ISCTURKEY 2007 SÖZLÜ BİLDİRİLERİ

Generalized ID-Based ElGamal Signatures with Message Recovery Said Kalkan, Kamer Kaya, and Ali Aydın Selçuk TIKLAYINIZ	An Identity-Based Key Infrastructure Suitable for Messaging Applications Ayşe Gül Karatop and Erkay Savas TIKLAYINIZ
Mobil Elektronik İmza: Ülkeler ve Uygulamalar Şeref SAĞIROĞLU, Demet KABASAKAL, Mustafa ALKAN TIKLAYINIZ	Comparing Substitution Boxes of the Third Generation GSM and Advanced Encryption Standard Ciphers Sedat Akleylek, Melek D. Yücel TIKLAYINIZ
A New Hierarchical Signature Scheme With Authorization Alper UĞUR, İbrahim SOĞUKPINAR TIKLAYINIZ	A New Approach to Keystream Based Cryptosystems Imran Erguler, Orhun Kara TIKLAYINIZ
Mobil Elektronik İmza: Senaryolar, Uygulamalar, Standartlar ve Ülkeler Demet KABASAKAL, Şeref SAĞIROĞLU, Mustafa ALKAN TIKLAYINIZ	Key Exchange Protocol Using Encryption Scheme Provably Secure Against CCA Jalaj Kumar Upadhyay TIKLAYINIZ
PKI-Lite: A PKI System with Limited Resources Oğuz Yayla, Sedat Akleylek TIKLAYINIZ	Security on Mobile Phones with Lightweight Cryptographic Message Syntax Murat Yasin KUBILAY, Albert LEVİ, Atilla ÖZGİT TIKLAYINIZ
A High Level Implementation of the RSEP Protocol Suleyman Kondakci TIKLAYINIZ	Bilgi ve İletişim Teknolojilerinde Kişisel ve Kurumsal Bilgi Güvenliğinin Sağlanması Köksal ÖZENÇ TIKLAYINIZ
E-imza'da Format Seçimi (XML, PDF'e karşı) F. Koray ATSAN TIKLAYINIZ	Kurumsal Bilgi Güvenliği: Güncel Gelişmeler Yılmaz VURAL, Şeref SAĞIROĞLU TIKLAYINIZ
Elektronik Doküman/Mektup'ların Kanıt Olabilmesi için Gereksinimler İbrahim SOĞUKPINAR TIKLAYINIZ	Bilgi Güvenliğinin Kurumsal Bazda Uygulanması Şeref SAĞIROĞLU, Eren ERSOY, Mustafa ALKAN TIKLAYINIZ
Ters Haritalama Tabanlı S-kutularının Cebirsel Açıdan iyileştirilmesi M. Tolga SAKALLI, Ercan BULUT, Andaç ŞAHİN, Fatma BÜYÜKSARAÇOĞLU, Ahmet KARADENİZ TIKLAYINIZ	Sayısal Görüntülerdeki Yerel Parlaklık Değişimine Dayalı Adaptif Steganografi M. Ulutaş, V.V.Nabiyev, G.Ulutaş TIKLAYINIZ
Design and FPGA Implementation of Hash Processor Murat Aşkar, Tuğba Şıltu Çelebi	Parçacık Sürü Optimizasyonu ile DWT-SVD Tabanlı Resim Damgalama Veysel Aslantaş, Abdullatif Doğan, Rifat Kurban

TIKLAYINIZ	TIKLAYINIZ
Fault-Tolerant Lagrange Representation Multiplication in the Finite Field GF(2k) Silvana Medo, Serdar Boztas TIKLAYINIZ	Diferansiyel Gelişim Algoritması ile Tekil Değer Ayrışımına Dayalı Resim Damgalama Veysel Aslantas, Ahmet Öz TIKLAYINIZ
New Findings on the Covering Sequence of Boolean Functions Güzin Kurnaz TIKLAYINIZ	Robust Video Watermarking Scheme in Transform Domains Ersin Elbasi, Ahmet M. Eskicioglu TIKLAYINIZ
Secret Sharing Schemes and Linear Codes Hakan Özadam, Ferruh Özbudak and Zülfikar Saygı TIKLAYINIZ	Sprott_94_A Kaotik Sisteminin Senkronizasyonu ve Bilgi Gizlemede Kullanılması İhsan Pehlivan, Yılmaz Uyaroğlu, M. Ali Yalçın, Abdullah Ferikoğlu TIKLAYINIZ
On Meier-Staffelbach's Fast Correlation Attack Esen Akkemik, Orhun Kara, Ayşegül Kurşunlu TIKLAYINIZ	An Adaptive Security Policy Design and Management for Distributed Systems Veli Hakkoymaz, İsmail Alan TIKLAYINIZ
Hash Function Designs Based on Stream Ciphers Meltem Sönmez Turan, Özgür Özuğur and Onur TIKLAYINIZ	An Efficient Concealed Data Aggregation Scheme for Wireless Sensor Networks Gwoboa Horng, Chien-Lung Wang and Tzung-Her Chen TIKLAYINIZ
Cryptanalysis of the Dedicated Hash Functions Ali Doğanaksoy, Onur Özen, Fatih Sulak, Kerem Varıcı, Emre Yüce TIKLAYINIZ	Secure Load Balancing for Wireless Sensor Networks via Inter Cluster Relaying Suat Özdemir TIKLAYINIZ
On the Security of the Encryption Mode of Tiger Onur Özen, Kerem Varıcı TIKLAYINIZ	TCP SYN Seli Saldırılarının Bulanık Mantık Kullanarak Tespiti Taner Tuncer, Yetkin Tatar TIKLAYINIZ
Multiple Error Detection in Block Ciphers K. Bucholc, E.Idzikowska TIKLAYINIZ	Ağ Kullanım Analizi ile Nüfuz Tespiti Rahim Karabağ, Hidayet Takçı, İbrahim Soğukpınar TIKLAYINIZ
Cryptographic Instruction Set Processor Design David Montgomery, Ali Akoglu TIKLAYINIZ	Kötücül ve Casus Yazılımlara Karşı Elektronik İmzanın Sağlamış Olduğu Korunma Düzeyi Gürol CANBEK, Şeref SAĞIROĞLU, Gazi Üniversitesi TIKLAYINIZ
Design and SystemC Implementation of a Crypto Processor for AES and DES Algorithms M. Aşkar, T.Egemen TIKLAYINIZ	Taktik Sahada Özel Bir Sertifika Doğrulama Problemine Alternatif Yaklaşım A. Betül Şaşıoğlu, Çağdaş Cirit, Zerrin Çakmakkaya, Bülent Örencik TIKLAYINIZ

	Anonymous Networked Group Communication: A Review and Meeting System Design Gokhan Demirel, Gozde Ayranci and Oznur Ozkasap TIKLAYINIZ