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 $Q \in E$

$$\begin{tikzcd}
E_0 \arrow[r, "\varphi_{\text{com}}"] \arrow[d, "\varphi_A"'] & E_1 \arrow[d, "\varphi_{\text{chall}}"] \\
E_A \arrow[r, "\varphi_{\text{resp}}"] & E_2
\end{tikzcd}$$

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!**

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 $Q \in E$

$$\begin{tikzcd}
E_0 \arrow[r, "\varphi_{\text{com}}"] \arrow[d, "\varphi_A"'] & E_1 \arrow[d, "\varphi_{\text{chall}}"] \\
E_A \arrow[r, "\varphi_{\text{resp}}"] & E_2
\end{tikzcd}$$

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**