LECTURE 4: Using higher-dimensional isogenies

Joint with Gabrielle Scullard

<u>Problem</u>: Given supersingular $E/\mathbb{F}_{p^2}$, and $\beta \in \mathrm{End}(E)$, together with $n \in \mathbb{Z}_{>0}$, determine β/n is an endomorphism of E.

I.e. Is there $\gamma \in \mathrm{End}(E)$ s.t. $n\gamma = \beta$?

If n is small:

If $E[n] \subseteq \ker \beta$, then there exists such a γ and β/n is an endomorphism.

This is not comp. feasible if n has a large prime factor.

~~Insted~~ Instead:

Solve this problem by using higher-dimensional isogenies.

<u>Higher-dim'l isogenies and the break of SIDH</u> (July 2022)

Castryck-Decru, Maino-Martindale-et. al, Robert

There, following problem is solved:

$E/\mathbb{F}_{p^2}$ supsing.

Bob has secret isogeny $\varphi_B : E \xrightarrow{\varphi_B} E_B$ with kernel B. $\deg \varphi = 3^b$, large b.

Bob also has to reveal $\varphi_B(P_A)$, $\varphi_B(Q_A)$ where $\langle P_A, Q_A \rangle$ are a basis for 2^a-torsion.

(DeFeo, Jao, Plût, 2014)

Idea used in 2022 break:

Construct a new isogeny from φ_B, a 2^a-isogeny

$$f : C \times E_B \to E \times X$$

ell. curves

whose ~~ker f, ker f~~ kernel, $\ker(f)$ can be computed and from which we can recover the secret subgroup $B = \ker \varphi_B$.

$$\begin{tikzcd}
E_0 \arrow[r, "\varphi_B", "\deg 3^b"'] \arrow[d, "\gamma"'] & E_B \arrow[d, "\gamma'"] \\
C \arrow[r] & X
\end{tikzcd}$$

$\deg 2^a - 3^b$

Kani's Lemma gives

2^q-isogeny

$f : C \times E_B \longrightarrow E \times X$.

- Abelian variety X defined over a fin. field k
- polarization $\lambda : X \longrightarrow X^\vee$
- Given any isogeny $\varphi : A \longrightarrow B$, denote by $\varphi^\vee : B^\vee \longrightarrow A^\vee$ the dual isogeny.
- Have <u>Rosati involution</u> (A, λ) given $\alpha \in \mathrm{End}(A) \otimes \mathbb{Q}$

$$\alpha \longmapsto \alpha^\dagger = \lambda^{-1} \circ \alpha^\vee \circ \lambda \in \mathrm{End}(A) \otimes \mathbb{Q}$$

Writing isogenies between products of ab. vars:

A = abelian var., $r > 1$ integer

φ_{ij} $1 \leq i,j \leq r$ isogenies $A \to A$

The <u>matrix form</u> of $\Phi: \underline{\underline{A}}^r \to A^r$

sending

$$(P_1, \ldots, P_r) \longmapsto (\varphi_{11}(P_1) + \ldots + \varphi_{1r}(P_r), \ldots, \varphi_{r1}(P_1) + \ldots + \varphi_{rr}(P_r))$$

is the matrix $M = (\varphi_{ij})_{1 \leq i,j \leq r}$

<u>Kani's Lemma:</u>

$$\begin{array}{ccc} A & \xrightarrow{f_1} & A_1 \\ {\scriptstyle f_2}\downarrow & & \downarrow {\scriptstyle f_1'} \\ A_2 & \xrightarrow[f_2']{} & B \end{array}$$

diagram commutes

$(d_1, d_2) = 1$

A, A_1, A_2, B ppav of dim g

$f_1 = d_1$-isogeny

$f_2 = d_2$-isogeny

Then $F = \begin{pmatrix} f_1 & \tilde{f}_1' \\ -f_2 & \tilde{f}_2' \end{pmatrix}$ is a

$d = d_1 + d_2$ - isogeny

$F : A \times B \longrightarrow A_1 \times A_2$ with

kernel

$\mathrm{Ker}\, F = \{(\tilde{f}_1(P), f_1'(P)) : P \in A_1[d]\}$

Here $\tilde{f}_1' : B \longrightarrow A_1$ given by

$$\tilde{f}_1' = \lambda_{A_1}^{-1} \circ f_1'^{\vee} \cdot \lambda_B$$

Similarly for $\tilde{f}_2'$.

The Divide Algorithm

Given: supersingular $E/\mathbb{F}_{p^2}$
$\beta \in \mathrm{End}(E)$, $n > 0$

Output: "Yes" if β/n is in $\mathrm{End}(E)$
"No" if $\beta/n \notin \mathrm{End}(E)$.

Step 1: Compute $\deg(\beta)$
If $n^2 \nmid \deg \beta$, output "No".
Otherwise, let $N := \frac{\deg(\beta)}{n^2}$.
($N = \deg$ of β/n if it is an endom.)

Step 2: Choose $a \in \mathbb{Z}$ s.t.
$N' := N + a$ is $\log(\deg \beta)$ powersmooth.

B is a powersmoothness bound on $n \in \mathbb{N}$ if n factors as $n = \ell_1^{e_1} \cdots \ell_r^{e_r}$ and $B \geq \max_i \ell_i^{e_i}$.

Step 3: $a = a_1^2 + a_2^2 + a_3^2 + a_4^2$

$\alpha \in \mathrm{End}(E^4)$ is an a-isogeny:

$$\alpha = \begin{pmatrix} a_1 & -a_2 & -a_3 & -a_4 \\ a_2 & a_1 & a_4 & -a_3 \\ a_3 & -a_4 & a_1 & a_2 \\ a_4 & a_3 & -a_2 & a_1 \end{pmatrix}$$

Step 4 Kani's Lemma

$$\begin{array}{ccc} E^4 & \xrightarrow{\beta/n \cdot Id_4} & E^4 \\ a\text{-Isogeny } \alpha \downarrow & & \downarrow \alpha \\ E^4 & \xrightarrow[\beta/n \cdot Id_4]{} & E^4 \end{array}$$

gives us an $(N+a)$-endom:

$$G : (E^8, \lambda) \longrightarrow (E^8, \lambda)$$

with kernel $K = \left\{ \left(\frac{\hat{\beta}}{n} \cdot Id_4, \alpha(P) \right) : P \in E^4[N+a] \right\}$

<u>Step 5</u>: Consider

$$F : E^8 \longrightarrow E^8/K$$

should have $E^8/K \cong K$.

Check this. If false, answer "No".

<u>Step 6</u>: Compare F and G.

If φ_n exists, must have

$\psi \in \mathrm{Aut}(E^8)$ s.t.

$$F = \psi G.$$