Şeyma Selcan Mağara

Applied Cryptography · Privacy Preserving Machine Learning · AI Security

University of Tübingen · Tübingen, Germany

seyma-selcan.magara@uni-tuebingen.de · sselcan.magara@gmail.com

sselcan.github.io · github.com/sselcan · linkedin.com/in/seyma-selcan-magara

Research Interests

My research sits between **applied cryptography** and **machine learning security**.

Privacy preserving computation. Secure multiparty computation, homomorphic encryption, and differential privacy: protocol design, security analysis under semi honest and malicious adversary models, and benchmarked implementations that run on real data, applied mainly to medical and genomic settings.

AI security. Adversarial attacks and model extraction, in particular how information released through model explanations becomes an exploitable channel.

The two connect: systems that need privacy guarantees also need to survive an adversary who queries them. I want to extend this work toward **confidential computing** and the **robustness of machine learning at scale**.

Education

Ph.D. in Computer Science **Nov 2022 to Sep 2026** ***(expected)***

University of Tübingen *Tübingen, Germany*

- Medical Data Privacy and Privacy Preserving Machine Learning Lab (MDPPML). Advisor: Dr. Mete Akgün.

M.Sc. in Computer Science and Engineering **2019 to 2022**

Sabancı University *Istanbul, Turkey*

- Advisor: Prof. Dr. Erkay Savaş. Full tuition waiver with monthly stipend.

B.Sc. Electronics Engineering and B.Sc. Computer Science **2013 to 2019**

Sabancı University *Istanbul, Turkey*

- Double major degree. Full tuition waiver with monthly stipend.

Research Experience

Doctoral Researcher **Nov 2022 to present**

MDPPML Lab, University of Tübingen *Tübingen, Germany*

- Designed, analysed, and implemented MPC protocols in modern C++, benchmarked over real networks: three party medical record linkage, logistic regression combining secret sharing with differential privacy, helper assisted three party sorting over 2 out of 2 additive sharing, and a CNN training pipeline for breast cancer MRI data.
- Federated analysis of VCF files for rare disease variant discovery, and the HALTA project on the FLAME platform, where I identified and helped fix a trust boundary violation in the generation of correlated randomness.
- Model extraction attacks through explainable AI, studying how released explanations leak enough information to reconstruct a target model, and evaluating defences on that channel.

Graduate Researcher **2019 to 2022**

Cryptography and Information Security Group, Sabancı University *Istanbul, Turkey*

- Homomorphic encryption for secure inference on genomic data, including a multi label tumour classification pipeline using SVM and XGBoost over encrypted data, entered in the iDASH 2020 international competition on secure genome analysis.

Publications

[1] **Ş. S. Mağara**, N. Dietrich, A. B. Ünal, M. Akgün. "Accelerating Privacy-Preserving Medical Record Linkage: A Three-Party MPC Approach". *Journal of Biomedical Informatics*, 2025.

[2] **Ş. S. Mağara**, I. Motorcu, E. Ş. Mektepli, C. Baykara, A. B. Ünal, M. Akgün. "Secure and Efficient Logistic Regression With Secret-Sharing MPC and Differential Privacy". *IEEE Access*, 2025.

[3] **Ş. S. Mağara**, C. Yıldırım, F. Yaman, B. Dilekoğlu, F. R. Tutaş, E. Öztürk, K. Kaya, Ö. Taştan, E. Savaş. "ML with HE: Privacy Preserving Machine Learning Inferences for Genome Studies". *ACM CCS Workshop on Privacy Preserving Machine Learning (PPML)*, 2021.

[4] B. Balaban, **Ş. S. Mağara**, C. Yilgor, A. Yucekul, I. Obeid, J. Pizones, F. Kleinstueck, F. J. S. Perez-Grueso, F. Pellisé, A. Alanay, E. Savaş, Ç. Bağcı, O. U. Sezerman, European Spine Study Group. "Privacy-Preserving Machine Learning (PPML) Inference for Clinically Actionable Models". *IEEE Access*, 2025.

[5] J. Jentsch, A. B. Ünal, **Ş. S. Mağara**, M. Akgün. "Privacy Preserving Data Imputation via Multi-Party Computation for Medical Applications". *IEEE International Conference on E-health Networking, Application & Services (HealthCom)*, 2024.

[6] **Ş. S. Mağara**, E. Havemann, D. Jutz, A. B. Ünal, M. Akgün. "Privacy-Preserving Detection of Rare Disease-Associated Cell Subsets via Secure Multi-Party Computation". *International Meeting on Computational Intelligence Methods for Bioinformatics and Biostatistics (CIBB)*, 2026.

[7] **Ş. S. Mağara**, A. B. Ünal, M. Akgün. "Efficient Helper-Assisted Three-Party Sorting for 2-out-of-2 Additive Sharing". (Under review.)

Teaching and Supervision

Supervision and Teaching **2022 to present**
University of Tübingen *Tübingen, Germany*

- Supervise master's students on thesis and project work in secure computation.
- Contribute to teaching in cryptography and privacy preserving machine learning courses.

Teaching Assistant **2017 to 2021**
Sabancı University *Istanbul, Turkey*

- Cryptography, Distributed Systems, Logic and Digital System Design, Discrete Mathematics.

Awards and Honours

- 5th place, iDASH 2020 international competition on secure genome analysis.
- Full tuition waiver with monthly stipend, M.Sc. programme, Sabancı University.
- Full tuition waiver with monthly stipend, B.Sc. double major programme, Sabancı University.

Technical Skills

Cryptography	Secure multiparty computation, homomorphic encryption, differential privacy, security analysis under semi honest and malicious models
AI security	Model extraction, adversarial attacks, leakage through explanation channels, threat modelling and defence evaluation
Programming	Modern C++, Python, Bash, Rust (basic)
Systems	Multithreading, socket level networking, CMake, Git, gdb, Valgrind, Linux, CI pipelines, benchmarking and profiling
Languages	Turkish (native), English (C1), German (B1)