Cihangir Tezcan

Tel: 0090 312 210 5016
e-mail: cihangir {at} metu.edu.tr
Middle East Technical University
Fen Edebiyat Fakültesi Dekanlığı
06800 Ankara TURKEY

Last Update: 12.06.2018

Born: 18.03.1985, Ankara
Citizenship: Turkey
Marital Status: Single

EDUCATION

2009 – 2014	Ph.D.: Middle East Technical University / Ankara – TURKEY Cryptography CGPA: 3.79/4.00
2007 – 2009	M.S.: Middle East Technical University / Ankara – TURKEY Cryptography CGPA: 4.00/4.00
2003 – 2007	B.S.: Middle East Technical University / Ankara – TURKEY Mathematics CGPA: 3.04/4.00

WORK EXPERIENCE

4.4.2017 – 4.1.2018	Post-Doctoral Researcher at Ruhr Universität Bochum, GERMANY
2015 – *Present*	Affiliated Faculty at Department of Cyber Security, METU, TURKEY
2014 – *Present*	Affiliated Faculty at Department of Cryptography, METU, TURKEY
2012 – *Present*	Teaching Assistant at Department of Mathematics, METU, TURKEY
2012 – *Present*	Computer Coordinator at Faculty of Arts and Sciences, Dean's Office
2011 – 2012	Researcher at Faculty of Arts and Sciences, METU, TURKEY
2010 – 2011	Teaching Assistant at EPFL, SWITZERLAND
2008 – 2010	Research Assistant at Department of Cryptography, METU, TURKEY

PUBLICATIONS

Journal Papers

1. Gregor Leander, **Cihangir Tezcan**, Friedrich Wiemer. *Searching for Subspace Trails and Truncated Differentials*. IACR Trans. Symmetric Cryptology. 2018(1): 74-100 *(Journal impact factor to be determined)*

2. **Cihangir Tezcan**. *Improbable Differential Attacks on PRESENT using Undisturbed Bits*. Journal of Computational and Applied Mathematics, 259, Part B(0):503-511, (2014) **(SCI)** ***(Web of Science Core Collection citation: 7)***

3. **Cihangir Tezcan** and Ali Aydın Selçuk. *Improved Improbable Differential Attacks on CLEFIA: Expansion Technique Revisited*. Information Processing Letters 116(2), 136-143, (2016) **(SCI-E)**

International Conference Papers

1. **Cihangir Tezcan**, Lorenzo Grassi, Christian Rechberger, Gregor Leander, Friedrich Wiemer. *Weak-Key Subspace Trails and Applications to AES*. ASIACRYT (2018) *(Under Review)*

2. **Cihangir Tezcan**. *Brute Force Cryptanalysis of Mifare Classic Cards on GPU*. Proceedings of the 3rd International Conference on Information Systems Security and Privacy, 524-528, Porto, Portugal, ICISSP (2017)

3. **Cihangir Tezcan**, Galip Oral Okan, Asuman Şenol, Erol Doğan, Furkan Yücebaş, Nazife Baykal. *Differential Attacks on Lightweight Block Ciphers PRESENT, PRIDE, and RECTANGLE Revisited*. Lightsec 2017, Lecture Notes in Computer Science, vol. 10098, 18-32, Springer (2017)

4. **Cihangir Tezcan**, Ali Doğanaksoy, Galip Oral Okan, Asuman Şenol, Erol Doğan, Furkan Yücebaş, Nazife Baykal. *On Differential Factors.* Iscturkey 2016, Proceedings of IX. International conference on Information Security and Cryptology, 103-110 (2016)

5. **Cihangir Tezcan**. *Truncated, Impossible, and Improbable Differential Analysis of Ascon*. Proceedings of the 2nd International Conference on Information Systems Security and Privacy, 325-332, Rome, Italy, ICISSP (2016)

