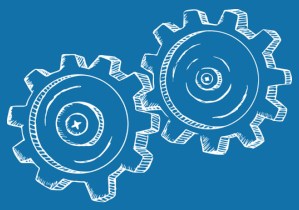

Analysing and Protecting Post Quantum Schemes against Side Channel Attacks

Advisor: **Maciej Czuprynko**

Motivation

The emergence of a powerful quantum computer threatens the security of current digital signature schemes. To prepare for this, the National Institute of Standards and Technology (NIST) initiated a call for post-quantum Key Encapsulation Mechanisms (KEMs) and digital signature schemes. Currently, the selection of KEMs has ended. On the other hand, the 2nd round of the submission for additional signature schemes is ongoing. In both cases, one aspect of the implementation of the schemes that must be considered is the resistance to side channel attacks and the cost to protect against them.
In this project, multiple schemes are of interest: HQC, FEAST, CROSS and SQIsign. The only KEM being HQC. As such, the project can be taken up by one or more students. The goal then is to analyse the security of the schemes and/or to propose countermeasures.

Goals and Tasks

- Get familiar with the scheme and get to know existing side channel attacks.
- Analyse the security of the scheme and/or propose countermeasures.
- Implement the proposed attack/countermeasure on a microcontroller and benchmark its cost.

Literature

- Mentioned scheme specifications:
  https://pqc-hqc.org
  https://faest.info
  https://cross-crypto.com
  https://sqisign.org

Courses & Deliverables

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in Post Quantum Cryptography and Side Channel attacks
- Knowledge of Python and C/C++
- "Side-Channel Security" course is recommended

Advisor Contact

maciej.czuprynko@tugraz.at