

PART 3

New Dimensions

SQLsign

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

SQLsign2

A new algorithm to translate ideals to isogenies.

2020

2021

2022

2023

2024

The SIKE breaks

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

SQLsignHD

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

PART 3
New Dimensions

HD representations

instead of describing 1D isogeny $\varphi : E \rightarrow E'$ by its kernel $\ker \varphi$,
we can also describe it by $E, P_1, \dots, P_n, \varphi(P_1), \dots, \varphi(P_n)$, for enough points $P_i \in E$

then, with Kani's lemma & improvements, compute $\varphi(Q)$ for any other $Q \in E$