MSc/BSc projects in our group (1)

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.

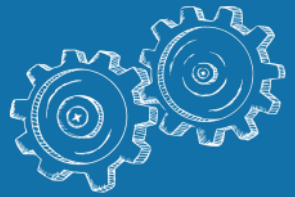
The goal of this project is to design compact and side-channel secure implementations for client-side HE operations (i.e., key generation, encryption, decryption, etc.). The target platform (FPGAs -RTL or HLS-, Microcontroller, etc.) can be determined based on the interest of the student. **Two students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

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

MSc/BSc projects in our group (2)



High-performance architecture for NIST PQC selected schemes CRYSTALS-Kyber and CRYSTALS-Dilithium

Advisor: **Aikata, Ahmet Can Mert**

Motivation

With the selection of CRYSTALS-Kyber and CRSYATLS-Dilithium for PQC standardization, several designers are coming up with low-area or high-performance architectures. One cryptoprocessor, *Kali*, focuses on the former design goal.

The goal of this project is the latter, proposing a high-performance implementation for these schemes outperforming the existing results in the literature. Also, you will be able to realize and verify your design on an Alveo U250 accelerator card.

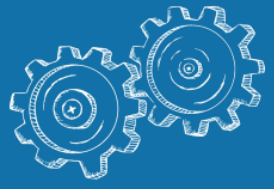
Literature

› A. Aikata et al.
KaLi: A Crystal for Post-Quantum Security
https://eprint.iacr.org/2022/1086
2022

Courses & Deliverables

☑ **Master Project**
Project code
Report

MSc/BSc projects in our group (3)



Side-channel evaluation of NIST PQC selected schemes CRYSTALS-Kyber and CRYSTALS-Dilithium

Advisor: **Aikata Aikata, Ahmet Can Mert**

Motivation

NIST has selected CRYSTALS-Kyber and CRSYATLS-Dilithium for standardization. Now the users need efficient and secure implementations to deploy them. Our group has designed a unified cryptoprocessor, `KaLi`, for both schemes. Together we will embark on a journey of protecting it against side-channel analysis. This will involve the application of the traditional masking scheme as well as exploring alternate cheaper countermeasures.

Goals and Tasks

- Understand the schemes and their implementations.
- Come up with efficient masking method.

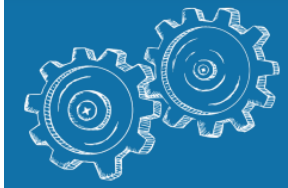
Literature

› A. Aikata et al.
KaLi: A Crystal for Post-Quantum Security
https://eprint.iacr.org/2022/1086
2022

Courses & Deliverables

- ☑ **Master Project**
  - Project code
  - Report
  - Presentation

MSc/BSc projects in our group (4)



Vectorizing isogeny-based signature scheme

Advisor: **Anisha Mukherjee and David Jacquemin**

Motivation

Isogenies between supersingular elliptic curves have turned heads among the post quantum cryptographic community. But there are only a handful of isogeny-based signature schemes because creating large challenge sets for them turned out to be easier said than done. SQISign emerges as a game-changer in this context, with signature and key sizes smaller than all other post-quantum signature schemes!
For this, it makes use of a special set of bijections, the 'Deuring correspondence'.

A starting point for your work would be to identify the main building blocks of the scheme and the clever interchange of domains between ideals in quaternion algebra and isogenies between elliptic curves. Next, you would analyse the code and figure out which parts of it could be effectively vectorized.
Your main goal in this thesis would be to accelerate the different algorithms involved in the Deuring correspondence.

Literature

- *SQISign: compact post-quantum signatures from quaternions and isogenies*

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

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

MSc/BSc projects in our group (5)

Hardware acceleration of Zero-Knowledge Proof systems.

Contact person: Florian Hirner and Ahmet Can Mert

Classical topics in Cryptographic Engineering

Random Number Generation

1. Unified hardware for all statistical tests including several new ones.
2. Studying and designing new kinds of TRNGs
3. Active attacks on RNGs.

Physically Unclonable Function (PUF)

1. Implementing PUFs in FPGAs
2. Studying machine learning attacks on them

Symmetric-key Cryptography

1. Efficient implementation of lightweight ciphers
2. Side-channel protection using masking