoritmasının çıktısı RSA algoritmasının girişi olacağı için aradaki fark için kalan bitlere lojik 0 değeri atanmaktadır. PGP ile güvenli elektronik posta gönderimi FPGA ile gerçekleştirilmiştir. Bu gerçekleştirme sonunda 19347 dilime sahip alan kullanılmıştır. Devrenin gerçekleştirilme süresinde harcanan saat frekansı ise 63.731 MHz olarak analiz edilmiştir [24].

IV. Sonuçlar ve Tartışma

Bu çalışmada hassas verilerin güvenliğinin hem bulut ortamında hem de kişisel depolama ortamlarında saklanırken güvenlik ve gizliliğin sağlanmasına yönelik kriptoloji yöntemleri ele alınmıştır. Bu yöntemler klasik kriptoloji ve kuantum sonrası kriptoloji olmak üzere incelenmiştir. Klasik kriptoloji algoritmalarının ilki olarak kabul edilen Sezar Şifreleme Algoritması'nda karakterler belirli bir sayı ölçüsünde ötelenerek şifreli veri elde edilmektedir. Şifreleme mantığından dolayı güvenlik konusunda öteleme yapılan sayısal değer bilindiğinde veri çözümlenebilmektedir [25]. Belirli sayısal değerin yerine kullanılacak anahtar ile alıcı ve göndericinin birbirleriyle güvenli haberleşmesinin sağlanması simetrik şifrelemedir. Bu yöntemde kullanılan en bilindik algoritma AES algoritmasıdır. AES'de ortak anahtar ile veri şifrelenmekte ve aynı anahtar ile veri çözümlenmektedir. Bu anahtarın saldıran tarafından elde edilmesi verinin şifresinin çözülmesine sebep olacaktır [26]. Asimetrik şifreleme yöntemlerine ise en etkin algoritma RSA algoritmasıdır. RSA'de iki farklı anahtar bulunmaktadır. Bunlardan ilki genel ve sisteme dahil olan kullanıcılara tanımlanan anahtardır. Diğer anahtar ise her bir kullanıcıya özgü tanımlanan anahtardır. Bu özel ve genel anahtar sayesinde uçtan uca şifreleme sistemi oluşturulmaktadır. Saldırgan şifreli verinin çözümünde genel anahtarı öğrense bile kullanıcıya özgü anahtarı da bilmesi gerekmektedir [26].

TABLO I. KLASİK KRİPTOLOJİ İLE KUANTUM KRİPTOLOJİ FARKLARI

KLASİK KRİPOGRAFİ	KUANTUM KRİPOGRAFİ
Matematiksel hesaplamaya dayanır.	Kuantum mekaniğine dayanır.
Yaygın olarak kullanılır.	Sofistikedir.
Dijital imza var.	Dijital imza mevcut değil.
Bit hızı hesaplama gücüne bağlıdır.	Ortalama bit hızı 1 MBPS'dir.
Bit depolama 2n n-bit dizeleri.	Bit depolama bir n-bit dize
Bilgi işlem gücü arttıkça gerekli derecelendirme.	Fizik yasalarına dayanır.
İletişim ortamı bağımsız.	İletişim ortamı bağımlı.

RSA algoritmasının ötesinde Kuantum kriptografi anahtar dağıtım sistemlerinden BB84 ve B92 Protokolleri yer almaktadır. Kuantum mekaniğinin kopyalanamazlık ilkesi gereği saldırı anında iletişimi kuran tarafların müdahaleyi anlaması mümkün olmaktadır. Kuantum algoritmalarından Shor, Grover ve Deutsch algoritmaları kuantum bilgisayarları oluşturmak için Fourier dönüşümü ve kuantum hesaplama kavramları kullanılarak geliştirilmiştir [27].

Tablo 1'de kuantum kriptoloji ile klasik kriptoloji arasındaki değerlendirme sunulmuştur. Günümüz bilgisayarlarıyla klasik kriptoloji algoritmalarından RSA Şifreleme Algoritmasındaki n değerini çarpanlarına ayırmak yıllar sürebilir. Bu işlemi ancak büyük ölçekli kuantum bilgisayarlar kısa sürede gerçekleştirebilmektedir. Böyle bir

durum olması halinde açık anahtarlı şifreleme algoritmalarında köklü değişiklikler yapılması gerekmektedir. Zira kuantum bilgisayarları için hali hazırda kullanılan açık anahtarlı şifreleme algoritmasını çözmek hiç de zor olmayacaktır. Açık Anahtarlı Şifreleme algoritmalarının güvenliğinin çok büyük asal sayıların çarpanlarına ayrılma zorluğuna dayanması büyük ölçekli kuantum bilgisayarlarla aşılabilecek bir noktadır. Sonuç olarak Shor Algoritması büyük ölçekli kuantum bilgisayarlarda kullanılması durumunda Açık Anahtarlı Sistemlerdeki çarpanlara ayırma zorluğu ortadan kalkmış olacaktır.

KAYNAKLAR

[1] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006, October). Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security (pp. 89-98). Acm.

[2] Toyran, M., Pedersen, Thomas B., Hasekioğlu, A.S. Atilla, Can, M.Ali, Berber, S., "Bilgi Güvenliğinde Kuantum Teknikler", IV. Ağ ve Bilgi Güvenliği Sempozyumu, Bildiriler Kitabı, 2011.

[3] Coşkun, A. ,Ülker, Ü., "Ulusal Bilgi Güvenliğine Yönelik Bir Kriptografi Algoritması Geliştirilmesi ve Harf Frekans Analizine Karşı Güvenirlik Tespiti", Bilişim Teknolojileri Dergisi, Cilt: 6, Sayı: 2, Mayıs 2013.

[4] Sakallı, Muharrem Tolga. "Modern şifreleme yöntemlerinin gücünün incelenmesi.", Trakya Üniversitesi / Fen Bilimleri Enstitüsü / Bilgisayar Mühendisliği Anabilim Dalı Doktora Tezi, 2006

[5] Yerlikaya, Tarık, Ercan Buluş, and Nusret BULUŞ. "Kripto algoritmalarinin gelişimi ve önemi." Akademik Bilişim Konferansları (2006): 9-11.

[6] Çakar, H., Varol, A. "Bilgi Güvenliği ve RSA Şifreleme Algoritmasının İncelenmesi", Kocaeli Üniversitesi, Kocaeli, Bildiriler Kitabı, 2007

[7] AYGÜN, E., "AES Şifreleme ve Esnek Kümeler Yardımıyla Elde Edilen Yeni Bir Kriptosistem", Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, Cilt 35, Sayı 1, 2019.

[8] Ruth, J. Anitha, Sirmathi, H., Meenakshi, A. "Secure Data Storage And Intrusion Detection In The Cloud Using MANN And Dual Encryption Through Various Attacks", The Institution Of Engineering And Technology Journals, 2019, Vol. 13 Iss. 4, pp. 321-329.

[9] Bodur, H., Kara, R., Zavrak, S. "RSA Şifreleme Algoritması Kullanılarak SMS İle Güvenli Mesajlaşma Yöntemi", 2015.

[10] Yerlikaya,T., Buluş, E., Buluş, N. "Asimetrik Şifreleme Algoritmalarında Anahtar Değişim Sistemleri"

[11] Yerlikaya,T., Buluş, E., Buluş, N. "RSA Şifreleme Algoritmasının Pollard Rho Yöntemi ile Kriptanalizi", Akademik Bilişim, 2007.

[12] Kodaz,H., Botsali F., "Simetrik ve asimetrik Şifreleme Algoritmalarının Karşılaştırılması", Teknik-Online Dergi, Cilt 9, Sayı:1, 2010.

[13] Aksakalli, Işil, K., "Bulut Bilişimde Güvenlik Zafiyetleri, Tehditleri ve Bu Tehditlere Yönelik Güvenlik Önerilerinin İncelenmesi", Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:5, No:1, S:8-34

[14] Kuantum Kriptografi," http://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/kuantum-kriptografi", Erişim Tarihi:13 Temmuz 2019

[15] Toyran, Mustafa. "Quantum cryptography." 2007 IEEE 15th Signal Processing and Communications Applications. IEEE, 2007.

[16] Gümüş, E., "Kuantum Kriptografi ve Anahtar Dağıtım Protokolleri", Akademik Bilişim'11 - XIII. Akademik Bilişim Konferansı Bildirileri 2 - 4 Şubat 2011 İnönü Üniversitesi, Malatya

[17] Toyran, M., "Optik Ağlarda Kuantum Kriptografi Kullanarak Güvenli İletişim"

[18] Ege, B., "Kuantum Mekaniğinden Kuantum Bilgisayarlara", Bilim ve Teknik, Ekim 2012

[19] Ulucan, H., "Süperiletken Kubitli Kuantum Bilgisayarlar ve Kuantum Hesaplama", Gelişim Üniversitesi / Fen Bilimleri Enstitüsü / Mekatronik Mühendisliği Anabilim Dalı Yüksek Lisans Tezi, 2017

[20] Toyran, M., Pedersen, T. B., Hasekioğlu, A. A., Can, M. A., & Berber, S. Bilgi Güvenliğinde Kuantum Teknikler. BİLDİRİLER KİTABI, 1998.

[21] Susam Ö.C., " Quantum Circuit Synthesis", İstanbul Teknik Üniversitesi / Fen Bilimleri Enstitüsü / Mühendislik ve Teknoloji / Nanobilim ve Nano Mühendislik Anabilim Dalı / Nanobilim ve Nanomühendislik Programı / Yüksek Lisans Tezi, 2015

[22] İncetaş, O., Sağiroğlu, Ş., "Kuantum Kriptografide Gönderilen Foton Sayısının, Gürültüsüz Ortamda Elde Edilen Anahtar Uzunluklarına Etkisi", Süleyman Demirel Üniversitesi Mühendislik Bilimleri ve Tasarım Dergisi, 2015

[23] Toyran, Mustafa. "A study on information reconciliation problem in quantum key distribution." 2016 24th Signal Processing and Communication Application Conference (SIU). IEEE, 2016.

[24] Çelik, V., Yalçin; Berna, Ö., "Güvenli Elektronik Posta Sistemi PGP'nin FPGA Üzerinde Tasarımı ve Gerçeklenmesi"

[25] Sinaga, M. D., Sembiring, N. S. B., Tambunan, F., & Sianturi, C. J. M.. Hybrid Cryptography WAKE (Word Auto Key Encryption) and Binary Caesar Cipher Method For Data Security. In 2018 6th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-5). IEEE, 2018.

[26] Mathur, H., & Alam, Z. Analysis in symmetric and asymmetric cryptology algorithm. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 4(1), 2015.

[27] Benchasattabuse, N., Chongstitvatana, P., & Apomtewan, C. Quantum Rough Counting and Its Application to Grover's Search Algorithm. In 2018 3rd International Conference on Computer and Communication Systems (ICCCS) (pp. 21-24), 2018.

Secure Quantum Communication Based on Clifford Scrambling With Blind Trent

Ihsan Yilmaz
Department of Computer Engineering
Faculty of Engineering
Canakkale Onsekiz Mart University
Canakkale, TURKEY
Email: iyilmaz@comu.edu.tr

Erdi Acar
Department of Computer Engineering
Faculty of Engineering
Canakkale Onsekiz Mart University
Canakkale, TURKEY
Email: erdiacar@stu.comu.edu.tr

***Abstract*—In this study, we investigate the safe quantum communication with blind Trent using Clifford Scrambling. Clifford Scrambling, which gives maximum mixing for this purpose, was experimentally tested for three-qbit in IBM Quantum Experience's 5-qbit superconducting quantum processor. In this context, the circuit of Clifford Scrambling, which is used to model black holes [6] and provides maximum mixing, is generalized from three qbit to n-qbit. By using n qubit Clifford Scrambling in our protocol, secure quantum communication with blind tend was obtained.**

***Ozet-* Bu calismada, Clifford Scrambling kullanilarak kor Trent ile guvenli kuantum iletisim incelenmektedir. Bu amac icin maksimum karistirma veren Clifford Scrambling'i deneysel olarak IBM Quantum Experience'n 5-qubitlik super-iletken kuantum islemcisinde 3-qubit icin test edildi. Bu baglamda, kara delikleri modellemek [6] icin kullanilan ve maksimum karistirma veren Clifford Scrambling'in devresini 3-qubitten n-qubit'e genellestirildi. n qubitlik Clifford Scrambling protokolumuzde kullanilarak, kor trendli guvenli kuantum iletisimi elde edildi.**

***Index Terms*—Secure Quantum Communication, Clifford Scrambling, Blind Protocol**

I. Introduction

Scrambling is very important for quantum communication, because information on quantum chanel is scrambled at late times. Quantum scrambling is the distribution of local information throughout a whole system as scrambling [**?**]. There are many studies on the quantum scrambling in the literature. Jiang et al. [**?**] studied quantum image scrambling by using Arnold and Fibonacci taransition. They also suggested Hilbert scrambling for quantum images [**?**]. Zhou et al. [**?**] suggested quantum image scrambling depending on disordering bit-plane of pixsel. Also, Heidari et al. [**?**] purposed dual quantum image scrambling method.

Scrambling recently emerged as a powerful tool for characterizing chaos in black holes. It has been found that many of the tools and ideas advanced in the context of black hole physics are useful in characterizing the scrambling behavior of general multi-system systems [**?**]. Recently, Beni Yoshida and Norman Y. Yao [**?**] suggested Clifford Scrambling for this type scrambling. They used Clifford Scrambling to characterize scrambling in the black holes. Also, they imply that "Clifford Scrambling gives maximally scrambling since Clifford Scrambling operator delocalizes as Pauli operators for scrambling of information" . So, we will use Clifford Scrambling to get a secure protocol. For this aim, we generalize circuit of Clifford Scrambling, which is used for black holes [**?**], from three qubit to n-qubit. Using Clifford Scrambling for n qubit, we get secure quantum communication with blind Trent.

Our study is organized as follows. In Sec. II, the generalization circuits of Clifford Scrambling are given. In Sec. III, we introduce the our protocol based on Clifford Scrambling with blind trent. In Sec.IV and V, the security analysis of the protocol and some results are implied, respectively.

II. The Generalization Circuit of Clifford Scrambling

Beni Yoshida and Norman Y. Yao [**?**] suggested circuit of Clifford Scrambling for three qubits as follows;

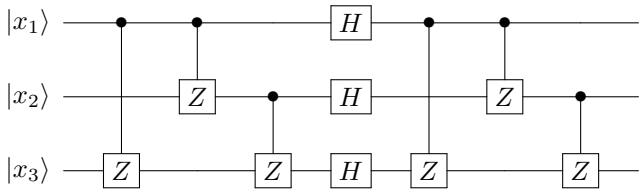


Fig.1: 3-Qubit Clifford Scrambler [**?**]

In Fig.1, H represents a Hadamard gate, while Z is a two-qubit controlled-Z gate (dots control and Z target). All unitary operator is scrambler at the highest level because consists of Pauli operator.

Let us test the 3-Qubit Clifford Scrambling operator on IBM Quantum Experience [**?**]. In IBM Q Experience, the compiler will attempt to combine the gates. The barrier is an instruction to the compiler to prevent these combinations being made. We give the experimental results as follows;

Fig.2: 3-Qubit Clifford Scrambling circuit on IBM Q Experience

Fig.3: Result of 3-Qubit Clifford Scrambling

We can conclude from fig.3 that Clifford Scrambling works as scrambler. Also , we can generalize the circuit in Fig.1 for

n-qubits as follows:

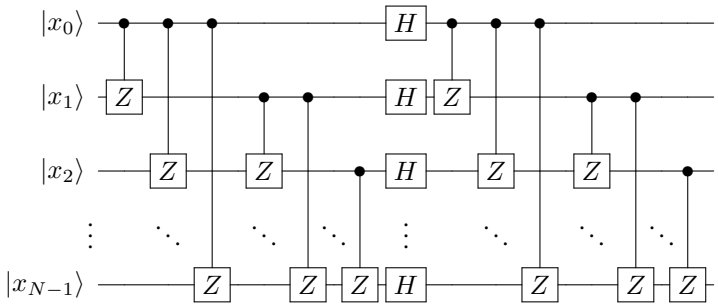


Fig.4: N-Qubit Clifford Scrambler

The circuit in Fig.4 consists of N(N-1)/2 controlled-Z gates and N Hadamard(H) gates. In our protocol, we will use Clifford Scrambler (C_s) for n-qubits scrambler operator .

III. The Protocol Based on Clifford Scrambling with Blind Trent

We follows the steps of algorithm which is developed by Sahin and Yilmaz [**?**] (references there in). Let's start narration our protocol.The members of protocol are Alice, Bob and Blind Trent. Alice wants to send message $m = \{m_0 m_1 m_2 ... m_{N-1}\}, m_i \in \{0, 1\}$ to Bob. Blind Trent is the administrator of the protocol and reliable. Blind Trent make some communications to secure the protocol. Bob can retrieve and verify the message m with the help of Blind Trent. The protocol consist of the the following steps.

Fig.5: Scheme of The Protocol Based on Clifford Scrambling with Blind Trent

1) Alice shares the secret key K_{AB} with Bob while Blind Trent shares the secret key K_{TA} with Alice and the secret key K_{TB} with Bob. The K_{AB}, K_{TA} and K_{TB} secret keys of the protocol members are shared using the quantum key distribution protocol [**?**], [**?**]. Secret keys are used to encrypt the quantum message and to prevent intruders. K_{AB}, K_{TA} and K_{TB} secret keys are generated only once.

2) Alice express the message m in the quantum calculation bases $\{0 \rightarrow |0\rangle, 1 \rightarrow |1\rangle\}$. We assume that the length of the message m is $|m| = N$. The length of the entire message to be sent may be greater than N. In this case, the message can be divided into N-length segments. Each segments can be sent in different sessions.

$$|m\rangle = \bigotimes_{i=0}^{N-1} |m_i\rangle \tag{1}$$

where $|m_i\rangle \in \{|0\rangle, |1\rangle\}$.

3) Blind Trent creates a permutation P of a set of $\{1, 2, ..., N\}$ as follows [**?**]:

$$P = \begin{bmatrix} 1 & 2 & ... & N \\ P(1) & P(2) & ... & P(N) \end{bmatrix} \tag{2}$$

$P(i)$ is expressed on a binary basis and Blind Trent prepares the quantum state $|P\rangle$ [**?**]. Blind Trent creates encrypted versions of that permutation as follows:

$$|P_A\rangle = E_{K_{TA}}(|P\rangle) \tag{3}$$

$$|P_B\rangle = E_{K_{TB}}(|P\rangle) \tag{4}$$

E_K is a quantum one-time pad encryption algorithm presented by Kim et. al [**?**]. It was also used by Yilmaz [**?**] to maximize protocol security and to prevent pirate attacks. To further improve the security of this encryption algorithm, we reorganized Zhang et.al's [**?**] quantum key algorithm for the 32-bit version. Then, Blind Trent sends the encrypted $|P\rangle$ state to Alice through the quantum channel.

4) Alice decrypts the $|P_A\rangle$ state with the secret key K_{TA} to obtain the $|P\rangle$ state, then performs measurement.
5) Alice applies the N-qubit Clifford Scrambling operator(C_s) given in Fig. 4 to the message $|m\rangle$.
6) The result of each qubit of the C_s is applied by Alice the permutation P, which is specified by Blind Trent.

Let us express signing phase.

7) Alice reordered the qubits . Also, the secret key is applied to each qubit. As a result of the permutation $|P\rangle$ applied by Alice, the final state is as follows:

$$|A(Q)\rangle = C_s(P(i))(C_s(|m\rangle)) \tag{5}$$

where $i = 0...N$.

8) As result of the secret key K_{AB} applied by Alice, the final state is as follows:

$$|A(S)\rangle = E_{K_{AB_{P_A(i)}}}(|A(Q)\rangle) \tag{6}$$

9) Alice sends $|A(S)\rangle$ to Bob through quantum channel.
10) Alice encrypts the $C_c(|m\rangle)$ with using the secret key K_{AB} with the encryption algorithm and sends it to Blind Trent through the quantum channel.

$$|AT(S)\rangle = E_{K_{AB}}(C_s(|m\rangle)) \tag{7}$$

11) Blind Trent encrypts the $|AT(S)\rangle$ with using the secret key K_{TB} with the encryption algorithm and sends it to Bob through the quantum channel.

$$|TB(S)\rangle = E_{K_{TB}}(|AT(S)\rangle) \tag{8}$$

Let us express verification phase.

12) Bob decrypts $|TB(S)\rangle$ with secret key K_{BT} and gets $|AT(S)\rangle$. Bob decrypts the $|AT(S)\rangle$ with the secret key K_{AB} and obtains the $C_s(|m\rangle)$ state.Bob applies $C_s^\dagger$ and measures $|m\rangle$ state and saves the results as $\tilde{m}$.

13) Bob decrypts $|A(S)\rangle$ with secret key K_{AB} and gets $|A(Q)\rangle$.
14) Bob asks to Blind Trent for permutation P. Then, Blind Trent sends $|P_B\rangle$ to Bob via the quantum channel. Bob

decrypts the $|P_B\rangle$ state with the secret key K_{TB} to obtain the permutation P, then performs measurement. Thus Bob obtain P. Bob solves the $|A(Q)\rangle$ state with permutation $C_s^\dagger(P(i))$ and obtain $C_s(|m\rangle)$.

15) Bob applies $C_s^\dagger$ and measures $|m\rangle$ state and saves the results as $\bar{m}$. Bob checks the equality of $\tilde{m}$ and $\bar{m}$. If $\tilde{m} = \bar{m}$, Bob declares that the message is verified, otherwise the message is rejected and the protocol is canceled. If the message m is verified, Bob encrypts the verified m message and sends it to Blind Trent.

$$|BT(S)\rangle = E_{K_{BT}} |m\rangle \tag{9}$$

16) Blind Trent asks Alice for the message m. Alice encrypts the valid message m to the encryption algorithm and sends it to Blind Trent.

$$|AT(S)\rangle = E_{K_{AT}}(|m\rangle) \tag{10}$$

17) Blind Trent decrypts $|AT(S)\rangle$ secret key K_{AT} and makes measurement and gets $\tilde{m}$. Blind Trent checks the equality of $\tilde{m}$ and $\bar{m}$. If they are equal, Blind Trent stores the message with Alice's identification.

