

Asst. Prof. CİHANGİR TEZCAN

Personal Information

Email: cihangir@metu.edu.tr

Web: <https://cihangir.forgottenlance.com>

Education Information

Doctorate, Middle East Technical University, Institute of Applied Mathematics, Cryptography, Turkey 2009 - 2014

Post Graduate, Middle East Technical University, Institute of Applied Mathematics, Cryptography, Turkey 2007 - 2009

Under Graduate, 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

Post Graduate, 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

Assistant Professor, Middle East Technical University, Graduate School Of Informatics, Cybersecurity, 2019 - Continues
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

Director of the Center, Middle East Technical University, Presidency Office, Cyber Defense and Security Research Center, 2020 - Continues

Head of Department, Middle East Technical University, Graduate School of Informatics, Cybersecurity, 2020 - Continues

Advising Theses

Tezcan C., OPTIMIZATION OF ADVANCED ENCRYPTION STANDARD (AES) ON CUDA, Post Graduate, B.ÇELİK(Student), 2019

TEZCAN C., Optimization of advanced encryption standard (AES) on CUDA, Post Graduate, B.Çelik(Student), 2019

TEZCAN C., The criticality problems in neutron transport theory for extremely anisotropic scattering Kernels., Doctorate, C.Yıldız(Student), 1984

Designed Lessons

Tezcan C., Lightweight Cryptography for the Internet of Things, Post Graduate, 2019 - 2020

Tezcan C., Applied Cryptology, Post Graduate, 2015 - 2016

Tezcan C., Applied Cryptanalysis, Post Graduate, 2015 - 2016

Articles Published in Journals That Entered SCI, SSCI and AHCI Indexes

- I. **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 (Journal Indexed in SCI)
- II. **Optimization of Advanced Encryption Standard on Graphics Processing Units**
TEZCAN C.
IEEE ACCESS, vol.9, pp.67315-67326, 2021 (Journal Indexed in SCI)
- III. **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 (Journal Indexed in SCI)
- IV. **Improbable differential attacks on PRESENT using undisturbed bits**
TEZCAN C.
JOURNAL OF COMPUTATIONAL AND APPLIED MATHEMATICS, vol.259, pp.503-511, 2014 (Journal Indexed in SCI)

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 (Other Refereed National Journals)
- 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 (Journal Indexed in ESCI)

Refereed Congress / Symposium Publications in Proceedings

- I. **On the Fly Encryption via GPU**

- TEZCAN C.
1st High Performance Computing and Applications, 21 November 2019
- II. **Hafif Blok Şifrelerin Ekran Kartları ile Kriptanalizi**
TEZCAN C.
SAVTEK 2018 9. Savunma Teknolojileri Kongresi, Turkey, 27 - 29 June 2018
- III. **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
- IV. **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
- V. **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
- VI. **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
- VII. **Truncated, imposable, 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
- VIII. **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
- IX. **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
- X. **Differential Factors Improved Attacks on SERPENT**
TEZCAN C., ÖZBUDAK F.
LightSec 2014, İstanbul, Turkey, 1 - 02 September 2014
- XI. **Cryptanalysis of PRESENT via CUDA devices**
TEZCAN C., TEMİZEL A.
GPU Technology Conference (GTC), San-Jose, United States Of America, 24 - 27 March 2014
- XII. **Improbable differential attacks on SERPENT using undisturbed bits**
TEZCAN C., Taşkin H. K. , Demircioğlu M.
7th International Conference on Security of Information and Networks, SIN 2014, Glasgow, United Kingdom, 9 - 11 September 2014, pp.145-150
- XIII. **Improbable Differential Cryptanalysis**
TEZCAN C.
6th International Conference on Security of Information and Networks, 26 - 28 November 2013
- XIV. **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
- XV. **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

XVI. **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

XVII. **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., Dođanaksoy A., Project Supported by Other Private Institutions, İstatistiksel Test Paketi Geliřtirilmesi, 2016 - 2017

Tezcan C., Dođanaksoy A., TUBITAK Project, Sözde Diferansiyel Faktörler ve Blok Sifre Atakları Zaman Karmařıklıkları, 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

Citations

Total Citations (WOS):99

h-index (WOS):4