Doç. Dr. CİHANGİR TEZCAN

Kişisel Bilgiler

E-posta: cihangir@metu.edu.tr
Web: https://cihangir.forgottenlance.com

Uluslararası Araştırmacı ID'leri
ScholarID: IeCTf2IAAAAJ
ORCID: 0000-0002-9041-1932
Publons / Web Of Science ResearcherID: D-1331-2010
ScopusID: 24447139500
Yoksis Araştırmacı ID: 192349

Eğitim Bilgileri

Doktora, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi Anabilim Dalı, Türkiye 2009 - 2014
Yüksek Lisans, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi Anabilim Dalı, Türkiye 2007 - 2009
Lisans, Orta Doğu Teknik Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, Türkiye 2003 - 2007

Yabancı Diller

İngilizce, C2 Ustalık
Almanca, B2 Orta Üstü
Fransızca, B2 Orta Üstü
Portekizçe, B2 Orta Üstü

Yaptığı Tezler

Doktora, Improbable differential cryptanalysis, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi Anabilim Dalı, 2014
Yüksek Lisans, Impossible differential cryptanalysis of reduced round HIGHT, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi Anabilim Dalı, 2009

Araştırma Alanları

Bilgi Sistemleri, Haberleşme ve Kontrol Mühendisliği, Paralel Algoritmalar , Bilgi Güvenliği ve Güvenilirliği, Kriptoloji, Kuantum Kriptografi, Bilgisayar Ağları, Cebirsel Geometri, Kombinatorik, Olasılık Kuramı, Stokastik Süreçler, Sayılar Kuramı, Sayısal Analiz

Akademik Unvanlar / Görevler

Doç. Dr., Orta Doğu Teknik Üniversitesi, Enformatik Enstitüsü, Siber Güvenlik Anabilim Dalı, 2022 - Devam Ediyor
Dr. Öğr. Üyesi, Orta Doğu Teknik Üniversitesi, Enformatik Enstitüsü, Siber Güvenlik Anabilim Dalı, 2019 - 2022

Araştırma Görevlisi, Orta Doğu Teknik Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, 2011 - 2019
Dr. Öğr. Üyesi, Ruhr-Universitaet Bochum, Matematik, 2017 - 2018
Araştırma Görevlisi, Ecole Polytechnique Federale De Lausanne, Computer And Communication Sciences, 2010 - 2011
Araştırma Görevlisi, Orta Doğu Teknik Üniversitesi, Uygulamalı Matematik Enstitüsü, Kriptografi Anabilim Dalı, 2008 - 2010

Akademik İdari Deneyim

Enstitü Yönetim Kurulu Üyesi, Orta Doğu Teknik Üniversitesi, Enformatik Enstitüsü, Siber Güvenlik Anabilim Dalı, 2022 - Devam Ediyor
Anabilim/Bilim Dalı Başkanı, Orta Doğu Teknik Üniversitesi, Enformatik Enstitüsü, Siber Güvenlik Anabilim Dalı, 2020 - Devam Ediyor
Uygulama ve Araştırma Merkezi Müdürü, Orta Doğu Teknik Üniversitesi, Rektörlük, Siber Savunma ve Güvenlik Uygulama ve Araştırma Merkezi, 2020 - Devam Ediyor