IV. The security Analysis of the Protocol

Let us examine security of our protocol. Basic requirements of quantum digital signature protocols to ensure complete security: the signature should not be rejected by the signatory and any pirate cannot impersonate the signature of signatory.

First, we consider the attacks that can be done within the protocol. We assume that Bob is a pirated member and wants to create Alice's signature. Even if Bob knows the details of the signature protocol he cannot create Alices signature because of blind Trent. Bob cannot create Alices signature without knowledge of Trent. After the end of the legal signature protocol, Bob may change correct message m to $\bar{m}$. Due to Blind Trent's knowledge of the correct message m, Bob cannot deceptiveness.

Secondly, any pirate may try to fake Alices signature. The situations in the $C_s(|m\rangle)$ results can be rearranged by permutation of Blind Trend to create an accurate signature of Alice. Therefore, any attacker cannot commit fraud. Even if any attacker obtains permutations, the permutations will be rearranged by the blind Trent for each signature session. Blind Trent must be part of the protocol so any pirate cannot achieve collective forgery. Also, any attacker can change the $C_s(|m\rangle)$ result by applying a unitary transformation. Bob and Blind Trent can check the m and $\bar{m}$ equality to detect this change.

Alice and Bob cannot refuse the signature because of the administration of protocol by Blind Trent. Blind Trent controls some communications in the protocol. Alice can send a different $|\tilde{m}\rangle$ to Blind Trent and claim that the signature is not his. Blind Trent can check whether Alice's $|\tilde{m}\rangle$ and Bob's $|\bar{m}\rangle$ messages are equal. In this way decide whether the Blind Trent signature protocol is valid or not.

From the above security analysis may say that protocol based on Clifford Scrambling provides unconditionally security. In addition, our protocol provides secure transfer of messages.

V. Conclusion

In this sudy, we suggested secure quantum communication protocol depending on Clifford scrambling. we first checked if the Clifford scrambler operator was working on a real quantum computer. When we experimentally test Clifford scrambling for three qubit on the quantum processor of IBM Quantum Experience, we can easily see that we get the maximum scrambling for three q-bit. Also, we can generalize the circuit of Clifford scrambling from three qubit to the n-qubit. we increased key length to 32 bits to increase security. Security analysis of the protocol shows that we could obtain secure quantum communication by using Clifford scrambling for n-qubits as a scrambler which has the ability to resist against unauthorized attacks . This communication may be used for cloud quantum computers due to blind.

Acknowledgment

We would like to thank the referees for making our article more understandable.

References

[1] K. A. Landsman, C. Figgatt, T. Schuster, N. M. Linke, B. Yoshida, N. Y. Yao and C. Monroe, Verified quantum information scrambling, Nature, 567:6165, 2019. [Online]. Available: https://doi.org/10.1038/s41586-019-0952-6

[2] Jiang,N.,Wu,W.Y., Wang, L., the quantum realization of Arnold and Fibinacci image crambling, Quant.inf.Process.13(5),1223-1236,2014.

[3] Jiang,N.,Wang, L., Wu,W.Y., Quantum Hilbert image scrambling,Int.J.Theor.Phys.53(7),2463-2484,2014.

[4] Zhou,R.G., Sun, Y.J.,Fan, P., Quantum image gray-code and bit plane scrambling,Quant.inf.Process.14(5),1717-2734,2015.

[5] Heidari, S. et al., Dual quantum image scrambling method, Quant.inf.Process.doi: https://doi.org./10.1007,2019.

[6] Beni Yoshida and Norman Y. Yao, *Disentangling Scrambling and Decoherence via Quantum Teleportation*, Phys. Rev. X 9, 011006, 2019. [Online]. Available:10.1103/PhysRevX.9.011006

[7] C. H. Bennett and G. Brassard,,*Quantum cryptography: Public key distribution and coin tossing*, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing.vol. 175, no. 6, pp. 661663, 1984.

[8] A. K. Ekert,Quantum cryptography based on bells theorem, Phys. Rev. Lett., vol.67, p.8, 1991. [Online]. Available: https://doi.org/10.1103/PhysRevLett.67.661

[9] I. Ylmaz, Quantum group proxy digital signature based on quantum fourier transform by using blinded and non blinded trent, International Journal of Information Security Science, vol. 6, no. 4, pp. 79 86, 2017.

[10] E.Sahin and I. Ylmaz, Security of NEQR Quantum Image by Using Quantum Fourier Transform with Blind Trend, International Journal of Information Security Science, vol. 7, no. 1, pp. 20 25, 2018.

[11] T. Kim, J. W. Choi, N. S. Jho, and S. Lee, Quantum messages with signatures forgeable in arbitrated quantum signature schemes, International Journal of Information Security Science, Physica Scripta, vol. 90, no. 2, p.025101, 2015. [Online]. Available:http://stacks.iop.org/1402-4896/90/i=2/a=025101

[12] W. Zhang, D. Qiu, and X. Zou, Improvement of a quantum broadcasting multiple blind signature scheme based on quantum teleportation, Quantum Information Processing, vol. 15, no. 6, pp. 24992519, 2016. [Online]. Available: https://doi.org/10.1007/s11128-016-1289-9

[13] The IBM Quantum Experience,[Online]. Available: https://www.research.ibm.com/ibm-q/

Kuantum Kriptanalizin Siber Güvenlikteki Yeri

The Role of Quantum Cryptanalysis in Cyber Security

Muharrem Tuncay GENÇOĞLU

Fırat Üniversitesi Teknik Bilmler Meslek Yüksek Okulu

mt.gencoglu@firat.edu.tr

Özet— Bu çalışmada gelişen kuantum teknolojileri ile birlikte siber dünyada güveliğin öneminin daha da belirginleşmesi sebebiyle bu alanda kullanılan kuantum teknikler anlatılmaya çalışılmıştır. Kuantum kriptografinin olduğu yerde mutlaka kuantum kriptanalizde olmak zorundadır. Kuantum Kriptanaliz, bazı kuantum mekaniksel sistemlerden, bir takım kuantum mekaniksel etkilerden yararlanarak yani kısacası kuantum bilgisayarlar kullanarak şifre kırmayla ilgilenen kriptografik bir uygulama alanıdır. Hem kuantum kriptografi hemde kuantum kriptanaliz hakkında yeteri kadar Türkçe kaynağın olmaması nedeniyle bu araştırma, milli siber güvenlik çalışmalarına katlıda bulunması amacıyla kaleme alınmıştır.

Anahtar Kelimeler—Kuantum Kriptanaliz, Siber Güvenlik

Abstract—In this study, quantum techniques used in this field are tried to be explained because of the importance of security in cyber world with the developing quantum technologies. Where quantum cryptography exists, it must be in quantum cryptanalysis. Quantum Cryptanalysis is a cryptographic field of application which deals with the use of some quantum mechanical systems, a number of quantum mechanical effects, in other words, using quantum computers. Since there is not enough Turkish resources on both quantum cryptography and quantum cryptanalysis, this research has been written in order to contribute to national cyber security studies.

Keywords —Quantum Cryptanalysis, Cyber Security

I. GİRİŞ

Verilerin; işlenmesi esnasında iç/dış tüm casusluk türü saldırılara karşı korunması ve iletimi, saklanması esnasında güvenliğinin sağlanması siber güvenlik olarak tanımlanabilir. Bilginin bir takım yerine koyma, yer değiştirme ya da bazı matematiksel işlemler ile okunamaz hale getirildiği geri dönüşümlü yöntemler, gizli yazı yazma sanatı olarak bilinen kriptografi biliminin konusudur. Kriptografi; bilginin güvenliğini sağlamak amacıyla şifreleme ve şifre çözme işlemleri ile ilgilenmektedir. Bu nedenle siber dünyada veri güvenliği genellikle kriptografik yöntemler kullanılarak sağlanır. Modern kriptografinin veri güvenliğini sağlamak adına ortaya koyduğu başlıca hizmetleri; gizlilik, bütünlük, kimlik doğrulama ve inkârın önüne geçmedir. İhtiyaca göre bunların birinden, bir kaçından ya da tamamından faydalanmak gerekebilir. Siber dünyada iletişimin güvenliği, başkası tarafından dinlenme, mesajın içeriğinin değiştirilmesi, kimlik taklidi ve inkar etme şeklindeki tehditlerin bertaraf edilmesi ile mümkündür. Günümüzde bunun sağlanması için başvurulan ana yöntem kriptografidir.

Kriptografinin gizlilik hizmeti; bilginin gerçek alıcı haricindeki 3. kişiler tarafından kesinlikle anlaşılmamasını temineder. Bu amaçla, bilgiyi şifrelemede kullanılan başlıca yöntemdir [1,2].

II. KUANTUM KRİPTOGRAFİ

Kriptoloji bilimi, matematiğin alt dalı olup; matematiksel tekniklerden faydalanıp şifreleme sistemlerini kullanarak bilgiyi gizleme sanatı ve bilimi olarak bilinen kriptografi ve matematiksel yöntemleri, bilinen bütün hesaplama gücünü ve tasarım zayıflıklarını kullanarak, mevcut bilgi güvenliği sistemlerini alt etme olarak tanımlanan kriptanalizden oluşur.

Modern kripto sistemlerde en ciddi sorun anahtar dağıtım problemi olarak bilinen gizli anahtarın güvenliğidir. Bu nedenle anahtar dağıtım problemlerinin ve risklerinin olmadığı bir kripto sisteme ihtiyaç vardır. Bu da teknolojik gelişmelerden etkilenmeyen ve uzun vadeli, kalıcı gizlilik sağlayan yeni bir alan olan kuantum kriptografidir.

Kuantum kriptografi, siber alandaki güvenliğin kuantum mekaniğine ait belirsizlik ilkesi, foton polarizasyonu, dolaşıklık gibi kanunlar ile teminat altına alınan kriptografi tekniğidir. Asıl avantajı, kanıtlanmış evrensel kuantum mekaniği yasalarına dayanması, bunların klasik olarak eşdeğerinin bulunmaması ve güvenliğin ispatlanabilir olmasıdır.

Mevcut kuantum kriptografi şu an klasik ve kuantum kısımlardan oluşmaktadır;

Kuantum Kısım; Kuantum Anahtar Dağıtımı, Klasik Kısım ise geleneksel kriptografi ile şifrelemeden oluşur.

Günümüzde kuantum kriptografinin çalışma prensibi ise şu şekildedir:

•Anahtar, taraflar arasında kuantum anahtar dağıtımı ile dağıtılır, böylece anahtar dağıtım problemi de çözülmüş olur. Güvenliği kanıtlanmış, tamamen güvenli tek anahtar dağıtım yöntemi kuantum anahtar dağıtımıdır.

•Şifreleme, vernam şifresi ile yapılır. Vernam şifresi kırılmazlığı teorik olarak ta ispatlanmış tek şifredir.

Aralarında çok mesafe olan kişiler arasında aynı, tesadüfi ve güvenli bir gizli anahtar oluşturulması Kuantum Anahtar Dağıtım protokolleri ile sağlanır. Anahtar dağıtımı sırasındaki iletişime müdahale olup olmadığının açığa çıkarabilmesi ise kuantum mekaniği kanunlarıyla sağlanır ki bu klasik iletişimde benzeri olmayan özelliklerdendir.

KAD'ın çalışma ilkesi ise;

•Güvenli olarak anahtar dağıtımı yapılır,

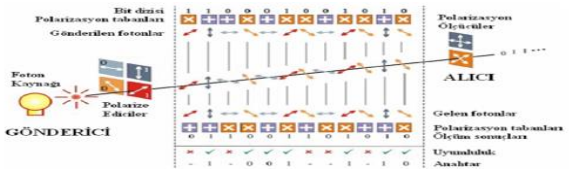
•Güvenliğin sağlanmasında şüphe olursa, protokolün iptali ve tekrarı gerekir.

KAD da kuantum mekaniğinin en temel ilkelerinden olan Heisenberg belirsizlik ilkesi kullanılarak güvenli iletişim garanti altına alınır. Bu ilke ilk defa Alman fizikçi W. Heisenberg tarafından "birbirine bağlı iki büyüklükten birinin ölçülmesindeki duyarlılık arttıkça diğerinin ölçülmesindeki duyarlılık azalır. Öyle ki, ölçümler sonucu her iki büyüklüğe ait belirsizliğin çarpımı daima Planck sabitinden büyük veya enaz ona eşittir" şeklinde ifade edilmiştir. Bu gerçek kısaca; "Bilinmeyen bir kuantum sistemi ölçmek o sistemi değiştirecektir" demektir. Buradan hareketle bu şekildeki bir mekanizma ile temsil edilen kuantum bilgi de değişecektir. Bu prensiple bir kuantum sistemin belirli özellikteki çiftlerinin aynı anda hiçbir zaman tam olarak ölçülemeyeceği ifade edilir. Bu nedenle, belirsizlik ilkesinin bir sonucu olarak, kuantum bilgiyi bozmadan üzerinde ölçüm yapmak ve onu edinmek mümkün değildir. Bu da kuantum bilgi kopyalanamaz sonucunu getirir. Yani bilgi ile iletişimde olan saldırganın varlığını tespit edebilmek mümkündür [3-5].

KAD, iletişim için temel kuantum parçacıklarından ve fotonlardan faydalanır. Anahtar bitlerini temsil etmek içinde foton polarizasyonundan yararlanılır. Yani anahtar taşıyıcısı olarak her bir anahtar biti için tek bir foton kullanılır.

KAD Protokolleri

Yukarıda anlatılan ilkelere dayanan basit bir KAD protokolü Şekil 1 te görülmektedir.

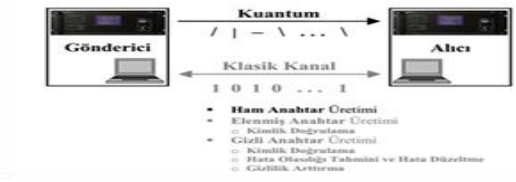


Şekil 1. Basit anlamda bir KAD protokolü

Bugüne kadar kuantum kriptografi için bir çok anahtar dağıtım protokolü önerilmiş olup bunlar şu şekildedir:

- *BB84 Protokolü*

Bahsedilen bu ilkelere dayanan ve şuan kullanılan, hem kuantum hem de klasik kısımdan meydana gelen, Charles Bennelt ve Gilles Brassard tarafından ilk defa 1984 yılında önerilen, BB84 protokolü Şekil 2 de görülmektedir.



Şekil 2. BB84 protokolü

-Kuantum Kısım: Aday anahtar bitlerinin ayrı ayrı foton tanecikleriyle transferinden meydana gelir.

1. Gönderici, ham anahtar bitlerini KRSÜ kullanarak rastgele oluşturur. Her bir biti, bir fotonun polarizasyonu ile ifade edilmiş fotonları, iletişimin tek yönlü olduğu, dış ortam ile etkileşimden yeterince izole edilmiş olan kuantum kanal üzerinden rastgele tabanda teker teker alıcıya gönderir.

2. Alıcı, gelen her bir fotonu rastgele seçilen bir tabanda ölçer. Eğer göndericinin seçimi ile seçilen taban aynı ise, ölçümsonucu da göndericinin biti ile aynı olacaktır. Farklı bir taban seçilmişse, ölçüm sonucu %50 ihtimalle doğruolacaktır. Ancak bu bilinmemektedir. Aynı durum istenmeyen kişi için de geçerlidir.

-Klasik Kısım: Alıcının ölçüm sonuçlarının değerlendirilmesinden oluşur.

3. Alıcı, bütünüyle iletim ve ölçümler tamamlandıktan sonra, klasik bir kanal yardımıyla yalnızca gelen fotonları hangi tabanlarda ölçtüğünü, açıklar. Gönderici, aynı tabanı kullandıkları indeksleri alıcıya açıklar. İdeal olarak bu indekslerdeki bitlerde aynı olmalıdır.

4. Bitlerin bit alt kümesi, aradaki 3. kişinin varlığının tespiti için açıklanır. Aynı tabanların kullanıldığı bitlerde aynı olmalıdır. Aksi durumda, ilgili fotonlara müdahale var demektir. Bu durumda protokolün iptali gerekir. Dış etkenlerden dolayı %15 lik bir hataya kadar protokolün devamına izin verilebilir.

5. Kalan ortak bitler her şey güvenli ise gizli anahtar olarak kabul edilir.

- *B92 Protokolü*

BB84'ün mucitlerinden Charles Bennett tarafından önerilen bu protokol her kubiti 0º veya 45º polarizasyonla ifade eder. B92 protokolünde 0 kubit,0º polarizasyona sahip fotonlar,1 kubit ise 45º polarizasyona sahip fotonlar anlamındadır.

Alıcı gönderilen fotonları okumak için BB8protokolündeki gibi düz ve köşegen filtreler kullanır. Ancak 0º veya 45º olarak okunan polarizasyonlu fotonları eler ve bunları anahtara dahil etmez. Polarizasyonları 90º ve 135º olanları anahtar olarak alır.

- *E91 Protokolü*

1. Gönderici aşağıda belirtilen durumda N spin çifti hazırlar;

$$|\psi>=\frac{1}{\sqrt{2}}(|\uparrow\downarrow>-|\downarrow\uparrow>)=\frac{1}{\sqrt{2}}(|01>-|10>)$$

2. Ardından her bir çiftin 2. Spinini herkese açık bir kuantum kanaldan gönderir.

3. Sonra herkese açık bir kanalda yaptıkları ölçüm yönlerini açıklarlar.

4. Eğer spinin aynı yöndeki bileşenini ölçmüşlerse göndericinin sonucu alıcının sonucunun eksi işaretlisidir.

2. ve 3. çift gibi değişik yönlerde ölçümler almışlar ise bunu anahtarda kullanmazlar.

- SARG04 Protokolü

Kuantum kriptografinin ticari uygulamalarında kullanılan bu protokol 2004 yılında önerilmiştir. Bu protokol, BB84 türü protokoller için, ileri yıllarda kullanılacağı tahmin edilen teknolojilerin ne büyüklükte bir risk oluşturacağını ispatlamaktadır.

- EPR- EKERT Protokolü

BB84 de kullanılan Heisenberg belirsizlik ilkesinin kullanılmadığıdığı bir protokoldür. Burada kuantum halleri birbirine birleşik iki foton kullanımak suretiyle, tarafların her birine birer foton gelir. Kuantum halleri bir birine zıt olan bu fotonlardan kuantum haller tahmin edilerek, ortak bir kod anahtarı elde edilebilir [6-15].

III. KUANTUM KRİTANALİZ

Bazı kuantum mekaniksel sistemlerden, bir takım kuantum mekaniksel etkilerden yararlanarak yani kısacası kuantum bilgisayarlar kullanarak şifre kırmayla ilgilenen kriptografik bir uygulama alanıdır. Kuantum kriptanalize en meşhur örnek bir matematikçi olan Peter Shor tarafından 1994 yılında önerilen, çarpanlara ayırma problemini çözmenin verimli bir yolunu ortaya koyan, shor algoritmasıdır. Shor algoritması bazı simetrik şifreleme algoritmalarını, bir kuantum bilgisayar yardımıyla çok büyük tam sayıları kolaylıkla çarpanlarına ayırarak, kıracaktır.

Bir başka örnek ise, bir bilgisayar bilimcisi olan Lov Grover tarafından önerilen, kuantum bilgisayar yardımıyla, kaba kuvvet saldırısı marifetiyle anahtar aramalarının karesel olarak daha hızlı yapılabileceğini belirten Grover algoritmasıdır.

Kuantum özel kanallar, kuantum simetrik şifreleme, kuantum hesaplama gibi kuantum kriptanalizde kapsamlı bir kuantum bilgisayarın yapılmasını beklemektedir. Donanımcıların kuantum bilgisayarları hayata geçirmek için çalışmalarıyla birlikte bu bilgisayarlarda kullanılabilecek algoritmaları geliştirmek için bilgisayar bilimciler ve matematikçiler de harekete geçmişlerdir. Ancak uzun yıllardır kuantum mekaniğinin kullanıldığı, bilginin kübitlerde saklandığı bu ortamda, kuantum bitlerin süperpozisyon özelliğini kullanarak işlem yapan çok az sayıda kuantum algoritması geliştirebilmişlerdir. Deutsch, Shor ve Grover algoritmaları bunların içerisinde en çok bilinenleridir.

- **Deutsch Algoritması**

Bu algoritma bilim tarihinde bilinen ilk kuantum algoritmasıdır. Deutsch algoritması, yalnızca tek bir kubit üzerinde işlem yapabilme özelliği sayesinde bugün klasik algoritmaların yetersiz kaldığı yerde kuantum algoritmalarının harikulade bir işlem hızı sayesinde sonuca ulaşabilmesi yönüyle oldukça önemli bir yer işgal etmektedir. Daha sonraki yıllarda geliştirilen Shor ve Grover algoritmalarının ilham kaynağıda yine Deutsch algoritması olmuştur.

- **Shor Algoritması**

Bugün için yalnızca bilimsel amaçlı deneyler yapmak amacıyla geliştirilen kuantum bilgisayarların laboratuvar ortamında test edilmesinde özellikle iki kuantum algoritması öne çıkmaktadır ki bunlar Shor algoritması ve Grover algoritmasıdır. Kuantum bilgisayarlarda çok büyük sayıları kolaylıkla çarpanlarına ayırabilme özelliğine sahip Shor algoritması, belirli bir olasılık dâhilinde periyot bulma özelliğiyle kriptoloji alanında oldukça ehemmiyetli bir yere sahiptir. Mevcut şifreleme sistemleri, çok büyük sayıların klasik bilgisayarlar tarafından makul zaman da çarpanlarına ayrılamayacağı varsayımına dayanır. Ancak laboratuvar ortamları için geliştirilmiş ve çok az sayıda kubite sahip kuantum bilgisayarların çok büyük sayıları olağan üstü hızla çarpanlarına ayırabilmesi, kriptoloji biliminin temellerini derinden etkileyerek kuantum kriptoloji adı ile yeni bir bilim dalının ortaya çıkmasına vesile olmuştur. Shor Algoritması klasik ve kuantum olmak üzere iki kısımdan oluşur;

-Klasik Kısım

Çarpanlara ayırma problemi bir mertebe/ periyot bulma problemine indirgenir. N'in asal çarpanlarının bulunması ile ilgili algoritma aşağıdaki gibidir;

1. Rastgele bir $\propto< N$ sayısı üretir.
2. $OBEB(\propto, N)'i$hesaplar. $Eğer\ OBEB(\propto, N) \neq 1\ ise\ \propto, N$ 'in bir asal çarpanıdır, işlem tamam.
3. $N^2 \leq Q = 2^m \leq 2N^2$ olan bir Q belirler ve $f(x) = \propto^x \ mod\ N$ fonksiyonunun r periyodunun bulunması için kuantum kısma geçer.
4. Eğer r tek ise 1. adıma döner.
5. Eğer $\propto^{\frac{r}{2}} \equiv -1\ (mod\ N)$ise 1. adıma döner.
6. $OBEB\left(\propto^{\frac{r}{2}} \pm 1, N\right) = N$ 'in asal çarpanı ise işlem tamam.

