Curriculum Vitae **Esra Günsay**

PERSONAL DATA

Universitat des Saarlandes
Stuhlsatzenhaus 5, Saarbrücken, GERMANY
E-mail : esra(dot)guensay(at)cispa.de

RESEARCH INTERESTS

Provable Security, Cryptographic Protocols, Key Exchange and Secure Messaging.

EDUCATION

CISPA Helmholtz Center for Information Security, Saarbrücken, GERMANY

Ph.D. in Computer Science — Sep. 2023 - Present

- Supervisor: Prof. Dr. Cas Cremers

Middle East Technical University, Ankara, TURKEY

M.Sc. in Cryptography — Mar. 2021

- Thesis Title: *"Zero Knowledge Range Proofs and Applications on Decentralized Constructions"*
- Supervisor: Prof. Dr. Murat Cenk

TOBB University of Economics and Technology, Ankara, TURKEY

B.Sc. in Mathematics — Sep. 2018

- *Summa cum laude*
- Full Scholarship during five years from TOBB University

AWARDS AND HONORS

- Comprehensive Full Scholarship from TOBB University during B.Sc. studies.
- TOBB University High Honor Student during B.Sc. studies.

ACADEMIC EXPERIENCE

Middle East Technical University, Ankara, TURKEY

Research & Teaching Assistant — Feb. 2020 - Sep. 2023

TEACHING EXPERIENCE

Middle East Technical University, Ankara, TURKEY

Teaching Assistant

- IAM 502 Stream Ciphers, Spring 2023
  - Capacity 20 to 50 students each semester.

- MAT 119 Calculus with Analytic Geometry, Fall 2022
  - Capacity of 3000 students.
  - Including every-week recitations, office hours.

- IAM 504 Public Key Cryptography, Spring 2022
  - Capacity 20 to 50 students each semester.

- IAM 501 Introduction to Cryptography, Fall 2020, Fall 2021
  - Capacity 30 to 60 students each semester.
  - Including graduate level C++ mini-course

- IAM 512 Block Ciphers, Spring 2020, Spring 2021
  - Capacity 20 to 50 students each semester.
  - Responsible to explain linear and differential cryptanalysis.
  - Implementing AES, DES, RC6, Mars, Serpent, Twofish, etc.

Industrial Experience

FAME Crypt, Ankara, TURKEY

Full-time Project Researcher — Jan. 2020 – Mar. 2020

Projects

METU Technopark Research Project, *Secure and Privacy Protected Blockchain Based System Development for Banking*, 2020.

Publications

- C. Cremers, **E. Günsay**, V. Wesselkamp, M. Zhao, "*ETK: External-Operations TreeKEM and the Security of MLS in RFC 9420*", under submission, 2025.
- **E. Günsay***, C. B. Onur, and M. Cenk, "*A different base approach for better efficiency on range proofs*", Journal of Information Security and Applications 85, 103860, 2024.
- **E. Günsay***, O. Yayla, "*Decentralized Anonymous IoT Data Sharing with Key-Private Proxy Re-Encryption.*," International Journal of Information Security Science, 2023, 13.1: 23-39.
- **E. Günsay***, C. B. Onur and M. Cenk, "*An Improved Range Proof with Base-3 Construction.*," 2021 14th International Conference on Security of Information and Networks (SIN), 2021, pp. 1-6.

Professional Work

Peer Review Activities

- Design, Codes and Crptography - Springer.

Organization

- 15th International Conference on Information Security and Cryptology (IEEE-ISC TURKEY 2022), Presidential Public Library, Ankara, Turkey, October 19-20, 2022 **(Local Organizer)**.
- ISC Turkey - IEEE, Anatolian Crypt 2020: Computational Science and Engineering Conference, Middle East Technical University, Ankara, Turkey, September 9-11, 2020 **(Local Organizer)**.

Memberships

Systems Security Research Laboratory (S2RL) - Blockchain Workgroup, METU Computer Engineering Department

Society for Industrial and Applied Mathematics (SIAM) - Student Memberships

Skills

Programming: C, C++, Python, Matlab, MS Office
Test Scores: IELTS: 7
Languages: English (Advanced), Turkish (Native), German (Intermediate)

References

References are available upon request.