ISC turkey

TELEKOMÜNİKASYON KURUMU

1926 GAZİ ÜNİVERSİTESİ

ODTÜ

ULUSLARARASI KATILIMLI BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ KONFERANSI

INFORMATION SECURITY & CRYPTOLOGY CONFERENCE WITH INTERNATIONAL PARTICIPATION

13 14 Aralık *December* 2007

bilimsel program

scientific programme

geleceğini koru!
secure the future!

www.iscturkey.org

cmsproject+

bilimsel program
scientific programme

1.gün first day

13 Aralık December 2007
Perşembe Thursday

	GRAND BALL ROOM III	GRAND BALL ROOM II	MAGNOLIA HALL
09:00 - 10:00	**KAYIT** REGISTRATION		
10:00 - 10:20	**AÇILIŞ TÖRENİ /** OPENING CEREMONY		
10:20 - 11:20	**"Electronic Identification in Finland"** Pekka JELEKÄİNEN / FINLAND		
11:20 - 11:30	**ÇAY / KAHVE ARASI -** TEA / COFFEE BREAK		
11:30 - 13:00	**PANEL** **ENTERPRISE INFORMATION SECURITY IN FINANCIAL SECTOR**		
13:00 - 14:00	**ÖĞLE YEMEĞİ -** LUNCH		
	GRAND BALL ROOM III	**GRAND BALL ROOM II**	**MAGNOLIA HALL**
14:00 - 14:20	45 **Security on Mobile Phones with Lightweight Cryptographic Message Syntax** Murat YASİN KUBİLAY, Albert LEVİ, Atilla ÖZGİT	30 **Generalized ID-Based ElGamal Signatures with Message Recovery** Said KALKAN, Kamer KAYA, Ali Aydın SELÇUK	92 **New Findings on the Covering Sequence of Boolean Functions** Güzin KURNAZ
14:20 - 14:40	86 **Mobile Electronic Signature: Countries And Applications** **Mobil Elektronik İmza: Ükeler ve Uygulamalar** Şeref SAĞIROĞLU, Demet KABASAKAL, Mustafa ALKAN	55 **A New Approach to Keystream Based Cryptosystems** İmran ERGÜLER, Orhun KARA	88 **Comparing Substitution Boxes of the Third Generation GSM and Advanced Encryption Standard Ciphers** Sedat AKLEYLEK, Melek D. YÜCEL
14:40 - 15:00	93 **Mobile Electronic Signature: Scenarios, Applications, Standards and Countries** **Mobil Elektronik İmza: Senaryolar, Uygulamalar, Standartlar ve Ükeler** Demet KABASAKAL, Şeref SAĞIROĞLU, Mustafa ALKAN	48 **An Identity-Based Key Infrastructure Suitable for Messaging Applications** Ayşegül KARATOP, Erkay SAVAŞ	34 **Ters Haritalama Tabanlı S-kutularının Cebirsel Açıdan İyileştirilmesi** M.TOLGA SAKALLI, Ercan BULUŞ, Andaç ŞAHİN, Fatma BÜYÜSARAÇOĞLU, Ahmet KARADENİZ
15:00 - 15:20	**ÇAY / KAHVE ARASI -** TEA / COFFEE BREAK		

