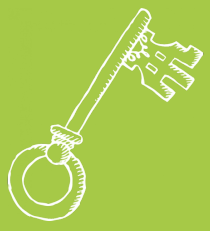

Efficient Implementations for Client-Side Homomorphic Encryption

Advisor: **Florian Krieger**

Motivation

Fully Homomorphic encryption (FHE) is often considered the Holy Grail of cryptography as it allows arbitrary computations on encrypted data. This fundamental privacy-preserving property of FHE opens various application scenarios such as encrypted AI inference or confidential blockchain transactions. However, deploying FHE is challenging due to its performance overhead by orders of magnitude. Most works target accelerating server-side operations, while little attention has been given to client-side operations.

The goal of this thesis is to focus on the underexplored client-side operations in FHE. We already have a set of implementation ideas to make FHE more client-friendly, such as optimized parameter selection or computation offloading to the server. Your task in this thesis is to explore these ideas further, implement them, and evaluate these techniques. In addition, you can investigate the side-channel aspects of client-side FHE, either by attacking existing implementations or by applying countermeasures such as masking.

Goals and Tasks

- Get familiar with existing FHE schemes (e.g. CKKS)
- Implement efficient and secure client-side FHE
- Evaluate and analyze your implementation

Literature

- F. Krieger et al.
  Aloha-HE: A Low-Area Hardware Accelerator for Client-Side Operations in Homomorphic Encryption
  DATE 2024
  doi:10.23919/DATE58400.2024.10546608

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in the topic
- Understanding of basic cryptography

Advisor Contact

florian.krieger@tugraz.at