PART 5

A 1D Miracle?

2020

SQIsign

A new isogeny-based signature scheme, with **high soundness.**

2021

2022

SQIsign2

A new algorithm to translate ideals to isogenies.

The SIKE breaks

In a series of three papers, SIKE was destroyed using **HD isogenies** in the summer of 2022.

2023

AprèsSQI

Signing will be slow... We push verification to the limits using extension fields.

SQIsignHD

Use the SIKE attacks! Represent the response as a **HD isogeny**. Required 4/8-dimensions.

2024

More 1D?

Recent works seem to allow improved signing for Après-primes, *(and more...)*

Going 2D

Simultaneously, three works adapted SQIsignHD to enable verification with **2D isogenies**

PART 5

A 1D Miracle?

Remember this slide?

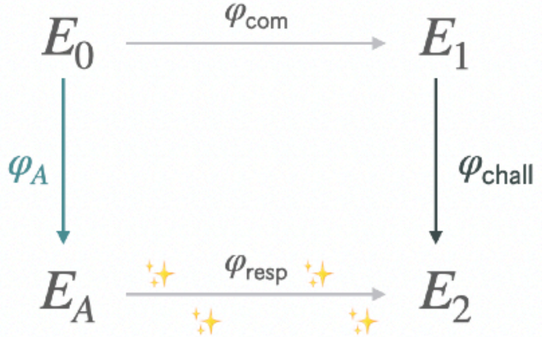
PART 3

New Dimensions

extension fields

in signing, we want to keep working over $\mathbb{F}_{p^2}$ for efficiency reasons

Idea: signing is slow anyway, what if we work over $\mathbb{F}_{p^{2k}}$ during signing, and push verification speeds to the absolute limits?



1 instead of (slow) translation of I_{resp} to φ_{resp} in 13 blocks....

2 slower translation using $\mathbb{F}_{p^{2k}}$ arithmetic but only 4 blocks!

✗ **signing is now even slower, using extension fields, takes literal seconds**

✓ **faster primes!**

✓ **fewer blocks!**

✓ **FAST verification!**

Radboud University

Radboud University

[2024/778]: Hiroshi Onuki, Kohei Nakagawa *"Ideal-to-isogeny algorithm using 2-dimensional isogenies and its application to SQIsign"*