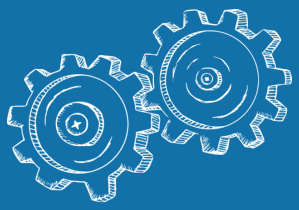

Efficient Arithmetic for Post Quantum Cryptography

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. In particular, the focus is to explore efficient multiplication algorithms and modular reductions (such as the Montgomery reduction).

Goals and Tasks

- Understand the multiplication and modular reduction algorithms.
- Implement the algorithms and compare them to find the most efficient one.
- Propose optimizations.

Literature

- Multiplication algorithms
  https://en.wikipedia.org/wiki/Multiplication_algorithm
- Montgomery reduction
  https://en.wikipedia.org/wiki/Montgomery_modular_multiplication

Courses & Deliverables

- ☑ **Introduction to Scientific Working**
  Short report on background
  Short presentation
- ☑ **Bachelor Project**
  Project code and documentation
- ☑ **Bachelor's Thesis**
  Project code
  Thesis
  Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in Post Quantum Cryptography
- Knowledge of Python and C/C++

Advisor Contact

maciej.czuprynko@tugraz.at