IAIK | Institute of Applied Information Processing and Communications

Analysis of Side-channel protections for polynomial multiplication.

Advisor: **Aikata**

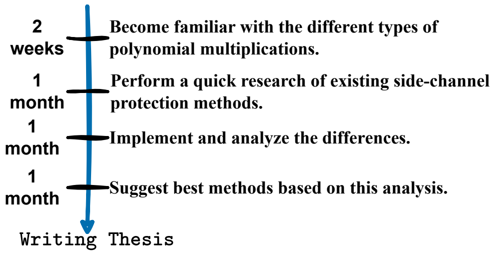
DATE: November 20, 2024

Motivation

The lattice-based post-quantum schemes (PQC) consist of two giant building blocks, Keccak and polynomial multiplier. They deal with security-critical components and therefore require side-channel protections. There are various methods to protect Keccak, however very few ingenious ways for the polynomial multiplier based on scheme specifications.

Thus, this thesis would aim at analyzing the naive methods and compare them with the newly proposed scheme-specific optimized methods. This analysis would be performed for multiple lattice-based PQC schemes in Software. Depending on the interest it can further be extended to Hardware. The icing on the cake would be a new method that can surpass the existing methods.

Goals and Tasks



2 weeks — Become familiar with the different types of polynomial multiplications.

1 month — Perform a quick research of existing side-channel protection methods.

1 month — Implement and analyze the differences.

1 month — Suggest best methods based on this analysis.

Writing Thesis

Literature

- Aikata Aikata, Andrea Basso, Gaetan Cassiers, Ahmet Can Mert, and Sujoy Sinha Roy
  Kavach: Lightweight masking techniques for polynomial arithmetic in lattice-based cryptography
  https://eprint.iacr.org/2023/517

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 ☑ SEM

Prerequisites

- Interest in the topic area
- Basic knowledge of programming in C/C++ (for SW) or Verilog/VHDL (for HW)

Advisor Contact

aikata@iaik.tugraz.at