Ege Erdoğan

ege@erdogan.dev | Homepage | LinkedIn | GitHub | Google Scholar |

Education

Technical University of Munich (Grade: **1.4**/1) — Munich, Germany
MSc in Informatics — *2022 – Present*

Koç University — Istanbul, Turkey
BSc in Computer Engineering & Mathematics — *2017 – 2022*
Cryptography, Security, and Theory specialization

Üsküdar American Academy — Istanbul, Turkey
High School — *2012 – 2017*

Research Experience

TUM DI-LAB — October 2023 – *Present*
Technical University of Munich — *Munich, Germany*
- **Supervisors**: Hannes Stärk, MSc. (MIT), Céline Marquet, MSc. (TUM)
- Flow matching for molecules, protein-ligand binding affinities (work-in-progress).

Student Research Assistant (HiWi) — June 2023 – *Present*
Technical University of Munich — *Munich, Germany*
- **Supervisor**: Mahdi Dhaini, MSc. (Prof. Florian Matthes)
- Explainable AI/NLP. Help with literature reviews, implementation and writing.

Guided Research — April 2023 – October 2023
Technical University of Munich — *Munich, Germany*
- **Supervisor**: Simon Geisler, MSc. (Prof. Stephan Günnemann)
- Adversarial robustness of graph neural networks.
- Implemented and evaluated an attack combining the evasion & poisoning threat models.

Student Research Assistant (HiWi) — November 2022 – March 2023
Helmholtz Munich, Institute of Computational Biology — *Munich, Germany*
- **Supervisor**: Dr. Ignacio Ibarra. (Prof. Fabian Theis)
- Inference of protein binding specifities.

Research Intern — July 2020 – October 2022
Koç University Cryptography, Security, and Privacy Research Group — *Istanbul, Turkey*
- **Supervisors:** Assoc. Prof. Alptekin Küpçü, Asst. Prof. Ercüment Çiçek
- Privacy-preserving collaborative machine learning.
- Design/implement attacks and defenses. Supervised summer interns in the group.

Peer-Reviewed Research

1. **Ege Erdogan**, Simon Geisler, Stephan Günnemann. "Poisoning × Evasion: Symbiotic Adversarial Robustness for Graph Neural Networks", 2023; arxiv/2312.05502. *New Frontiers in Graph Learning Workshop (NeurIPS GLFrontiers 2023).*
2. Mahdi Dhaini, Wessel Poelman, **Ege Erdogan**. "Detecting ChatGPT: A Survey of the State of Detecting ChatGPT-Generated Text", 2023; aclanthology.org/2023.ranlp-stud.1. *Student Research Workshop (at RANLP '23).*
3. **Ege Erdogan**, Alptekin Küpçü, A. Ercüment Çiçek. "SplitGuard: Detecting and Mitigating Training-Hijacking Attacks in Split Learning", 2022; doi.org/10.1145/3559613.3563198. *The 21st Workshop on Privacy in the Electronic Society (at ACM CCS '22).*
4. **Ege Erdogan**, Alptekin Küpçü, A. Ercüment Çiçek. "UnSplit: Data-Oblivious Model Inversion, Model Stealing, and Label Inference Attacks Against Split Learning", 2022; doi.org/10.1145/3559613.3563201. *The 21st Workshop on Privacy in the Electronic Society (at ACM CCS '22).*
5. **Ege Erdogan**, Can Arda Aydın, Öznur Özkasap, Waris Gill. "Demo – Zelig: Customizable Blockchain Simulator", 2021; arXiv:2107.07972. *The 40th International Symposium on Reliable Distributed Systems (SRDS '21).*

Preprints

1. **Ege Erdogan**, Unat Tekşen, Mehmet Salih Çeliktenyıldız, Alptekin Küpçü, A. Ercüment Çiçek. "SplitOut: Out-of-the-Box Training-Hijacking Detection in Split Learning via Outlier Detection", 2023; arxiv.org/abs/2302.08618. *Under review.*

Teaching

Undergraduate Tutor (x2) Feb. 2021 – June 2021 *and* Sep. 2021 - Jan. 2022
Koç University *Istanbul, Turkey*

- Weekly tutoring sessions and help with course administration for the *Computer Networks* course.

Undergraduate Teaching Assistant Sep. 2020 – Jan. 2021
Koç University *Istanbul, Turkey*

- Weekly problem sessions and office hours for the *Introduction to Programming with Python*.

Non-Research Work Experience

Software Development Intern July 2020 – Aug. 2020
Proteams *Istanbul, Turkey*

- Implemented features for different parts of a mobile application, including its back-end server, database, and admin panel.

Summer Intern July 2019
IBM *Istanbul, Turkey*

- Worked within the IBM Cloud & Cognitive team. Built a chatbot to answer questions by IBM new hires. Developed a web interface for a neural network music generation system.

Software Development Intern Feb. 2018 – April 2018
Bitlo Cryptocurrency Exchange *Istanbul, Turkey*

- Started learning and gained experience using the Spring framework to build web applications. Gained practice with the Java language.

Extracurricular Programs

- Admitted to the ML Safety (Spring 2023) course, organized by The Center for AI Safety.
- *Presenter*. Workshop on Privacy in the Electronic Society, organized as part of the ACM Conference on Computer and Communications Security, November 2022.
- *Presenter*. The 40th International Symposium on Reliable Distributed Systems, September 2021.

Skills & Interests

Languages: Turkish (native), English (fluent), German (beginner)
Computer Languages
Primary: Python (PyTorch for ML)
Others: Java/JavaScript (web development), Go (distributed systems)
Academic interests: Safety & privacy in ML, generative models, geometric ML.