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: 23.01.2015

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
2010 - 2011 (cancelled)	Ph.D.: Ecole Polytechnique Federale de Lausanne / SWITZERLAND
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

PUBLICATIONS

Journal Papers

1. **Cihangir Tezcan**. *Improbable Differential Attacks on PRESENT using Undisturbed Bits*. Journal of Computational and Applied Mathematics, 259, Part B(0):503-511, 2014.

Conference Papers

1. **Cihangir Tezcan** and Ferruh Özbudak. Differential Factors: Improved Attacks on SERPENT, Lightsec 2014, to appear.

2. Rusydi H. Makarim and **Cihangir Tezcan**. Relating Undisturbed Bits to Other Properties of Substitution Boxes, Lightsec 2014, to appear.

3. **Cihangir Tezcan**, Halil Kemal Taşkın, Murat Demircioğlu. *Improbable Differential Attaks 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)

4. **Cihangir Tezcan**. *Improbable Differential Cryptanalysis*. SIN'13, 6th International Conference on Information Security and Cryptology, Nov 26-28 2013, Aksaray, Turkey.

5. **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).

6. **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. Springer 2011

7. **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. Springer (2010).

8. 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. Springer 2009.

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

Work in Progress

1. **Cihangir Tezcan** and Ali Aydın Selçuk. *Improved Improbable Differential Attacks on CLEFIA : Expansion Technique Revisited*. Submitted to Informations Processing Letters.

Theses

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

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

WORK EXPERIENCE

2012 – *Present*	Teaching Assistant at Department of Mathematics, METU, TURKEY
2012 – *Present*	Computer Coordinator at Faculty of Arts and Sciences, METU
2012 – 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

PROFESSIONAL ACTIVITIES

Organizing Committee:

- *ISCTURKEY 2013*, Ankara, Turkey, 2013

Program Committee:

- *SIN'15 (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*
- *SIN'14 (7th International Conference on Security of Information and Networks), 9-11 September 2014, Glasgow, Scotland,*
- *SIN'13 (6th International Conference on Security of Information and Networks), 26-28 November 2013, Aksaray, Turkey,*

External Reviewer:

- *CT-RSA 2015*, San Francisco, USA, 2015
- *FSE 2015*, İstanbul, Turkey, 2015
- *LightSec 2011*, Istanbul, Turkey, 2011

AWARDS:

- TÜBİTAK M.S. Scholarship (2007-2009)
- METU Graduate Courses Performance Award
  - 2009- 2010 Academic year (PhD)
  - 2007- 2008 Academic year (MSc)
- METU Dean's High Honor List:
  - 2006- 2007 Academic year I. semester
  - 2006- 2007 Academic year II. semester
- METU Dean's Honor List:
  - 2005- 2006 Academic year II. semester
  - 2004- 2005 Academic year II. semester

PROJECTS

Improbable Differential Cryptanalysis of Block Ciphers (TÜBİTAK 1001, No: 112E101): 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 analyse the security and resistance of the known block ciphers against this new technique. The project started in October 2012 and ended in October 2013.

SADIST – A Statistical Randomness Test Suite: During this project I examined previously known randomness tests and provided an alternative approach to Maurer's Universal Statistical Test. I also implemented the whole test suite. Project started in 2007 and ended in 2009.

LANGUAGES

- Turkish (Native)
- English (Fluent)
- French (A2)
- German (Beginner)
- Portuguese (Beginner)

RESEARCH INTERESTS

- Cryptanalysis
- Parallel Computing on GPUs
- Algebraic Geometry
- Algebraic Number Theory
- Randomness

OTHERS

- I have been practicing Capoeira since 2007 and have the 7^{th} belt of the Grupo Muzenza Capoeira School (Highest is 22nd)
- Programming languages: C, C++, PERL, CUDA, PHP, SQL