Siber Güvenlik ve Savunma
Cyber Security and Defence

BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ KONFERANSI
ISC Turkey

5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı

5th International Conference on Information Security & Cryptology

17-18 Mayıs
May 2012

ODTÜ Kültür ve Kongre Merkezi
METU Culture and Congress Center
Ankara-TURKEY

Bilimsel Program
Scientific Programme

Düzenleyenler / Conveners

T.C. ULAŞTIRMA DENİZCİLİK VE HABERLEŞME BAKANLIĞI

BİLGİ GÜVENLİĞİ DERNEĞİ

Destekleyenler / In Collaboration with

BTK BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

ODTÜ

ISCTURKEY 2012 PROGRAM

1. gün first day 17 MAYIS MAY 2012 PERŞEMBE THURSDAY

09:00 -10:00 **KAYIT** REGISTRATION

09:45 -10:00 **ÇAY-KAHVE ARASI** TEA/COFFEE BREAK

10:00 -10:45 **AÇILIŞ VE PROTOKOL KONUŞMALARI** OPENING CEREMONY — **ANA SALON**/MAIN HALL - **KEMAL KURDAŞ**

Sn. Prof. Dr. Mustafa ALKAN
ISCTurkey Konferans Eşbaşkanı/Bilgi Güvenliği Derneği Başkanı *ISCTurkey Conference Chairman/Head of Information Security Association*

Sn. Dr. Tayfun ACARER
Bilgi Teknolojileri ve İletişim Kurumu Başkanı *President of Information Technologies and Communications*

Sn. Prof. Dr. Ahmet ACAR
ODTÜ Rektörü *Rector of METU*

Sn. Prof. Dr. Rıza AYHAN
Gazi Üniversitesi Rektörü *Rector of Gazi University*

Sn.Prof. Dr. Nejdet ÜNÜVAR
Türkiye Büyük Millet Meclisi (TBMM) Bilişim ve İnternet Komisyonu Başkanı *NGAT (National Grand Assembly of Turkey)*

Sn. Binali YILDIRIM
Denizcilik, Ulaştırma ve Haberleşme Bakanı *Minister of Transport, Maritime and Communications*

10:45 -11:00 **ÇAY-KAHVE ARASI** TEA/COFFEE BREAK

11:00 -12:00 **DAVETLİ KONUŞMACI** KEYNOTE SPEAKER — Oturum Başkanı Chairman **Prof. Dr. Ersan AKYILDIZ** METU, **Dr. Rodica TIRTEA** European Network and Information Security Agency - ENISA **Title:** European Perspective on National Information Security and Privacy

12:00 -13:00 **ÖĞLE ARASI** LUNCH BREAK

13:00 -14:45 **PANEL 1**

SİBER GÜVENLİK CYBER SECURITY
Oturum Başkanı Chairman
Prof. Dr. Şeref SAĞIROĞLU
Gazi University

Konuşmacılar Speakers

Prof. Dr. Nazife BAYKAL ODTÜ Enformatik Enstitüsü Müdürü / *Director of METU Informatics Institute*
Prof. Dr. Türksel BENGSHİR KAYA TODAEİ e-Devlet Merkezi Müdürü / *Director of e-Government Center*
Ömer TEKELİ EGM Bilişim Suçları Dairesi Başkanı / *Head of EGM Cyber Crime Department*
Bilge KARABACAK TÜBİTAK BİLGEM UEKAE Bilişim Sistemleri Güvenliği Bölümü Yöneticisi / *Director of Information System Security Department*
Ali YAZICI ASELSAN Kripto ve Bilgi Güvenliği Müdürü / *Director of Crypto and Information Security Department*
Temsilci, *Savunma Sanayi Müsteşarlığı*
Temsilci, *Ulaştırma, Denizcilik ve Haberleşme Bakanlığı*
Temsilci, *BTK*

14:45 -15:00 **ÇAY-KAHVE ARASI** TEA/COFFEE BREAK

15:00 -15:45 **DAVETLİ KONUŞMACI** KEYNOTE SPEAKER — Oturum Başkanı Chair **Prof.Dr. Fatoş Tünay Yarman VURAL** METU**, Prof. Dr. Nasır MEMON** Director of the Information Systems and Internet Security (ISIS) Laboratory **Title:** Biometric Rich Gestures: A Touching Farewell To Passwords?