-Kuantum Kısım

Periyot bulma problemini çözmek için bir kuantum algoritma içeren kuantum mekaniğini kullanılarak mertebe/periyot bulma işlemi gerçekleştirilir.

1. Saklayıcılar ilklendirilir;

   $Q^{-\frac{1}{2}} \sum_{x=0}^{Q-1} |x, 0>$, m qubitlik giriş, $m/2$ qubitlik çıkış.
2. f(x), kuantum bir fonksiyon olarak gerçeklenip yukarıdaki kuantum duruma uygulanır.

   $Q^{-\frac{1}{2}} \sum_x |x, f(x)>$. Tüm olası $Q = 2^m$durumun bir süperpozisyonudur. Dolayısıyla tüm olası girişler ve çıkışlar saklayıcılardadır.
3. İkinci yarıda ölçüm yapılır;

   $\frac{1}{c} \sum_{0 \leq x \leq 2^m} |x, u>$. Burada c, toplamdaki terimlerin sayısının kareköküdür. Yani vektör uzunluğunu 1 yapmak için gereken faktördür.

Bu ölçüm, bir u (mod N) sayısı verir ve tüm sistemi $|x, u>$ şeklindeki durumların bir lineer kombinasyonuna zorlar ki; tüm $a^x \equiv u\ (mod\ N)$durumları elde edilir.

4. Giriş saklayıcısına kuantum fourier dönüşümü uygulanır;

   $U_{QFT} \left|x>= Q^{-\frac{1}{2}} \sum_y W^{xy} |y\ >\right.$, burada

   $W = e^{\frac{2\pi}{Q}}, 0 \leq y < Q.$

Kuantum fourier dönüşümü periyodu bulmak için gerekli olan frekansları ölçer. Eğer r 2^m in bir böleni ise elde edilen frekanslar f_0 temel frekansının katlarıdır ve $rf_0 = 2^m$ olur. Ancak genelde r, 2^min böleni değildir. Bu durumda ise; bazı baskın frekanslar olacaktır ve bunlar bir $f_0$temel frekansının yaklaşık katları olur. Yani $rf_0 \approx 2^m$dir. Kuantum fourier dönüşümü sonucu olan kuantum durum üzerinde ölçüm yapılır ve bir $f = j.f_0$ frekansı belirlenir.

5. r 'yi elde etmek için $frekans = \frac{Uzunluk}{Periyot}$ tanımı kullanılarak dizinin kaç defa tekrar ettiğini hesaplayan $\frac{j.f_0}{r.f_0} \approx \frac{f}{2^m} \Rightarrow \frac{j}{r} \approx \frac{f}{2^m}$ ilişkisi üzerinde sürekli bölme açılımı uygulanır. Çünkü

uzunluğu belli olan bir dizinin frekansı bulunursa periyodu da bulunur.

Euler'in $\emptyset$ fonksiyonu, p, q asal ve $N = p.q$ olmak üzere; $\emptyset(N) = (p-1)(q-1)$ alınarak $r \leq \emptyset(N) < N$ eşitsizliğinden r periyodu bulunur. Genel olarak, yukarıdaki bölme açılımından N'den küçük en son payda aranılan r periyodudur.

6. $a^r \equiv 1 (\text{mod N})$ ise işlem tamamlanır.

7. $a^r \not\equiv 1 \ (\text{mod N})$ ise 1.adıma geri dönülür.

Bu algoritmanın kuantum kısmı için her bir N ve a ya bağlı olan özel olarak kuantum devreler tasarlanır. Yöntem bazen düzgün çalışmayabilir, bu durumda algoritma yeniden tasarlanır ve baştan çalıştırılır.

- **Grover Algoritması**

Oldukça büyük veri tabanlarında taranan bilginin çok detaylı olarak formüle edilmesine ihtiyaç duymadan hızlı bir şekilde bulunmasını sağlayan Grover algoritması (GSA) da diğer kuantum algoritmalarının birçoğunda ki gibi olasılık teorisine dayalı işleyen bir algoritmadır. Bu nedenle doğru cevabı bulabilmesi için veriler üzerinde çoğu zaman sadece bir kez değil, birden fazla çalıştırılması gerekmektedir. Bu algoritma doğru olma olasılığı en yüksek olan cevabı aynı verileri birden fazla işleyerek bulur.

1. İlklendirme: Walsh-Hadamard dönüşümü uygulanarak aşağıdaki süperpozisyon elde edilir;

$$\left|\delta\right> = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x>.$$

2. Yeneleme: Aşağıdaki tüm işlemler M defa tekar edilir;

a) Mevcut süperpozisyondaki her bir $|x>$ durumu için

F(x) =1 ise faz π radyanlık döndürülür, aksi takdirde sistem değişmemiştir durdurulur.

b) Walsh-Hadamard dönüşümü ve Faz rotasyon matrisinden oluşan

$$D_{ij} = \begin{cases} \frac{2}{N}, & i \neq j \\ -1 + \frac{2}{N}, & i = j \end{cases}$$

difizyon dönüşümü uygulanır.

3. Ölçüm: Ortaya çıkan süperpozisyon ölçülür ve genliklerin belirlediği olasılıklara göre bir durum elde edilir [15-19].

VI. SONUÇ

Kriptograflarla kriptanalistler arasında yıllardır süregelen mücadele yeni yüzyılda kuantum alanında da devam edecektir. Zira gizli anahtar üretiminde kullanılan KRSÜ ve kuantum kriptografi şimdilik anahtar dağıtımı için kullanılmaktadır. Hatta birer ticari ürün olarak piyasaya sürülmüş durumdadır. Günümüzde kuantum teknolojiyle güvenli olarak mesaj 150 km den daha fazla mesafelere gönderilmesi başarılmış durumdadır. Bununla beraber IBM piyasaya sürülebilir 50-kubit kuantum bilgisayarı, ABD'den bir ekip 51-kubitlik kuantum simülatörü ve kanadali D-wave şirketi 2000-kubitlik bilgisayarı ilan ederken Google sadece 6-kubit kullanan dünyanın en hızlı quantum çipini geliştirdiğini duyurdu. Ayrıca Madrid Teknik üniversitesi araştırmacıları faktörizasyon problemi dediğimiz çarpanlarına ayırma problemi için faktörizasyonda kullanılan aritmetiği taklit eden bir kuantum simülatörü teorik olarak kurguladılar [20,21]. Tüm bu gelişmeler açıkça ortaya koymuştur ki**; Temel bilimler de ve Matematikte kim öndeyse gelecek onundur.**

Günümüzde milli güvenliğimiz açısından en önemli hususların başında milli bilgi güvenliği gelmektedir. Bu nedenle milli güvenliğimizin en önemli güvencesi de dışa bağımlılıktan kurtulmaktır. Son yıllarda yaşanan bilimsel ve teknolojik ilerlemeleri takip etmek, yakalamak ve önüne geçmek adına en kısa zamanda KRSÜ, kuantum kriptografi, kuantum kriptanaliz, kuantum bilgisayar, kuantum haberleşme gibi teknolojiler üzerinde yoğunlaşıp çalışmalara başlamalı ve bu alanda milli kuantum teknolojileri seferberliği başlatılmalıdır.

KAYNAKLAR

[1] M. Toyran, Bilgi Güvenliğinde Kuantum Teknikler, Iv. Ağ Ve Bilgi Güvenliği Ulusal Sempozyumu, Ankara, 2011.

[2] U. K Boyacı,. Günümüzde Kriptoloji, UEKAE Dergisi, Sayı 1, Ankara, 2013, s 32-41.

[3] T. Dereli, İletişimde mutlak güvenlik için kuantum kriptografi, Bilim Teknik, Ankara, Sayı 500, s 54-57, Temmuz 2009.

[4] Z. Gedik, Kuantum Bilgisayarları, Bilim Teknik, Ankara, Sayı 500, s 57-58, Temmuz 2009.

[5] Ş. Kalem, Kuantum Bilgi Güvenliğine Doğru, UEKAE Dergisi, Sayı 1, Ankara, 2013, s 42-47.

[6] C. H. Bennet, G.Brassard, Quantum Cryptography: Public Key Distribution and Coin Tossing, Theoretical Computer Science, vol. 560, 2014, pp. 7–11.

[7] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum Cryptography, Reviews of Modern Physics,2002, pp. 1-57.

[8] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, M. Peev, The Security of Practical Quantum Key Distribution, Reviews of Modern Physics, 2009, pp. 1301-1351.

[9] C. Elliott, Quantum cryptography, Security & Privacy Magazine, IEEE, USA, Vol. 2, Issue: 4, pp. 57–61, July-Aug. 2004.

[10] J. Mullins, Making unbreakable code, Spectrum, IEEE, USA,Vol. 39, Issue: 5, pp. 40–45, May.2002.

[11] M. A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000, pp. 28-36.

[12] C. P. Williams, S. H. Clearwater, Explorations in QUANTUM COMPUTING, Springer-Verlag NewYork, Inc. TELOS,1998.

[13] W. Trappe, L. C. Washington, Introduction to Cryptography with Coding Theory, Prentice-Hall, Inc. 2002, pp. 450-466.

[14] M. Toyran, EEB Mühendisliklerinde Kuantum Hesaplama Eğitimi, 3. EEB Mühendislikleri Eğitimi Sempozyumu, İstanbul 2006.

[15] E. Gümüş, Kuantum Kriptografi ve Anahtar Dağıtım Protokolleri, Akademik Bilişim Konferansı Bildirileri, 2-4 Şubat Malatya 2011

[16] X. Bonnetain, M. Plasencia, Hidden Shift Quantum Cryptanalysis and Implications, 24th International Conference on the Theory and Application of Cryptology and Information Security, Australia, December 2–6, 2018.

[17] B. Ege, Kuantum Mekaniğinden Kuantum Bilgisayarlarına, Bilim Teknik, Ankara, Sayı 541, s 12-14, Ekim 2012.

[18] A. Yamamura, H. Ishizuka, Quantum cryptanalysis of block ciphers, Research Institute for Mathematical Sciences, Kyoto University, 2000, pp. 235-243.

[19] T. Beth, J. Muller-Quade, R. Steinwandt, Cryptanalysis of a Practical Quantum Key Distribution with Polarization-Entangled Photons, Quantum Physics, 2004, pp. 3865-3871.

[20] J. Rosales, V. Martin, Quantum Simulation of the Factorization Problem, Phys. Rev. Lett. 117, 2016, pp. 200502.

[21] J. Rosales, V. Martin, Quantum simulation of the integer factorization problem: Bell states in a Penning trap, Phys. Rev. A 97, 2018, pp. 032325.

Smart City Services

Akıllı Şehir Hizmetleri

Murat DENER
Computer Sciences and Engineering
Graduate School of Natural and Applied Sciences
Gazi University
Ankara, Turkey
muratdener@gazi.edu.tr

***Öz*— Bu çalışmada akıllı şehir hizmetleri, uygulamaları tartışılmıştır. Akıllı şehirlerle ilgili güncel literatür detaylı olarak araştırılmış ve akıllı şehir kavramı ile ilgili yapılan en son çalışmalar sunulmuştur. Ayrıca, akıllı şehir uygulamaları Akıllı Ulaşım, Akıllı Yönetişim, Akıllı Ekonomi, Akıllı Çevre, Akıllı Sağlık, Akıllı Endüstri, Akıllı Güvenlik, Akıllı Yaşam olmak üzere 8 kategoriye ayrılmış ve bu kategorilere yaklaşık 300 sistem dağıtılmıştır. Bu süreçte hem deneyim hem literatür ve akıllı şehir çalışmaları göz önünde bulundurulmuştur. Çalışmanın akıllı şehirle ilgili tüm paydaşlar için yararlı olduğu düşünülmektedir.**

***Anahtar Sözcükler*— Akıllı Şehir, Akıllı Sistem, Hizmetler, Uygulamalar**

***Abstract*— In this study, smart city services, applications are discussed. The current literature on smart cities has been searched in detail and the latest studies on the concept of smart city have been given. In addition, smart city applications were divided into 8 categories as Smart Transportation, Smart Governance, Smart Economy, Smart Environment, Smart Health, Smart Industry, Smart Security, Smart Life, and nearly 300 systems were distributed to these categories. In this process, both the experience and literature and smart city studies have been taken into consideration. The study is considered to be beneficial for all stakeholders related to smart city.**

***Keywords*— Smart City, Smart System, Services, Applications**

I. INTRODUCTION

Smart cities represent a multidisciplinary field that is constantly evolving with the development of information and communication technologies. Cost, resource constraints and continuous software updates are some of the issues that affect the implementation of smart cities. It should be noted, however, that smart city is not only a technical issue, but a smart governance as a process of institutional change and acceptance of the geopolitical nature of attractive visions of socio-technical governance [1,2,3]. Smart cities generally aim to efficiently organize and manage city resources through a digital layer at the top of the old infrastructure.Proper management of this digital layer and the services deployed on it becomes more important as the tendency towards digitization continues at an increasing pace and with the participation of various actors [4].

Smart cities combine the existing infrastructure of the city with the developing IoT technologies to form a new city. People are the focus of the smart city. Therefore, the concept of Smart City appeals to many people and institutions. Together with the smart city, we can see intelligent systems in transport, energy, health, education and many other areas of our lives. Despite the rapid development of the technologies required to develop intelligent systems, the communication and security of these technologies poses new challenges in increasing complexities. In this way, the developed systems are independent from each other, the data can not be used as a common, technologies emerge as systems can not talk to each other [4,5].

In this study, a comprehensive and up-to-date literature review is made and smart city services and applications are mentioned. Applications are divided into eight categories. These; Smart Transportation, Smart Governance, Smart Economy, Smart Environment, Smart Health, Smart Industry, Smart Security, Smart Life. Firstly, in the current studies, which intelligent systems are realized are explained. Then, Smart applications were presented in a broad category. In the last section, the results of the study are given.

II. SERVICES of SMART CITIES

In recent years, smart city services in research have consisted of smart transportation, smart environment, smart energy, and smart health.

The studies related to Smart Transportation are given below.

The authors [6] have proposed a solution to improve traffic signal settings in smart cities. In the proposed solution, a two-stage optimization framework is presented. It was emphasized that while traffic should be optimized more frequently during peak hours of traffic, it should be less optimized at times when traffic is normal. In addition, it is stated that the distances are provided to the account to provide smooth transitions between successive traffic signals. In this system, a hybrid genetic algorithm is used.

The authors [7] suggest ACO and PSO algorithms to develop a new communication model in VANET applications in smart cities. In the proposed system, it is aimed to minimize the level of congestion by directing the vehicles with the appropriate route technique. In line with this goal, new clustering techniques and agent utilization processes have been utilized.

The authors [8] present a comparative analysis of smart transport systems for sustainable environments in smart cities. Advantages and disadvantages of existing transportation systems are determined and it is said that it is not only aimed at preventing congestion and pollution but also providing traffic safety and decreasing the number of traffic accidents. By promoting autonomous vehicles in the sector and promoting them in traffic, they say that sustainable transportation will be provided.

The authors [9] offer picture-based video visualization on the Google map for observation in smart cities. In the proposed solution, the traffic flows are taken from the video and visualized on the google map.

The authors [10] described the practicalities and challenges of smart transportation systems supported by the Unmanned Aerial Vehicle for the Smart City. While Unmanned Aerial Vehicles have the potential to be one of the most important components of future smart cities, various research and practice have noted some difficulties due to battery limitations.

The authors [11] offer real traffic and mobile scenario work for smart cities using a new imaging and tracking system. In four different real scenarios, two human mobility (public building and discotheque); and two were traffic monitoring systems (urban and intercity routes).The analysis was conducted to make accurate estimates. In addition, different data mining techniques have been implemented to model and verify traffic estimation methods, system reliability. With the results obtained, it is shown that many processes can be realized to solve different problems in the city.

The authors [12] have proposed a conceptual model in the form of irrigation and motorway lights using IoT for Smart Cities. The model interacts with all the modules in the various city parks, subway and highway lighting modules and is effective in efficient use of resources.

The authors [13] propose a system that discourages noisy vehicles in the smart city. This paper describes the design, implementation, and deployment of a highway noise monitoring device on a top mounting device designed to track the noise causing devices on a specified volume level.

The authors [14] have proposed smart infrastructure design for smart cities. They have introduced a new approach for the Roadside Unit used in smart transport systems. In the approach, active Roadside Units are communicating with vehicles while inactive ones are switched to sleep mode. In this way, energy saving is provided and the performance of the network is accelerated.

The studies related to Smart Environment are given below.

The authors [15] have designed smart LED street lighting systems for smart cities. The design features a centralized web server that provides weather information and real-time sensor data from each LED street lamp and provides a dynamic and flexible web interface for authorized users. Thanks to the adjustable CCT LED arrays used in the proposed system, traffic accidents can be reduced when the visibility such as fog, turbidity is low.

The authors [16] have developed a smart waste collection system. Using the ant colony algorithm, they found the most effective way to collect waste, and the data mining approach to waste container planning. They have designed an integrated waste bin to reduce the cost of collection and environmental pollution. With this system, trucks' oil costs, carbon emissions, traffic-truck erosion, noise pollution, environmental pollution and working hours have been significantly reduced.

The authors [17] suggest a smart framework for assessing the impact of air pollution on the sustainability of the city. Entropy method is used to obtain initial weights of air pollution indicators and Bayesian and neural networks are used to obtain objective weights. The proposed method was tested for evaluating the effect of air pollution on the economic development of Wuhan City in China, and the test results were successful.

The authors [18] state that the greatest challenge in smart cities is to transform not all of them, but all existing technologies, into a common unity that fulfills the anticipated goals. In order to work consistently with building blocks, the system should be decomposed and a systematic approach should be adopted. In the article, one of the building blocks of smart street lamps in a smart city is showing this approach.

The studies related to Smart Energy are given below.

The authors [19] provide the Internet-of-Things software infrastructure that provides energy management and simulation of new control policies in a region. The integration of heterogeneous IOT devices for the monitoring and management of an entire province, the sharing of building and energy network resources for visualization of both energy politics at the building and district level, as well as the simulation, evaluation of the quality of the energy model of buildings are the content of the work.

The authors [20] have developed a hierarchical decision-making strategy for smart city energy management. The proposed decision process enables the energy manager to manage the city energy system as a whole and to address different urban areas with integrated structured and transparent planning.

The authors [21] propose a new micro grid storage system in the field of smart cities. It is stated that renewable energy resources should be considered in the investments to be made for smart cities. A storage unit for the Electric Vehicle and the Unmanned Aerial Vehicle has been developed.

The studies related to Smart Health are given below.

The authors [22] propose a system for identifying elderly people's hand movements using an inexpensive Raspberry Pi to help elderly people who cannot walk or speak to communicate with caregivers when they need help.

The authors [23] suggest an automated health monitoring system for patients who complain of voice complications in smart cities.

The authors [24] suggest a face expression monitoring system for improved health care in smart cities. With this system, registered doctors and careers can constantly monitor

patients' feelings and take appropriate precautions when necessary.

The authors [25] recommend a Parkinson's disease monitoring framework for use in smart cities. In this framework, city dwellers regularly monitor their health and receive feedback on Parkinson's disease.

According to the authors [26], while the population in cities continues to increase rapidly, air pollution becomes a serious problem for public health from public health. Among all pollutants, they noted that there are direct correlations between particulate matter (PM2.5) and various serious health problems, such as lung cancer, premature death, asthma, and cardiovascular and respiratory diseases. They recommend an open framework for monitoring the participant PM2.5 in smart cities,

In addition, Citizen Participation, Disabled Citizens, Smart Houses, Smart Tourism, Smart Campus has also been done with some studies.

The authors [27] have developed a knowledge-based citizen participation platform for decision support in smart cities. A citizen participation and communication platform is being provided to make new ideas using phones, tablets or PCs.

The authors [28] suggest service architecture for smart cities using social networks platforms. If additional information is needed after the information obtained from the sensors, they may be collected from social networks.

The authors [29] have developed a Participant Perceptive system for smart cities. A transport trip quality measurement system has been developed using a system designed for smart phone detection and efficient collection and management of survey data.

The authors [30] propose a comprehensive system for monitoring urban accessibility in smart cities. In the system, it is aimed to minimize the difficulties that these people face in the city by monitoring the movement flows, routes, place and destination of the disabled citizens. The information of these people is obtained dynamically and stored in the cloud.

The authors [31] have indicated the basic requirements for smart houses that are needed within the context of Smart cities. The essential requirements are divided into seven categories, Heterogeneity, Self-configurability, Extensibility, Contextual Consciousness, Usability, Security and Privacy Protection, and Intelligence. These items are explained in detail.

The authors [32] have worked in smart cities on energy saving through smart houses. Research topics are energy consumption in Singapore dwellings, public programs and politics in energy saving, technology use in energy saving, and household awareness of energy saves in smart homes.

The authors [33] make initial analyzes of the feasibility of the IOT approach and suggest a specific architecture for sustainable tourism application. The architecture of the city of Cagliari (Italy) has been adapted for the optimization of the movement of ship-ship tourists, taking into account such factors as transportation information and turnaround times.

The authors [34] explain how both hardware and a software-based sensor platform can be deployed on a university campus. In this context, a network of different sensors was established on the university campus and environmental events were monitored.

Even though these studies have been carried out in recent years, smart city applications are very many and varied.

In Table 1, smart city applications are classified.

