Assoc. Prof. CİHANGİR TEZCAN

Personal Information

Email: cihangir@metu.edu.tr
Web: https://cihangir.forgottenlance.com

International Researcher IDs

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

Education Information

Doctorate, Middle East Technical University, Institute of Applied Mathematics, Cryptography, Turkey 2009 - 2014
Postgraduate, Middle East Technical University, Institute of Applied Mathematics, Cryptography, Turkey 2007 - 2009
Undergraduate, Middle East Technical University, Faculty of Arts and Sciences, Department of Mathematics, Turkey 2003 - 2007

Foreign Languages

English, C2 Mastery
German, B2 Upper Intermediate
French, B2 Upper Intermediate
Portuguese, B2 Upper Intermediate

Dissertations

Doctorate, Improbable differential cryptanalysis, Middle East Technical University, Institute of Applied Mathematics, Cryptography, 2014
Postgraduate, Impossible differential cryptanalysis of reduced round HIGHT, Middle East Technical University, Institute of Applied Mathematics, Cryptography, 2009

Research Areas

Information Systems, Communication and Control Engineering, Parallel Algorithms, Information Security and Reliability, Cryptography, Quantum Cryptography, Computer Networks, Algebraic Geometry, Combinatorics, Probability Theory, Stochastic Processes, Number Theory, Numerical Analysis

Academic Titles / Tasks

Associate Professor, Middle East Technical University, Graduate School of Informatics, Cybersecurity, 2022 - Continues
Assistant Professor, Middle East Technical University, Graduate School of Informatics, Cybersecurity, 2019 - 2022

Research Assistant, Middle East Technical University, Faculty of Arts and Sciences, Department of Mathematics, 2011 - 2019
Assistant Professor, Ruhr-Universitaet Bochum, Mathematics, 2017 - 2018
Research Assistant, Ecole Polytechnique Federale De Lausanne, Computer And Communication Sciences, 2010 - 2011
Research Assistant, Middle East Technical University, Institute of Applied Mathematics, Cryptography, 2008 - 2010

Academic and Administrative Experience

Enstitü Yönetim Kurulu Üyesi, Middle East Technical University, Graduate School of Informatics, Cybersecurity, 2022 - Continues
Head of Department, Middle East Technical University, Graduate School of Informatics, Cybersecurity, 2020 - Continues
Manager of Research and Application Center, Middle East Technical University, Presidency Office, Siber Savunma ve Güvenlik Uygulama ve Araştırma Merkezi, 2020 - Continues

Supervised Theses

Tezcan C., Image-based malware family classification with deep learning and a new dataset, Postgraduate, E.MUTLU(Student), 2024
Tezcan C., An analysis of Kerberoasting attack and detection with supervised machine learning algorithms, Postgraduate, Y.AKSÜT(Student), 2024
Tezcan C., FPGA-friendly compact and efficient AES-like 8x8 S-Box, Postgraduate, A.MALAL(Student), 2023
Tezcan C., A permissioned blockchain-based model for digital forensics, Postgraduate, N.ALIZADEH(Student), 2023
Tezcan C., Detecting android obfuscation methods with LSTM, Postgraduate, B.ULUKAPİ(Student), 2022
Tezcan C., Compact and flexible NTRU implementation on FPGA, Postgraduate, S.EMİR(Student), 2022
Tezcan C., DIFFERENTIAL-LINEAR CRYPTANALYSIS OF ASCON AND DRYGASCON, Postgraduate, A.BAŞAK(Student), 2021
Tezcan C., Impossible and improbable differential cryptanalysis of Spook algorithm, Postgraduate, O.BOLEL(Student), 2021
Tezcan C., Acartürk C., Anomaly-based intrusion detection using machine learning: a case study on probing attacks, Postgraduate, E.TUFAN(Student), 2020
Tezcan C., OPTIMIZATION OF ADVANCED ENCRYPTION STANDARD (AES) ON CUDA, Postgraduate, B.ÇELİK(Student), 2019
Baykal N., Tezcan C., Lynxtun, Postgraduate, G.ORAL(Student), 2018
DOĞANAKSOY A., TEZCAN C., DIFFERENTIAL CRYPTANALYSIS ON LBLOCK USING DIFFERENTIAL FACTORS, Postgraduate, M.ÖĞÜNÇ(Student), 2018
ÖZKAN YILDIRIM S., TEZCAN C., Differential factors and differential cryptanalysis of block cipher pride, Postgraduate, E.DOĞAN(Student), 2017
BETİN CAN A., TEZCAN C., Improved differential attacks on rectangle, Postgraduate, A.ŞENOL(Student), 2017

