PART 2
The BREAK

SQIsign

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

SQIsign2

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.

PART 2

The BREAK

Castryck & Decru (2022)

$$\begin{tikzcd} E_0 \arrow[r, "\psi"] \arrow[d, "\varphi"'] & E_A \arrow[d, "\varphi'"] \\ E_B \arrow[r, "\psi'"] & E_{AB} \end{tikzcd}$$

in SIDH/SIKE the secrets are φ and ψ