PART 6

THE BEAST

Remember that I said verification is relatively easy?

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