

## PART 2

# The BREAK

### SQLsign

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

### SQLsign2

A new algorithm to translate ideals to isogenies.

2020

2021

2022

2023

2024

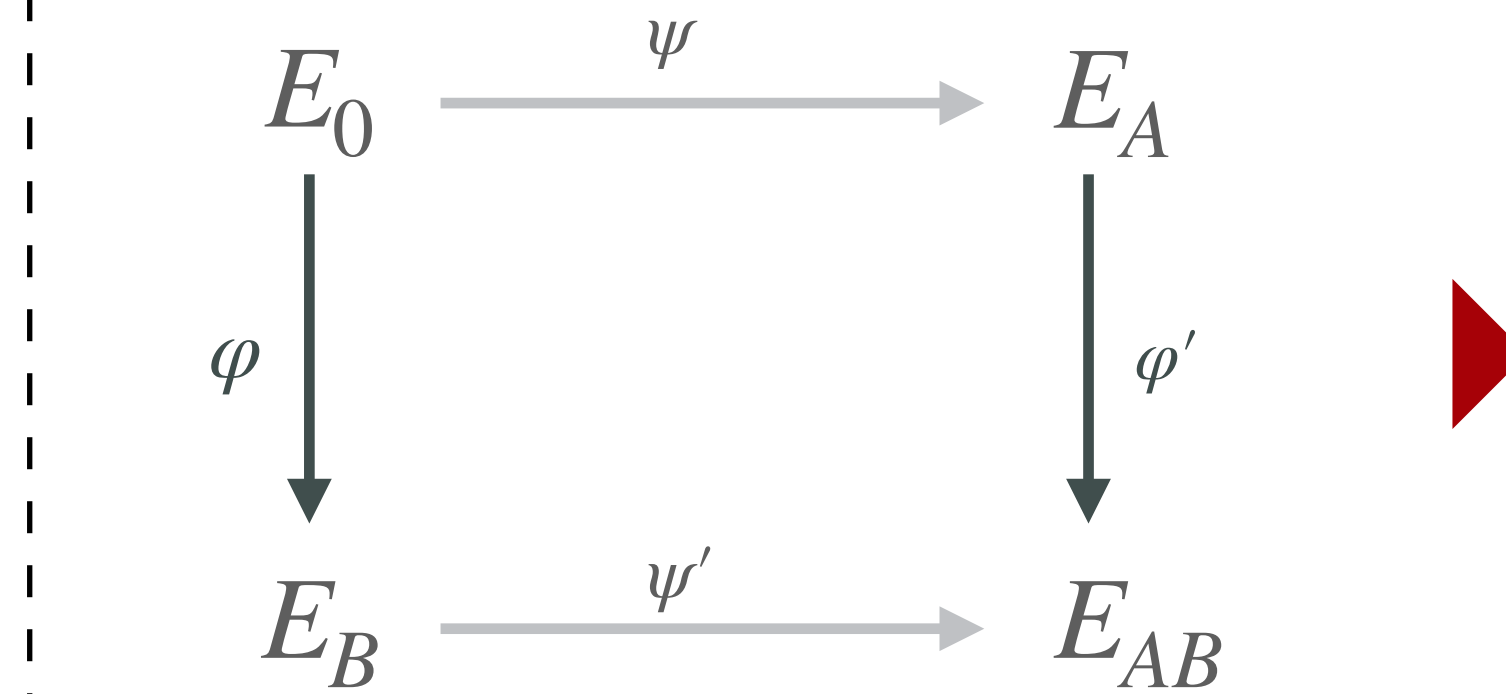
### The SIKE breaks

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

## PART 2

# The BREAK

Castruck & Decru (2022)



in SIDH/SIKE the secrets are  $\varphi$  and  $\psi$

