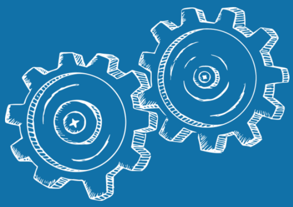
IAIK | Institute of Applied Information Processing and Communications



Evaluation of modular multiplication methods used in lattice-based cryptography on FPGA/ASIC

Advisor: **Aikata**

Posted on: Sep 19, 2024

Motivation

The modular multiplier is a fundamental arithmetic operation used in lattice-based cryptography which uses modular arithmetic excessively. Thus, the performance and area of a modular multiplier implementation have a significant impact on the overall performance of a lattice-based cryptography implementation. In the literature, several modular multiplier implementations are targeting different applications or target device constraints.

This thesis targets presenting a comparison of different modular multiplier implementations in hardware in literature. Specifically, this thesis will present the area and performance results of different modular multiplication implementations in FPGA/ASIC platforms targeting lattice-based cryptography.

Goals and Tasks

- Getting familiar with lattice-based cryptography and the different types of modular multiplication methods. [2-Weeks]
- A literature search of existing methods. [1-Month]
- Implement and obtain area/performance results of different methods. [1-Month]
- Analysis of the results and preparing documentation. [1-Month]
- If possible, propose optimizations for the existing methods (optional)

Literature

- D. Soni et al.
  Design Space Exploration of Modular Multipliers for ASIC FHE accelerators
  https://ieeexplore.ieee.org/abstract/document/10129292

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 SystemVerilog and Python

Advisor Contact

aikata@iaik.tugraz.at