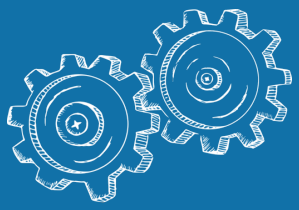

# Accelerating integer arithmetic for isogenies

Advisor: **Anisha Mukherjee and David Jacquemin**

## Motivation

Isogeny-based protocols have become a key family of post-quantum cryptographic schemes. However, there are only a few isogeny-based signature schemes, as creating large challenge sets for them has proven more difficult than anticipated. SQISign has emerged as a breakthrough, offering signature and key sizes smaller than any other post-quantum signature schemes.

The core performance of SQISign relies on efficient large-sized modular arithmetic. The primary goal of this thesis is to design dedicated and efficient modular arithmetic in hardware for SQIsign.

## Goals and Tasks

- Understand integer and modular arithmetic modules in SQIsign. [4 - 5 weeks]
- Implement the functions of integer unit in hardware. [8 - 10 weeks]
- Investigate possible optimizations for field arithmetic and other low-level operations. Final thesis preparation. [5 - 8 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

☑ **Master Project**
Project code
Report
Presentation

– OR –

☑ **Master's Thesis**
**+ DiplomandInnenseminar (CS)**
Initial presentation
Project code
Thesis (60+ pages)
Final presentation

## Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

## Prerequisites

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

## Advisor Contact

anisha.mukherjee@tugraz.at