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 $E, P_1, ..., P_n, \varphi(P_1), ..., \varphi(P_n)$, for enough points $P_i \in E$

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



PART 3 New Dimensions

In the words of the HD master

"If we know the value of $\varphi: E \to E'$ on enough nice points, then we know how to efficiently evaluate it everywhere"

- Damien Robert



HD representations

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

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