15:45 -16:30 **DAVETLİ KONUŞMACI** KEYNOTE SPEAKER — **Joshua MARPET** Data Devastation **Title:** Gaming the Digital Forensics System

16:30 -18:00

ÇALIŞTAY 1 WORKSHOP
BİLGİ GÜVENLİĞİ STK TOPLANTISI MEETING of INFORMATION SECURITY CSOs

Başkan Chairman
Prof. Dr. Mustafa ALKAN
BGD Başkanı
ISA President of Turkey

SALON HALL A

OTURUM SESSION 1:**AĞ GÜVENLİĞİ** NETWORK SECURITY
Oturum Başkanı Session Chairman:
Prof.Dr. Ali YAZICI, Atılım University

36 Ipv6 Ağlarda Solucan Dağılım Saldırıları ve Önlemler Uraz YAVANOĞLU* (Gazi Üniversitesi), Suat ÖZDEMIR (Gazi Üniversitesi), Şeref SAĞIROĞLU (Gazi Üniversitesi)

34 An Application Of Decision Trees In Intrusion Detection Atilla ÖZGÜR* (ISKUR), Hamit ERDEM (Başkent Üniversitesi)

52 A Two-Layer Fuzzy Genetic Algorithm for Designing Intrusion Detection System Ghazaleh JAVADZADEH* (Sharif University of Technolog),Reza AZMİ

39 Radius Regularization using Learning Automata for Spherical Intelligent Anomaly Detectors Neda AFZALI* (Alzahra University), Reza AZMI, Boshra PISHGOO

SALON HALL B

OTURUM SESSION 2:**SİBER GÜVENLİK** CYBER SECURITY
Oturum Başkanı Session Chairman:
Yrd.Doç.Dr./Assist.Prof.Dr. Murat KOYUNCU, Atılım University

43 Topic-Based Probabilistic Approach to Criminal Network for Suspect Investigation Arzu KAKIŞIM*, (Gebze Yüksek Teknoloji Enstitüsü) İbrahim SOGUKPINAR (Gebze Yüksek Teknoloji Enstitüsü)

67 Bilişim Suçlarında Delillendirme Çağlar ULKUDERNER* (Profelis Bilişim)

69 Siber Güvenlik Makro Analiz Modeli Önerisi ve Türkiye'nin Analizi Hakan ŞENTÜRK* (KHO Savunma Bilimleri Enstitüsü), Celal Zaim ÇİL (Çankaya Üniversitesi),Şeref SAĞIROĞLU (Gazi Üniversitesi)

76 Operating System Evaluation Using Choquet Integral in Terms of Cyber Threats Kerim GÖZTEPE* (War Colleges Command, Army War College), Ahmet EJDER (War Colleges Command)

87 Siber Güvenlik Persfektifinden Makineler Arası İletişim Uygulamalarının İncelenmesi Alper ÖZBİLEN (BTK-TİB), İlhami ÇOLAK (Gazi Üniversitesi), Şeref SAĞIROĞLU (Gazi Üniversitesi)

SALON HALL C

ÇALIŞTAY WORKSHOP 2: **YAN KANAL ANALİZİ ve GÖMÜLÜ SİSTEMLER**
SIDE ANALYSIS and EMBEDED SYSTEMS
Başkan Chair: **Doç. Dr. Sıddıka Berna Örs Yalçın**

Konuşmacılar Speakers

Elif Bilge Kavun
Lightweight Cryptography - What do we really mean by "Lightweight"?
Ahmet Arış
High Speed RSA Implementation
Dr. Amir Moradi
Implementation Attacks against Real-World Targets
David Oswald
Hands-on Side Channel Attacks against Smart Cards and Other Tokens
Dr. Tolga Yalçın
Use of Hardware as a Mathematical Cryptanalysis Tool

SALON HALL D

OTURUM SESSION 3: **BİLGİ GÜVENLİĞİ** INFORMATION SECURITY
Oturum Başkanı Session Chairman:
Y. Doç. Dr./ Asst. Prof. Dr. **Sedat AKLEYLEK Samsun 19 Mayıs Üni.**