Table 1. Detailed Smart City Applications

Smart Transportation	**Smart Governance**
Driverless coaches	Analysis
Electronic payment systems	Determination of policies
Face reading	Distributed management
Fingerprint reading	Document tracking system
Fuel automation	Executive
Harmonized, connected automobiles	Interactive municipality
Lighting control systems	Municipal operation management center
Mobile payment systems	Online public services
Mobile speed detection system	Planning
Personalized transportation information	Scope of services
Reading cards	Smart public administration
Red light infringement detection systems	Smart management
Retina reading	Web discovery tool
Smart ticket	
Smart traffic management	**Smart Economy**
Smart park	Blockchain
Smart roads	Counterparty lending
Smart junction	Coverage growth
Smart stop	Data-based risk analysis
Smart parking	Data-based insurance
Speed warning security systems	Democratization through mass financing
Traffic light control systems	Dynamic pricing
Traffic jam	IoT data + play = changing behavior
Travel services	New digital payment systems
Vehicle tracking systems	Robotic
	Smart finance
	Smart growth
	Sustainable growth
Smart Environment	**Smart Health**
Air quality follows	Athletic care
Advanced flood warning	Artificial intelligence use
Animal farm monitoring systems	Decentralization of networks from institutions to health services
Animal tracking	E-Health
Chemical leak detection in rivers	Elderly supervision systems
Cooperation in energy markets	Fall detection
Demand response devices	Health and welfare services
Distributed production with renewable resources	Home care
Drinking water monitoring	Insurance and financing
Earthquake early detection	Locating systems for doctors in the hospital
Electric vehicle charging	Medical refrigerators
	Patient monitoring systems

Electromagnetic field levels
Energy management
Environmental access control
Explosive and hazardous gases
Fire systems
Following noise pollution
Forest fire detection
Golf fields
Green houses
Hydroponics
Integral power
Landslide and avalanche prevention
Leak inspection
Levels of marine pollution
Liquid asset
Lower consumption through play
Natural gas distribution information system
Noisy urban maps
Micro networks
Meteorology station network
Monitoring systems for agricultural activities
Organic fertilizer
Photovoltaic installations
Pollution control
Power line monitoring systems
Predictive maintenance planning
Radiation levels
River floods
Seasonal thermal energy storage
Security & urgency
Silo stock calculation
Smart animal breeding
Smart bike rental
Smart counters
Smart energy
Smart farming
Smart lighting
Smart measurement
Smart networks
Smart street lamps
Smart water management
Smart waste
Smartphone detection
Snow level monitoring
Structural health
Patient supervision
Personalization of treatments over large data
Robotics in treatment and care
Self-measurement
Strengthening of patients
Systems for monitoring various health parameters
Ultraviolet radiation
3d printing

Smart Industry

Advanced construction materials and machinery
Asset tracking System
Automotive diagnosis
Custom products
Fleet tracking
Incompatibility detection of storage
Indoor air quality
Indoor location
Integrated photovoltaics
Improved construction procedures
Item location
Material science
M2M Applications
NFC payment
Ordering to the robot
Personalized delivery
Platform
Presence of ozone
Proximity products
Robotics
Route tracking and control system
Sensor systems
Shipment quality
Smart construction
Smart industrial control
Smart logistics
Smart manufacturing
Smart product management
Smart retail
Smart shopping application
Smart urban distribution
Stock control and transition security
Supply chain control
Temperature monitoring
Virtual test room
Wireless monitoring of Swimming pool remote measurement
Tank level
Toxic gas levels
Use of excess heat
Water flow
Water leaks
Water and sewer infrastructure information system
Waste management
Weather, air pollution detection systems
Wi-fi - station

Smart Security

Cyber security
Data-based crime prevention programs
Detection of weapon sounds
Drones for risk assessment
Emergency applications
Emergency response and disaster services
Intrusion detection systems
Land exploration systems
Monitoring systems for friendly forces
Monitoring systems of enemy movements
Monitoring systems for personnel and military vehicles
Preventive armrest
Supervision systems for war zones
Systems for determining the speed and location of targets
infrastructure

Smart Life

Airbnb / uber
Automated garage entry
Building security systems
Collection management and security system
Company colleges
Control of electronic devices in homes
Crowd management
Culture and tourism movements
Disability-oriented services
Disaggregation of education
Dynamic energy consumption
Education digitalization
Energy use and matching of fullness
E-training applications
Free and reliable internet access
Health follow up
Home appliance control
Independent robot guides
Interior navigation
iBeacon way
Landscape control
Library management platform
Life-long learning
Online education
Person and object tracking systems
Personal learning and counseling
Personalization of education
Phone library
Preservation of art and goods
Renewable energy
Security
Smart buildings
Smart campus
Smart education
Smart feedback
Smart home environments systems
Smart houses
Smart reloading
Smart phone museum guide
Smart promotion

	Smart society Smart tourism and entertainment Social responsibility projects Software technologies Usage-based cleaning

III. CONCLUSIONS

Today, smart city studies are continuing rapidly. Both positive and negative situations can be experienced. For example, while developing technologies are positive, difficulties in coordination of these technologies stand out as a negative situation. In addition, not only technical procedures are sufficient to create a smart city, but a large stakeholder group needs to act jointly. This study was carried out in order to support these studies. In this study, the most recent smart city studies carried out in the world are explained and smart systems are categorized in detail. In fact, for a city to be exactly a smart city, it must contain all the systems in Table 1. In addition, these systems must be able to communicate with each other. Otherwise, cities with only very few intelligent systems and structures where these systems cannot see each other can still be described as smart cities.

REFERENCES

[1] S. C. Mukhopadhyay, T. Islam, "Innovative Technologies and Services for Smart Cities", Electronics, Vol. 8(4), and Article Number: 376, DOI: 10.3390/electronics8040376, 2019.

[2] A. Meijer, M.P.R. Bolívar, "Governing the smart city: A review of the literature on smart urban governance". International Review of Administrative Sciences, Vol 82, pp. 392–408, 2016.

[3] M. Angelidou, "Smart cities: A conjuncture of four forces", Cities, Vol. 47, pp. 95–106, 2015.

[4] F. Sivrikaya, N. Ben-Sassi, X. T. Dang, O. C. Görür, C. Kuster, "Internet of Smart City Objects: A Distributed Framework for Service Discovery and Composition" IEEE ACCESS, Vol. 7 pp. 14434-14454, DOI: 10.1109/ACCESS.2019.2893340, 2019.

[5] C. Yin, Z. Xiong, H. Chen, J.Wang, D. Cooper, and B. David, "A literature survey on smart cities", Science China Information Sciences, Vol. 58 (10), pp. 1-18, 2015.

[6] Z. Y. Li, M. Shahidehpour, S. Bahramirad, A. Khodaei, "Optimizing Traffic Signal Settings in Smart Cities", IEEE Transactions on Smart Grid, Vol. 8(5), pp. 2382-2393, 2017.

[7] Y. Hernafi, M. Ben Ahmed, M. Bouhorma, "ACO and PSO Algorithms for Developing a New Communication Model for VANET Applications in Smart Cities", Wireless Personal Communications, Vol. 96(2), pp. 2039-2075, 2017.

[8] A. Balasubramaniam, A. Paul, W. H. Hong, H. Seo, J. H. Kim, "Comparative Analysis of Intelligent Transportation Systems for Sustainable Environment in Smart Cities", Sustainability, Vol. 9(7), DOI: 10.3390/su9071120, 2017.

[9] F. Mehboob, M. Abbas, S. Rehman, S. A. Khan, R. Jiang, A. Bouridane, "Glyph-based video visualization on Google Map for surveillance in smart cities", Eurasip Journal on Image and Video Processing, DOI: 10.1186/s13640-017-0175-4, 2017.

[10] H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri, A. Tuncer, "UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges", IEEE Communications Magazine, Vol. 55(3), pp. 22-28, 2017.

[11] A. Fernandez-Ares, A. M. Mora, M. G. Arenas, P. Garcia-Sanchez, G. Romero, V. Rivas, P. A. Castillo, J. J. Merelo, "Studying real traffic and mobility scenarios for a Smart City using a new monitoring and tracking system", Future Generation Computer Systems-The International Journal of Escience, Vol. 76, pp. 163-179, 2017.

[12] V. K. Solanki, M. Venkatesan, S. Katiyar, "Conceptual Model for Smart Cities: Irrigation and Highway Lamps using IoT", International Journal of Interactive Multimedia and Artificial Intelligence, Vol. 4(3), pp. 28-33, 2017.

[13] A. Agha, R. Ranjan, W. S. Gan, "Noisy vehicle surveillance camera: A system to deter noisy vehicle in smart city", Applied Acoustics, Vol. 117, pp. 236-245, 2017.

[14] K. R. Ota, T. Kumrai, M. X. Dong, J. Kishigami, M. Y. Guo, "Smart Infrastructure Design for Smart Cities", IT Professional, Vol. 19(5), pp. 42-49, 2017.

[15] P. T. Daely, H. T. Reda, G. B. Satrya, J. W. Kim, S. Y. Shin, "Design of Smart LED Streetlight System for Smart City With Web-Based Management System", IEEE Sensors Journal, Vol. 17(18), pp. 6100-6110, 2017.

[16] Z. Oralhan, B. Oralhan, Y. Yigit, "Smart City Application: Internet of Things (IoT) Technologies eased Smart Waste Collection Using Data Mining Approach and Ant Colony Optimization", International Arab Journal of Information Technology, Vol. 14(4), pp. 423-427, 2017.

[17] Q. Y. Wang, H. N. Dai, H. Wang, "A Smart MCDM Framework to Evaluate the Impact of Air Pollution on City Sustainability: A Case Study from China", Sustainability, Vol. 9(6), DOI: 10.3390/su9060911, 2017.

[18] M. Lom, O. Pribyl, "Modeling of Smart City Building Blocks Using Multi-Agent Systems", Neural Network World, Vol. 27(4), pp. 317-331, 2017.

[19] F. G. Brundu, E. Patti, A. Osello, M. Del Giudice, N. Rapetti, A. Krylovskiy, M. Jahn, V. Verda, E. Guelpa, L. Rietto, "IoT Software Infrastructure for Energy Management and Simulation in Smart Cities", IEEE Transactions on Industrial Informatics, Vol. 13(2), pp. 832-840, 2017.

[20] R. Carli, M. Dotoli, R. Pellegrino, "A Hierarchical Decision-Making Strategy for the Energy Management of Smart Cities", IEEE Transactions on Automation Science and Engineering, Vol. 14(2), pp. 505-523, 2017.

[21] V. N. Coelho, I. M. Coelho, B. N. Coelho, G. C. de Oliveira, A. C. Barbosa, L. Pereira, A. de Freitas, H. G. Santos, L. S. Ochi, F. G. Guimaraes, "A communitarian microgrid storage planning system inside the scope of a smart city", Applied Energy, Vol. 201, pp. 371-381, 2017.

[22] T. Ganokratanaa, S. Pumrin, "Hand Gesture Recognition Algorithm for Smart Cities based on Wireless Sensor", Internatıonal Journal of Online Engineering, Vol. 13(6), pp. 58-75, 2017.

[23] Z. Ali, G. Muhammad, M. F. Alhamid, "An Automatic Health Monitoring System for Patients Suffering From Voice Complications in Smart Cities", IEEE Access, Vol. 5, pp. 3900-3908, 2017.

[24] G. Muhammad, M. Alsulaiman, S. Amin, A. Ghoneim, M. F. Alhamid, "A Facial-Expression Monitoring System for Improved Healthcare in Smart Cities", IEEE Access, Vol. 5, pp. 10871-10881, 2017.

[25] M. Alhussein, "Monitoring Parkinson's Disease in Smart Cities", IEEE Access, Vol. 5, pp. 19835-19841, 2017.

[26] L. J. Chen, Y. H. Ho, H. C. Lee, H. C. Wu, H. M. Liu, H. H. Hsieh, Y. T. Huang, S. C. C. Lung, "An Open Framework for Participatory PM2.5 Monitoring in Smart Cities", IEEE Access, Vol. 5, pp. 14441-14454, 2017.

[27] Z. Khan, J. Dambruch, J. Peters-Anders, A. Sackl, A. Strasser, P. Frohlich, S. Templer, K. Soomro, "Developing Knowledge-Based Citizen Participation Platform to Support Smart City Decision Making: The Smarticipate Case Study", Information, Vol. 8(2), DOI: 10.3390/info8020047, 2017.

[28] B. C. Chifor, I. Bica, V. V. Patriciu, "Sensing service architecture for smart cities using social network platforms", Soft Computing, Vol. 21(16), pp. 4513-4522, 2017.

[29] Z. Xiao, H. B. Lim, L. Ponnambalam, "Participatory Sensing for Smart Cities: A Case Study on Transport Trip Quality Measurement", IEEE Transactions on Industrial Informatics, Vol. 13(2), pp. 759-770, 2017.

[30] H. Mora, V. Gilart-Iglesias, R. Perez-del Hoyo, M. D. Andujar-Montoya, "A Comprehensive System for Monitoring Urban Accessibility in Smart Cities", Sensors, Vol. 17(8), DOI: 10.3390/s17081834, 2017.

[31] T. K. L. Hui, R. S. Sherratt, D. D. Sanchez, "Major requirements for building Smart Homes in Smart Cities based on Internet of Things Technologies, Future Generation Computer Systems-The International Journal of Escience, Vol. 76, pp. 358-369, 2017.

[32] A. Bhati, M. Hansen, C. M. Chan, "Energy conservation through smart homes in a smart city: A lesson for Singapore households", Energy Policy, Vol. 104, pp. 230-239, 2017.

[33] M. Nitti, V. Pilloni, D. Giusto, V. Popescu, "IoT Architecture for a Sustainable Tourism Application in a Smart City Environment", Mobile Information Systems, DOI: 10.1155/2017/9201640, 2017.

[34] S. Trilles, A. Calia, O. Belmonte, J. Torres-Sospedra, R. Montoliu, J. Huerta, "Deployment of an open sensorized platform in a smart city context", Future Generation Computer Systems-The International Journal of Escience, Vol. 76, pp. 221-233, 2017.

Windows Sistemlerinde Post Exploitation İşlemleri İçin Bir Araç Geliştirilmesi

Developing a Tool for Post Exploitation in Windows Systems

Sedat KIZILÇINAR
Bilgisayar Mühendisliği
Teknoloji Fakültesi
Gazi Üniversitesi
Ankara, Türkiye
sedat.kizilcinar@priviasecurity.com

Bünyamin CİYLAN
Bilgisayar Mühendisliği
Teknoloji Fakültesi
Gazi Üniversitesi
Ankara, Türkiye
bciylan@gazi.edu.tr

ÖZET

Günümüzde, kurum ve kuruluşlar genellikle Windows sistemlerini kullanmaktadır. Kullanılan bu sistemleri hiyerarşik bir düzen içerisinde çalışması için bir domain ortamının oluşturulması gerekmektedir. Bu domain ortamının oluşmasında Active Directory etkin rol almaktadır. Active Directory, ağ üzerindeki nesnelerin bir düzen içerisinde işleyişlerini devam edebilmelerini yönetimsel bir dizin hizmeti sağlamaktadır. Bu hizmet, Domain Controller adı verilen bir sunucu yapısı üzerinde kurulmaktadır. Bu yapı, hiyerarşik olarak en üstte bulunup, bütün yönetimsel işlemleri gerçekleştirmektedir. Domain ortamında en üst yetkileri üzerinde barındıran Domain Controller makinesinin güvenliği, domain ortamındaki herhangi bir istemci makinesinden daha önemlidir. Çünkü bir saldırganın amacı, Domain Controller makinesini ele geçirmektir. Saldırganlar girmiş oldukları domain ağ üzerinde Domain Controller makinesini ele geçirmek için birçok işlem gerçekleştirmektedir. Sonuç olarak, domain ağı üzerindeki tespit edilen güvenlik açıklarının kapatılması ve risklerin en aza indirgenmesi için önerilerde bulunulmuştur.

***Anahtar Kelimeler*—Sömürü Sonrası, Etki Alanı Yöneticisi, Windows Sistemleri, Active Directory**

ABSTRACT

Today, organizations often use Windows systems. In order for these systems to work in a hierarchical order, a domain environment must be created. Active Directory plays an active role in the formation of this domain environment. Active Directory provides an administrative directory service so that objects on the network can continue to function in an order. This service is installed on a server structure called Domain Controller. This structure is hierarchically at the top and performs all administrative operations. The security of the Domain Controller machine, which hosts the highest privileges in the domain environment, is more important than any client machine in the domain environment. Because the purpose of an attacker is to take over the Domain Controller machine. Intruders are performing a number of operations to take over the Domain Controller machine on the domain network they have entered. As a result, recommendations were made to close the identified security vulnerabilities on the domain network and to minimize the risks.

***Keywords*—Post Exploitation, Domain Controller, Windows Operation Systems, Active Directory**

I.GİRİŞ

Günümüzde gelişen teknoloji ile birlikte güvenliğin önemi artmaktadır[1]. Kurum ve kuruluşlar teknolojiyi yakından takip edip sistemleri üzerinde yeni güncellemeler yapmaktadır. Fakat sistemleri üzerinde gerekli kontrolleri yapmadıkları veya eksik güncelleme yaptıkları için sistemlerde güvenlik açıkları ortaya çıkmaktadır. Bu güvenlik açıkları ise bir saldırgan tarafından fark edildiğinde sistemler saldırıya maruz kalmaktadır. Saldırgan erişim sağladığı kritik verileri kopyalama, çalışanlarınıza ait kişisel veya finansal verilere

sahip olmak, bu verileri değiştirmek veya silmek gibi işlemleri gerçekleştirmektedir. Bu tür saldırılara karşı sistemlerin koruması için güncellemeler ve konfigürasyon işlemleri eksiksiz bir şekilde tamamlanmalıdır. Ayrıca sistemlerin güvenlik önlemleri arttırılabilmektedir.

Saldırganlar, genellikle sistemlerinizde güvenlik açıklarını tespit ettiklerinde direkt saldırmamaktadır. Öncelikle sistemleriniz hakkında bilgi sahibi olmak için bilgi toplama işlemlerini gerçekleştirmektedirler. Sistemlerin üzerindeki işletim sistemi bilgisi, sistemler üzerinde çalışan belli başlı yazılımların sürüm bilgisi, dışarıya açık bırakılan ağın portları hakkında bilgi edinmek saldırganlar için önem arz etmektedir. Genellikle bu bilgiler elde edildikten sonra saldıganlar sistemleri ele geçirmeye çalışmaktadır. Ele geçirilin sistem üzerinde zararlı script çalıştırılıp yüksek yetki elde edildikten sonra kimlik bilgilerin özet metin olarak elde edilmektedir. Bu kimlik bilgilerinin arasında kritik kimlik bilgisi elde edilmediği zaman domain ağındaki diğer sistemlere erişim sağlanılarak kritik kimlik bilgisi elde edilerek domain ağı ele geçirilir. Bu çalışma da ise modern saldırıları gerçekleştirilerek farklı teknikler ile bu bilgileri elde etmeyi, bu doğrultuda araç geliştirmeyi ve post exploitation sürecinin exploitation sürecinden daha önemli bir süreç olduğu belirtilecektir.

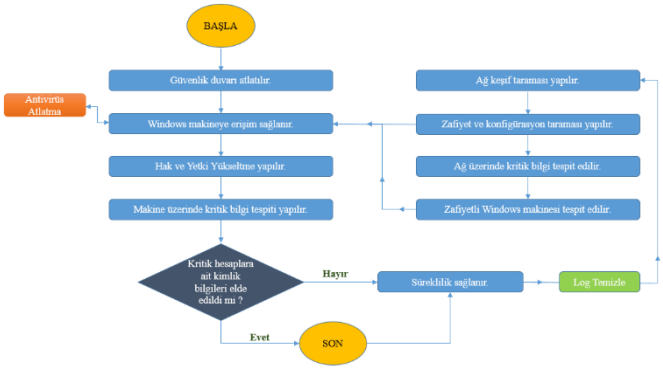
II. POST EXPLOITATION

Saldırganların, hedef domain ağı üzerindeki bir sisteme erişim sağlandıktan ve yetkiler yükseltildikten sonra başlayan sürece post exploitation denir. Yani erişim sağladıktan sonra bu erişimin kalıcı hale getirilmesi ve sürdürülmesi amaçlanmaktadır. Post exploitation sürecinde amaç domain ağını ele geçirmektedir. Domain ağı ise Active Directory denilen bir dizin hizmeti tarafından yönetilmektedir[2]. Active Directory ise ağ üzerindeki nesneler hakkındaki bilgileri depolayıp yöneticiler ve kullanıcılar için bu bilgileri bulup kullanmayı kolay hale getiren bir dizin hizmetidir[3].

Post exploitation sürecinin başarılı bir şekilde gerçekleşmesi için bazı işlemlerin gerçekleşmesi gerekmektedir. Bu işlemler ise;

- Domain Ağ Hakkında Bilgi Toplama
- Yerel Ağ Taraması Gerçekleştirme
- Kimlik Bilgilerin Elde Edilmesi
- Hak ve Yetki Yükseltme
- Uzak Makine Bağlantısı Sağlama gibi temel işlemlerdir.

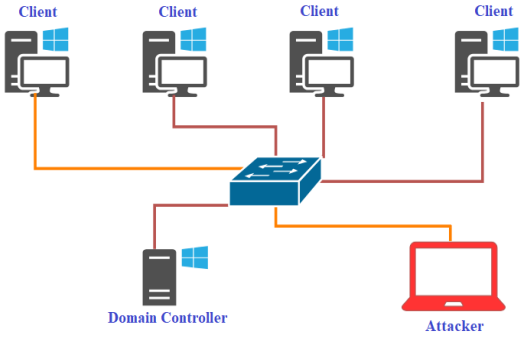
Bu işlemler gerçekleştirilerek saldırgan domain ağ üzerinde hedefe yönelik işlemleri başarılı bir şekilde gerçekleştirebilmektedir



Şekil 1: Post Exploitation İşlemlerinin Akışı

Şekil 1'de gösterilen akış diyagramı, kurum ve kuruluşlarda bulunan domain ortamını ele geçirmeye yönelik izlenilecek adımları göstermektedir. Bu adımların sırasıyla tamamlanması hedef domain ortamının başarılı bir şekilde ele geçirilmesi ile sonuçlanacaktır[4].

