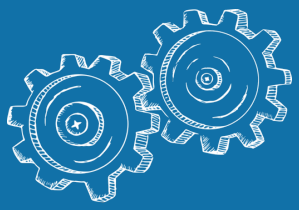


Compact and Side-channel Secure Implementations for Client-side Homomorphic Encryption Operations

Advisor: **Ahmet Can Mert**

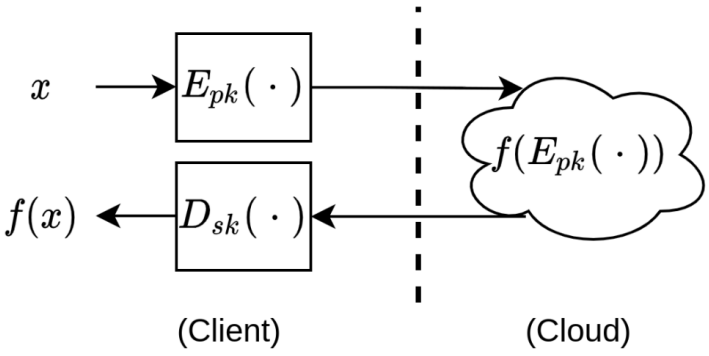
Motivation

Homomorphic encryption (HE) enables computation on the encrypted data. Although the acceleration of cloud-side HE operations has gained broad attention, there are only a few works on the efficient implementation of client-side HE operations.

The goal of this project is to design compact and side-channel secure implementations for client-side HE operations (i.e., key generation, encryption, decryption, etc.). The target platform (FPGAs -RTL or HLS-, Microcontroller, etc.) can be determined based on the interest of the student. **Two students can work on this project.**

Goals and Tasks

- Get familiar with the schemes and their client-side operations.
- Analyze main building blocks used in client-side HE operations (i.e., polynomial multiplication and sampling).
- Propose design methodologies for compact and side-channel secure client-side implementations.
- Implement and evaluate the final architecture using the proposed methodologies.



Literature

- Z. Azad et al.
  RACE: RISC-V SoC for En/decryption Acceleration on the Edge for Homomorphic Computation
- F. Aydin et al.
  RevEAL: single-trace side-channel leakage of the SEAL homomorphic encryption library

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

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

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in HW/SW design
- Programming (C/C++, Verilog)

Advisor Contact

ahmet.mert@iaik.tugraz.at