48 Güvenli Q Sürü Bellek Yazılım Yongası Üreten Dilbilim Örneği Fevzi ÜNLÜ* (Ege ve Yaşar University)

49 Cycle Counting For Information Security in I@I Swarm Internet Generating Q Swarm Memory Fevzi ÜNLÜ* (Ege ve Yaşar University)

62 Metin ve Grafiksel Öğeleri Birleştiren Yeni bir Parola Tabanlı Kimlik Doğrulama Yöntemi Murat AKPULAT (Gümüşhane Üniversitesi), Kemal BICAKCI* (TOBB/ETÜ), Ugur CİL (TOBB/ETU)

75 Covert Channels Detection using Process Mining Amir Jalaly BIDGOLY* (University of Isfahan), Behrouz Tork LADANI (University Of Isfahan), Ahmad Baraani DASTJERDI (University of Isfahan)

83 Information and Computer Security Awareness of Elementary and High School Students: Sample of Kahramanmaraş City Mehmet TEKEREK* (KSU)

SALON HALL E

OTURUM SESSION 4: **KABLOSUZ AĞLARDA GÜVENLİK** SECURITY IN WIRELESS NETWORKS
Oturum Başkanı Session Chairman:
Doç. Dr. /Assoc. Prof. Dr. **Ali Aydın SELÇUK** Bilkent Üni.

5 On Applications of Privacy-Preserving Collaborative Filtering Schemes Alper BİLGE, Cihan KALELİ, İbrahim YAKUT, Hüseyin POLAT* (Anadolu Üniversitesi)

17 Kablosuz Algılayıcı Ağlarda Güvenli Ortam Erişim Protokolleri Feyza Yıldırım OKAY* (Gazi Üniversitesi), Suat OZDEMIR (Gazi Üniversitesi)

19 Anonymous RFID Authentication Protocol Without a Trusted Party Muhammed Ali BİNGÖL* (TUBITAK BILGEM UEKAE), Mehmet Sabir KİRAZ (TUBITAK BILGEM), Suleyman KARDAS (TUBITAK BILGEM UEKAE), Fatih BİRİNCİ(TUBITAK BILGEM)

72 Recommender System Based on Group Trust Somayeh NAGHSBANDI* (Isfahan University), Behrouz Tork LADANI (University of Isfahan)

SALON HALL F

16:30-18:00 **FİRMA SUNUMLARI**

16:30-18:00 **Ağlarda Yeni Güvenlik Tehtidleri, Akın TOSUNLAR,** VİGASİS

17:00-17:15 **Adli Bilişim ve Sayısal Sahtecilik (Elektronik Belgede Tarih Değiştirme) Özgür YURDUSEV,** VİGASİS

17:15-18:00 **Desktop Sanallaştırma ile Veri Güvenliği Sağlama, Levent TOPRAK** HUAWEI

13:00 -18:00

FUAYE / FOYER

POSTER ALANI
POSTER OTURUMU
POSTER SESSION

13:00-18:00
FUAYE FOYER

1 Ipv6 Security Vulnerabilities
Harith DAWOOD* (Cihan University)

15 Digital Watermarking Enhancement for Satellite Images Using a DCT Algorithm
Mustafa ABUGHARSA* (Misurata University), Mohamed SULLABI (Misurata University), Alhusain TAHER (Misurata University)

44 Enhancing SIEM Correlation Rules Through Baselining Ertuğrul AKBAŞ* (ANET)

33 Encrypted Individual Multiple Choice Questions Mehtap Kose ULUKOK* (Cyprus International University), Zehra Boratas ŞENSOY (Cyprus International University)

63 Şifrelemenin Modellenmesi ve Modern Kriptosistemin Tasarımı Erkan BAYAR* (Marmara Üni.), Hakan KAPTAN (Marmara Üni.)

