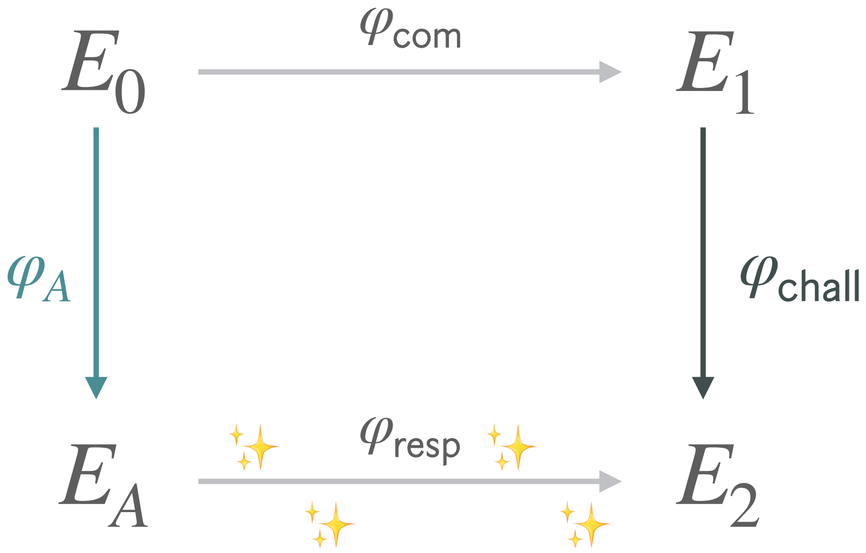
PART 3

New Dimensions

HD representations

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

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



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

2 HD representation: E_A is known, give points P_i and $\varphi_{\text{resp}}(P_i)$

✓ **faster primes!**

✓ **FASTER signing!**

✓ **THE BEST security!**

✗ **verification is now a 4D- or 8D-isogeny... difficult, complex, and rather slow**

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.