III. POST EXPLOITATION SENARYOSU



Şekil 2: Post Exploitation Senaryosu Örneği

Kurum ve kuruluşlarda bulunan domain ağını ele geçirmeye yönelik yapılan bir saldırı sürecidir. Bu post exploitation işlemi şekil 2 gibi gösterilen yerel ağ üzerinde gösterilmektedir[5]. Gösterildiği gibi yerel ağ üzerinde domain ortamı oluşturulmuştur. Saldırgan domain ağında bulunan bir makine üzerinden öncelikle hak ve yetkilerini yükseltmesi gerekmektedir. Çünkü saldırganın edinmek istediği kritik bilgiler yüksek hak ve yetkilere sahip kullanıcıların erişebildiği bilgidir. Yüksek hak ve yetkiler elde edildikten sonra makine üzerinde bulunan bütün kullanıcı kimlik bilgileri elde edilmektedir. Bu kullanıcı kimlik bilgileri arasında domain ağı için kritik önem taşıyan kritik bilgiler saldırganın hedeflediği amaçlardan biridir. Saldırgan domain ağı hakkında kritik öneme sahip kimlik bilgilerini ele geçirmediği zaman makine üzerinde yaptığı işlemlerin log kayıtlarını temizleyerek ağ üzerinde keşif taraması gerçekleştirmektedir. Saldırgan yapılan bu keşif taraması sonucunda güvenlik açığı veya konfigürasyon eksikliklerinden faydalanarak yerel ağ üzerinde bulunan diğer makinelere yönelik sızma girişiminde bulunmaktadır.

Geliştirilen post exploitation aracı, bu süreci kısaltmaya yönelik güncel bir modül çalıştırılması sonucunda sürecin uygulanacağı kapsam daraltılmaktadır. Böylelikle post exploitation sürecinde zamandan tasarruf elde edilmektedir. Ayrıca kullanılan modül, domain ağına yönelik kritik bilgi barındıran makineleri tespit etmektedir. Bu kritik bilgi domain admin'in kimlik bilgisidir. Saldırgan domain admin'in kimlik bilgilerinin bulunduğu makine yönelik zafiyet taraması gerçekleştirip makineyi ele geçirmektedir. Makine ele geçirildikten sonra saldırgan hak ve yetki yükseltme işlemi gerçekleştirecektir. Hak ve yetki yükseltme işleminden sonra makine üzerindeki bütün kimlik bilgileri elde edilmektedir. Bu kimlik bilgileri arasından domain admin kimlik bilgisi alınmaktadır. Böylelikle saldırgan hedefine ulaşarak, Domain Controller makinesi dahil bütün makineler erişim sağlanarak domain ortamı ele geçirilmiş olacaktır. Böylelikle saldırı başarılı bir şekilde sonuçlanmıştır.

IV. POST EXPLOITATION ARAÇLARI

Windows sistemlerine yönelik post exploitation işlemlerinin yapılması için belli başlı araçlar geliştirilmitir. Bu araçların özellik olara birbirlerinden farklılıkları bulunmaktadır. Bu araçlar ile ilgili tanımlamalar Tablo 1'de gösterilmektedir.

Tablo 1: Post Exploitation Araçları Tanımı

Aracın Adı	Açıklaması
Nishang	Powershell dilinde yazılmış script kodları bulunmaktadır. Bu kodlar ile bilgi toplama, ağ tarama, hak yükseltme, kimlik bilgilerin elde edilmesi, arka kapı oluşturma gibi özellikleri barındırmaktadır[6].
Powersploit	Powershell dilinde yazılmış scriptleri barındırmaktadır. Nishang aracındaki özellikleri, antivirüs ve firewall bypass gibi özellkleri barındırmaktadır[7].
Empire	Powershell Empire ile Python EmPyre projelerinin birleşiminden oluşur. Bir posr exploitation framework olup kriptolojik olarak güvenli iletişim ve esnek bir mimari sunamktadır[8].
P0wnedshell	Saldırgan bakış açısıyla hazırlanmış powershell scriptlerini .NET ortamı üzerinde C# programlama dili ile yazılmıştır. İçerisinde diğer post exploitation araçlarında bulunan bazı müdlleri barındırmaktadır. Ayrıca Active Directy'e yönelik modern saldırılar gerçekleştirilmektedir. Böylelikle sistemi koruyan ekip üzerrinde farkındalık yaratıp sistemi korumalarına yönelik bakış açısı kazandıran bir araçtır[9].

Tablo 1'de belirtildiği gibi post exploitation araçlarının birbirlerine olan farklılıkları ve benzerlikleri bulunmaktadır. Geliştirilen post exploitation aracındaki avantajlar ise Tablo 1'deki araçlara göre farklılıklarını gösterecektir. Geliştirilen post exploitation aracının avantajları ve dezavantajları Tablo 2'de gösterilmektedir.

Tablo 2: Geliştirilen aracın Avantajları ve Dezavantajları

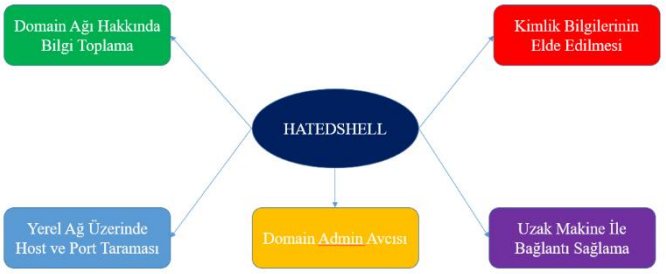
Avantajlar	Dezavantajları
Grafiksel kullanıcı arayüzü oluşturularak kullanıcı dostu bir araç olarak geliştirildi. Ayrıca konsol arayüzü de bulunmaktadır.	Sadece Windows sistemlerine yönelik geliştirilmesi
Kullanıcıya yapacağı her işlem için öncesinden işlem hakkında bilgi notu bulunmaktadır.	Hak ve yetki yükseltmek için var olan modüllerin yetersiz kalınbilmesi
Domain Admin Avcılığı özelliği eklenerek post exploitation sürecinin en kısa sürede sonuçlanmasını sağlamaktadır.	.NET framework'ü olan bağımlılığı
Diğer araçlarda ağ taramalarında tek tarama türü var iken geliştirilen araçta ARP ve ICMP olarak iki tarama türü vardır.	-
Uzak masaüstü bağlantısının sağlanması	-
Komutları kendisine özel bir komut satırı istemcisi üzerinden gerçekleştirmesi	-

Geliştirilen post exploitation aracı üzerinde diğer araçlarda bulunan bazı scriptler bulunmaktadır. Tablo 2'de gösterilen avantajları bu araç üzerinde eklenilen özellikleri ve post exploitation araçlarından farklılıklarını göstermektedir. Ayrıca dezavantajları göz ününe alındığında geleceğe yönelik aracın geliştirilmesi durumunda günceleştirilebilir. Böylelikle post exploitation sürecine yönelik bir araştırma veya makale yazımında aracı geliştirmeye yönelik çalışma yapılabilir.

V. POST EXPLOITATION ARACI GELİŞTİRME

İsim olarak hated sözcüğü nefret edilen anlamını taşımaktadır. Shell sözcüğüyle bir araya getirilerek oluşturulmuştur. Hatedshell, p0wnedshell post exploitation aracı ile entegre edilmiş grafiksel kullanıcı arayüzü olan bir post exploitation aracıdır. Powerview modüllerini kullanarak domain ağı hakkında bilgi toplama işlemeleri gerçekleştirmektedir. P0wnedshell aracından farklı olarak ağ üzerinde host ve port tespitini ARP ve ICMP paketlerini

kullanarak gerçekleştirmektedir. Bellekte bulunan kimlik bilgilerini elde etmek için kendisine özel bir çalışma uzayı oluşturup üzerinde mimkatz aracını çalıştırmaktadır. User-Hunter modülü kullanılarak Domain ağ üzerinde Domain Admin kimlik bilgilerinin bulunduğu makineler tespit edilmektedir. PsExec Tools kullanılarak kimlik bilgileri ile uzak makinelerde komut çalıştırılabilmektedir.

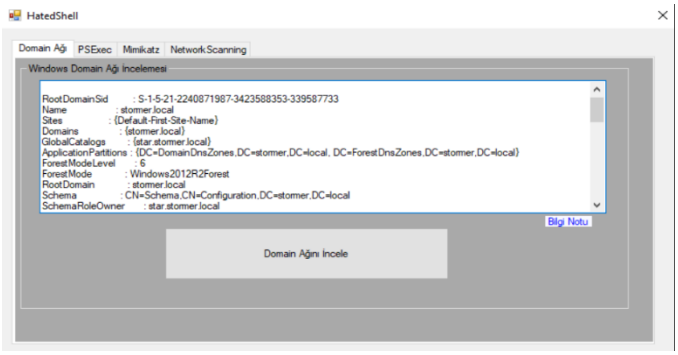


Şekil 3: Geliştirilen Post Exploitation Aracı Özellikleri

Şekil 3'te gösterilen özellikle geliştirilen aracın barındırmış olduğu özellikleri göstermektedir. Bunlardan en önemli özellik domain admin avcısı özelliği olup post exploitation sürecinin kısa sürede sonuçlanmasını sağlamaktadır. Çünkü bu özellik domain admin kimlik bilgilerini ele geçirmek amacıyla, domain admin kullanıcısının giriş yaptığı makineleri tespit etmektedir.

VI. DENEYSEL ÇALIŞMA

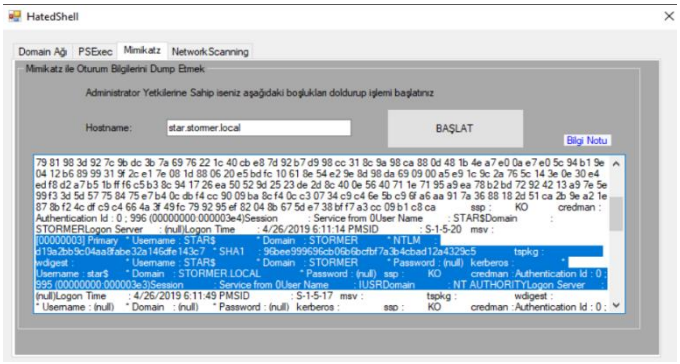
Öncelikle sızılan domain ağı üzerinde bilgi toplanması gerekmektedir. Geliştirilen araç ile domain ağının adını, RootDomainSid bilgileri vb. bilgiler elde edilmektedir. Bu işlem şekil 4'te gösterilmektedir.



Şekil 4: Domain Ağı Hakkında Bilgi Toplama

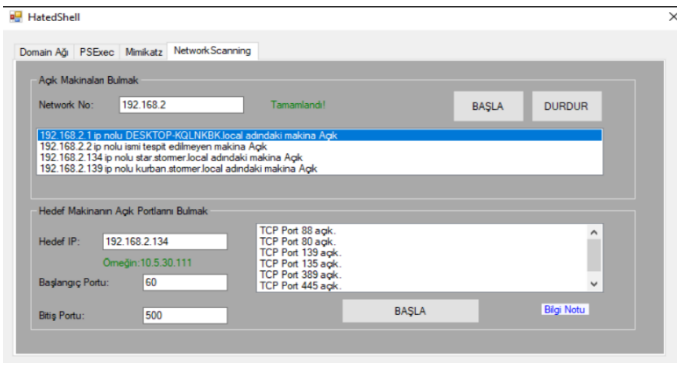
Şekil 4'te domain ağı ile ilgili kritik bilgiler elde edilmiştir. Bu bilgiler arasında RootDomainSid bilgisi ile kerberos bileti üretilmesinde kullanılmaktadır[10]. Kerberos bileti ile saldırgan sisteme tanımladığı kullanıcı ile isteğine bağlı olarak 10 yıla kadar kullanıcıyı tanımlayıp istediği zaman sisteme girebilmektedir.

Ayrıca var olan makine üzerinde kimlik bilgilerinin elde edilmesine yönelik işlemlerin gerçekleştirilmesi gerekmektedir. Elde edilen bilgiler doğrultusunda Domain ağına yönelik işlemlerin gerçekleştirilmesi için önem arz etmektedir. Elde edilen kimlik bilgiler arasında domain ağında bulunan yetkili bir kullanıcının kimlik bilgileri elde edildiğinde saldırının başarılı bir şekilde ilerlendiği anlaşılmaktadır[11]. Bu işlem Şekil 5'te gösterilmektedir.



Şekil 5: Kimlik Bilgilerinin Elde Edilmesi

Eğer elde edilmiş makine üzerindeki kimlik bilgileri arasında domain ağındaki yüksek yetkili bir kullanıcıya ait kimlik bilgileri elde edilmemiş ise, domain ağına yönelik network taraması gerçekleştirilerek domain ağı üzerinde bulunan diğer makinelerin açık portları tespit edilmektedir[12]. Bu tespit edilme işlemi şekil 6'da gösterilmektedir.



Şekil 6: Network Taramasının Gerçekleştirilmesi

Network taraması gerçekleştirildikten sonra var olan domain ağı üzerinde makine sayısı fazla olması post exploitation sürecini uzatabilmektedir. Post exploitation sürecinin kısa tutmaya yönelik geliştirilmiş aracın içerisinde bulunan domain admin avcısı özelliği bulunmaktadır. Bu özellik doğrultusunda Local Administrator yetkisinin aktif olduğu makineler tespit edilmektedir. Local Administrator yetkisinin aktif olduğu makinelerde genellikle kritik işlemler

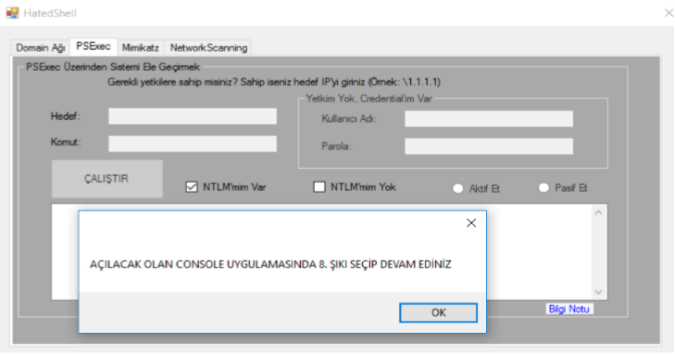
gerçekleştirildiği için Domain Admin kullanıcısının bu makinelere giriş yapabileceği düşünüldüğünde post exploitation süreci kısaltılabilmektedir. Bu işlem şekil 7'de gösterilmektedir.

```
UserDomain      : STORMER
UserName        : Administrator
ComputerName    : star.stormer.local
IPAddress       : 192.168.2.134
SessionFrom     :
SessionFromName :
LocalAdmin      : True
```

Şekil 7: Domain Admin Avcısı Özelliği

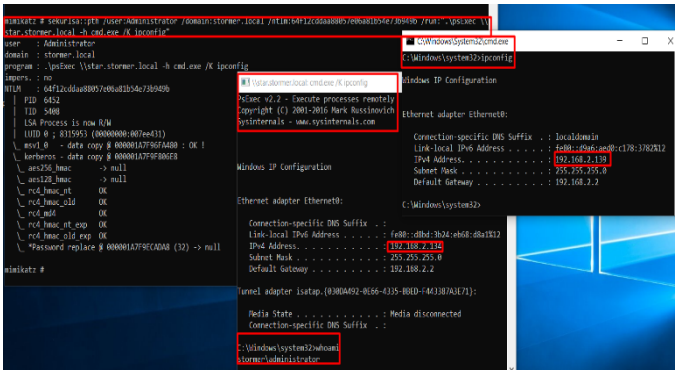
Bu işlemler doğrultusunda Domain Admin makinesinin bilgilerini ele geçirdikten sonra hedef makineyi ele geçirip makine üzerindeki kimlik bilgilerini elde ettiği durumunda Domain Admin kullanıcısının sahip olduğu kimlik bilgilerinin elde edecektir. Böylelikle Post exploitation işlemini başarılı bir şekilde sonuçlanmaktadır.

Ayrıca elde edilen kimlik bilgileri ile Domain Controller makinesine yönelik uzaktan bağlantı işlemleri gerçekleştirilebilmektedir. Geliştirilen araçta bu özellik bulunmaktadır. Böylelikle Domain Admin kimlik bilgilerinin kullanarak Domain Controller makinesini erişim sağlanmaktadır. Bu işlemler şekil 8 ve şekil 9'da gösterilmektedir.



Şekil 8: Uzak Makine bağlantısının sağlanması

Şekil 8'de saldırganın elde ettiği kimlik bilgileri doğrultusunda tasarlanan grafik arayüzü üzerinden hedef makineye bağlanmasını sağlamaktadır. Kimlik bilgileri açık metin olarak ele geçirildiğinde işe yarayan bir arayüzdür.



Şekil 9: Domain Controller Makinesinin Bağlantısı

Şekil 9'da ise elde edilen kimlik bilgileri özet metin olarak ele geçirildiği zaman grafik arayüzünden komut satırı arayüzüne yönlendirerek hedef makine ile bağlantı sağlanılmaktadır. Bu durum göz önüne alındığında şekil 9'da Domain Controller makinesine erişim sağlanıldığı görülmektedir[13,14]. Böylece post exploitation işlemi kısa sürede ve başarılı bir şekilde sonuçlanmıştır.

VII. SONUÇ

Kurum ve kuruluşlarda bilişim sistemlerinin güvenliğinin sadece dışarıya yönelik güvenlik önlemleri almanın yetersiz olduğu görülmüştür. Saldırganların güvenlik önlemlerini atlayarak domain ağ üzerindeki sistem işleyişini etkileyecek kritik saldırılar yapılabileceği sonucuna varılmıştır. Bütün sistemi ve üst düzey yetkilerin elde edilmesiyle domain ağı saldırgan kontrolüne girebilmektedir. Sistemler üzerinde kritik güvenlik açıkları tespit edilmiştir. Sistemler üzerinde gerekli güncellemeler yapılmamaktadır. Domain Admin kullanıcısının kimlik bilgileri basit parola kullanımı olduğu tespit edilmiştir. Domain Admin kullanıcı Domain Controller dışındaki makinelere kimlik bilgileri ile giriş yaptığı tespit edilmiştir. İşlemler gerçekleştirildikten sonra sistem yöneticileri tarafından bellekten kimlik bilgilerinin temizlenmediği tespit edilmiştir. Yerel ağ üzerinde makinelerin birbirleri arasındaki iletişimin sağlanması için açılan portlar dışında farklı portların açık olduğu tespit edilmiştir. Açık olan portların güvenlik açığı barındırdığı tespit edilmiştir. Ağ altyapısının yanlış yapılandığı görülmüştür. Ağ üzerinde makineler arasındaki erişim kontrolünün yetersiz olduğu tespit edilmiştir. Belirtilen bu bilgiler senaryo sırasında elde edilen bulgulardan yola çıkarak anlatılmıştır. Bulgular, ekran görüntülerinde gösterilmektedir. Kurum ve kuruluştaki çalışan güvenlik ekiplerinin geliştirilmiş olan güvenlik aracını kullanmaları önem arz etmektedir. Çünkü bu araç post exploitation sürecini kısa sürede ve diğer post exploitation araçlarının içerisindeki modülleri içerisinde barındırmanın yanında farklı tekniklerle modern saldırıları gerçekleştirmektedir. Ayrıca ekiplerin bu doğrultuda post exploitation sürecinin, exploitation sürecinden daha kritik olduğunun farkındalığının artmasını sağlayacaktır.

Kurum ve kuruluşlardaki siber güvenlik ekipleri veya bu alanda akademik olarak çalışmalarını sürdüren araştırmacılar

için de geliştirilmeye açık bir araçtır. Bu araç üzerinde windows sistemlerine yönelik teorik anlamdaki post exploitation senaryolarınızı gerçekleştirmek için yazmış olduğunuz özgün scriptleri eklenilmesi doğrultusunda çalıştırabilirsiniz. Çünkü içerisinde scriptleri çalıştırması için kendi içerisinde bir komut satırı istemcisini kullanmaktadır. Ayrıca çalışmada belirtilen dezavantajları ortadan kaldırmak için çalışmalar yapılabilecek ortamı sunmaktadır. Siber güvenlik araştırmacısı veya siber güvenlik ekipleri aracı geliştirmeye yönelik scriptler yazabilmektedir.

KAYNAKLAR

[1] Anderson, James P. Computer security technology planning study. Vol. 1. ESD-TR-73-51, 1972.

[2] Dias, John. A guide to microsoft active directory (ad) design. No. UCRL-MA-148650. Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States), 2002.

[3] Internet:https://docs.microsoft.com/tr-tr/windowsserver/identity/ad-ds/get-started/virtual-dc/active-directory-etki alanı-services-overview Son Erişim Tarihi: 12/04/2019

[4] Internet: https://www.siberportal.org/red-team/microsoft-etki alanı-environmentpenetration-tests/microsoft-etkialanı-environment-penetration-testing-methodologyon-corporate-networks/ Son Erişim Tarihi: 14/04/2019

[5] Swan, Michael Jon. "Discovery and visualization of active directory domain controllers in topological network maps." U.S. Patent No. 8,045,486. 25 Oct. 2011.

