

# Design space exploration of CRYSTALS-Dilithium'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-Dilithium is selected as one of the post-quantum digital signature winners. CRYSTALS-Dilithium is a lattice-based cryptography scheme and it uses polynomial multiplication excessively. Thus, the implementation performance of CRYSTALS-Dilithium'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 Dilithium'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 polynomial multiplication methods of Dilithium.

## Goals and Tasks

-  Get familiar with CRYSTALS-Dilithium'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

- > [L. Beckwith et al.](#)  
High-Performance Hardware Implementation of CRYSTALS-Dilithium  
<https://ieeexplore.ieee.org/abstract/document/9609917>

## Courses & Deliverables

- Master Project**  
Project code  
Report  
Presentation
- OR –
- Master's Thesis + Diplomandinenseminar (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@tugraz.at](mailto:aikata@tugraz.at)