Forschungspraxis, Master's Thesis

Homomorphic Encryption for Machine Learning

Homomorphic encryption (HE) schemes are increasingly attracting attention in the era of large scale computing. While lattice-based approaches have been well-studied, recently first progress has been made towards establishing code-based alternatives. Preliminary results show that such alterative approaches might enable undiscovered functionalities not present in current lattice-based schemes. In this project, we particularly study novel code-based Partial/Somewhat HE schemes tailored to applications in artificial intelligence and federated learning.

After familiarizing with SotA methods in relevant fields (such as [1]), the student should analyze the requirements for use-cases at hand and explore suitable modifications to current schemes and novel approaches.


Prerequisites

- Strong foundation in linear algebra
- Channel Coding
- Security in Communications and Storage
- Basic understanding of Machine Learning concepts

Advisors

Sebastian Bitzer, Maximilian Egger