Endomorphisms via Splittings

Sabrina Kunzweiler and Min-Yi Shen

No Affiliation

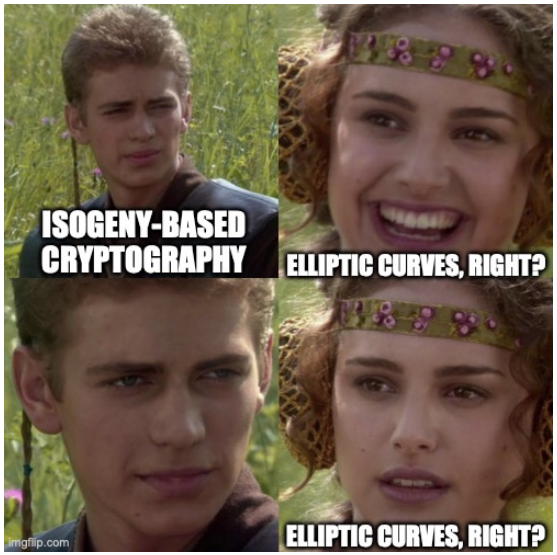
April 10, 2026

Cryptography Seminar of Creach Labs

Thanks for the invitation! I hope you enjoy today's isojourney!

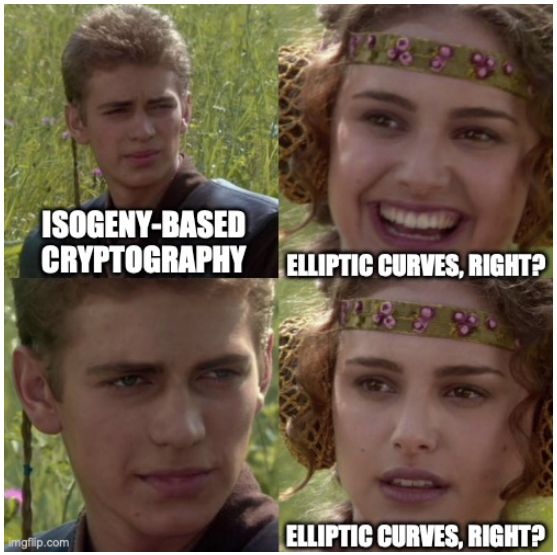
Table of Contents

What does ‘dimension’ mean?



In isogeny-based cryptography, the main objects are the *principally polarized abelian varieties (PPAV)*.

What does ‘dimension’ mean?



In isogeny-based cryptography, the main objects are the *principally polarized abelian varieties (PPAV)*.

One-dimensional PPAV: *elliptic curve*

Two-dimensional PPAV: *p.p. abelian surface (PPAS)*

— We have two flavors of PPAS over $\bar{\mathbb{F}}_q$: products of elliptic curves (reducible) and Jacobians of genus-2 curves (irreducible).

One-dimensional Assumptions

Two famous assumptions:

`Isogeny`: Given two supersingular elliptic curves E and E', find an isogeny $\varphi\colon E \to E'$

`EndRing`: Given a supersingular elliptic curve E, find the endomorphism ring $\mathrm{End}(E)$ of E.

One-dimensional Assumptions

Two famous assumptions:

`Isogeny`: Given two supersingular elliptic curves E and E', find an isogeny $\varphi\colon E \to E'$

`EndRing`: Given a supersingular elliptic curve E, find the endomorphism ring $\mathrm{End}(E)$ of E.

We now consider the following problem:

`OneEnd`: Given a supersingular elliptic curve E, find a non-constant endomorphism of E.

OneEnd and EndRing

Clearly, OneEnd $\to$ EndRing. But how about EndRing $\to$ OneEnd?

OneEnd and EndRing

Clearly, OneEnd $\to$ EndRing. But how about EndRing $\to$ OneEnd?

A natural idea: Running a OneEnd oracle again and again.

OneEnd and EndRing

Clearly, OneEnd $\to$ EndRing. But how about EndRing $\to$ OneEnd?

A natural idea: Running a OneEnd oracle again and again.

