KASTEL - Institut für Informationssicherheit und Verlässlichkeit
Lehrstuhl Prof. Dr. J. Müller-Quade
https://crypto.kastel.kit.edu

Efficient and Secure Multiparty Computation via Trusted Execution Environment

Bachelor's/Master's Thesis

Secure Multiparty Computation (MPC) is a powerful tool for several parties to compute a function together without revealing their private inputs. The main drawback of MPC is that (malicious secure) protocols often require heavy communication amoung parties. A lot of recent papers make use of Trusted Execution Environment (TEE) to accerlerate communictation-inefficient MPC protocols and ensure malicious security, by simply assuming that TEE is fully trusted. In this work, we want to propose a hybrid solution using both MPC and TEE, without giving fully trust to TEE.

Scope of the work

- Getting familiar with MPC protocols.
- Having an overview of different TEE models.
- Benchmarking the existing (open source) frameworks.
- You have two ways to finalize your work:
  - You make use an existing **python** framework and rewrite the low level TEE layer to manage data transfer between CPU and a simulated TEE environment.
  - You implement your work from scratch. This requires you to build a simple network application with socket and configure a TEE environment by yourself (e.g. SGX, TDX or a simulated TEE environment).

Requirements

- Bachelor/Master student in Computer Science, Electrical Engineering or similar.
- Excellent programming skill in python (or C++, depending on which option above you choose) including trouble shooting and environment setup.
- Highly motivated for this topic.
- Basic knowledge of TEE or MPC is a bonus.

What we offer

- A possibility to write and contribute to a scientific paper.
- A close supervision.

Contact

In case of interest or for further information, please contact Yufan Jiang, yufan.jiang@kit.edu.