Yönetilen Tezler

Tezcan C., FPGA-friendly compact and efficient AES-like 8x8 S-Box, Yüksek Lisans, A.MALAL(Öğrenci), 2023
Tezcan C., A permissioned blockchain-based model for digital forensics, Yüksek Lisans, N.ALIZADEH(Öğrenci), 2023
Tezcan C., Compact and flexible NTRU implementation on FPGA, Yüksek Lisans, S.EMİR(Öğrenci), 2022
Tezcan C., Detecting android obfuscation methods with LSTM, Yüksek Lisans, B.ULUKAPİ(Öğrenci), 2022
Tezcan C., DIFFERENTIAL-LINEAR CRYPTANALYSIS OF ASCON AND DRYGASCON, Yüksek Lisans, A.BAŞAK(Öğrenci), 2021
Tezcan C., Impossible and improbable differential cryptanalysis of Spook algorithm, Yüksek Lisans, O.BOLEL(Öğrenci), 2021
Tezcan C., Acartürk C., Anomaly-based intrusion detection using machine learning: a case study on probing attacks, Yüksek Lisans, E.TUFAN(Öğrenci), 2020
Tezcan C., OPTIMIZATION OF ADVANCED ENCRYPTION STANDARD (AES) ON CUDA, Yüksek Lisans, B.ÇELİK(Öğrenci), 2019
Baykal N., Tezcan C., Lynxtun, Yüksek Lisans, G.ORAL(Öğrenci), 2018
DOĞANAKSOY A., TEZCAN C., DIFFERENTIAL CRYPTANALYSIS ON LBLOCK USING DIFFERENTIAL FACTORS, Yüksek Lisans, M.ÖĞÜNÇ(Öğrenci), 2018
ÖZKAN YILDIRIM S., TEZCAN C., Differential factors and differential cryptanalysis of block cipher pride, Yüksek Lisans, E.DOĞAN(Öğrenci), 2017
BETİN CAN A., TEZCAN C., Improved differential attacks on rectangle, Yüksek Lisans, A.ŞENOL(Öğrenci), 2017

Tasarladığı Dersler

Tezcan C., Blockchain and Cryptocurrency Technologies, Yüksek Lisans, 2021 - 2022
Tezcan C., Lightweight Cryptography for the Internet of Things, Yüksek Lisans, 2019 - 2020
Tezcan C., Applied Cryptology, Yüksek Lisans, 2015 - 2016
Tezcan C., Applied Cryptanalysis, Yüksek Lisans, 2015 - 2016

SCI, SSCI ve AHCI İndekslerine Giren Dergilerde Yayınlanan Makaleler

I. **FPGA-friendly compact and efficient AES-like 8 × 8 S-box**
Malal A., TEZCAN C.
Microprocessors and Microsystems, cilt.105, 2024 (SCI-Expanded)

II. **GPU accelerated 3DES encryption**
Altınok K. F., Peker A., Tezcan C., Temizel A.
CONCURRENCY AND COMPUTATION-PRACTICE & EXPERIENCE, cilt.34, sa.9, 2022 (SCI-Expanded)

III. **Key lengths revisited: GPU-based brute force cryptanalysis of DES, 3DES, and PRESENT**
TEZCAN C.
JOURNAL OF SYSTEMS ARCHITECTURE, cilt.124, 2022 (SCI-Expanded)

IV. **Anomaly-Based Intrusion Detection by Machine Learning: A Case Study on Probing Attacks to an Institutional Network**
Tufan E., TEZCAN C., ACARTÜRK C.
IEEE ACCESS, cilt.9, ss.50078-50092, 2021 (SCI-Expanded)

V. **Optimization of Advanced Encryption Standard on Graphics Processing Units**
TEZCAN C.
IEEE ACCESS, cilt.9, ss.67315-67326, 2021 (SCI-Expanded)

VI. **Improved improbable differential attacks on ISO standard CLEFIA: Expansion technique revisited**
TEZCAN C., SELÇUK A. A.
INFORMATION PROCESSING LETTERS, cilt.116, sa.2, ss.136-143, 2016 (SCI-Expanded)

VII. **Improbable differential attacks on PRESENT using undisturbed bits**
TEZCAN C.
JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, cilt.259, ss.503-511, 2014 (SCI-Expanded)

Diğer Dergilerde Yayınlanan Makaleler

I. **Analysis of Ascon, DryGASCON, and Shamash Permutations**
TEZCAN C.
International Journal of Information Security Science, cilt.9, sa.3, ss.172-187, 2020 (Hakemli Dergi)