In fact, OneEnd $\longleftrightarrow$ EndRing by [PW24].

Solving OneEnd is also an important issue in isogeny-based cryptography.

OneEnd and EndRing

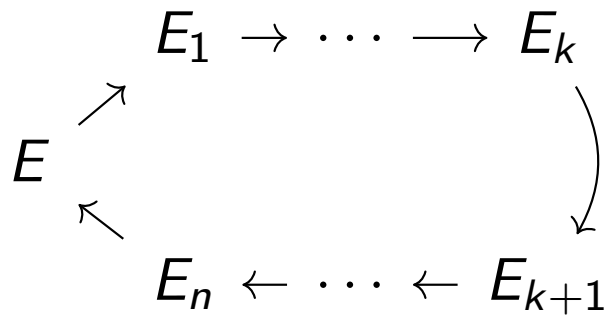
Clearly, OneEnd $\to$ EndRing. But how about EndRing $\to$ OneEnd?

A natural idea: Running a OneEnd oracle again and again.

In fact, OneEnd $\longleftrightarrow$ EndRing by [PW24].

Solving OneEnd is also an important issue in isogeny-based cryptography.

The best known attacks heuristically have running time $\tilde{O}(\sqrt{p})$.



Two-dimensional Assumptions

$$A \dashrightarrow B$$

Computing a connecting isogeny of two PPAS is a hard problem.

Two-dimensional Assumptions

$$A \dashrightarrow B$$

Computing a connecting isogeny of two PPAS is a hard problem.

The best known attack [CS20]: Finding $A \to E_1 \times E_2$ and $B \to E_3 \times E_4$ first.

Two-dimensional Assumptions

$$A \dashrightarrow B$$

Computing a connecting isogeny of two PPAS is a hard problem.

The best known attack [CS20]: Finding $A \to E_1 \times E_2$ and $B \to E_3 \times E_4$ first. Finding an ℓ^a-isogeny $\alpha_1 \circ \cdots \circ \alpha_a \colon E_1 \to E_3$ and an ℓ^b-isogeny $\beta_1 \circ \cdots \circ \beta_b \colon E_2 \to E_4$.

Two-dimensional Assumptions

$$A \dashrightarrow B$$

Computing a connecting isogeny of two PPAS is a hard problem.

The best known attack [CS20]: Finding $A \to E_1 \times E_2$ and $B \to E_3 \times E_4$ first. Finding an ℓ^a-isogeny $\alpha_1 \circ \cdots \circ \alpha_a \colon E_1 \to E_3$ and an ℓ^b-isogeny $\beta_1 \circ \cdots \circ \beta_b \colon E_2 \to E_4$. If $a \equiv b \mod 2$, say $a \geq b$, then we set $\beta_{b+1} = \tilde{\beta}_b$, $\beta_{b+2} = \beta_b$, ..., $\beta_{a-1} = \tilde{\beta}_b$, $\beta_a = \beta_b$. Then

$$(\alpha_1 \times \beta_1) \circ \cdots \circ (\alpha_a \times \beta_a) \colon A \to B.$$

Two-dimensional Assumptions

$$A \dashrightarrow B$$

Computing a connecting isogeny of two PPAS is a hard problem.

The best known attack [CS20]: Finding $A \to E_1 \times E_2$ and $B \to E_3 \times E_4$ first. Finding an ℓ^a-isogeny $\alpha_1 \circ \cdots \circ \alpha_a \colon E_1 \to E_3$ and an ℓ^b-isogeny $\beta_1 \circ \cdots \circ \beta_b \colon E_2 \to E_4$. If $a \equiv b \mod 2$, say $a \geq b$, then we set $\beta_{b+1} = \tilde{\beta}_b$, $\beta_{b+2} = \beta_b$, ..., $\beta_{a-1} = \tilde{\beta}_b$, $\beta_a = \beta_b$. Then

$$(\alpha_1 \times \beta_1) \circ \cdots \circ (\alpha_a \times \beta_a) \colon A \to B.$$

The attack motivates the following problem.

`Splitting`: Given an irreducible PPAS A, find an isogeny $F \colon A \to E \times E'$.

