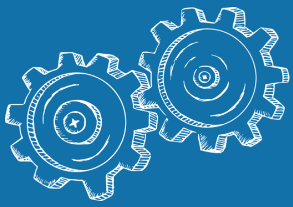
IAIK | Institute of Applied Information Processing and Communications



Let's Secure the Party: homomorphic encryption for multiple clients

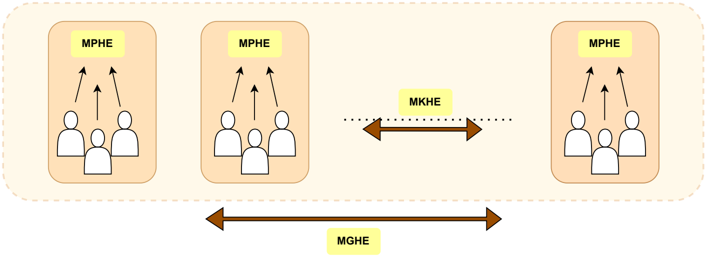
Advisor: **Anisha Mukherjee**

Motivation

Homomorphic Encryption (HE) has emerged as a key technology for secure computation over encrypted data, even in privacy-preserving multi-party computation (MPC) scenarios. Current research focuses on optimizing HE schemes to support multiple participants while preserving efficiency and security. One advanced scenario involves a multi-group HE scheme, where several distinct groups—each consisting of multiple clients—collaborate for homomorphic computation on their encrypted data. This thesis will focus on generalizing parameters for certain functionalities and optimizing certain modules of such a scheme based on the available proof-of-concept implementation. The implementation will mostly deal with polynomial arithmetic so an in-depth knowledge of the scheme's nuances are not a pre-requisite.

Goals and Tasks

- **Get familiar with existing methods:** Study the basics of HE (only a general idea is enough) and understand the current implementation of the various functionalities. [4 - 5 weeks]
- **Identify scopes of improvement and finalize:** Extend parameter support of a few functionalities and look for possible optimizations. [4 - 5 weeks]
- **Validate your code:** Ensure that the new implementation produces results consistent with the original code and finalize documentation. [4 - 5 weeks]



Literature

› Hyesun Kwak, Dongwon Lee, Yongsoo Song, and Sameer Wagh
A General Framework of Homomorphic Encryption for Multiple Parties with Non-interactive Key-Aggregation
https://eprint.iacr.org/2021/1412

Courses & Deliverables

☑ **Introduction to Scientific Working**
Short report on background
Short presentation

☑ **Bachelor Project**
Project code and documentation

☑ **Bachelor's Thesis**
Project code
Thesis
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ MATH

Prerequisites

› Interest in the topic area

› Programming (C/C++, Python)

Advisor Contact

anisha.mukherjee@iaik.tugraz.at