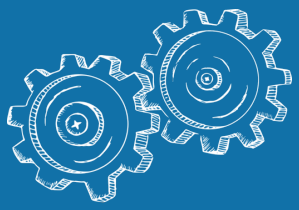


Side-channel evaluation of NIST PQC selected schemes CRYSTALS-Kyber and CRYSTALS-Dilithium

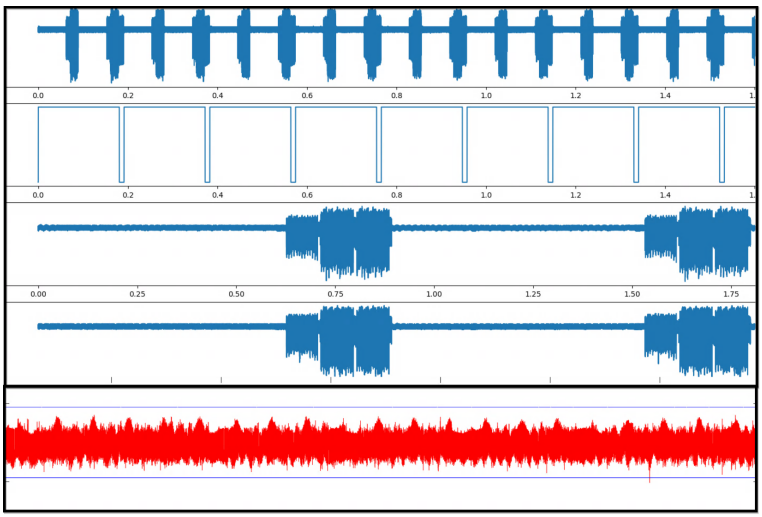
Advisor: **Aikata Aikata, and Ahmet Can Mert**

Motivation

NIST has selected CRYSTALS-Kyber and CRSYATLS-Dilithium for standardization. Now the users need efficient and secure implementations to deploy them. Our group has designed a unified cryptoprocessor, `KaLi`, for both schemes [1]. Together we will embark on a journey of protecting it against side-channel analysis. This will involve the application of the traditional masking scheme as well as exploring alternate cheaper countermeasures.

Goals and Tasks

- Understand the schemes and their implementations.
- Come up with efficient masking method.
- Explore alternate cheap countermeasures.



Literature

› [1] *KaLi: A Crystal for Post-Quantum Security*

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 implementation security
- Programming (C/C++, Verilog)

Advisor Contact

aikata@iaik.tugraz.at