Two-dimensional Assumptions

$$A \dashrightarrow B$$

Computing a connecting isogeny of two PPAS is a hard problem.

The best known attack [CS20]: Finding $A \to E_1 \times E_2$ and $B \to E_3 \times E_4$ first. Finding an ℓ^a-isogeny $\alpha_1 \circ \cdots \circ \alpha_a \colon E_1 \to E_3$ and an ℓ^b-isogeny $\beta_1 \circ \cdots \circ \beta_b \colon E_2 \to E_4$. If $a \equiv b \mod 2$, say $a \geq b$, then we set $\beta_{b+1} = \tilde{\beta}_b$, $\beta_{b+2} = \beta_b$, ..., $\beta_{a-1} = \tilde{\beta}_b$, $\beta_a = \beta_b$. Then

$$(\alpha_1 \times \beta_1) \circ \cdots \circ (\alpha_a \times \beta_a) \colon A \to B.$$

The attack motivates the following problem.

`Splitting`: Given an irreducible PPAS A, find an isogeny $F \colon A \to E \times E'$.

The best known attack heuristically has running time $\tilde{O}(p)$.

Bridges

Our main contribution is the reductions from OneEnd (and Isogeny) to the variants of Splitting.

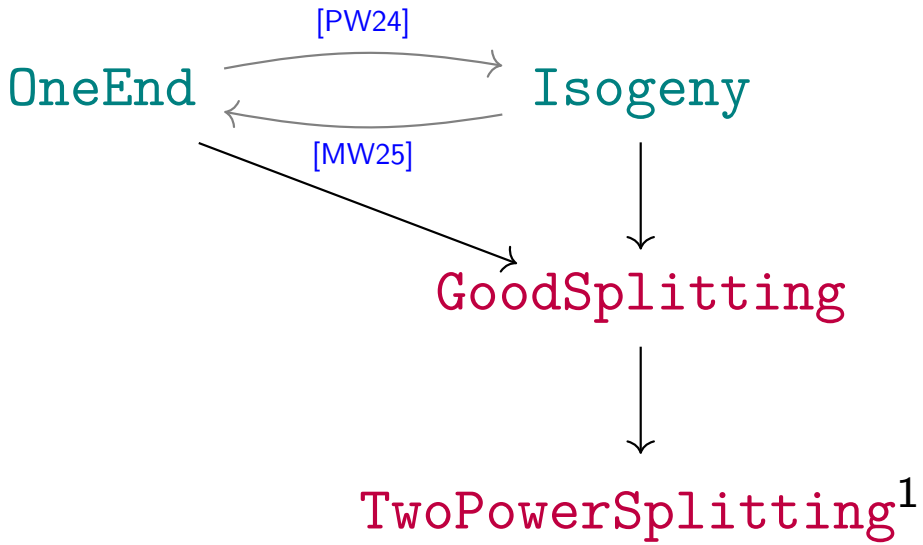


Figure: Our reductions

[1] It is essentially GoodSplitting with an additional degree restriction, making it much more practical to implement.

What?!

We solve `OneEnd` by solving (variants of) `Splitting`.

What?!

We solve `OneEnd` by solving (variants of) `Splitting`.

So why did we make the things even harder?

What?!

We solve OneEnd by solving (variants of) Splitting.

So why did we make the things even harder?

Splitting is not only a (relatively) less-studied problem but also a very 'different' problem $\dashrightarrow$ new tools to solve it.[2]

[2] Tiny remark: There is also an ongoing Splitting-OneEnd project, which has a better running time, related to our framework.

Table of Contents

Two-dimensional Isogenies

1. For an isogeny $f : A \to B$ between two PPAS A and B, there exists the ***adjoint isogeny*** $\tilde{f} : B \to A$ such that $f \circ \tilde{f} = [N]_A$ and $\tilde{f} \circ f = [N]_B$.

Two-dimensional Isogenies

1. For an isogeny $f : A \to B$ between two PPAS A and B, there exists the ***adjoint isogeny*** $\tilde{f} : B \to A$ such that $f \circ \tilde{f} = [N]_A$ and $\tilde{f} \circ f = [N]_B$.

