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 $Q \in E$

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

isogeny embedding (rough sketch)

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

$$\begin{tikzcd} E \arrow[r, "\varphi"] \arrow[d, "{[x]}"'] & E' \arrow[d, "{[x]}"] \\ E \arrow[r, "\varphi"] & E' \end{tikzcd}$$

We know and can compute $[x]$ easily! So we can apply Kani's!

$$\Phi : E \times E' \to E \times E'$$

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

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

isogeny embedding (rough sketch)

We want to embed the 1-dimensional isogeny $\varphi : E \to E'$ 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 $x \in \mathbb{Z}$

$$\begin{tikzcd} E \arrow[r, "\varphi"] \arrow[d, "{[x]}"'] & E' \arrow[d, "{[x]}"] \\ E \arrow[r, "\varphi"] & E' \end{tikzcd}$$

We know and can compute $[x]$ easily! So we can apply Kani's!

$$\Phi : E \times E' \to E \times E'$$

As Φ of degree 2^n, easy to compute and we can use Φ to compute $\varphi(Q)$ for any other point $Q \in E$