1.gün firstday

13 Aralık December 2007 Perşembe Thursday

15:20 - 16:20

"Mobile Signature"
Deniz TUNÇALP / TÜRKİYE

TURKCELL

GRAND BALL ROOM III	GRAND BALL ROOM II	MAGNOLIA HALL FIRST FLOOR
16:30 - 16:50		
33 **Sayısal Görüntülerdeki Yerel Parlaklık Değişimine Dayalı Adaptif Steganografi** Mustafa ULUTAŞ, V. NABIYEV, G. ULUTAŞ	**49** **Hash Function Designs Based on Stream Ciphers** Meltem SÖNMEZ TURAN, Özgür ÖZUĞUR, Onur KURT	**62** **Design and SystemC Implementation of a Crypto Processor for AES and DES Algorithms** Murat AŞKA, Tufan EGEMEN
16:50 - 17:10		
52 **Parçacık Sürü Optimizasyonu Kullanarak DWT-SVD Tabanlı Resim Damgalama** Veysel ASLANTAŞ, Abdullatif DOĞAN, Rifat KURBAN	**59** **Cryptanalysis of Dedicated Hash Functions** Ali DOĞANAKSOY, Onur ÖZEN, Fatih SULAK, Kerem VARICI, Emre YÜCE	**47** **Cryptographic Instruction Set Processor Design** David MONTGOMERY, Ali AKOĞLU
17:10 - 17:30		
85 **Diferansiyel Gelişim Algoritması ile Tekil Değer Ayrışımına Dayalı Resim Damgalama** Veysel ASLANTAŞ, Ahmet ÖZ	**65** **On the Security of Encryption Mode of Tiger** Onur ÖZEN, Kerem VARICI	**46** **Multiple Error Detection in Block Ciphers** Krzysztof BUCHOLC, Ewa IDZIKOWSKA
17:30 - 17:50		
96 **Robust Video Watermarking Scheme in Transform Domains** Ersin ELBASİ, Ahmet M.ESKİCİOĞLU	**39** **Design and FPGA Implementation of Hash Processor** Murat AŞKAR, Tuğba ÇELEBİ ŞİLTU	**25** **Sprott_94_A Kaotik Sisteminin Senkronizasyonu ve Bilgi Gizlemede Kullanılması** İhsan PEHLİVAN, Yılmaz UYAROĞLU, Mehmet Ali YALÇIN, Abdullah FERİKOĞLU
17:50 - 18:10	**ÇAY / KAHVE ARASI -** TEA / COFFEE BREAK	
GRAND BALL ROOM III	GRAND BALL ROOM II	MAGNOLIA HALL FIRST FLOOR
18:10 - 18:30		
18 **Bilgi ve İletişim Teknolojilerinde Kişisel ve Kurumsal Bilgi Güvenliğinin Sağlanması** Köksal ÖZENÇ	**97** **Fault Tolerant Multiplication in the Finite Field GF(2k)** Silvana MEDOS, Serdar BOZTAŞ	**40** **E-imza'da Format Seçimi (XML, PDF'e karşı)** F. Koray ATSAN

1.gün firstday

13 Aralık December 2007 Perşembe Thursday

	GRAND BALL ROOM III	GRAND BALL ROOM II	MAGNOLIA HALL FIRST FLOOR
18:30 - 18:50	31 **Kurumsal Bilgi Güvenliği: Güncel Gelişmeler** Yılmaz VURAL, Şeref SAĞIROĞLU	53 **Secret Sharing Schemes and Linear Codes** Hakan ÖZADAM, Ferruh ÖZBUDAK, Zülfükar SAYGI	79 **Elektronik Döküman/Mektup'ların Kanıt Olabilmesi için Gereksinimler** İbrahim SOĞUKPINAR
18:50 - 19:10	98 **Application Of Information Security On Organizational Basis** **Bilgi Güvenliğinin Kurumsal Bazda Uygulaması** Şeref SAĞIROĞLU, Eren ERSOY, Mustafa ALKAN	43 **Key Exchange Protocol Using Encryption Scheme Provably Secure Against CCA** Jalaj KUMAR UPADHYAY	32 **The Level of Protection of E-sign Against Malware and Spyware** **Kötücül ve Casus Yazılımlara Karşı Elektronik İmzanın Sağlamış Olduğu Korunma Düzeyi** Gürol CANBEK, Şeref SAĞIROĞLU
19:10 - 19:30	41 **An Adaptive Security Policy Design and Management for Distributed Systems** Veli HAKKOYMAZ, İsmail ALAN	38 **On Meier-Staffelbach's Fast Correlation Attack** Esen AKKEMİK, Orhun KARA, Ayşegül KURŞUNLU	
19:30 -	**AÇILIŞ RESEPSİYONU** OPENING RECEPTION @ GRAND BALLROOM FOYER		

poster sunuşlar
poster presentations

GRAND BALL ROOM III

1.gün firstday | 13 Aralık December 2007 Perşembe Thursday

Mobil/Elektronik İmza
Mobile/Electronic Signature

080 · Çağdaş yönetişim sürecinde e-imza sisteminin rolü / A.MARŞAP

Mobil ve Elektronik İmza ile İlgili Çekişmeli Olaylar
Judgements Related to Mobile and Electronic Signatures

