

Timing experiments on isogeny-based signature schemes




Advisor: **Anisha Mukherjee and David Jacquemin**

Motivation

Isogeny-based protocols have emerged as one of the leading families of post-quantum cryptographic schemes, especially the submission of SQISign to the NIST standardization process. These protocols offer significant advantages, including signature and key sizes smaller than any other post-quantum signature schemes. Recently, newer variants have also been published. All of these variants have only proof-of-concept implementation with very little experiments being run on them.

This thesis will focus on working with the available SQISign libraries to obtain timing results for several functions and parameter sets. Note that the experimentation will deal with getting familiar with the libraries and working with them, so an in-depth knowledge of isogeny-based mathematical concepts is not a pre-requisite.

Goals and Tasks

-  Familiarity with basic SQISign and associated libraries. [4 - 5 weeks]
-  Analyse the run-time of the various functions and experiment with different parameters [7 - 9 weeks]
-  Provide insights on the obtained results and final documentation [1 - 2 weeks]



Literature

- > [Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski](#)
SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies
https://doi.org/10.1007/978-3-030-64837-4_3

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
- MATH

Prerequisites

- > Interest in the topic area
- > Programming (C/C++, Python)

Advisor Contact

anisha.mukherjee@tugraz.at