71 Casus Yazılımların Bilgisayar Sistemlerine Bulaşma Belirtileri ve Çözüm Önerileri
Resul DAŞ* (Fırat Üniversitesi), Şahin KARA (Sakarya Üniversitesi)

18 Sazan Avlama (Phishing): Kullanılan Teknikler ve Bunlardan Korunma Yöntemleri
Ali ŞENOL* (Gazi Üniversitesi), Hacer KARACAN (Gazi Üniversitesi)

23 Server Based Encryption (SERBASEN)Protocol on Air Gap Network Ahmet AYŞAN* (Turkish Air Force Academy), Güray YILMAZ

37 Utilizing a Graphical User Interface for Image Encryption based on Chaotic Algorithm Hidayet OĞRAŞ* (Batman University), Mustafa TÜRK (Fırat University) Thanh Viet PHAM

41 Security Directions in Cloud Computing Environments
Zeynab Abbasi KHALİFELU (Islamic Azad University), Farhad Soleimanian GHAREHCHOPOGH* (Hacettepe University)

82 Akıllı Şebekelerde Siber Güvenlik ve Mahremiyet
Elif Üstündağ SOYKAN* (TÜBİTAK), Seda Demirağ ERSÖZ

ISCTURKEY 2012 PROGRAM

2. gün second day 18 MAYIS MAY 2012 CUMA FRIDAY

10:00 -12:00

SALON MAIN HALL: KEMAL KURDAŞ

10:00 -10:10 **ABOUT ISCISC'12** — Dr. Mohammad Taghi Alavi, Honorary chair of ISCISC'12 (9th International Conference on Information Security and Cryptology IRAN

10:10 -11:00 **EĞİTİM** — Ulusal Bilgi Güvenliğinde Log Yönetiminin Önemi Akın SAĞBİLGE, CRYPTECH

11:10 -12:00 **FİRMA SUNUMU** — Ağ Güvenliği ve Güvenlik Çözümleri HUAWEI

SALON HALL A

OTURUM SESSION 5:
KRİPTOGRAFİK PROTOKOLLER FOUNDATIONS OF CRYPTOGRAPHY **Oturum Başkanı**
Session Chairman: **Y. Doç. Dr./Asst. Prof. Dr. Zülfikar SAYGI, METU**

20 Elektronik Seçim: Norveç'in İnternet Üzerinden Oylama Sistemi ve Kriptografik Altyapısı,
Uğur BOYACİ* (TÜBİTAK BİLGEM), Fatih BİRİNCİ (TUBITAK BILGEM), Mehmet Sabir KİRAZ (TÜBİTAK BİLGEM)

66 Compressed Data Public Key Cryptosystems with DLP Over Extension Fields, Muhammad ASHRSF* (METU), Baris KIRLAR (Suleyman Demirel University)

42 Optimal Control Formulation of Query Model for Authentication Systems, Ali SEZER* (METU), Ferruh OZBUDAK (METU), Ustun YILDIRIM (METU)

73 On The Use Of Continued Fractions For Mutual Authentication, Amadou KANE* (Université Laval)

77 Formalization of Blind Signature Using the Inductive Method, Najmeh Sadat MIRAMIRKHANI* (Sharif University of Technolog) Rasool JALILI (Sharif University of Thechmilogy)

SALON HALL B

OTURUM SESSION 6:
KRİPTOANALİZ CRYPTANALYSIS **Oturum Başkanı** Session Chairman:
Doç.Dr./Assoc. Prof. Dr. Ali DOĞANAKSOY, METU

21 Notes on Bent Functions in Polynomial Forms,
Nese OZTOP* (METU) Onur KOCAK (METU) Zulfukar SAYGI (TOBB ETU) Onur KURT (METU)

28 Security Margin of 5-Round DEAL, Orhun KARA* (TÜBİTAK BİLGEM UEKAE)

47 How Biased Are Linear Biases?,
Orhun KARA* (TÜBİTAK BİLGEM UEKAE) Adnan BAYSAL (TÜBİTAK BİLGEM UEKAE)

SALON HALL E

BİLGİ GÜVENLİĞİ INFORMATION SECURITY
Oturum Başkanı Session Chairman: **Yrd.Doç.Dr./Assist.Prof.Dr. Sinan KALKAN,** METU
10:00-10:30 **Siber Tehditlere karşı Bilgi Güvenliği Bilinci Oluşturma ve Eğitim Yöntemleri, Murat AYTUN,** HRIKA Genel Müdürü
10:30-11:00 **VoIP Güvenlik Uyumluluğu: VoIP'i Ağ Güvenlik Planlamasına Dâhil Etmek, Melih TAŞ,** NETAŞ
11:00-11:30 **SIP Saldırı Teknikleri ve Savunma Yöntemleri, Eren AKÇA, Gülten DOĞANÇ,** NETAŞ

SALON HALL C

SİBER GÜVENLİK ve SAVUNMA KOORDİNASYON KURULU TOPLANTISI
CYBER SECURITY and DEFENCE COORDINATION BOARD MEETING
Eş Başkanlar Chairs **Prof. Dr. Ersan AKYILDIZ, Prof.Dr. Şeref SAĞIROĞLU**

Not: Bu toplantı herkese açık değildir.
Sadece davetli kurul üyeleri katılabilecektir.
Note: Only the Board Members Can Attend This Meeting.

