



Matrices in Hermite Normal Form for memory constrained devices

Advisor: **Anisha Mukherjee**

Motivation

The rise of quantum computers threatens the security of currently deployed cryptographic primitives such as digital signatures. To address this, NIST initiated a call for post-quantum signatures, leading to the proposal of a number of new schemes. One such candidate is called SQIsign which has the smallest signature sizes. However, the SQIsign implementation currently demands a large RAM, making microcontroller deployment challenging.

The aim of this thesis will be to investigate memory optimisation that can be introduced for the scheme, but with a focus on only one particular algorithm: the computation of the Hermite Normal Form. Essentially, given any matrix, the algorithm returns an upper triangular one that preserves some properties of the input matrix. This computation leads to large blow ups in the size of the elements, and thus a large memory consumption. As such, it is an interesting starting point for memory optimization.

Goals and Tasks

-  Explore the algorithm that computes the Hermite Normal Form.
-  Investigate possible optimization to reduce the memory usage.
-  Implement the algorithm.

Literature

- > Hermitian normal form implementation
<https://github.com/SQISign/the-sqisign/blob/main/src/quaternion/ref/generic/hnf/hnf.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

anisha.mukherjee@tugraz.at