High-performance architecture for NIST PQC selected schemes CRYSTALS-Kyber and CRYSTALS-Dilithium

Advisor: **Aikata**

Motivation

With the selection of CRYSTALS-Kyber and CRSYATLS-Dilithium for PQC standardization, several designers are coming up with low-area or high-performance architectures. One cryptoprocessor, *Kali*, focuses on the former design goal.

The goal of this project is the latter, proposing a high-performance implementation for these schemes outperforming the existing results in the literature. Also, you will be able to realize and verify your design on an Alveo U250 accelerator card.

Goals and Tasks

- Get familiar with the schemes and analyze their main building blocks.

- Propose methodologies for high-performance implementations (e.g., unrolling operations such as NTT).

- Implement and verify the final architecture using the proposed methodologies.

Literature

> A. Aikata et al.
> KaLi: A Crystal for Post-Quantum Security
> https://eprint.iacr.org/2022/1086
> 2022

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 hardware design

> Programming (C/C++, Verilog)

Advisor Contact

aikata@iaik.tugraz.at