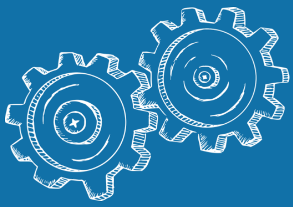
IAIK | Institute of Applied Information Processing and Communications



Analyzing and Integrating Novel Side-channel Countermeasures into Lattice-based Crypto

Advisor: **Rishub Nagpal**

Motivation

New quantum resistant public-key cryptographic algorithms, such as CRYSTALS-Kyber and CRYSTALS-Dilithium, are being deployed after having been chosen for standardization by NIST. However, these new schemes suffer from unique implementation challenges and are vulnerable to side-channel attacks. To resist, new countermeasures tailored specifically to the algorithms need to be studied, developed and implemented securely to ensure device safety for the future.

This project involves integrating a newly developed countermeasure against SPA attacks into optimized ARM implementations of lattice-based crypto[1]. Following the implementation, the countermeasure(s) must be tested on a real device: the Cortex-M4. For more details, contact the linked email.

Goals and Tasks

- Get familiar with the state-of-the-art in post-quantum cryptography
- Integrate a new countermeasure into the PQM4 library
- Perform an SPA attack on a real device to test your new countermeasure

Literature

- M. J. Kannwischer et al.
  PQM4: Post-quantum crypto library for the ARM Cortex-M4
  https://github.com/mupq/pqm4
- T. Tosun, A. Moradi, and E. Savas
  Exploiting the Central Reduction in Lattice-Based Cryptography
  Cryptology ePrint Archive, Paper 2024/066 2024
  https://eprint.iacr.org/2024/066
  https://eprint.iacr.org/2024/066

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in PQC and Side-channel attacks
- Programming in C/ARM Assembly

Advisor Contact

rishub.nagpal@iaik.tugraz.at