6. **Cihangir Tezcan**. *Differential Factors Revisited: Corrected Attacks on PRESENT and SERPENT*. Lightsec 2015, Lecture Notes in Computer Science, vol. 9542, 21-33, Springer (2015) ***(Web of Science Core Collection citation: 1)***

7. **Cihangir Tezcan** and Ferruh Özbudak. *Differential Factors: Improved Attacks on SERPENT*, Lightsec 2014, Lecture Notes in Computer Science, vol. 8898, pp. 69-84. Springer (2014)

8. Rusydi H. Makarim and **Cihangir Tezcan**. Relating Undisturbed Bits to Other Properties of Substitution Boxes, Lightsec 2014, Lecture Notes in Computer Science, vol. 8898, pp. 109- 125. Springer (2014)

9. **Cihangir Tezcan**, Halil Kemal Taşkın, Murat Demircioğlu. *Improbable Differential Attacks on SERPENT using Undisturbed Bits*. In: Poet, R., Rajarajan, M. (eds.) Proceedings of the 7th International Conference on Security of Information and Networks, Glasgow, Scotland, UK, September 9-11, 2014. p. 145. ACM (2014)

10. **Cihangir Tezcan**. *Improbable Differential Cryptanalysis*. SIN'13, Proceedings of the 6th International Conference on Security of Information and Networks, Aksaray, Turkey, November 26-28 ACM (2013)

11. **Cihangir Tezcan**. *Improbable Differential Attack on PRESENT using Undisturbed Bits*. In International Conference on Applied and Computational Mathematics (ICACM 2012), Book of Abstracts, Ankara, TURKEY (3 October 2012)

12. **Cihangir Tezcan** and Serge Vaudenay. *On Hiding a Plaintext Length by Preencryption*. In Lopez J., Tsudik G. (eds.) ACNS 2011. LNCS, vol. 6715, pp. 345-358, Nerja, Spain, Springer (2011) ***(Web of Science Core Collection citation: 1)***

13. **Cihangir Tezcan**. *The Improbable Differential Attack: Cryptanalysis of Reduced Round CLEFIA*. In Gong G., Gupta K. C. (eds.) INDOCRYPT 2010. LNCS, vol. 6498, pp. 197-209. Hyderabad, India, Springer (2010) ***(Web of Science Core Collection citation: 12)***

14. Kerem Varıcı, Onur Özen, **Cihangir Tezcan** and Çelebi Kocair. *Lightweight Block Ciphers Revisited: Cryptanalysis of Reduced Round PRESENT and HIGHT*. In Boy C., Nieto J. G. (eds.), ACISP 2009. LNCS, vol. 5594, pp. 90-107. Brisbane, Australia. Springer (2009) ***(Web of Science Core Collection citation: 34)***

National Conference Papers

1. **Cihangir Tezcan**. *Hafif Blok Şifrelerin Ekran Kartı ile Kriptanalizi*. SAVTEK , 27-29 June, Ankara (2018)

2. **Cihangir Tezcan** and Ali Doğanaksoy. *Alternative Approach to Maurer's Universal Statistical Test*. In 3rd Information Security & Cryptography Conference, Ankara, December (2008)

Theses

1. M.Sc. Thesis: *Impossible Differential Cryptanalysis of Reduced Round HIGHT*, July 2009. Department of Cryptography, METU. Advisor: Assoc. Prof. Ali Doğanaksoy

2. Ph.D. Thesis: *Improbable Differential Cryptanalysis*, June 2014. Department of Cryptography, METU. Advisor: Assoc. Prof. Ali Doğanaksoy. Co-advisor: Ersan Akyıldız.