064 · Güvenli Elektronik Arşivleme: Standartlar, Yapılar ve İşlevler M.ÖZARAR, B.KIRIMER, M. Ö. DEMİRKOL

066 · Denizcilik Sektöründe Uydu Tabanlı İletişimin Bilgi Güenliği ve Şifrelenmesi Ö.KILIÇ, A.SOLAK, H.GERÇEKÇİOĞLU

Bilgi Güenliği
Information Security

007 · Kurumlar Üstü Bilgi Güenliği Stratejisi E.KUMAŞ

012 · The First Step in Improving Security Awareness: A Simple Self-assessment Framework / S. KONDAKCI

Kablosuz Güenlik
Wireless Security

022 · Kablosuz Sensör Ağlarda Güvenli Yönlendirme H. İ.TARHAN, Z. A. GÜRKAŞ, M. A. AYDIN

Ağ Güenliği
Network Security

071 · Topolojik Bağımlı Otomatik Sistem Güvenliği Tarama Yötemi / E.AKBAŞ

İnternet Güenliği
Internet Security

058 · Effectiveness of Two Factor Authentication for Preventing Fraudulent Transactions During Session Hijacking Attacks on Online Business F.UÇAR, Ş.ÇAKIR

E-Devlet Uygulamaları
E-government Applications

063 · T.C. Sanayi ve Ticaret Bakanlığı e-imza Uygulaması / F. K. ATSAN

2.gün seconday | 14 Aralık December 2007 Cuma Friday

Algoritmalar
Algorithms

057 · DSA Sisteminin Çalıştırılması ve Test Edilmesi Oğuz YAYLA

Steganografi
Steganography

028 · Spectral Estimation Methods: Comparison and Performance Analysis on a Steganalysis Application / T. MATARACIOĞLU, Ü. TATAR

Kriptoloji
Cryptology

074 · Improving Correlation Attacks on Stream Ciphers / S. BOZTAŞ, A. RAO, K. SRINIVASAN

Kriptanaliz
Cryptanalysis

082 · On Algebraic Attacks Using Groebner Basis Oğuz YAYLA, Hakan ÖZADAM

Verimli Kriptografi Yazılı ve Donanı Uygulamaları
Software and Hardware Implementations

061 · Rings of low multiplicative complexity and fast multiplication in finite fields $\mathbb{F}_{2^N}$ Murat CENK, Ferruh ÖZBUDAK

Blok Şifreleme Sistemleri
Block Ciphers

075 · Extended Linear Cryptanalysis and Extended Piling Up Lemma / S. BOZTAŞ, Q. LI

geleceğini koru!
secure the future!

2.gün seconday

14 Aralık December 2007 Cuma Friday

	GRAND BALL ROOM III	GRAND BALL ROOM II	MAGNOLIA HALL FIRST FLOOR
09:40 - 10:40	"The evolution of Mobile Signature Services around the world" Tapio VAILAHTI / FINLAND	Valimo VALUE IN MOBILE	BİLGİ GÜVENLİĞİ DERNEĞİ | Microsoft Katkılarıyla **TEMEL BİLGİ GÜVENLİĞİ KURSU** Bilgisayarınızı Koruyun! Kendinizi Koruyun! Ailenizi Koruyun! Kurumunuzu Koruyun!
10:40 - 11:00	**ÇAY / KAHVE ARASI -** TEA / COFFEE BREAK		
11:00 - 12:00	"Applying Mobile Signatures to New Generation Documents and Applications How to make PDF reliable, secure and legal valid" Peter KOERNER / GERMANY	Adobe	
12:00 - 13:00	**ÖĞLE YEMEĞİ** LUNCH		