2. An isogeny f is called an (N, N)-***isogeny*** if its kernel is isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

Two-dimensional Isogenies

1. For an isogeny $f : A \to B$ between two PPAS A and B, there exists the ***adjoint isogeny*** $\tilde{f} : B \to A$ such that $f \circ \tilde{f} = [N]_A$ and $\tilde{f} \circ f = [N]_B$.

2. An isogeny f is called an (N, N)-***isogeny*** if its kernel is isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

3. An isogeny is determined by its kernel up to isomorphism.

Two-dimensional Isogenies

1. For an isogeny $f : A \to B$ between two PPAS A and B, there exists the ***adjoint isogeny*** $\tilde{f} : B \to A$ such that $f \circ \tilde{f} = [N]_A$ and $\tilde{f} \circ f = [N]_B$.

2. An isogeny f is called an (N, N)-***isogeny*** if its kernel is isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

3. An isogeny is determined by its kernel up to isomorphism.

4. The types:
   $E_1 \times E_2 \to E_3 \times E_4$: ***Product isogeny***
   $E_1 \times E_2 \to \mathrm{Jac}(C_1)$: ***Gluing isogeny***
   $\mathrm{Jac}(C_1) \to E_1 \times E_2$: ***Splitting isogeny***
   $\mathrm{Jac}(C_1) \to \mathrm{Jac}(C_2)$: ***Generic isogeny***

Good Isogenies

Given two $(2,2)$-isogenies $f_1 : A \to B$ and $f_2 \circ B \to C$:

1. $\ker(f_2 \circ f_1) = (\mathbb{Z}/2\mathbb{Z})^4 \Rightarrow (2,2,2,2)$-isogeny
2. $\ker(f_2 \circ f_1) = (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^2 \Rightarrow (4,2,2)$-isogeny
3. $\ker(f_2 \circ f_1) = (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \Rightarrow (4,4)$-isogeny

Good Isogenies

Given two $(2,2)$-isogenies $f_1 : A \to B$ and $f_2 \circ B \to C$:

1. $\ker(f_2 \circ f_1) = (\mathbb{Z}/2\mathbb{Z})^4 \Rightarrow (2,2,2,2)$-isogeny
2. $\ker(f_2 \circ f_1) = (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^2 \Rightarrow (4,2,2)$-isogeny
3. $\ker(f_2 \circ f_1) = (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \Rightarrow (4,4)$-isogeny

Given an (N_1, N_1)-isogeny f_1 and an (N_2, N_2)-isogeny f_2, we say f_2 is a ***good extension*** of f_1 if $f_2 \circ f_1$ is an $(N_1 N_2, N_1 N_2)$-isogeny. Equivalently, $\ker(f_2) \cap \ker(\tilde{f_1}) = \{0\}$.

Kani's Lemma

Our usage of Kani's lemma:

An (N, N)-product isogeny $F : E \times E' \to E_1 \times E_2$ corresponds to the following commutative diagram (***isogeny diamond***).

$$\begin{array}{ccc} E & \xrightarrow{\phi_1} & E_1 \\ {\scriptstyle \phi_2}\downarrow & & \downarrow{\scriptstyle \psi_2} \\ E_2 & \xrightarrow{\psi_1} & E' \end{array}, \quad \deg \phi_i = \deg \psi_i = d_i, \ d_1 + d_2 = N$$

Moreover, the matrix form of F is

$$\begin{pmatrix} \phi_1 & \hat{\psi}_2 \\ -\phi_2 & \hat{\psi}_1 \end{pmatrix}$$

The Theta Coordinates[3]

We implement our algorithms in level-2 theta coordinates, so we informally introduce the necessary contents in the following few slides.

[3] For the clear and detailed references of the theta theory, I recommend Dr. Dartois' papers and thesis.

The Theta Coordinates[3]

We implement our algorithms in level-2 theta coordinates, so we informally introduce the necessary contents in the following few slides.

