



Design space exploration of CRYSTALS-Kyber's polynomial multiplication in hardware

Advisor: **Aikata**





Posted on: Sep 19, 2024

Motivation

The National Institute of Standards and Technology (NIST) started a competition to select the next quantum-secure (post-quantum) cryptographic schemes in 2016. The competition concluded in 2022 and CRYSTALS-Kyber is selected as the winner of the post-quantum key-encapsulation mechanism. CRYSTALS-Kyber is a lattice-based cryptography scheme and it uses polynomial multiplication excessively. Thus, the implementation performance of CRYSTALS-Kyber's NTT-based polynomial multiplication has a significant impact on the performance of the overall scheme (both in SW and HW).

The goal of this project is to perform a design space exploration of Kyber's polynomial multiplication for HW platforms. The project will focus on different NTT methods (unrolled, iterative, pipelined, etc.) to evaluate the performance and area cost of different approaches. The project ultimately targets creating an open HW-library for the polynomial multiplication methods of Kyber.

Goals and Tasks

-  Get familiar with CRYSTALS-Kyber's polynomial multiplication operation.
-  Study the existing methods and implementations in literature.
-  List different design methodologies targeting different performance/area goals.
-  Implement and evaluate different architectures.

Literature

- > [F. Yaman et al.](#)
A Hardware Accelerator for Polynomial Multiplication Operation of CRYSTALS-KYBER PQC Scheme
<https://ieeexplore.ieee.org/abstract/document/9474139>

Courses & Deliverables

- Master Project**
Project code
Report
Presentation
- OR –
- Master's Thesis + DiplomandInnenseminar (CS)**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

- CS ICE SEM

Prerequisites

- > Interest in cryptographic hardware design
- > Programming (Python, SystemVerilog)

Advisor Contact

aikata@iaik.tugraz.at