[6] Internet:https://www.priviasecurity.com/kaynaklar/makale/Nishang-ile-WindowsPost-Exploitation-Part-1 Son Erişim Tarihi: 21/05/2019

[7] Internet:https://github.com/PowerShellMafia/PowerSploit Son Erişim Tarihi: 15/05/2019

[8] Internet:https://github.com/EmpireProject/Empire Son Erişim Tarihi:15/05/2019

[9] Internet: https://github.com/Cn33liz/p0wnedShell Son Erişim Tarihi: 22/04/2019

[10] Internet:https://www.researchgate.net/publication/331435646_Attacking_the_Windows_Domain_Building_Defending_and_Attacking_Modern_Computer_Networks Son Erişim Tarihi: 03/09/2019

[11] Internet:https://www.researchgate.net/publication/265308071_Attacking_the_Windows_Kernel Son Erişim Tarihi: 03/09/2019

[12] Internet:https://www.researchgate.net/publication/335490774_PRACTICAL_APPROACH_FOR_SECURING_WINDOWS_ENVIRONMENT_ATTACK_VECTORS_AND_COUNTERMEASURES Son Erişim Tarihi: 03/09/2019

[13] Internet:https://www.researchgate.net/publication/321385119_Practical_Approach_for_Securing_Windows_Environment_Attack_Vectors_and_Countermeasures Son Erişim Tarihi: 03/09/2019

Internet:https://www.researchgate.net/publication/330054994_Bypassing_Windows_Defender_Detect_Flaws_in_Your_Systems_Using_Ethical_Attacks Son Erişim Tarihi: 03/09/2019

Kimlik Tabanlı Kimlik Doğrulamalı Anahtar Anlaşma Protokolleri Üzerine Bir Çalışma

A Study on ID-Based Authenticated Key Agreement Protocols

1st Gülnihal Öztürk
Kriptografi Bölümü
ODTÜ Uygulamalı Matematik Enstitüsü
FAME CRYPT
Ankara, Türkiye
e185513@metu.edu.tr

2nd Dr. Öğretim Üyesi Ayşe Nurdan Saran
Bilgisayar Mühendisliği
Çankaya Üniversitesi
Ankara, Türkiye
buz@cankaya.edu.tr

***Öz*—Anahtar anlaşma protokolleri (AAP) kullanıcılar arasında ortak anahtar oluşturur. Açık anahtar tabanlı AAP son zamanlarda eski protokollerdeki eksiklikleri giderici küçük değişiklikler ile tasarlanmıştır. Bu değişiklikler kimlik tabanlı, kimlik doğrulamalı, eşleştirme tabanlı ve bunların kombinasyonları gibi protokol çeşitlerini ortaya çıkarmıştır. Bu çalışmada, kimlik doğrulama yöntemlerinden eşleştirme ve eliptik eğrilere dayalı kimlik tabanlı üç protokol karşıştırılmıştır: Shim-Yuan-Li [1], Tseng 2015 [2] ve Tseng 2017 [3]. Sonucunda bilinen anahtar, ileriye dönük gizlilik, anahtar-uzlaşma kimliğe bürünme esnekliği ve bilinmeyen anahtar paylaşım gibi güvenlik özelliklerini sağladığı kanısına vardık. Tseng 2017 [3] aralarında en yüksek verime sahip olan protokoldür.**

***Anahtar Sözcükler*—anahtar anlaşma, kimlik tabanlı, kimlik doğrulamalı, eşleştirme .**

***Abstract*—Key agreement protocols (KAP) construct a shared key between the participants.Public key-based KAP, recently, are designed by fixing the security flaws of the previous works with minor changes. These changes branch out protocol types like ID-based, authenticated, pairing based or combinations of them. In our study, we compare Shim-Yuan-Li [1], Tseng 2015 [2] and Tseng 2017 [3] which are the ID-based authenticated key agreement protocols based on pairing and elliptic curve. We conclude that they provide known-key, forward secrecy, key-compromise impersonation and unknown key-share security properties. Tseng 2017 [3] is the most efficient one among the mentioned protocols.**

***Keywords*—key agreement, ID-based, pairing, authenticated .**

I. Introduction

Key agreement is an important cryptographic protocol to establish a common session key over an open channel by two or more participants. Therefore, it is the corner stone of confidential communications. The key agreement protocols are mostly public key-based. The most known one was proposed by Diffie-Hellman [4]. It is constructed by using the discrete logarithm problem. Then, another idea was arised in the public key-based key agreement protocols: ID-based key agreement protocol based on pairing. It is aimed to simplify the storage and management of the key in the protocols. The first ID-based authenticated key agreement protocol (ID-AKA) based on pairing was proposed by Smart [5]. However, Shim [6] proved that this protocol does not provide the security of previous session keys and proposed another protocol for ID-AKA based on pairing, but his protocol is vulnerable to man-in-the-middle attack. Yuan and Li [1] found a solution for Shim's problem, and proposed a new ID-AKA based on pairing by modifying the Shim's protocol.Tseng 2017 [3] and Tseng 2015 [2] proposed ID-AKA elliptic curve based and pairing-based respectively for mobile user's. In this study, we compare three recent papers based on Shim's ID-AKA; Shim-Yuan-Li's protocol (SYL) [1], Tseng 2017 protocol (THY) [3] and Tseng 2015 protocol (THTT) [2]. First, we give the reviews of the protocols, and then analyze the security and efficiency according to their performance test results.

II. Preliminaries

A. Notations

We explain the protocols with similar terminology by using same notations in this paper. The notations are given below for simplicity.

G_1 is additive cyclic group with prime order p, G_2 is multiplicative cyclic group with prime order p, e is a bilinear map from $G_1 \times G_1$ to G_2, P is generator of additive group G_1, s is master key of system $s \in \mathbb{Z}_p^*$, P_{pub} is public key of system, S_{ID} is private key of the user with identity ID, H_1, H_2, H_3, H_4 are hash functions from $\{0,1\}^*$ to G_1, f_1, f_2, f_3, f_4 are hash functions from $\{0,1\}^*$ to $\{0,1\}^n$ where n is a fixed length and $2^n < p$, H is key derivation function, ID is identity of any participant, A is identity of Alice and B is identity of Bob. In the (THY) and (THTT) protocols, Alice and Bob represents client and server respectively.

B. Security Assumptions

The protocols that we compare are based on Computational Diffie-Hellman problem and Bilinear Diffie-Hellman Problem which cannot be solved with polynomial-time algorithms using classical computers. They can indeed be solved with polynomial-time quantum computer algorithm in the future.

C. Security Requirements

We determine below-mentioned properties to analyze the protocols.

Known-Key Security : In each round, Alice and Bob should generate a unique key which is independent from the other rounds, and it should not be exposed if other secret keys are compromised.

Forward Secrecy : If an adversary gets the secret keys of Alice and Bob, he should not recover session keys used in the past.

Key-Compromise Impersonation : If an adversary knows Alice's secret key, he should not impersonate others to Alice.

Unknown Key-Share : After protocol, Alice makes sure that she shared the key only with Bob. Besides, Bob is certain about sharing the key only with Alice.

III. Review of Protocols

In this section, we give the work-flows of protocols:
Setup: The Key Generation Center (KGC) selects G_1, G_2,bilinear map e, generator P, H_1, H_2, f_1, f_2, f_3, f_4, master key of system $s \in \mathbb{Z}_p^*$ and H .

In the SYL protocol, KGC computes public key of the system $P_{pub} = sP$ and publishes $< G_1, G_2, e, P, P_{pub}, H_1, H >$.

In the THY protocol, KGC computes public key of the system $P_{pub} = sP$ and publishes $< G_1, P, P_{pub}, f_1, f_2, f_3, f_4 >$.

In the TSTT protocol, KGC computes public key of the system $P_{pub} = sP$ and publishes $< G_1, G_2, e, P, P_{pub}, H_1, H_2, f_1, f_2, f_3, f_4 >$.

A. Shim, Yuan and Li's Protocol (SYL) [1]

Key Extract For a user with identity ID the public key is computed as $Q_{ID} = H_1(ID)$ and the private key is generated as $S_{ID} = sQ_{ID}$ by the KGC.

Authenticated Key Agreement

1) Alice chooses a random number $a \in \mathbb{Z}_p^*$, computes $T_A = aP$ and sends T_A to Bob.
2) Bob chooses a random number $b \in \mathbb{Z}_p^*$, computes $T_B = bP$ and sends T_B to Alice.
3) After taking T_B, Alice computes $sk_A = aT_B$ and the shared secret $K_{AB} = e(aP_{pub} + S_B, T_B + Q_B)$.
4) Similarly, after taking T_A, Bob computes $sk_B = aT_A$ and the shared secret $K_{BA} = e(T_A + Q_A, bP_{pub} + S_B)$.
5) Then they have the same shared secret, $K_{AB} = K_{BA}$ where $K_{AB} = e(P,P)^{abs} e(P,Q_B)^{as} e(Q_A,P)^{bs} e(Q_A,Q_B)^{s}$ and compute the session key as $H(A, B, sk_A, K_{AB})$ and $H(A, B, sk_B, K_{BA})$.

B. Tseng, Huang and You's Protocol (THY) [3]

Key Extract For a user with identity ID the KGC chooses a random number $l \in \mathbb{Z}_p^*$ and computes $Q_{ID} = lP$, $h_{ID} = f_1(ID, Q_{ID})$, $R_{ID} = l + h_{ID}s$ and gives to a user the private key pair as $S_{ID} = (R_{ID}, Q_{ID})$. The user receiving the private key pair can validate it by checking if the equality $R_{ID}P = Q_{ID} + h_{ID}P_{pub}$ holds or not.

Authenticated Key Agreement

1) Alice chooses a random number $a \in \mathbb{Z}_p^*$, computes $T_A = aP$ and sends A, Q_A, T_A to Bob.
2) After taking A, Q_A, T_A, Bob chooses a random number $b \in \mathbb{Z}_p^*$, computes $T_B = bP$, $h_A = f_1(A, Q_A)$, $sk_B = (b + R_B)(T_A + Q_A + h_A P_{pub}) \oplus bT_A$, $Auth_B = f_2(A, B, T_A, T_B, sk_B)$ and sends $Q_B, T_B, Auth_B$ to Alice.
3) After taking $Q_B, T_B, Auth_B$, Alice computes $sk_A = (a + R_A)(T_B + Q_B + h_B P_{pub}) \oplus aT_B$. Then she checks if $Auth_B = f_2(A, B, T_A, T_B, sk_A)$ holds or not. If the equality holds, Bob is authenticated. Alice computes $Auth_A = f_3(A, B, T_A, T_B, sk_A, Auth_B)$ and sends $Auth_A$ to Bob.
4) After taking $Auth_A$, Bob checks if $Auth_A = f_3(A, B, T_A, T_B, sk_B, Auth_B)$, holds or not. If the equality holds, Alice is authenticated.
5) Then they both compute the session key as $f_4(A, B, T_A, T_B, sk_A, Auth_B, Auth_A)$ and $f_4(A, B, T_A, T_B, sk_B, Auth_B, Auth_A)$.

C. Tseng, Huang, Tsai and Tseng's Protocol (THTT) [2]

Key Extract For a user with identity ID the KGC chooses a random number $l \in \mathbb{Z}_p^*$. Then KGC computes $Q_{ID,1} = lP$, $h_{ID} = f_1(ID, Q_{ID,1})$, $R_{ID,1} = l + h_{ID}s$, $Q_{ID,2} = H_1(ID)$, $R_{ID,2} = sQ_{ID,2}$ and gives to user the private key tuple as $S_{ID} = (R_{ID,1}, R_{ID,2}, Q_{ID,1})$.

Authenticated Key Agreement

1) Alice chooses a random number $a \in \mathbb{Z}_p^*$, make offline computations $T_{A,1} = aP$, $T_{A,2} = aQ_{A,2}$, $W = H_2(T_{A,1}, T_{A,2})$ $V = (a + R_{A,1})W + R_{A,2}$. Then she sends $A, Q_{A,2}, T_{A,1}, T_{A,2}, V$ to Bob.
2) After taking $A, Q_{A,2}, T_{A,1}, T_{A,2}, V$, Bob computes $W = H_2(T_{A,1}, T_{A,2}), h_A = f_1(A, Q_{A,1})$ and $Q_{A,2} = H_1(A)$. Then he checks if $e(P,V) = e(T_{A,1} + Q_{A,1}, W)e(P_{pub}, h_A W + Q_{A,2})$ holds or not. If the equality holds, Bob accepts to communicate with Alice. Then, Bob chooses a nonce N, computes $sk_B = sT_{A,2}$, $Auth_B = f_2(A, T_{A,1}, T_{A,2}, V, N, sk_B)$ and sends $N, Auth_B$ to Alice.
3) After taking $N, Auth_B$, Alice computes $sk_A = aR_{A,2}$ Then she checks if $Auth_B = f_2(A, T_{A,1}, T_{A,2}, V, N, sk_A)$ holds or not. If the equality holds, Alice accepts Bob. Alice continues by computing $Auth_A = f_3(A, T_{A,1}, T_{A,2}, V, N, sk_A, Auth_B)$ and sends $Auth_A$ to Bob.
4) After taking $Auth_A$, Bob checks if $Auth_A = f_3(A, T_{A,1}, T_{A,2}, V, N, sk_B, Auth_B)$ holds or not. If the equality holds, Bob accepts Alice.
5) Then they both compute the session key as $f_4(A, T_{A,1}, T_{A,2}, V, N, sk_A, Auth_B, Auth_A)$ and $f_4(A, T_{A,1}, T_{A,2}, V, N, sk_B, Auth_B, Auth_A)$

IV. Security Analysis

In this section, we analyze the security of the protocols.

A. Known-Key Security

SYL : Known-key security is satisfied since in each round Alice and Bob choose independent ephemeral private keys a and b. Adversary must compute abP for that session even he knows some other session keys and this is a Computational Diffie-Hellman problem.

THY : Known-key security is satisfied since in each round Alice and Bob choose independent ephemeral private keys a and b. Adversary must compute abP for that session to be able to compute sk_A or sk_B even he knows some other session keys, and this is a Computational Diffie-Hellman problem.

THTT : Known-key security is satisfied with the same reason in THY.

B. Forward Secrecy

SYL : Even adversary knows the secret keys S_A and S_B, he must compute abP from $T_A = aP$ and $T_B = bP$. This is a Computational Diffie-Hellman problem. Therefore, he cannot construct previous session keys.

THY : Even adversary knows the secret keys (R_A, Q_A) and (R_B, Q_B), he must compute abP from $T_A = aP$ and

$T_B = bP$ to compute sk_A or sk_B. This is a Computational Diffie-Hellman problem. Therefore, he cannot construct previous session keys.

THTT : Even adversary knows the secret keys S_A and S_B, he must compute sk_A or sk_B. This requires to compute $asH_1(ID)$ from $T_{A,2} = aH_1(ID)$ and $R_{A,2} = sH_1(ID)$. This is a Computational Diffie-Hellman problem. Therefore, he cannot construct previous session keys.

C. Key-Compromise Impersonation

SYL : Adversary knows Alice's private key S_A. He chooses $b \in \mathbb{Z}_p^*$ and sends to Alice. He takes $T_A = aP$ from Alice. He must compute $K_{AB} = e(P,P)^{abs}e(P,Q_B)^{as}e(Q_A,P)^{bs}e(Q_A,Q_B)^s$.

He cannot compute K_{AB} since he cannot compute $e(P,Q_B)^{as}$. He must know a or S_B to compute $e(P,Q_B)^{as}$. He knows $T_A = aP$, $P_{pub} = sP$ and must compute asP from these which is Computational Diffie-Hellman problem. Hence, he cannot impersonate Bob. He cannot impersonate Alice when he knows Bob's private key S_B because of the same reason.

THY : Adversary knows Alice's private key (R_A, Q_B). He gets A, Q_A, T_A from Alice. He chooses $b \in \mathbb{Z}_p^*$ and computes T_B, h_A. He must compute $sk_B = (b + R_B)(T_A + Q_A + h_A P_{pub}) \oplus bT_A$.

He cannot compute sk_B since he does not know R_B. Hence, he cannot impersonate Bob. Also, he cannot impersonate Alice when he knows Bob's private key (R_B, Q_B) because of the same reason.

THTT : Adversary knows Alice's private key $(R_{A,1}, R_{A,2}, Q_{A,1})$. He gets $Q_{A,2}, A, T_{A,1}, T_{A,2}, V$ from Alice. He computes $W, h_A, Q_{A,2}$. He checks $e(P,V) = e(T_{A,1} + Q_{A,1}, W)e(P_{pub}, h_A W + Q_{A,2})$. He chooses a nonce N.He cannot compute $sk_B = sT_{A,2}$ since he does not know s or to compute $saQ_{A,2}$ from $T_{A,2} = aQ_{A,2}$ and $R_{A,2} = sQ_{A,2}$ is Computational Diffie-Hellman problem.Hence, he cannot impersonate Bob. He cannot impersonate Alice when he knows Bob's private key $(R_{B,1}, R_{B,2}, Q_{B,1})$ since he needs to know Alice's private key to compute $V = (a + R_{A,1})W + R_{A,2}$.

D. Unknown Key-Share

All of the protocols use the user's ID or hash of the user's ID in their session keys. This provides known key-share for them.

E. Passive Attack

SYL : Adversary can obtain T_A and T_B over the network. He must still compute abP from these. In other words, he must break Computational Diffie-Hellman problem even he knows the master key. Hence, the protocol resists passive attack.

THY : Adversary can obtain A, Q_A, T_A, Q_B, T_B, $Auth_A$ and $Auth_B$ over the network. He must still compute abP from these to compute sk_A or sk_B. In other words, he must break Computational Diffie-Hellman problem even he knows the master key. Hence, the protocol resists passive attack.

THTT : Adversary can obtain A, $Q_{A,2}$, $T_{A,1}$, $T_{A,2}$, V, N, $Auth_A$ and $Auth_B$ over the network. He must still compute $asQ_{A,2}$ from these. For this, he must know a or s. He cannot compute a from aP or $aQ_{A,2}$ since it is a Diffie-Hellman problem but if he gets the master key s, then he can compute sk_B and the session key. However, the master key cannot be compromised from the network. Hence, the protocol resists passive attack.

F. Man-in-the-middle Attack

We analyze this attack in two ways. Firstly, adversary replaces the terms which include ephemeral keys with the ones computed with his own choice ephemeral keys. Secondly, adversary replaces the terms with the ones as in the attack on the Shim's protocol [6].

SYL : If adversary changes $T_A = aP$ with $a'P$ and $T_B = bP$ with $b'P$, then he can get corrupted sk_A and sk_B. However, he must still compute $e(Q_A, Q_B)^s$ to compute corrupted K_{AB} or K_{BA}. He cannot do this without knowing S_A, S_B or s itself.

If adversary changes $T_A = aP$ with $a'P - Q_B$, then he must compute $b(a'P - Q_B)$ without knowing b. To find b from bP is Diffie-Hellman problem. Hence, the protocol resists against man-in-the-middle attack.

THY : If adversary changes $T_A = aP$ with $a'P$ and $T_B = bP$ with $b'P$, then he can get corrupted sk_A and sk_B. However, he must still compute $a + R_A$ to compute true sk_A or $b + R_B$ to compute true sk_B. He cannot do this without knowing a, S_A, b or R_B.

If adversary changes $T_A = aP$ with $a'P - Q_B$, then he must compute $b(a'P - Q_B)$ without knowing b and $b + R_B$ without knowing b and R_B. To find b from bP is Diffie-Hellman problem and R_B is the private key of Bob.Hence, the protocol resists against man-in-the-middle attack.

THTT : If adversary changes $T_{A,2} = aQ_{A,2}$ with $a'Q_{A,2}$, then he can get corrupted sk_B. However, he must still know s which is the master key to compute corrupted sk_B. Also, Alice computes sk_A with her own knowledge. Even if adversary corrupts the sk_B, he cannot compute same session key with Alice. Hence, the protocol resists against man-in-the-middle attack.

G. Reveal Attack

SYL :

1) Adversary intercepts $T_A = aP$ from Alice. He chooses a random number $v \in \mathbb{Z}$. Then to impersonate Alice, he sends avP to Bob.
2) Adversary intercepts $T_B = bP$ from Bob. Then to impersonate Bob, he sends bvP to Alice.
3) Alice computes the variable from session key

$$\begin{aligned} K_{AB} &= e(aP_{pub} + S_A, T_B + Q_B) \\ &= e(P,P)^{abvs}e(P,Q_B)^{as}e(Q_A,P)^{bvs}e(Q_A,Q_B)^s \end{aligned}$$

Similarly, Bob computes the variable from session key

$$\begin{aligned} K_{BA} &= e(T_A + Q_A, bP_{pub} + S_B) \\ &= e(P,P)^{abvs}e(P,Q_B)^{avs}e(Q_A,P)^{bs}e(Q_A,Q_B)^s \end{aligned}$$

These variables must be equal to have same session key but they are different because of the interruption of adversary.

4) Adversary forms two different session keys with Alice and Bob. Therefore, when he asks the oracle to reveal session key with Alice, he gets only that session key but he cannot know Bob's.

Hence, the protocol resists against reveal attack.

THY :

1) Adversary intercepts $T_A = aP$ from Alice. He chooses a random number $v \in \mathbb{Z}$. Then to impersonate Alice, he sends avP to Bob.
2) Adversary intercepts $T_B = bP$ from Bob. Then to impersonate Bob, he sends bvP to Alice.
3) Alice computes session key with $T_A = aP$ and $T_B = bvP$. However, Bob computes session key with $T_A = avP$ and $T_B = bP$. To have the same session key, these variables must be equal but they are different because of the interruption of adversary.
4) Adversary forms two different session keys with Alice and Bob. Therefore, when he asks the oracle to reveal session key with Alice, he gets only that session key but he cannot know Bob's.

Hence, the protocol resists against reveal attack.

THTT : In this protocol, adversary can intercept messages from Alice.

1) Adversary intercepts messages from Alice. He chooses a random number $v \in \mathbb{Z}$. Then to impersonate Alice, he sends avP or $avQ_{A,2}$ or both to Bob instead of originals.
2) Alice computes the session key with $T_{A,1}$ and $T_{A,2}$. However, Bob computes the session key with avP and $avQ_{A,2}$. To have same session key, these variables must be equal but they are different because of the interruption of adversary.
3) Adversary forms two different session key with Alice and Bob. Therefore, when he asks the oracle to reveal session key with Alice, he gets only that session key but he cannot know Bob's.

Hence, the protocol resists against reveal attack.

As analyzed above, the protocols provide all the given security properties. Also, they resist against the passive, man-in-the-middle and reveal attacks.

V. Performance Analysis

We compare the performances according to the analyses in the original works using the following notations

- T_m : Cost of a scalar multiplication of point in G_1
- T_e : Cost of a biliniear pairing
- T_H : Cost of a hash function map to point in G_1

When we examine authenticated key agreement phase of the protocols, totally SYL requires $2T_e + 6T_m$ according to [1], THY requires $8T_m$ (according to [3] and THTT requires $3T_e + 6T_m + 3T_H$ according to [2].

According to Yuan and Li, bilinear pairing is an expensive operation. Also, Tseng et al. argues that hash function which maps to a point in G_1 can be implemented as a scalar multiplication in G_1. Therefore, we can also assume that T_m and T_H are equal. Thus, we can say that SYL requires $2T_e+6T_m$ and THTT requires $3T_e+9T_m$. Hence, in the lights of these arguments from the original articles, THY is more efficient than the others since no bilinear pairing operations is used and SYL is more efficent than THTT since it requires less bilinear pairing and multiplication operation.

VI. Conclusion

We compare the ID-based key agreements which are based on Shim's protocol. First, we explain them briefly. Then we analyse their security and efficiency. All of them are secure under the mentioned security properties and they all resist against the attacks which are examined. Although efficiencies are improved according to public key protocols, SYL and THTT are still not too fast since they use the bilinear pairing. However, THY is the fastest among all of them since it uses only scalar multiplications.

Acknowledgment

The authors would like to thank Associate Professor Ali Doğanaksoy for his guidance.

