Dilara Toprakhisar

Curriculum Vitae

Computerbeveiliging & Ind.Crypt.Leuven,
Kasteelpark Arenberg 10
3001 Heverlee
Belgium
✉ *dilara.toprakhisar@esat.kuleuven.be*

Date of birth: 16/10/1995
Nationality: Turkish
Country of Residence: Belgium

Education

2019–Present **Ph.D. in Cryptography**, *Cosic, KU Leuven*, Belgium.
Securing Against Physical Attacks - Fault Injection

2019–2021 **MS in Information Security Technology**, *Eindhoven University of Technology*, The Netherlands.
Graduation date: August 2021
GPA - 8.07/10
Thesis - 8.5/10: Behaviour of Algebraic Ciphers in Fully Homomorphic Encryption

2014–2019 **BS in Computer Science and Engineering**, *Sabancı University*, Turkey.
Graduation date: June 2019
GPA - 3.84/4
Mathematics Minor, GPA - 4.00/4

- Graduation Project: Design and Development of Homomorphic Multiparty Processing Infrastructure for Discovering Genetic Variants Associated with a Trait

2017 **Erasmus Exchange Program**, *Delft University of Technology*, The Netherlands, Computer Science.

Experience

Teaching Experience

2020 Q4 **Teaching Assistant**, *Eindhoven University of Technology*.

- Computer Networks and Security, Instructors: Tanir Ozcelebi, Jerry den Hartog

2015–2018 **Teaching Assistant**, *Sabancı University*.

- Advanced Programming, Instructor: Kamer Kaya
- Calculus, Instructor: Cem Güneri

2015 Fall **Learning Assistant**, *Sabancı University*.

- Nature of Science, Instructor: Zehra Sayers

Work Experience

12.2020 - 02.2021 **Research Assistant**, *Riscure*, The Netherlands.

- Fault Injection - SIFA on AES/DES

2020 **Summer Research Intern**, *Riscure*, The Netherlands.

- Internship Project: How to measure fault injection attack resistance of an implementation quickly? (SIFA)

2018 **Summer Research Intern**, *Delft University of Technology*, Cyber Security Group, The Netherlands.

- Internship Project: iDASH Privacy & Security Competition 2018/Track 2 - Secure Parallel Genome Wide Association Studies using Homomorphic Encryption

Publications

2022 Ashur, T. & Mahzoun, M. & Toprakhisar, D. Chaghri - an FHE-friendly Block Cipher. ACM Conference on Computer and Communications Security (CCS) in Los Angeles, U.S.A; Conference Date: 7-11-2022 Through 11-11-2022.

2022 Ashur, T. & Mahzoun, M. & Toprakhisar, D. How Not To Design an Efficient FHE-friendly Block Cipher: Seljuk. The Computer Journal Special Issue on Failed Approaches and Insightful Losses in Cryptology.

2021 Ashur, T. & Toprakhisar, D., A Comparative Study of Vision and AES in FHE Setting. May 2021. WIC symposium on Information Theory and Signal Processing in the Benelux, SiTB; Conference date: 20-05-2021 Through 21-05-2021.

2021 Ashur, T. & Mahzoun, M. & Toprakhisar, D. A Comparative Study of Vision and AES in FHE Setting. August 2021. The Conference for Failed Approaches and Insightful Losses in Cryptology, CFail; Conference date: 14-08-2021

Honors and Awards

2019 **ALSP Scholarship granted by Eindhoven University of Technology**.

- Full tuition wavier and monthly stipend granted

2014 **Full tuition wavier and housing granted by Sabanci University**.

- Received as the result of the success in the National University Entrance Exam, ranked as 1639th among 2 million participants in Turkey

2014 **Third honor's degree of graduation**, *Vefa High School*, Istanbul, Turkey.

Skills

Programming Skills	C, C++, C#, Python, Java, MS Visual Studio, Eclipse, MATLAB, R
Languages	Turkish (Native), English (Professional)