Designed Lessons

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

Published journal articles indexed by SCI, SSCI, and AHCI

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

II. **GPU accelerated 3DES encryption**
Altınok K. F., Peker A., Tezcan C., Temizel A.
CONCURRENCY AND COMPUTATION-PRACTICE & EXPERIENCE, vol.34, no.9, 2022 (SCI-Expanded)

III. **Key lengths revisited: GPU-based brute force cryptanalysis of DES, 3DES, and PRESENT**
TEZCAN C.
JOURNAL OF SYSTEMS ARCHITECTURE, vol.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, vol.9, pp.50078-50092, 2021 (SCI-Expanded)

V. **Optimization of Advanced Encryption Standard on Graphics Processing Units**
TEZCAN C.
IEEE ACCESS, vol.9, pp.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, vol.116, no.2, pp.136-143, 2016 (SCI-Expanded)

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

Articles Published in Other Journals

I. **Analysis of Ascon, DryGASCON, and Shamash Permutations**
TEZCAN C.
International Journal of Information Security Science, vol.9, no.3, pp.172-187, 2020 (Peer-Reviewed Journal)

II. **Searching for subspace trails and truncated differentials**
Leander G., Tezcan C., Wiemer F.
IACR Transactions on Symmetric Cryptology, vol.2018, no.1, pp.74-100, 2018 (Peer-Reviewed Journal)

Books

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

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

Refereed Congress / Symposium Publications in Proceedings

I. **GPU-Based Brute Force Cryptanalysis of KLEIN**
Tezcan C.

10th International Conference on Information Systems Security and Privacy, Rome, Italy, 26 - 28 February 2024, pp.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 February 2022, vol.1851 CCIS, pp.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 October 2020, vol.12804, pp.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 February 2022, pp.202-209

V. **On the Fly Encryption via GPU**
TEZCAN C.
1st High Performance Computing and Applications, 21 November 2019

VI. **Hafif Blok Şifrelerin Ekran Kartları ile Kriptanalizi**
TEZCAN C.
SAVTEK 2018 9. Savunma Teknolojileri Kongresi, Turkey, 27 - 29 June 2018

VII. **Brute Force Cryptanalysis of MIFARE Classic Cards on GPU**
Tezcan C.
3rd International Conference on Information Systems Security and Privacy (ICISSP), Porto, Portugal, 19 - 21 February 2017, pp.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 October 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, Turkey, 20 - 21 September 2016, vol.10098, pp.18-32

X. **Truncated Impossible and Improbable Differential Analysis of ASCON**
TEZCAN C.
2nd International Conference on Information Systems Security and Privacy (ICISSP), Roma, Italy, 19 - 21 February 2016, pp.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, Italy, 19 - 21 February 2016, pp.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, Germany, 10 - 11 September 2015, vol.9542, pp.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, Turkey, 1 - 02 September 2014, vol.8898, pp.109-125

XIV. **Differential Factors Improved Attacks on SERPENT**
TEZCAN C., ÖZBUDAK F.
LightSec 2014, İstanbul, Turkey, 1 - 02 September 2014

XV. **Cryptanalysis of PRESENT via CUDA devices**
TEZCAN C., TEMİZEL A.
GPU Technology Conference (GTC), San-Jose, United States Of America, 24 - 27 March 2014

XVI. **Improbable differential attacks on SERPENT using undisturbed bits**
TEZCAN C., Taşkin H. K., Demircioılu M.
7th International Conference on Security of Information and Networks, SIN 2014, Glasgow, United Kingdom, 9 - 11 September 2014, pp.145-150

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

XVIII. **On Hiding a Plaintext Length by Preencryption**
Tezcan C., Vaudenay S.
9th International Conference on Applied Cryptography and Network Security (ACNS), Spain, 7 - 10 June 2011, vol.6715, pp.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 December 2010, vol.6498, pp.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, Australia, 1 - 03 July 2009, vol.5594, pp.90-93

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

Supported Projects

Tezcan C., Doğanaksoy A., Project Supported by Other Private Institutions, İstatistiksel Test Paketi Geliştirilmesi, 2016 - 2017

Tezcan C., Doğanaksoy A., TUBITAK Project, Sözde Diferansiyel Faktörler ve Blok Sifre Atakları Zaman Karmasıklıkları, 2015 - 2016

ÖZBUDAK F., ÇOMAK P., SINAK A., CENK M., TEZCAN C., OTAL K., Project Supported by Higher Education Institutions, BOOLE FONKSİYONLARI, KODLAMA TEORİSİ VE KRİPTOGRAFİ, 2015 - 2015

TEZCAN C., Project Supported by Higher Education Institutions, Stochastic Models Forpricing And Hedging Derivatives İn Incomplete Makets: Structure, Calibration, Dynamical Programming, Risk Optimization, 2009 - 2009

Metrics

Publication: 34
Citation (WoS): 204
Citation (Scopus): 326
H-Index (WoS): 7
H-Index (Scopus): 9