Kaynaklar

[1] Q. Yuan and S. Li, "A new efficient id-based authenticated key agreement protocol," *IACR Cryptology ePrint Archive*, vol. 2005, p. 309, 2005.
[2] Y.-M. Tseng, S.-S. Huang, T.-T. Tsai, and L. Tseng, "A novel id-based authentication and key exchange protocol resistant to ephemeral-secret-leakage attacks for mobile devices," *IJDSN*, vol. 11, pp. 898 716:1–898 716:12, 2015.
[3] Y.-M. Tseng, S.-S. Huang, and M.-L. You, "Strongly secure id-based authenticated key agreement protocol for mobile multi-server environments," *International Journal of Communication Systems*, vol. 30, no. 11, p. e3251, 2017, e3251 IJCS-16-0586.R1. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.3251
[4] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Information Theory*, vol. 22, pp. 644–654, 1976.
[5] T. NPSMAR, "An identity based authenticated key agreement protocol based on the weil pairing," 2002.
[6] K. Shim, "Efficient id-based authenticated key agreement protocol based on weil pairing," 2003.

AB Komisyonu'nun Bilgi Güvenliğinin Sağlanması ve Bilginin Korunmasına İlişkin Politika Belgelerinin İncelenmesi

Examination of Policy Documents of European Union Commission on Ensuring Information Security and Protecting Information

Demet Soylu
Bilgi ve Belge Yönetimi Bölümü
Ankara Yıldırım Beyazıt Üniversitesi
Ankara, Turkey
dsoylu@ybu.edu.tr

Tunç Durmuş Medeni
Yönetim Bilişim Sistemleri Bölümü
Ankara Yıldırım Beyazıt Üniversitesi
Ankara, Turkey
tuncmedeni@ybu.edu.tr

İhsan Tolga Medeni
Yönetim Bilişim Sistemleri Bölümü
Ankara Yıdırım Beyazıt Üniversitesi
Ankara, Turkey
tolgamedeni@ybu.edu.tr

***Öz*—Bu çalışma Avrupa Birliği Komisyonu'nun bilgi güvenliğinin sağlanması ve bilginin korunmasına ilişkin politika belgelerini incelemeyi amaçlamaktadır. Çalışma kapsamında, Avrupa Parlamentosu Ve Konseyi'nin 2018/0328 Sayılı Siber Güvenlik Sanayi, Teknoloji Ve Araştırma Yetkinlik Merkezi'nin Yönetmeliği Ve Bilgilendirici Protokolü, Avrupa Komisyonu'nda İletişim Ve Bilgi Sistemlerinin Güvenliğinin Sağlanmasına Yönelik 10 Ocak 2017 Tarihli 2017/46 Sayılı Komisyon Kararı, Avrupa Parlamentosu Ve Avrupa Konseyi'nin 27 Nisan 2016 Tarihli Kişisel Verilerin Korunmasıyla İlişkin Yönetmeliği, Avrupa Birliği ve Parlamentosu'nun Yenilik Birliği İnisiyatifi, Avrupa Birliği ve Parlamentosu'nun Dijital Gündem İnisiyatifi, Avrupa Parlamentosu Ve Konseyi'nin 27 Nisan 2016 Tarihli 2016/679 Sayılı Kişisel Verilerin İşlenmesi Ve Verilerin Serbest Dolaşımına İlişkin Veri Koruma Yönetmeliği, ENISA, Avrupa Birliği'nin Veri Koruma Direktifi incelenmiştir. İlgili politika belgelerinin bilgi güvenliğinin sağlanmasına yönelik odaklandığı ve önceliklendirdiği konular, ilkeler, esaslar ele alınmıştır ve çalışmada paylaşılmıştır.**

Anahtar Kelimeler—Avrupa Komisyonu, politika belgeleri, bigi güvenliği, bilginin korunması, veri güvenliği

Abstract—This study aims to examine the policy documents of European Union Commission on ensuring information security and protection of information. Within the scope of the study, 2018/0328 numbered Regulation and Informative Protocol of Cyber Security Industry, Technology and Research Competency Center of European Parliament and Council, 10th January 2017 dated 2017/46 numbered Commission Decision for Ensuring the Secuity of Communication and Information Systems, 27th April 2016 dated Regulationn of European Parliament and European Union Commission concerning Protection of Personal Data, Innovation Alliance Initiative of European Parliament and European Union, Digital Agenda Initiative of European Union and Parliament, 27th April 2016 dated 2016679 numbered Data Protection Regulation of European Parliament and Council on Processing Personal Data and Free Movement of These Data, ENISA, Data Protection Directive of European Commission were examined. Subjects, principles, bases prioritized by these policy documents for ensuring information security were handled and shared within the scope of the study.

Key Words — European Commission, policy documents, information security, information protection, data security

I. GİRİŞ

Bireylerin günlük yaşamı ve günümüz ekonomisi dijital teknolojilere giderek daha fazla bağımlı hale geldikçe, vatandaşlar ciddi siber olaylara gittikçe daha fazla maruz kalmaktadır. Hem sivil alt yapı hem de askeri kapasitelerinin güvenli dijital sistemlere dayanması sebebiyle siber tehditlere karşı teknolojik alt yapıların geliştirilmesi önem taşımaktadır. Her geçen gün giderek artış gösteren zorlukların ve tehditlerin üstesinden gelmek ve güvenli bir siber eko-sistemi geliştirmek için Avrupa Birliği ilgili konudaki amaç ve ilkelerini geliştirerek faaliyet alanlarını genişletmiştir

Avrupa Birliği, .Avrupa Komisyonu ve Konseyi, üye ülkeler ve aday ülkelerdeki bilgi güvenliğinin sağlanmasına yönelik çeşitli çalışmalar gerçekleştirmiştir. Bu çalışmalar kapsamında, küresel ağlardaki yasa dışı ve zararlı içerikle mücadele yolunda İnternet'in daha güvenli kullanılmasına yönelik eylem planları kabul edilmiştir.

2017 yılında Siber Güvenlik alanında gerçekleştirilen gelişmeler göz önünde bulundurulduğunda, Avrupa Birliği Dış İlişkiler Güvenlik Politikaları Birliği Üst Düzey Temsilcisi, Avrupa Birliği'nin Avrupa Birliği'nin siber güvenliğini sağlama, güçlü teknolojik alt yapıları oluşturma, esnek bilgi sistemleri sağlama, siber tehditlere karşı caydırıcı sistemlerin oluşturulması konusunda hedeflerini Avrupa Birliği'nin hedeflerini ortaya koymuştur. Dijital dünyadaki hizmetlerin sunumunda büyük ölçekli ve güvenli koordineli anıt sistemlerin geliştirilmesi konusu ele alınmıştır.

Avrupa Birliği'nde 2016 yılında siber güvenlik konusunda Kamu-Özel Ortaklığının/İşbirliğinin yaratılması 2014-20 sınırları dâhilinde araştırma ve inovasyonu kolaylaştırmak için araştırma, sanayi ve kamu sektörü topluluklarını bir araya getiren ilk somut bir adımdı. 2020 finansal çerçevesi, araştırma ve inovasyonda iyi ve daha odaklı sonuçlarla odaklanması gerektiği düşünülmektedir. Avrupa Birliği, çok daha büyük ölçekli bir yatırım yapabilir ve yeni çok amaçlı teknolojiler alanında siber güvenlikle ilgili endüstriyel zorluk ve sorunlara yanıt veren yenilikçi çözümler geliştirmeyi ve kalıcı kapasiteler, havuz çalışmaları, yeterlilikler geliştirecek ve apay zeka, kuantum hesaplama, blok zinciri ve güvenli dijital kimlikler gibi daha etkin bir mekanizmaya ihtiyaç duyabilir. Avrupa Siber Güvenlik Yetkinlik Merkezi ile siber güvenlik yeterlilik merkezleri ağı aracılığıyla Birlik siber güvenlik kapasitesinin

güçlendirilmesi olasılığı düşünülmüştür. İlk adım olarak ve geleceğe yönelik planları şekillendirmek amacıyla Komisyon, Horizon 2020 kapsamında ulusal merkezlerin siber güvenlik yetkinliğini ve teknolojik alt yapıyı geliştirmede yeni bir ivme oluşturmak için bir araya getirilmelerine yardımcı olmak için pilot bir çalışma başlatmıştır [1]

II. AVRUPA PARLAMENTOSU VE KONSEYİ'NİN 2018/0328 (COD) SAYILI SİBER GÜVENLİK SANAYİ, TEKNOLOJİ VE ARAŞTIRMA YETKİNLİK MERKEZİ'NİN YÖNETMELİĞİ VE BİLGİLENDİRİCİ PROTOKOLÜ

Bu bağlamda, bu ilgili yönetmelik, Ulusal Koordinasyon Merkezi ağı ile bir Avrupa Siber Güvenlik Sanayi, Teknoloji ve Araştırma Yeterliliğinin kurulmasını önermektedir. Bu amaca yönelik yapılan işbirliği modeli, Avrupa siber güvenlik teknolojik ve endüstriyel ekosistemini teşvik etmeye yönelik işlerlik göstermelidir. Yetkinlik Merkezi, Ağın çalışmasını kolaylaştıracak ve koordine edecek ve siber güvenlik teknolojik gündemini yönlendirecektir. Yeterlilik Merkezi özellikle Dijital Avrupa ve Horizon Avrupa programlarının uygulanmasını sağlayarak hibe tahsis edilmesini sağlayacaktır. Dünyanın diğer bölgelerinde yapılan siber güvenliğe yapılan önemli yatırımlar göz önünde bulundurulduğunda, Yetkinlik Merkezi Avrupa ortaklığı olarak önerilmektedir. Bu şekilde Avrupa Birliği, üye ülkeler ve/veya ilgili sanayi kuruluşları ortak yatırımı teşvik etmektedir. Bu nedenle teklif, Üye Devletlerin Yetkinlik Merkezi ve Ağın faaliyetlerine orantılı bir miktarda katkıda bulunmalarını gerektirmektedir. Yönetim Kurulu, özel sektör, tüketici kuruluşları ve diğer ilgili paydaşlarla düzenli diyalog sağlamak için bir Endüstriyel ve Bilimsel Danışma Kurulu tarafından desteklenmektedir.

Avrupa Siber Güvenlik Endüstri, Teknoloji ve Araştırma Yeterlilik Merkezi, siber güvenliği (Dijital Avrupa Programı ve Horizon Avrupa) destekleyen çeşitli Birlik programları için tek bir uygulama organı olarak görev yapacak ve aralarındaki tutarlılığı ve sinerjiyi geliştirecektir. Bu inisiyatif ayrıca, nitelikli bir AB siber güvenlik işgücünün geliştirilmesine yardımcı olmak amacıyla siber güvenlik becerilerini geliştirmek için (örneğin sivil ve askeri eğitim sistemlerinde siber güvenlik müfredatı geliştirerek), eğitim politikası belirleyicilere uygun girdi sağlayarak Üye Devletlerin faaliyetlerini tamamlayacaktır. Bu inisiyatif, Dijital Avrupa Programları kapsamındaki Dijital İnovasyon Merkezlerinin çalışmalarını tamamlayacak ve destekleyecektir. Dijital İnovasyon Hub'ları KOBİ'ler ve orta büyüklükteki şirketlerin dijital teknoloji tarafından sağlanan akıllı yenilikler yoluyla iş / üretim süreçlerinin yanı sıra ürün ve hizmetlerini geliştirerek daha rekabetçi olmalarına yardımcı olur [1]

III. AVRUPA KOMİSYONU'NDA İLETİŞİM VE BİLGİ SİSTEMLERİNİN GÜVENLİĞİNİN SAĞLANMASINA YÖNELİK 10 OCAK 2017 TARİHLİ 2017/46 SAYILI KOMİSYON KARARI

Bu kararda da aşağıda belirtilen konular ele alınmıştır [2] :

- Komisyonun iletişim ve bilgi sistemleri, Komisyonun işleyişinin ayrılmaz bir parçasıdır ve BT (Bilgi Teknolojileri) güvenlik vakaları ve durumları, Komisyonun işlemleri üzerinde olduğu kadar bireyler, işletmeler ve Üye Devletler de dâhil olmak üzere üçüncü şahıslar üzerinde ciddi bir etkiye sahip olabilir.
- İletişim ve bilgi sistemleri, maruz kaldıkları risklerin olasılığı, etkisi ve niteliği ile orantılı bir koruma seviyesi ile hizmet sunmalıdır.
- Komisyonun BT güvenlik politikası, Komisyondaki güvenlik politikaları ile tutarlı bir şekilde uygulanmalıdır.
- İnsan Kaynakları ve Güvenlik Genel Müdürlüğü Güvenlik Müdürlüğü, Güvenlikten sorumlu Komisyon Üyesinin yetkisi ve sorumluluğu altında Komisyonda güvenlik konusunda genel sorumluluğa sahiptir.
- İletişim ve bilgi sistemlerinden sorumlu Komisyon departmanları tarafından uygun tedbirler geliştirilmeli ve uygulanmalı ve iletişim ve bilgi sistemlerinin korunmasına yönelik BT güvenlik önlemleri etkinlik ve etkinlik sağlamak için Komisyon genelinde koordine edilmelidir.

IV. AVRUPA PARLAMENTOSU VE AVRUPA KONSEYİ'NİN 27 NİSAN 2016 TARİHLİ KİŞİSEL VERİLERİN KORUNMASIYLA İLİŞKİN YÖNETMELİĞİ

Gerçek kişilerin kişisel verilerin işlenmesiyle ilgili olarak korunması temel bir haktır. Avrupa Birliği Temel Haklar Şartlarının 8. Maddesi ve Avrupa Birliği'nin İşleyişine İlişkin Anlaşmanın 16. Maddesi bireylerin kişisel verilerinin korunmasının öneminin altını çizmektedik. [3].

Avrupa Parlamentosu ve Konsey'in (4) 95/46 / EC sayılı Direktifi, işleme faaliyetleri bakımından gerçek kişilerin temel hak ve özgürlüklerinin korunmasını uyumlaştırmayı ve kişisel verilerin Üye Devletler arasında serbest akışını sağlamayı amaçlamaktadır. İç pazarın işleyişinden kaynaklanan ekonomik ve sosyal entegrasyon, kişisel verilerin sınır ötesi akışlarında önemli bir artışa neden olmuştur. Gerçek kişiler, dernekler ve AB'deki kuruluşlar dahil, kamu ve özel aktörler arasında kişisel veri alışverişi artmıştır. Üye Devletlerdeki ulusal otoritelere, görevlerini yerine getirebilme konusunda çağrı yapılmıştır. AB Birliği genelindeki gerçek kişiler için tutarlı bir koruma düzeyi sağlamak ve kişisel verilerin iç pazarda serbest dolaşımını engelleyen farklılıkları önlemek amacıyla, mikro, küçük ve küçük işletmeler dâhil olmak üzere ekonomik operatörler için yasal kesinlik ve şeffaflık sağlamak için bir Yönetmelik gerekmektedir. Bu verilerin kapsamına giren amaçlarla kişisel verilerin yetkili makamlarca işlenmesiyle ilgili olarak, Üye Devletlerin bu Yönetmelik kurallarının uygulanmasını sağlamak için daha spesifik hükümler sağlayabilmesi veya sunabilmesi gerekir. Bu yönetmelik, üye devletlerin belirli koşullar altında, bu tür bir kısıtlamanın gerekli ve orantılı bir tedbir teşkil etmesi durumunda, kamu güvenliği ve cezai suçların önlenmesi, soruşturulması, tespit edilmesi veya kovuşturulması veya kamu güvenliğine yönelik konularda tehditlerin önlenmesi

için belirli yükümlülükleri ve hakları yasalarla sınırlama imkânı sağlamalıdır [3]

V. YENİLİK BİRLİĞİ İNİSİYATİFİ

Avrupa Birliği Komisyonu'nun girişimlerinden biri de "Yenilik Birliği" inisiyatifidir. Bu inisiyatifin amacı, Avrupa Birliği araştırma alanını geliştirmek, bilgi güvenliğini ve kişisel verilerin korunmasını sağlamaktır. Bu inisiyatif kapsamında da Patent Mahkemesi kurmak, telif hakları ve marka adları çerçevesini modernleştirmek, SME'lerin Fikri Mülkiyet haklarının korunmasına yönelik iyileştirmelerde bulunmak, Avrupa Yenilik ortaklıklarını hayata geçirmek, Avrupa'nın geleceğini şekillendirecek endüstriyel teknolojiler geliştirilmesini sağlamak amaçlanmıştır. EIB (Avrupa Yatırım Bankası) ile işbirliği sağlanmasını desteklemek, karbon piyasasıyla ilgili yenilikçi teşvik mekanizmalarını geliştirmek, bunlarla ilgili idari süreçleri kolaylaştırmak, bilgi ortaklıkları geliştirmek, iş, araştırma ve yenilik üçgeni arasındaki ilişkileri geliştirmek amaçlanmıştır [4]

VI. DİJİTAL GÜNDEM İNİSİYATİFİ

Avrupa Birliği Komisyonu'nun girişimlerinden diğeri de "Avrupa için dijital gündem" inisiyatifidir. Bu inisiyatifin amacı, 2013 yılında herkesin geniş bant erişimine sahip olduğu, 2020 yılı itibariyle herkesin daha yüksek hızda internete (30 Mbs ve üstü) ve Avrupalı hane sakinlerinin %50 veya daha fazlasının 100 Mbs'in üzerinde internet bağlantısına abone olduğu, hızlı ve ultra hızlı ve birlikte işleyebilir uygulamalara dayalı bir Dijital Tek Pazardan, sürdürülebilir ekonomik ve sosyal faydalar sağlamaktır. Komisyon, Açık ve rekabetçi yüksek hızlı internet yapısı ve ilgili hizmetlere yatırımı teşvik eden istikrarlı bir yasal çerçeve sağlamayı, Avrupa'nın Avrupa'nın zengin kültürel mirasının dijitalleştirilmesine katkıda bulunmak, çevrimiçi içerik ve hizmetler açısından yüksek düzeyde güven ve itibar sunan, açık haklar rejiminin dengeli olduğu düzenleyici bir çerçeve sunmak, birden fazla ülke topraklarını kapsayan lisansların teşvik edilmesini sağlamak, hak sahipleri için güvenli AB web hizmetlerine yönelik bir alt yapı oluşturmak, Kilit stratejik alanlarda Avrupa'nın teknolojisini güçlendirmek ve ortaya çıkan pazarlara liderlik etmek için SME'lere yönelik hızlı büyüme koşulları oluşturmak ve tüm iş sektörlerinde bilgi teknolojisi yeniliklerini teşvik etmek amaçlarıyla araştırma ve yenilik fonları reformu gerçekleştirmek ve desteği arttırmak, özellikle dijital okur-yazarlık ve erişilebilirlik yoluyla tüm Avrupa vatandaşlarının internete erişimini ve kullanmasını desteklemek. amaçlanmıştır [4]

VII. ENISA

ENISA, bireylerin dijital ve siber güvenlik becerilerinin geliştirilmesini sağlamayı amaçlayan AB politika önerisidir ENISA, bilgi güvenliği konusunda farkındalık oluşturulmasını sağlayarak bilgi toplumuna katkıda bulunmayı amaçlamaktadır. Tüketicilerin, kurumların, bireylerin, işetmelerin ve kamu sektöründeki kurumların bilgi güvenliğinin sağlanmasına hizmet etmektedir. Avrupa Kurumlarını, Üye ülkelerini ve iş dünyasını desteklemektedir. Bu politika belgesi, Avrupa Birliği'nde referans gösterilen bir siber güvenlik politika belgesi haline gelmiştir. Elektronik iletişim, elektronik kimlik ve güvenlik hizmetleri alanında güvenlik hususlarını ele almaktadır. AB ve ulusal kamu yetkinlik ve uzmanlığının geliştirilmesini, güvenli bilgi ağlarının kullanıldığı bir toplum kültürü ve anlayışının benimsenmesini öngörmektedir. Avrupa Birliği'nde bilgi güvenliği konusunda politikaların geliştirilmesini desteklemektedir. Tavsiye kararları, farkındalık sağlayıcı ve artırıcı eğitimlerle veri güvenliği alanında kapasitenin geliştirilmesini sağlamaktadır [5]

VIII. AVRUPA PARLEMONTOSU VE KONSEYİ'NİN 27 NİSAN 2016 TARİHLİ 2016/679 SAYILI KİŞİSEL VERİLERİN İŞLENMESİ VE VERİLERİN SERBEST DOLAŞIMINA İLİŞKİN VERİ KORUMA YÖNETMELİĞİ

Avrupa Birliği'nin diğer çalışmalarından biri de Avrupa Parlamentosu ve Konseyi'nin 2016/679 sayılı ve 27 Nisan 2016 tarihli Kişisel Verilerin İşlenmesi ve bu verilerin serbest dolaşımında gerçek kişilerin korunmasına ilişkin 95/46/EC sayılı genel veri koruma yönetmeliğidir. Kişisel verilerin işlenmesinde gerçek kişilerin korunması bir temel haktır. Avrupa Birliği Temel Haklar Şartları ve Avrupa Birliğinin İşleyişine Dair Antlaşmanın 16 (1) Maddesi, herkese, kendisine ilişkin kişisel verilerin korunması hakkını tanımaktadır. Kişisel verilerin işlenmesinde gerçek kişilerin korunması ilkeleri ve buna ilişkin kurallar, uyruğu ya da ikamet yeri neresi olursa olsun, başta kişisel verilerin korunması hakkı olmak üzere bu kişilerin temel hak ve özgürlüklerine saygılı olmalıdır. Bu Yönetmelik, bir özgürlük, güvenlik ve adalet alanı ve bir ekonomik birliğin gerçekleştirilmesine, ekonomik ve toplumsal ilerlemeye, iç piyasa içerisindeki ekonomilerin güçlendirilmesi ve yakınlaştırılmasına ve gerçek kişilerin refahlarının geliştirilmesine katkı sağlamak adına hazırlanmış ve yayımlanmıştır. Hızlı teknolojik gelişmeler ve küreselleşme, kişisel verilerin korunmasında karşımıza yeni zorluklar çıkarmaya başlamıştır. [6]

IX. VERİ KORUMA DİREKTİFİ

Avrupa Birliği'nin diğer politika belgelerinden biri de Polis ve Cezai Yargılama Makamlarına yönelik Veri Koruma Direktifi, Bireylerin kişisel verilerinin, verileri polis ve cezai yargılama makamları tarafından işlenirken daha iyi korunmasını amaçlar. Ayrıca, AB ülkelerindeki polis ve cezai yargılama makamlarının soruşturmalar için gerekli olan bilgiyi daha etkin ve etkili bir şekilde paylaşmasını sağlayarak AB içerisindeki terör ve sınır ötesi suçlarla mücadelede işbirliğini geliştirmeyi amaçlar. Polis ve Cezai Yargılama Makamlarına yönelik Veri Koruma Direktifi, Genel Veri Koruma Düzenlemesi (Yönetmelik (AB) 2016/679) ile birlikte AB veri koruma reform paketinin bir parçasıdır. Direktif, verilerin kanunlara uygun bir adil bir şekilde işlenmesini, açık ve meşru amaçlarla toplanmasını, yalnızca bu amaçlar doğrultusunda işlenmesini, işlenme amaçları ile ilişkili olarak yeterli, ilgili ve yalnızca gerekli ve doğru ölçüde olmasını, yetkisiz veya yasa dışı işleme karşı belge güvenliğinin düzgün bir şekilde sağlanmış olmasını gerektirir. Ulusal makamlar, riske açık olan kişisel veriler için bir güvenlik düzeyi sağlamak amacıyla teknik ve örgütsel önlemler almalıdır. Veri işlemenin otomatik olarak yapıldığı durumlarda çeşitli önlemler alınmalıdır. Örneğin, yetkili olmayan kişilerin veri işleme için kullanılan ekipmana erişimi engellenmelidir, verilerin izinsiz bir şekilde kopyalanması,

değiştirilmesi ve kaldırılması engellenmelidir. Kişisel verilere yetkisiz olarak girilmesinin ve depolanmış kişisel verilen yetkisiz olarak görüntülenmesinin, değiştirilmesinin önüne geçilmelidir [6].

