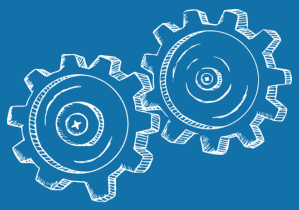

Vectorizing isogeny-based signature scheme

Advisor: **Anisha MUKHERJEE and David JACQUEMIN**

Motivation

Isogenies between supersingular elliptic curves have turned heads among the post quantum cryptographic community. But there are only a handful of isogeny-based signature schemes because creating large challenge sets for them turned out to be easier said than done. SQISign emerges as a game-changer in this context, with signature and key sizes smaller than all other post-quantum signature schemes!
For this, it makes use of a special set of bijections, the 'Deuring correspondence'.

A starting point for your work would be to identify the main building blocks of the scheme and the clever interchange of domains between ideals in quaternion algebra and isogenies between elliptic curves. Next, you would analyse the code and figure out which parts of it could be effectively vectorized.
Your main goal in this thesis would be to accelerate the different algorithms involved in the Deuring correspondence.

Goals and Tasks

- Accustom yourself with the Deuring correspondence and Vectorization
- Implement and evaluate the main algorithms of the Deuring correspondence using vectorization

Literature

- *SQISign: compact post-quantum signatures from quaternions and isogenies*

Courses & Deliverables

☐

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Familiar with programming in C language
- Interest in mathematical cryptography

Advisor Contact

{anisha.mukherjee,david.jacquemin}@iaik.tugraz.at