

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 Santos¹ and Krijn Reijnders²

¹ University College London
maria.santos.20@ucl.ac.uk

² Radboud University, Nijmegen, The Netherlands
krijn@cs.ru.nl

Q: Is it faster than 1D or 2D? A: No.

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 Santos¹ and Krijn Reijnders²

¹ University College London
maria.santos.20@ucl.ac.uk

² Radboud University, Nijmegen, The Netherlands
krijn@cs.ru.nl

Q: Is it faster than 1D or 2D? A: No.

Q: Is it much more difficult?

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