II. **Searching for subspace trails and truncated differentials**
Leander G., Tezcan C., Wiemer F.
IACR Transactions on Symmetric Cryptology, cilt.2018, sa.1, ss.74-100, 2018 (Hakemli Dergi)

Kitap & Kitap Bölümleri

I. **Experimentally Obtained Differential-Linear Distinguishers for Permutations of ASCON and DryGASCON**
Civek A. B., Tezcan C.
Information Systems Security and Privacy, Paolo Mori,Gabriele Lenzini,Steven Furnell, Editör, Springer Cham, Zug, ss.91-103, 2023

II. **Weak-Key Distinguishers for AES**
Grassi L., Rechberger C., Leander G., Tezcan C., Wiemer F.
Selected Areas in Cryptography, Orr Dunkelman,Michael J. Jacobson,Colin O'Flynn, Editör, Springer, Cham, Zug, ss.141-170, 2021

Hakemli Kongre / Sempozyum Bildiri Kitaplarında Yer Alan Yayınlar

I. **GPU-Based Brute Force Cryptanalysis of KLEIN**
Tezcan C.
10th International Conference on Information Systems Security and Privacy, Rome, İtalya, 26 - 28 Şubat 2024, ss.884-889

II. **Experimentally Obtained Differential-Linear Distinguishers for Permutations of ASCON and**

DryGASCON

CİVEK A. B., TEZCAN C.

7th and 8th International Conferences on Information Systems Security and Privacy, ICISSP 2021 and ICISSP 2022, Virtual, Online, 9 - 11 Şubat 2022, cilt.1851 CCIS, ss.91-103

III. **Weak-Key Distinguishers for AES**

Grassi L., Leander G., Rechberger C., Tezcan C., Wiemer F.

27th International Conference on Selected Areas in Cryptography (SAC), ELECTR NETWORK, 21 - 23 Ekim 2020, cilt.12804, ss.141-170

IV. **Differential-linear Attacks on Permutation Ciphers Revisited: Experiments on Ascon and DryGASCON**

Civek A. B., Tezcan C.

8th International Conference on Information Systems Security and Privacy (ICISSP), ELECTR NETWORK, 9 - 11 Şubat 2022, ss.202-209

V. **On the Fly Encryption via GPU**

TEZCAN C.

1st High Performance Computing and Applications, 21 Kasım 2019

VI. **Hafif Blok Şifrelerin Ekran Kartları ile Kriptanalizi**

TEZCAN C.

SAVTEK 2018 9. Savunma Teknolojileri Kongresi, Türkiye, 27 - 29 Haziran 2018

VII. **Brute Force Cryptanalysis of MIFARE Classic Cards on GPU**

Tezcan C.

3rd International Conference on Information Systems Security and Privacy (ICISSP), Porto, Portekiz, 19 - 21 Şubat 2017, ss.524-528

VIII. **On Differential Factors**

TEZCAN C., DOĞANAKSOY A., OKAN G. O., ŞENOL A., Doğan E., Yücebaş F., BAYKAL N.

11. INTERNATIONAL CONFERENCE ON INFORMATION SECURITY, 25 Ekim 2016

IX. **Differential Attacks on Lightweight Block Ciphers PRESENT, PRIDE, and RECTANGLE Revisited**

TEZCAN C., OKAN G. O., Senol A., Dogan E., Yucebas F., BAYKAL N.

5th International Workshop on Lightweight Cryptography for Security and Privacy (LightSec), Cappadocia, Türkiye, 20 - 21 Eylül 2016, cilt.10098, ss.18-32

X. **Truncated Impossible and Improbable Differential Analysis of ASCON**

TEZCAN C.

2nd International Conference on Information Systems Security and Privacy (ICISSP), Roma, İtalya, 19 - 21 Şubat 2016, ss.325-332

XI. **Truncated, impobible, and improbable differential analysis of ASCON**

TEZCAN C.