THESIS STUDENTS:

1. Burak Çelik. *Optimization of AES on CUDA Devices*. Department of Cyber Security (Co-advisor, in progress)

2. Asuman Şenol. *Improved Differential Attacks on RECTANGLE*. MSc. Degree 07.08.2017. Department of Cyber Security (Co-advisor)

3. Erol Doğan. *Differential Factors and Differential Cryptanalysis of Block Cipher PRIDE*. MSc. Degree 07.07.2017. Department of Cyber Security (Co-advisor)

DEVELOPMENT of a TOTALLY NEW COURSE:

1. CSEC507 - Applied Cryptology

2. CSEC508 - Applied Cryptanalysis

PROFESSIONAL ACTIVITIES

Journal Editor:

- ***IJACIS*** (The International Journal of Advanced Research in Computer and Information Security)*, since* 2017

Organizing Committee:

- ***ISCTURKEY 2013*** (6th International Conference on Information Security and Cryptology) Ankara, Turkey, 2013

Program Committee:

- ***ICISSP 2018*** (4th International Conference on Information Systems Security and Privacy)*, 22-24 January 2018, Funchal, Madeira, Portugal*
- ***SIN'18*** (The 11th International Conference on Security of Information and Networks)*, 10-12 September, Cardiff City, Wales*
- ***ICCT'17*** (1st International Conference on Intelligent Communication and Computational Techniques)*, 22-23 December, Jaipur, India*
- ***SIN'17*** (The 10th International Conference on Security of Information and Networks)*, 13-15 October, Jaipur, India*
- ***ISCTURKEY 2017*** (10th International Conference on Information Security and Cryptology)*, 20-21 October, Ankara, Turkey*
- ***ICISSP 2017*** (3rd International Conference on Information Systems Security and Privacy)*, 19-21 February 2017, Porto, Portugal*
- ***SIN'16*** (The 9th International Conference on Security of Information and Networks)*, New Jersey, USA*
- ***ICISSP 2016*** (2nd International Conference on Information Systems Security and Privacy)*, 19-21 February 2016, Rome, Italy*
- ***ISCTURKEY 2016*** (9th International Conference on Information Security and Cryptology)*, 25-26 October, Ankara, Turkey*
- ***SIN'15*** (The 8th International Conference on Security of Information and Networks)*, 8-10 September 2015, Sochi, Russia*
- ***ICISSP 2015*** (1st International Conference on Information Systems Security and Privacy)*, 9-11 February 2015, Angers, France*
- ***ISCTURKEY 2015*** (8th International Conference on Information Security and Cryptology)*, 30-31 October, Ankara, Turkey*
- ***SIN'14*** (The 7th International Conference on Security of Information and Networks)*, 9-11 September 2014, Glasgow, Scotland*
- ***SIN'13*** (The 6th International Conference on Security of Information and Networks)*, 26-28 November 2013, Aksaray, Turkey*

Journal Refereeing:

- *IET Information Security (Reviews: 2)*
- *The Computer Journal (Reviews: 2)*
- *Security and Communication Networks (Reviews: 2)*
- *Creative Education (Reviews: 1)*
- *Designs, Codes, and Cryptography (Reviews: 2)*
- *Journal of Sensors, Wireless Communication (Reviews: 2)*
- *Turkish Journal of Electrical Engineering & Computer Sciences (Reviews: 2)*

Conference Reviewer:

- **2018:** ***EUROCRYPT*** *(37th International Conference on the Theory and Applications of Cryptographic Techniques),* ***SIU*** *(26. IEEE Sinyal İşleme ve İletişim Uygulamaları Kurultayı)*
- **2017:** ***SAC*** *(24th Conference on Selected Areas of Cryptography)*
- **2016:** ***CHES*** *(18th Conference on Cryptographic Hardware and Embedded Systems),* ***LIGHTSEC*** *(5th International Workshop on Lightweight Cryptography for Security and Privacy)*
- **2015:** ***SAC*** *(22nd Conference on Selected Areas of Cryptography),* ***LATINCRYPT*** *(4th International Conference on Cryptology and Information Security in Latin America),* ***WCC*** *(9th Workshop on coding and Cryptography),* ***CT-RSA*** *(RSA Conference Cryptographers' Track),* ***FSE*** *(22nd International Workshop on Fast Software Encryption)*
- **2011:** ***LIGHTSEC*** *(1st International Workshop on Lightweight Cryptography for Security and Privacy)*

