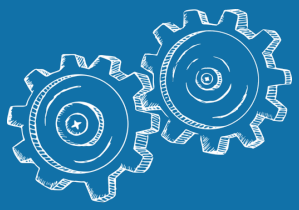


Analysis of polynomial multipliers for Post-quantum schemes in Software

Advisor: **Aikata**

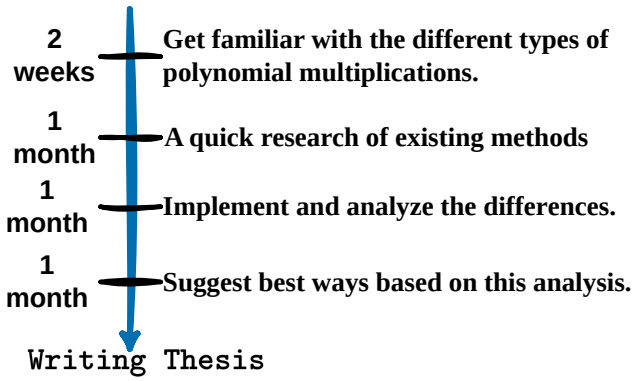
DATE: November 20, 2024

Motivation

Polynomial multiplication is the major building block in all lattice-based Post-quantum schemes. The literature presents several methods to perform this, however, it is difficult to gaze at the advantage or disadvantages of one approach over the other. This, not only depends on the scheme specification but also the environment under consideration.

The purpose of this thesis would be to pick distinct lattice-based schemes and analyze different multiplication methods. In conclusion, the best methods should be presented in software along the dimension of lightweight, and high-speed designs.

Goals and Tasks



Literature

- Matthias J. Kannwischer
  Polynomial Multiplication for Post-Quantum Cryptography
  https://kannwischer.eu/thesis/phd-thesis-print-version.pdf

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++

Advisor Contact

aikata@iaik.tugraz.at