SALON HALL D

OTURUM SESSION 7:
KULLANIŞLI GÜVENLİK ve STEGANOGRAFİ
USABLE SECURITY and STEGANOGRAPHY **Oturum Başkanı** Session Chairman:
Prof. Dr. Ziya AKTAŞ, Başkent University

68 Frei-Chen Maskeleri Tabanlı Yeni Bir Sır Paylaşım Tekniği, Veysel ASLANTAS (Erciyes Üniversitesi), Ebubekir KAYA* (Nevşehir Üniversitesi)

27 Gizli Görüntü Paylaşımında Kullanılan Eşik Şemalarının Performans Değerlendirilmesi,
Guzin ULUTAS* (Karadeniz Teknik Üniversitesi), Mustafa ULUTAS (Karadeniz Teknik Üniversitesi), Vasif NABIYEV (Karadeniz Teknik Üniversitesi)

46 An Imperceptible Watermarking Scheme based on Double Density Dual-Tree Discrete Wavelet Transform in combination with Singular Value Decomposition,
Mary AGOYI* (Cyprus International University), Devrim SERAL (Cyprus International University)

SALON HALL F

UYGULAMALI SUNUMLAR

10:00-11:00 **Fiziksel Güvenlik Çözümleri ile Kamu Güvenliği Sağlama, Fatih ERİKÇİ, HUAWEI**
11:00-12:00 **Phone2DOS – SIP Üzerinden Yeni Bir Saldırı Yöntemi ve Öneriler, Barış DİNLER, VİGASİS**

12:00 -13:00 **ÖĞLE YEMEĞİ** LUNCH BREAK

13:00 -15:00 **EĞİTİM** — KEP Özelinde Kritik Altyapı Güvenliği ve Entegre Yönetim Sistemleri, **Aysun TUNCER,** BGD Üyesi / ARMONES — SALON MAIN HALL: **KEMAL KURDAŞ**

15:00 -15:20 **ÇAY-KAHVE ARASI** TEA/COFFEE BREAK

SALON HALL C

ÇALIŞTAY WORKSHOP

ELEKTRONİK NOTER ve SİBER GÜVENLİK UYGULAMALARI E-NOTARY and CYBER SECURITY APPLICATIONS

Başkan Chairman
Yıldız BARLAS, BGD Yönetim Kurulu Üyesi

Konuşmacılar Speakers

Prof. Dr. Şebnem AKİPEK, Ankara Üniversitesi Hukuk Fakültesi
Doç. Dr. Leyla KESER BERBER, Bilgi Üniversitesi
Cengiz TANRIKULU, Adalet Bakanlığı
Orhan TURAN, Ankara 56. Noteri
Pınar ÜNALÇIN, Durağan Noteri

SALON HALL E

BİLGİ GÜVENLİĞİ SEKTÖR TOPLANTISI MEETING of SECTOR REPRESENTATIVES
Başkan Chairman:
Prof. Dr. Mustafa ALKAN, BGD

SALON HALL F

BGD GENÇ ÜNİVERSİTE TEMSİLCİLERİ TOPLANTISI MEETING of ISA YOUTH UNIVERSITY REPRESENTATIVES
Başkan Chairman:
Ezgi CANKURTARAN

SALON HALL A

OTURUM SESSION 8: **KRİPTOGRAFİNİN TEMELLERİ** FOUNDATIONS OF CRYPTOGRAPHY **Oturum Başkanı**
Session Chairman: **Doç. Dr./Assoc. Prof. Dr. Melek Diker YÜCEL, METU**

25 Hermite Polynomial Representation for Finite Fields Of Characteristic Three
Canan ÖZEL* (METU) Sedat AKLEYLEK (19 Mayis University), Ferruh OZBUDAK (METU)