PROJECTS

1. **Design and Analysis of Block Ciphers (TÜBİTAK 2219, No: 1059B191600050, Role: Post-Doctoral Researcher):** I visited Prof. Dr. Gregor Leander's Workgroup of Symmetric Cryptography at Faculty of Mathematics, RUHR Universität Bochum, Germany for 9 months (4.4.2017 – 1.4.2018) as a post-doctoral researcher. We provided new insights on the recently discovered cryptanalysis techniques of invariant subspace attacks and subspace trail attacks. We combined these two techniques and introduced Weak-key Subspace Trail attacks. With this new cryptanalysis technique we provided the longest distinguishers for AES in the weak-key setting. Moreover, we provided the longest distinguishers for AES in the chosen-key setting and found a distinguisher for full AES which was an open problem for a long time. Secondly, we provided efficient algorithms to find provably the longest subspace trails and provided security upper bounds for many ciphers for subspace trail cryptanalysis. Finally, we designed a lightweight block cipher called SILENT for GPUs by taking into account the GPU architectures.

2. **Improbable Differential Cryptanalysis of Block Ciphers (TÜBİTAK 1001, No: 112E101, Role: Scholarship Student):** I discovered the improbable differential cryptanalysis technique in early 2009 and by using it, I provided the best attack on Sony Corporation's block cipher CLEFIA in my Indocrypt 2010 paper. In this project we analyze the security and resistance of the known block ciphers against this new technique. The project started in October 2012 and ended in October 2013. During this Project we introduced two new S-box evaluation criteria that we call Undisturbed Bits and Differential Factors. We also provided the best known attacks on CLEFIA and SERPENT.

3. **Quasi-differential Factors and Time Complexity of Block Cipher Attacks (TÜBİTAK 1001, No: 115E447, Role: Researcher):** In this Project we use S-box weaknesses to reduce the time complexity of block cipher attacks. We experimentally verify our results using multiple GPUs and we obtain the fastest GPU implementations of block ciphers. Project was started in September 2015 and completed in 2017.

4. **ASELSAN – A Statistical Randomness Test Suite (BAP, Role: Researcher):** During this project we examined previously known randomness tests and provided an alternative approach to Maurer's Universal Statistical Test. I implemented the whole test suite which can be directly used to evaluate block ciphers, stream ciphers and hash functions. Project started in 2007 and ended in 2009. This project and the test suite are revised in 2017 in collaboration with Aselsan as a BAP Project.

5. **COMODO YAZILIM A.Ş. – Yeni Nesil Kurumsal Yedekleme Sistemi** (TÜBİTAK 1501, Role: Consultant) 01.08.2015 - 29.02.2016

6. **InfosecGlobal Turkey A.Ş. – Entropi Kaynağı Değerlendirme Yazılımı Geliştirilmesi** (Döner Sermaye Projesi, Role: Researcher) 18.12.2015 – 20.03.2016

7. **Fame Crypt – Güvenli ve Hızlı Blok Şifre Tasarım Projesi** (Döner Sermaye Projesi, Role: Researcher) 2017-2019

LANGUAGES

- Turkish (Native)
- English (C2)
- German (B1)
- French (A2)
- Portuguese (A1)

RESEARCH INTERESTS

- Cyber Security and Information Systems
- Symmetric Cryptography
- Cryptanalysis
- Parallel Computing on GPUs
- Algebraic Geometry
- Algebraic Number Theory
- Randomness

OTHERS

- I have been practicing Capoeira since 2007 and I am currently with Capoeira Alcateia
- I played football at TKİ in Turkish Amateur Football League (2000-2003)
- Programming languages: C, C++, PERL, CUDA, PYTHON, PHP, SQL