	GRAND BALL ROOM III	GRAND BALL ROOM II	MAGNOLIA HALL FIRST FLOOR
13:00 - 13:20	**13** **A High Level Implementation of the RSEP Protocol** Süleyman KONDAKCI	**69** **PKI-Lite: a PKI System with Limited Resources** Oğuz YAYLA, Sedat LEYLEK	**70** **Anonymous Networked Group Communication: A Review and Meeting System Design** Gökhan DEMİREL, Gözde AYRANCI , Öznur ÖZKASAP
13:20 - 13:40	**42** **An Efficient Concealed Data Aggregation Scheme for Wireless Sensor Networks** Gwo BOA HORNG, Chien-Lung WANG, Tzung- Her CHEN	**87** **A New Hierarchical Signature Scheme with Authorization** Alper UĞUR, İbrahim SOĞUKPINAR	**78** **Ağ Kullanım Analizi ile Nüfuz Tespiti** Rahim KARABAĞ, Hidayet TAKÇI, İbrahim SOĞUKPINAR
13:40 - 14:00	**83** **Secure Load Balancing for Wireless Sensor Networks via Inter Cluster Relaying** Suat ÖZDEMİR	**68** **An Alternative Approach to A Particular Certificate Validation Problem in Tactical Domain** **Taktik Sahada Özel Bir Sertifika Doğrulama Problemine Alternatif Yaklaşım** A. BETÜL ŞAŞIOĞLU, Çağdaş CİRİT, Zerrin ÇAKMAKKAYA, Bülent ÖRENCİK	**67** **TCP SYN Seli Saldırılarının Bulanık Mantık Kullanarak Tespiti** Taner TUNCER, Yetkin TATAR
14:00 - 14:20	**ÇAY / KAHVE ARASI -** TEA / COFFEE BREAK		
14:20 - 15:20	"Applications of Coding and Information Theory in Cryptology and Information Security" Serdar BOZTAŞ / AUSTRALIA	RMIT University	
15:20 - 15:40	**ÇAY / KAHVE ARASI -** TEA / COFFEE BREAK		

2.gün seconday

14 Aralık December 2007 Cuma Friday

15:40 - 16:20	**AVEA Mobil İmza Uygulamaları** Ayşegül CEYDA YILDIRIM / TÜRKİYE	avea

UYGULAMA SUNUMLARI GOOD PRACTICES @ GRAND BALLROOM III

16:20 - 16:40	Mobil İmza'da Sertifika Hizmet Sağlayıcı Deneyimleri ve Gelecek	**Can ORHUN** E-Güven Genel Müdürü	E-GÜVEN
16:40 - 17:00	Kurumsal Bilgi ve Belge Güvenliğinde Uluslararası Uygulamalar	**Ümit KARAKAYA** Karakaya Group Yönetim Kurulu Başkanı	karakaya group
17:00 - 17:20	6110 TEKYAAS Taktik Emniyetli Yerel Alan Ağ Sistemi • 2112 GSM / 2049 USB Kripto Modülü	**Bikem TEMURCU** Aselsan A.Ş. HC Kripto ve Bilgi Güvenliği Müdürlüğü	aselsan
17:20 - 17:40	Futijsu PalmSecure Teknolojisi	**N. UTKU ALTUNKAYA** ETP Limited Ürün Müdürü	etb
17:40 - 18:00		**Aydemir ŞAMAN** Türkiye İş Bankası Bilişim Teknolojileri Grup Müdürü	TÜRKİYE İŞ BANKASI Türkiye'nin Bankası
18:00 - 18:30	**KAPANIŞ OTURUMU** CLOSING CEREMONY		

geleceğini koru!
secure the future!

Düzenleyen kuruluşlar
Conveners

TELEKOMÜNİKASYON KURUMU

1926 Gazi Üniversitesi

ODTÜ

Konferans Ofisi
Conference Office

cmsproject+ meeting people

www.iscturkey.org

Platin Sponsor
Platinum Sponsor

TURKCELL

Altın Sponsor
Gold Sponsor

avea

Gümüş Sponsor
Silver Sponsor

BİLGİ GÜVENLİĞİ DERNEĞİ

TÜRK TELE KOM

Katkılarıyla.

Organizasyon / Konferans Ofisi
Organization / Conference Office

cmsproject+

CMS
Kongre Yönetim Sistemleri
Uluslararası Organizasyon
Yayıncılık Bilişim Hizmetleri
Ltd. Şti.

Dedekorkut Sokak No.16/4
Çankaya 06690 Ankara / Turkey
Tel : +90 312 442 8845
Fax : +90 312 441 2984
E-mail : info@iscturkey.org
: info@cmsproject.org
www.cmsproject.org