PART 3

New Dimensions

SQIsign

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

SQIsign2

A new algorithm to translate ideals to isogenies.

AprèsSQI

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

The SIKE breaks

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

SQIsignHD

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

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?