50 Alternate Models of Elliptic Curves: A Survey Baris KIRLAR* (Suleyman Demirel University), Muhammad ASHRSF (METU)

61 Optimal Frekans Atlamalı Diziler Seda KAHRAMAN* (TOBB ETÜ), Zulfukar SAYGI (TOBB ETÜ)

70 Cyclotomic Sayılar ve Sidel'nikov Dizileri Kamil OTAL* (TOBB ETU), Zulfukar SAYGI (TOBB ETÜ), Çetin ÜRTİŞ (TOBB ETÜ)

SALON HALL B

OTURUM SESSION 9: **KRİPTOANALİZ** FOUNDATIONS OF CRYPTOGRAPHY **Oturum Başkanı** Session Chairman: **Ferruh ÖZBUDAK, METU**

79 A Scalable Platform for Cryptanalysis of Computationally Intensive Algorithms
Hakan SOLMAZ* (Aselsan), Hasan ERDOĞAN (Aselsan), Rıza AYKAÇ (Aselsan)

81 A Proposed Attacking Method on Rabin's Cryptosystem
Sattar B SADKHAN * (University of Babylon)

24 Dinamik S-box Tabanlı Blok Şifrelerin Diferansiyel Kriptanalizi
Fatih ÖZKAYNAK* (Fırat University), Ahmet ÖZER (Fırat Üniversitesi), Sırma YAVUZ (Yıldız Teknik Üniversitesi)

26 Success Probability of The First Attack on Full Round GOST
Orhun KARA* (TÜBİTAK BİLGEM UEKAE), Ferhat KARAKOÇ (TÜBİTAK BİLGEM UEKAE)

SALON HALL D

OTURUM SESSION 10: **BİLGİ GÜVENLİĞİ** INFORMATION SECURITY **Oturum Başkanı** Session Chairman: **Dr.Orhun KARA** TÜBİTAK-BİLGEM

35 CAPTCHA Metinler için YSA Tabanlı Örüntü Tanıma Yaklaşımı
Uraz YAVANOGLU* (Gazi Üniversitesi) Begum MUTLU (Gazi Üniversitesi) Esra SAHİN (Gazi Üniversitesi)

56 Radyo Link ve Uydu Ağları Üzerinde Gelecek Nesil Dar Bant Terminal ile Yapılan Güvenli Haberleşme Test Sonuçları ve Değerlendirilmesi
Orkun DİLLİ* (Hv.Tek.Okl.K.lığı) Nursel AKÇAM (Gazi Üniversitesi) Murat KOYUNCU (Atılım Üniversitesi)

86 Kayıtlı Elektronik Posta Sistemi ve E-Posta Güvenliği
Mustafa ALKAN* (Gazi Üniversitesi), Mustafa ÜNVER (BTK), Hakan TEKEDERE (Gazi Üniversitesi)

ÇALIŞTAY WORKSHOP 3

Ana Salon Main Hall **KEMAL KURDAŞ**

SİBER SAVUNMA CYBER DEFENSE

Başkan Chairman
Ali YAZICI
BGD YK Üyesi
ASELSAN Kripto ve Bilgi Güvenliği Müdürü

Konuşmacılar Speakers

Ali IŞIKLI, ASELSAN
Bülent SOYDAL, HAVELSAN
Bülent BÜYÜKKAHRAMAN, NETAŞ
Dr. Atilla ÖZGİT, ODTÜ
Aysun TUNCER, BGD YK Üyesi
Dr. Sedat AKLEYLEK, Ondokuz Mayıs Üniversitesi
Ahmet KAPLAN, BGD Üyesi/ULAKBİM
Hakan YILDIRIM, BGD Üyesi/TBMM
Volkan ÖZTÜRK, BGD Üyesi/RTÜK,
Volkan KAPLAN, BGD Üyesi / Gümrük Müsteşarlığı Bilgi İşlem Dairesi Başkanı
S.Barış DİNLER, VIGASİS
Dr. Kerim GÖZTEPE, Harp Akademileri Komutanlığı
Dr. Gökhan ÖZBİLGİN, SPK
Burak ÇİFTER, BGD İstanbul Temsilci Yrd.
M. Ali İNCEEFE, BGD YK Üyesi

