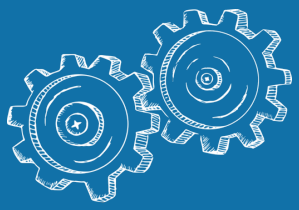

Efficient Hardware Implementation of the Gaussian Elimination

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. Among the promising candidates, several of them use the Gaussian elimination algorithm as a subroutine. For instance, in the signature scheme LESS, it is used to obtain a row reduced representation. It is also used in MAYO and UOV in order to solve a system of equations. The Gaussian elimination is an expensive operation and thus takes up a significant part of the run time, if not the most. As such, any improvement in this function leads to a similar improvements in the overall execution time.

This project thus aims to investigate hardware-specific optimizations which can be used to develop high-performance and/or low-area implementations of the Gaussian elimination.

Goals and Tasks

- Get familiar with the existing implementations of the Gaussian reduction.
- Implement optimizations for efficient hardware acceleration of the subroutine.
- Compare your results to other PQ signature hardware accelerators.

Literature

- Gaussian elimination
  https://en.wikipedia.org/wiki/Gaussian_elimination
- L. Beckwith et al.
  A High-Performance Hardware Implementation of the LESS Digital Signature Scheme
  Post-Quantum Cryptography

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 hardware design
- Knowledge of Verilog, Python and C/C++
- "Crypto on Hardware" course is recommended

Advisor Contact

maciej.czuprynko@tugraz.at