X. SONUÇ

Çalışma kapsamında incelenen politika belgelerinde, bilgi güvenliğinin sağlanması ve bilgilerin, verilerin korunmasının Avrupa Birliği'nin önceliklendirdiği konulardan biri olduğu görülmüştür. Avrupa Birliği, kişilerin, kurumların bilgilerinin ve verilerinin korunmasını sağlamaya yönelik önemli adımlar atmıştır. Üye Devletler'deki ilgili kurum ve kuruluşları, teşebbüsleri ve kişileri de veri güvenliğinin, siber güvenliğinin sağlanması konusunda gerekli adımları atmaya ve eylemde bulunmaya davet etmiştir. Avrupa Komisyonu, Avrupa Birliği'nin ve üye ülkelerin siber güvenlik alanındaki kapasitesini geliştirip Avrupa Birliği'ni dünyada öncü ve lider haline getirmeye çalışmıştır. Güvenliğin sağlanması konusunda hem kurumsal alt yapıları iyileştirmek hem de bu konuda ulusal, uluslararası, bireysel farkındalığa hizmet etmek amacıyla hibeler tahsis etmiştir. Bu alanda ayrıca, ilgili kurum ve kuruluşların işbirliği içinde bulunması sağlanmıştır.

KAYNAKLAR

[1] Eur Lex 2018). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0630 adresinden 03.08.2019 tarihinde erişilmiştir

[2] Eur Lex (2017). Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2017.006.01.0040.01.ENG adresinden 03.08.2019 tarihinde erişilmiştir.

[3] EUR Lex (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679 adresinden 03.08.2019 tarihinde erişilmiştir.

[4] EU Commission. https://ec.europa.eu/digital-single-market/en adresinden 02.08. 2019 tarihinde erişilmiştir.

[5] Enisa (2018). Enisa programming document 2019-2021. https://www.enisa.europa.eu/publications/corporate-documents/enisa-programming-document-2019-2021 adresinden 03.08.2019 tarihinde erişilmiştir.

[6] Eur Lex (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016R0679 adreinden 03.08.2019 tarihinde erişilmiştir.

TLS Protokolü'ne Yapılan Güncel Kriptografik Saldırılar

Current Cryptographic Attacks towards TLS Protocol

Duygu ÖZDEN
HAVELSAN Inc.
Ankara, Turkey
dozden@havelsan.com.tr

***Abstract*— Secure Socket Layer (SSL) and Transport Layer Security (TLS) are two commonly used certificate-based protocols to satisfy secure communication. They are widely used in e-commerce, governmental and military based systems, online messaging systems etc. This wide range of applications makes SSL / TLS an attractive attack surface for attackers. Due to critical vulnerabilities found in recent years, it can be said that all versions of SSL are now expired. Moreover, PCI DSS (Payment Card Industry Data Security Standard) said in 2018 that even TLS 1.0 should no longer be used in communications [1]. In this work, it will be told about some current vulnerabilities and attacks towards them as a cryptographic perspective in brief. It will be given some precautions and important points for mitigations of these attacks in order to enlighten security researchers and users actively mingle with these protocols.**

***Index Terms*— Protocol, certificate, attack, vulnerability, security**

***Özet*— Secure Socket Layer (SSL) ve Transport Layer Security (TLS), güvenli iletişimi sağlamak için yaygın olarak kullanılan iki sertifika tabanlı protokoldür. Yaygın olarak e-ticaret, devlet ve askeri tabanlı sistemler, çevrimiçi mesajlaşma sistemleri vb. sistemlerde kullanılmaktadır. Bu geniş uygulama yelpazesi, SSL / TLS'i saldırganlar için çekici bir saldırı yüzeyi yapmaktadır. Son yıllarda bulunan kritik güvenlik açıklıkları nedeniyle, SSL'nin tüm sürümlerinin miadının dolduğu söylenebilir. Ayrıca, PCI DSS (Ödeme Kartı Endüstrisi Veri Güvenliği Standardı) 2018'de, artık TLS 1.0'ın bile iletişimde kullanılmaması gerektiğini söylemiştir [1]. Bu çalışmada, kriptografik açıdan bu protokollerde mevcut güvenlik açıklıkları ve bunlara yönelik bazı güncel saldırılardan bahsedilecektir. Ayrıca, bu protokollerle aktif bir şekilde ilgilenen güvenlik araştırmacıları ile kullanıcıları aydınlatmak amacıyla alınabilecek bazı önlemler ve zararı azaltma teknikleri üzerinde durulacaktır.**

***Anahtar Kelimeler*— Protokol, sertifika, saldırı, açıklık, güvenlik**

I. INTRODUCTION

The concept of cyber security, which gained acceleration with the introduction of the internet into our lives, has expanded many of its concepts over time. Many advantages as well as disadvantages of the irreplaceable importance of the internet in our lives cannot be denied. In the sense of easy access to information, communication, health, trade, public transactions, critical infrastructure etc., this system has become one of the most important research areas of cyber security. In most of these systems, people share their personal data, some of the information that is critical to them. The criticality of these information also requires that they should be shared on a secure channel. One of the secure communication channels over the internet is the use of some security protocols on these platforms. TLS (and its processor SSL) protocol is one of them to ensure communication security generally between the client and the server over an insecure channel. SSL is developed by Netscape Communications in 1994 to allow secure access of a browser to a web server and became the accepted standard for web security [8]. The first version of SSL, SSL 1.0, was never released due to some vulnerabilities. After that, SSL 2.0 and SSL 3.0 are improved respectively. TLS, the following version of SSL, was developed in 1999 and mentioned in RFC (Request for Comments). The current versions are TLS 1.0, TLS 1.1, TLS 1.2 and TLS 1.3. The name of the protocol changed from SSL to TLS because TLS works over any bidirectional stream of bytes, not just sockets [8]. Today, SSL and TLS 1.0 are not recommended due to the very critical security vulnerabilities, but their security becomes more important due to the frequent use of these protocols. Another important aspect of TLS is the incontrovertible role of cryptographic infrastructure in ensuring security. Cryptographic protocols help the system to satisfy confidentiality, data integrity, authentication and non-repudiation properties. Confidentiality means protecting sensitive information from disclosure by unauthorized people. Data integrity is used to satisfy protection of data in order not to be altered or corrupted. Entity authentication is the corroboration of the identity of an entity and message authentication is corroborating the source of information [8]. Non-repudiation means preventing the denial of previous commitments. As with many systems, cryptography in SSL/TLS contains symmetric and asymmetric encryption algorithms, key exchange mechanisms, hash functions, mode of operations. In this study, some critical vulnerabilities and attacks of cryptographic mechanisms in TLS protocol will be emphasized.

Organization of this paper is as follows: In Section 2, a brief information about the role of TLS and importance of its security is given. In Section 3, current vulnerabilities and attacks towards

TLS are explained. It basically contains last 3 years and from cryptographic perspective. In Section 4, a conclusion and future recommendations are given.

II. RELATED WORK

This work is inspired by the study of Ronen et al. [7] in which they showed new cache attacks of TLS implementations. This study revealed a large system of attack surfaces found in all versions of TLS protocol. It is important to examine TLS as a widely used security protocol. The critical role of this protocol in transmitting sensitive information makes it the target of attacks. The need to examine the current vulnerabilities of TLS, as well as many known vulnerabilities since SSL, has once again been created with cache attacks. TLS, as it is known, is a cryptographic, certificate-based protocol.

In this study, it is aimed to present the suggestions for cryptographic improvements by examining the studies on the recent TLS vulnerabilities and attacks which have been discovered in the last 3 years.

III. CURRENT CRYPTOGRAPHIC ATTACKS AND VULNERABILITIES

In this study, recent developments in terms of cryptography related with TLS are examined. Research has shown that many interesting vulnerabilities and attacks have emerged, even in the last 3 years. Perhaps the most remarkable aspect of these is that they have been observed in the proposed algorithms. As always mentioned in security, it is difficult to provide the trade-off between confidentiality and availability. The attacks and vulnerabilities to be mentioned in this study provided an example of this generalization.

A. Drown Attack (2016)

This attack can be described and named as Decrypting RSA with Obsolete and Weakened Encryption. Drown, as the name suggests, allows an attacker to break encryption mechanism and obtain sensitive data from communication between client and server. While this attack affects 33% of HTTPS servers in 2016, fortunately, SSL Labs states that it is 1.2% in 2019 [9]. However, this percentage should not be underestimated.

A web server is vulnerable to this attack if it supports SSL 2.0 or secret key is used on another server that allows SSL 2.0. This is because of the fact that many companies reuse the certificates or keys on their servers. In this case, even if the web server does not support SSL 2.0, this attack can be successful with a connection from another supporting server [2].

B. SLOTH Attack (2016)

This attack means that Security Losses from Obsolete and Truncated Transcript Hashes. This causes finding collision of hash function used in TLS signature. Such weak algorithms like MD5 and SHA1 used in TLS 1.1, 1.2 and 1.3 and affected by this attack. In such attacks, the security of the system is halved. That is for example, the 128-bit security introduced by MD5 drops to 64-bit [10]. This situation reveals the severity of the attack [3].

C. Sweet32 Attack (2016)

One of the recent attacks to be mentioned is Sweet32. This attack can be carried out against 64-bit block cipher algorithms such as 3DES, one of the encryption algorithms commonly used in the TLS protocol. In Sweet32, if an attacker can capture substantially many network traffic between web browser and website, which have 3DES in TLS protocol, he can recover secure HTTP cookies [11]. In the PoC of this attack, researchers claim that it takes less than 2 days. This attack is based on a birthday attack to break short-length block cipher algorithms such as 3DES. Indeed, 3DES is one of the most widely used algorithm in HTTPS connection after AES. The article related to Sweet32 recommends that web servers should be configured to support 128-bit algorithms. Also, TLS renegotiation or limiting HTTP/1.1 Keep-Alive, SPDY and HTTP/2 with 3DES can be solutions [11]. This vulnerability is referred to CVE-2016-2183. Currently, TLS 1.0, 1.1 and 1.2 supports 3DES but it is not recommended after this attack [4].

D. ROBOT Attack (2017)

Another attack is ROBOT (Return of Bleichenbacher's Oracle Threat). This is an interesting study related with the attack that is found 21 years ago by Daniel Bleichenbacher. This old attack is a padding oracle attack affecting RSA-based encryption schemes in SSLv2 [12]. In other respects, ROBOT attack contains some covariations about Bleichenbacher's attack which allows an attacker to make RSA decryption and some other operations using private key on some TLS servers. According to ROBOT attack researchers, some of the most commonly used websites like Facebook, PayPal, affected by this attack. It allows an attacker to passively capture traffic and decrypt it. The researchers released PoC of the attack and a detection tool to scan vulnerable hosts [5].

E. ROCA Vulnerability (2017)

ROCA (Return of Coppersmith's Attack) is a vulnerability which affects RSA key generation. Using this vulnerability, a remote attacker can calculate private key by just having user's public key [13]. It is feasible to break 1024- or 2048-bit RSA encryptions which is a danger as a most commonly used length in RSA today. In other words, it is a threat for RSA key generation in which security depends on integer factorization problem [6]. This vulnerability is referred to CVE-2017-15361.

F. New Cache Attacks on TLS Implementations (2018)

This attack shows that it affects all TLS versions and it is efficient enough to break the mechanism. The most valuable mitigation technique for these types of attacks is using OAEP (Optimal Asymmetric Encryption Padding) or ECEIS (Elliptic Curve Integrated Encryption Scheme) for asymmetric encryption, Elliptic Curve Diffie-Hellman for key exchange mechanism [7].

This attack tested in various TLS implementations and OpenSSL, Amazon s2n, Mozilla NSS, WolfSSL, GnuTLS, MbedTLS and Apple CoreTLS were found to be vulnerable [14]. Cache attack uses side channel analysis of cache access timings of these libraries. A successful exploitation could be able to break RSA key exchange or RSA signature which is used

in these TLS implementations. Note that, RSA key exchange is used during handshake process to negotiate a shared secret. Figure 1 shows this type of attack over RSA signature process [14]. Note that, TLS 1.3 supports RSA signature.

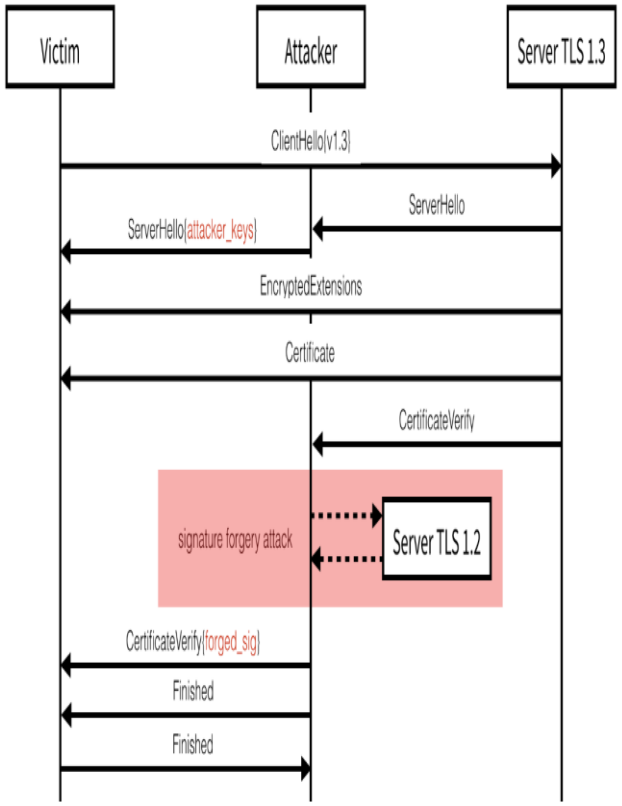


Fig. 1. Signature Forgery Attack

IV. CONCLUSION AND FUTURE WORK

Communicating with a web-based system always reveals the importance of security, especially with regards to the privacy. Personal data are the most valuable information assets of human beings. In this regard, especially in recent years, a number of legal arrangements have been made in our country. TLS protocol plays important role in transferring personal data over the internet. Moreover, since this protocol is based on the cryptography, it could benefit somehow from the confidentiality, data integrity, authentication and non-repudiation features of cryptographic mechanisms [8]. The degree of sensitivity of the subject emphasizes the importance of analyzing and following up on current developments. This study aims to be an enlightener for the security of TLS based on recent developments. Within this context, some of the very recent attacks and vulnerabilities of TLS protocol examined. These are basically cryptography-related studies. They are DROWN Attack, SLOTH Attack, Sweet32 Attack, ROBOT Attack, ROCA Vulnerability and New Cache Attacks on TLS Implementations.

This study once again demonstrated the importance of cryptography at every stage from protocol design to implementation. When looking at the current attacks, it can be said that the first problem is caused by weak algorithm selection. It is seen that many cryptographic algorithms, which are no longer recommended, are still being used in many current websites. In addition, it is necessary to proceed by closing all existing vulnerabilities, reducing the attack surface and taking all of these into consideration in the design of the new version of TLS protocol. To achieve all this, it is important that software engineers and cryptologists should work together.

Figure 2 shows the usage of SSL certificate authorities for websites from w3techs statistics [15]. These statistics demonstrate the inadequacy of the use of a certified website as well as the security of the certificate-based protocol. First, sensitive information input system should be reliable and then the mechanism used in the background should be strong.

Figure 3 shows Qualys SSL Labs results of the website ISCTurkey2019 (https://iscturkey.org) as an example of HTTPS website [16]. Also, Figure 4 shows keychest.net analysis of the conference website. It can be said that almost all known vulnerabilities and attacks including the ones in this study do not affect this website. However, these results do not mean that the site is completely resistant to these attacks. A detailed study should be carried out on this subject.

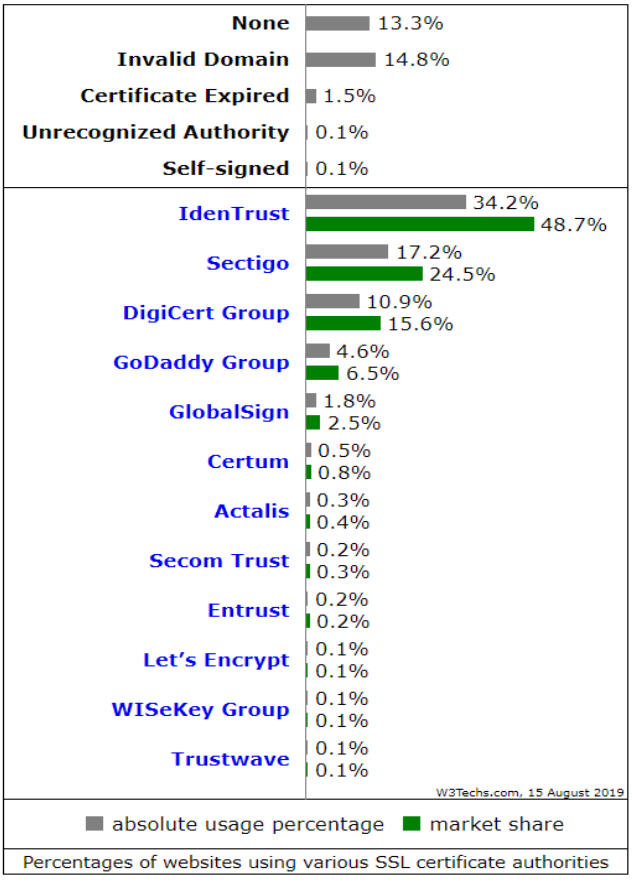


Fig. 2. Usage of SSL Certificates According to Certificate Authorities

Fig. 3. https://iscturkey.org Qualys SSL Labs Analysis

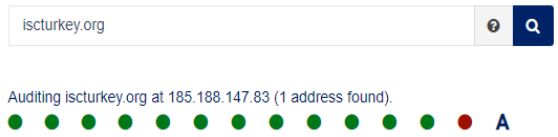


Fig. 4. https://iscturkey.org keychest Analysis

ACKNOWLEDGMENT

I would like to thank Salih Talay and Emre Yüce from HAVELSAN for their valuable guidance while preparing this study. Their advices enlighten me to produce much better work than I can.

REFERENCES

[1] L. Gray, "Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS", Blog.pcisecuritystandards.org, 2019. [Online]. Available: https://blog.pcisecuritystandards.org/are-you-ready-for-30-june-2018-sayin-goodbye-to-ssl-early-tls . [Accessed: Mar.10, 2019].

[2] N. Aviram, et al., *DROWN: Breaking TLS Using SSLv2*, 2016.

[3] K. Bhargavan and G. Leurent, "Transcript collision attacks: Breaking authentication in TLS, IKE, and SSH,", 2016.

[4] K. Bhargavan and G. Leurent, "On the practical (in-) security of 64-bit block ciphers: Collision attacks on HTTP over TLS and OpenVPN," in *ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 456-467.

[5] H. Böck, J. Somorovsky, and C. Young, "Return of Bleichenbacher's Oracle Threat (ROBOT)," in *27th USENIX Security Symposium*, 2018, pp. 817-849.

[6] M. Nemec, M. Sys, P. Svenda, D. Klinec, and V. Matyas, "The return of coppersmith's attack: Practical factorization of widely used rsa moduli," in *ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1631-1648.

[7] E. Ronen, et al., *The 9 Lives of Bleichenbacher's CAT: New Cache ATtacks on TLS Implementations*, 2018.

[8] D. Ozden, *Analysis of recent attacks on SSL/TLS protocols*, 2016.

[9] "The DROWN Attack," Mar.13, 2016. [Online]. Available: https://drownattack.com. [Accessed: Dec.10, 2018].

[10] "Security Losses from Obsolete and Truncated Transcript Hashes," [Online]. Available: https://www.mitls.org/pages/attacks/SLOTH. [Accessed: Feb.12, 2018].

[11] "Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN," [Online]. Available: https://sweet32.info. [Accessed: Mar.17, 2018].

[12] H. Böck, "Return of Bleichenbacher's Oracle Threat," 2017. [Online]. Available: https://robotattack.org. [Accessed: Mar.24, 2018].

[13] "ROCA: Vulnerable RSA generation (CVE-2017-15361)," [Online]. Available: https://crocs.fi.muni.cz/public/papers/rsa_ccs17. [Accessed: Apr.10, 2018].

[14] "The 9 Lives of Bleichenbacher's CAT: New Cache ATtacks on TLS Implementations," [Online]. Available: https://www.cryptologie.net/article/461/the-9-lives-of-bleichenbachers-cat-new-cache-attacks-on-tls-implementations. [Accessed: Jun.1, 2019].

[15] "Usage of SSL certificate authorities for websites," [Online]. Available: https://w3techs.com/technologies/overview/ssl_certificate/all. [Accessed: Jul.18, 2019].

[16] "SSL Server Test," [Online]. Available: https://www.ssllabs.com/ssltest. [Accessed: Jul.18, 2019].