

PART 3
New Dimensions

HD representations

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

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

In the words of the HD master

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

- Damien Robert



PART 3 New Dimensions

HD representations

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

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

In the words of the HD master

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

- Damien Robert



isogeny embedding (rough sketch)

We want to embed the 1-dimensional isogeny $\varphi : E \rightarrow E'$ and
we assume we know P_1, \dots, P_n and images $\varphi(P_1), \dots, \varphi(P_n)$.
Assume for the moment that $\deg \varphi = 2^n - x^2$ for some $x \in \mathbb{Z}$

$$E \xrightarrow{\varphi} E'$$