SALON HALL A

ÇALIŞTAY WORKSHOP

ADLİ BİLİŞİM VE SAYISAL SAHTECİLİK DIGITAL FORENSICS and FRAUD

Başkan Chairman:
Prof. Dr. F. Tünay Yarman VURAL, ODTÜ

Konuşmacılar Speakers

Emrehan HALICI, Milletvekili, ***Adli Bilişim için Kurumsal Gelişim***
Prof. Dr. Ufuk ÇAĞLAYAN, Boğaziçi Üniversitesi, ***Elektronik Delil Ne Demektir ve Klasik Delilden Farkı Nedir?***
Osman Nihat ŞEN, TİB Internet Daire Başkanı, **Hukukçuların ve Adli Bilişim Uzmanlarının Eğitimi**
Mehmet ORAL, İstanbul Barosu Avukatı, **Türk Adalet Sisteminde Elektronik Delil Kullanımı ve Karşılaşılan Sorunlar**
Prof. Dr. Vahit BIÇAK, Polis Akademisi, **Türkiye'de ve Dünyadaki Elektronik Delil Yasalarının Karşılaştırılması**

SALON HALL B

OTURUM SESSION 11: **KRİPTOGRAFİK DONANIMLAR ve KUANTUM KRİPTOGRAFİ** CRYPTOGRAPHIC HARDWARE and QUANTUM CRYPTOGRAPHY **Oturum Başkanı** Session Chairman: Dr. Tolga YALÇIN

30 Kuantum Anahtar Dağıtımında (KAD) Gizli Anahtar Uzlaştırma: CASCADE Protokolü ve LDPC Kodları Mustafa TOYRAN* (TÜBİTAK), Burcu KORKMAZ (Ege Üniversitesi), Thomas PEDERSEN (TÜBİTAK), A. S. Atilla HASEKİOĞLU (TÜBİTAK), Pars MUTAF (Ege Üniversitesi), M. Ali CAN (TÜBİTAK)

45 A True Random Number Generator and Test Platform Built in FPGA
Salih YILDIRIM* (ASELSAN), Cuneyt BAZLAMACCI

59 Quantum Random Number Generators Mustafa TOYRAN (TÜBİTAK), Thomas PEDERSEN* (TÜBİTAK), A. S. Atilla Hasekioğlu (TÜBİTAK), M. Ali CAN (TÜBİTAK), Fikret HACIZADE (TÜBİTAK)

SALON HALL F

OTURUM SESSION 12:
BİLGİ GÜVENLİĞİNDE YENİ YAKLAŞIMLAR NEW APPROACHES TOWARDS INFORMATION SECURITY
Başkan Chairman: **Dr.Mehmet Sabir KİRAZ, TÜBİTAK-BİLGEM**

SALON HALL D

GÜVENLİK UZMANLAR KURULU TOPLANTISI BOARD MEETING of SECURTIY EXPERTS
Başkanı Chairman **Alper ÖZBİLEN, BGD**
Başkan Yardımcısı Vice Chairman **Ersen ELMAOĞULLARI, SYMANTEC**
Başkan Yardımcısı Vice Chairman **Uraz YAVANOĞLU, Gazi Üniversitesi**

22 On the Random Oracle Model and the Game Hopping Technique Turgut HANOYMAK* (METU), Murat AK (Bilkent University)	**65 Burke Shaw Kaotik Sisteminin Güvenli Haberleşme İçin Elektronik Devre Gerçeklemesi ve Senkronizasyon Uygulaması** İsmail Koyuncu* (Düzce Üniversitesi), Yılmaz UYAROĞLU (Sakarya Üniversitesi), İhsan PEHLİVAN (Sakarya Üniversitesi)
31 Oyun Teorisi Kullanılarak Bulut Bilişimde Ölçeklendirebilir Güvenlik Değerlendirmesi Evrim FURUNCU* (Gebze Institute of Technology), Ibrahim SOGUKPINAR (Gebze Institute of Technology)	**10 DSAB – An Efficient Approach for Security in MANET** Rahul Saha* (Lovely Professional University), Gulshan SHARMA (Lovely Professional University), Mritunjay RAI (Lovely Professional University)

KONFERANS ve ÇALIŞTAY BAŞKANLARI DEĞERLENDİRME TOPLANTISI CONFERENCE and WORKSHOP EVALUATION MEETING

KAPANIŞ CLOSING CEREMONY