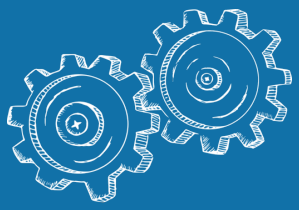

Efficient Arithmetic for Post Quantum Cryptography

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 digital signature schemes. This lead to the development of novel schemes, which often introduce the use of new, in the context of cryptography, arithmetic algorithms. As such, it is interesting to research optimizations for efficient implementations. One such case is SQIsign signature scheme. Currently, there exists a C implementation of the scheme. However, not much consideration was made to implement it efficiently.
In this context, the goal of the project is to implement arithmetic on big integers. As a starting point, we would consider the most used operations such as addition, multiplication, division and modular reduction. There, the possible optimization will be explored and compared.

Goals and Tasks

- Understand the operations that need to be implemented.
- Get familiar with the arithmetic operations and their efficient implementations.
- Implement the algorithms and compare them to find the most efficient one.
- Propose optimizations.

Literature

- Multiplication algorithms
  https://en.wikipedia.org/wiki/Multiplication_algorithm
- SQIsign arithmetic functions
  https://github.com/SQISign/the-sqisign/blob/main/src/mini-gmp/mini-gmp.c

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
- Knowledge of Python and C/C++
- "Crypto on Software" course is recommended

Advisor Contact

maciej.czuprynko@tugraz.at