2nd International Conference on Information Systems Security and Privacy, ICISSP 2016, Rome, İtalya, 19 - 21 Şubat 2016, ss.325-332

XII. **Differential Factors Revisited: Corrected Attacks on PRESENT and SERPENT**

TEZCAN C.

4th International Workshop on Lightweight Cryptography for Security and Privacy (LightSec), Bochum, Almanya, 10 - 11 Eylül 2015, cilt.9542, ss.21-33

XIII. **Relating undisturbed bits to other properties of substitution boxes**

Makarim R. H., TEZCAN C.

3rd International Workshop on Lightweight Cryptography for Security and Privacy, LightSec 2014, İstanbul, Türkiye, 1 - 02 Eylül 2014, cilt.8898, ss.109-125

XIV. **Differential Factors Improved Attacks on SERPENT**

TEZCAN C., ÖZBUDAK F.

LightSec 2014, İstanbul, Türkiye, 1 - 02 Eylül 2014

XV. **Cryptanalysis of PRESENT via CUDA devices**

TEZCAN C., TEMİZEL A.

GPU Technology Conference (GTC), San-Jose, Amerika Birleşik Devletleri, 24 - 27 Mart 2014

XVI. **Improbable differential attacks on SERPENT using undisturbed bits**
TEZCAN C., Taşkin H. K., Demircioglu M.
7th International Conference on Security of Information and Networks, SIN 2014, Glasgow, Birleşik Krallık, 9 - 11 Eylül 2014, ss.145-150

XVII. **Improbable Differential Cryptanalysis**
TEZCAN C.
6th International Conference on Security of Information and Networks, 26 - 28 Kasım 2013

XVIII. **On Hiding a Plaintext Length by Preencryption**
Tezcan C., Vaudenay S.
9th International Conference on Applied Cryptography and Network Security (ACNS), İspanya, 7 - 10 Haziran 2011, cilt.6715, ss.345-358

XIX. **The Improbable Differential Attack: Cryptanalysis of Reduced Round CLEFIA**
Tezcan C.
11th International Conference on Cryptology in India, Hyderabad, Pakistan, 12 - 15 Aralık 2010, cilt.6498, ss.197-209

XX. **Lightweight Block Ciphers Revisited: Cryptanalysis of Reduced Round PRESENT and HIGHT**
Ozen O., Varici K., Tezcan C., Kocair C.
14th Australasian Conference on Information Security and Privacy, Brisbane, Avustralya, 1 - 03 Temmuz 2009, cilt.5594, ss.90-93

XXI. **Alternative Approach to Maurer's Universal Statistical Test**
TEZCAN C., DOĞANAKSOY A.
3rd Information Security and Cryptology Conference ISC Turkey, Türkiye, 25 - 27 Aralık 2008

Desteklenen Projeler

Tezcan C., Doğanaksoy A., Diğer Özel Kurumlarca Desteklenen Proje, İstatistiksel Test Paketi Geliştirilmesi, 2016 - 2017
Tezcan C., Doğanaksoy A., TÜBİTAK Projesi, Sözde Diferansiyel Faktörler ve Blok Sifre Atakları Zaman Karmasıklıkları, 2015 - 2016
ÖZBUDAK F., ÇOMAK P., SINAK A., CENK M., TEZCAN C., OTAL K., Yükseköğretim Kurumları Destekli Proje, BOOLE FONKSİYONLARI, KODLAMA TEORİSİ VE KRİPTOGRAFİ, 2015 - 2015
TEZCAN C., Yükseköğretim Kurumları Destekli Proje, Stochastic Models Forpricing And Hedging Derivatives İn Incomplete Makets: Structure, Calibration, Dynamical Programming, Risk Optimization, 2009 - 2009

Metrikler

Yayın: 34
Atıf (WoS): 197
Atıf (Scopus): 320
H-İndeks (WoS): 7
H-İndeks (Scopus): 9