PART 6

THE BEAST

Remember that I said verification is relatively easy?

1D SQIsign

Verification recomputes a 2^{1000} isogeny

$$\varphi_{\text{resp}} : E_A \to E_2$$

in a number of blocks

$$\varphi_i : E^{(i)} \to E^{(i+1)}$$

All of this is done over $\mathbb{F}_{p^2}$ and requires a few essential building blocks that we know for a long time now.

- isogeny-evaluation formulas
- pairing-based techniques
- efficient basis sampling
- point compression
- curve normalisation

2D SQIsign

Verification recomputes a 2^{128} isogeny

$$E_1 \times E_2 \to F_1 \times F_2$$

in a single block.

All of this is done over $\mathbb{F}_{p^2}$, and for such "short" 2D-isogenies, we essentially only need formulas to evaluate the isogeny.

These have recently been studied by Dartois, Maino, Pope, Robert using theta-models.

(If you ever heard of Richelot isogenies between hyperelliptic curves, they are essentially the same, but different…)

2D 1D-SQIsign

Map the 2^{1000} isogeny from 1D SQIsign over $\mathbb{F}_{p^2}$ to a 2D isogeny over $\mathbb{F}_p$ using Scholten's construction and Costello's isogenies.

Requires *tons of work* as we now don't do a single "short" 2D-isogeny, but a number of blocks.

So, we developed:

- pairing-based techniques
- efficient basis sampling
- point compression
- curve normalisation

PART 6

THE BEAST

Remember that I said verification is relatively easy?

Return of the Kummer:
a toolbox for genus 2 cryptography

Maria Corte-Real Santos[1] and Krijn Reijnders[2]

[1] University College London
maria.santos.20@ucl.ac.uk
[2] Radboud University, Nijmegen, The Netherlands
krijn@cs.ru.nl

2D 1D-SQIsign

Map the 2^{1000} isogeny from 1D SQIsign over $\mathbb{F}_{p^2}$ to a 2D isogeny over $\mathbb{F}_p$ using Scholten's construction and Costello's isogenies.

Requires *tons of work* as we now don't do a single "short" 2D-isogeny, but a number of blocks.

So, we developed:

- pairing-based techniques
- efficient basis sampling
- point compression
- curve normalisation