• We denote by θ^A a *level-2 theta structure* on a g-dimensional PPAV A: This structure defines an embedding $A/\langle\pm 1\rangle \hookrightarrow \mathbb{P}^{2^g-1}$.
— $g = 2$: $A/\langle\pm 1\rangle \hookrightarrow \mathbb{P}^3$.

[3] For the clear and detailed references of the theta theory, I recommend Dr. Dartois' papers and thesis.

The Theta Coordinates[3]

We implement our algorithms in level-2 theta coordinates, so we informally introduce the necessary contents in the following few slides.

• We denote by θ^A a *level-2 theta structure* on a g-dimensional PPAV A: This structure defines an embedding $A/\langle\pm 1\rangle \hookrightarrow \mathbb{P}^{2^g-1}$.
— $g = 2$: $A/\langle\pm 1\rangle \hookrightarrow \mathbb{P}^3$.

• In particular, $\theta^A(0)$ is called the *theta null point* of A. In our case ($g = 2$), $\theta^A(0)$ determines A up to isomorphism.

[3] For the clear and detailed references of the theta theory, I recommend Dr. Dartois' papers and thesis.

The Theta Coordinates[3]

We implement our algorithms in level-2 theta coordinates, so we informally introduce the necessary contents in the following few slides.

• We denote by θ^A a *level-2 theta structure* on a g-dimensional PPAV A: This structure defines an embedding $A/\langle\pm 1\rangle \hookrightarrow \mathbb{P}^{2^g-1}$.
— $g = 2$: $A/\langle\pm 1\rangle \hookrightarrow \mathbb{P}^3$.

• In particular, $\theta^A(0)$ is called the *theta null point* of A. In our case ($g = 2$), $\theta^A(0)$ determines A up to isomorphism.

• There are different level-2 theta structures on a single PPAV A: They are all related by *symplectic transformations*.

[3] For the clear and detailed references of the theta theory, I recommend Dr. Dartois' papers and thesis.

The Product Theta Structure

Regarding a product $A := E \times E'$ of elliptic curves, we have a natural candidate of the theta structure — the ***product theta structure***, denoted by $\theta^A = \theta^E \times \theta^{E'}$:

$$\theta^A((P, P')) = (x_0x'_0 : x_0x'_1 : x_1x'_0 : x_1x'_1)$$

where $\theta^E(P) = (x_0 : x_1)$ and $\theta^{E'}(P') = (x'_0 : x'_1)$.

Furthermore, we explicitly know how to convert a non-product structure to the product one.

Hadamard Transform

We introduce an important symplectic transform — the ***Hadamard transform***.

It is defined as multiplication by a Hadamard matrix $\mathcal{H}_g$:

$$\mathcal{H}_g \in M_{2^g}, \quad \mathcal{H}_0 = \begin{pmatrix} 1 \end{pmatrix}, \quad \mathcal{H}_{i+1} = \begin{pmatrix} \mathcal{H}_i & \mathcal{H}_i \\ \mathcal{H}_i & -\mathcal{H}_i \end{pmatrix}$$

Hadamard Transform

We introduce an important symplectic transform — the ***Hadamard transform***.

It is defined as multiplication by a Hadamard matrix $\mathcal{H}_g$:

$$\mathcal{H}_g \in M_{2^g}, \quad \mathcal{H}_0 = \begin{pmatrix} 1 \end{pmatrix}, \quad \mathcal{H}_{i+1} = \begin{pmatrix} \mathcal{H}_i & \mathcal{H}_i \\ \mathcal{H}_i & -\mathcal{H}_i \end{pmatrix}$$

— $g = 1$: $\mathcal{H}_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $g = 2$: $\mathcal{H} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$

Hadamard Transform

We introduce an important symplectic transform — the ***Hadamard transform***.

It is defined as multiplication by a Hadamard matrix $\mathcal{H}_g$:

$$\mathcal{H}_g \in M_{2^g}, \quad \mathcal{H}_0 = \begin{pmatrix} 1 \end{pmatrix}, \quad \mathcal{H}_{i+1} = \begin{pmatrix} \mathcal{H}_i & \mathcal{H}_i \\ \mathcal{H}_i & -\mathcal{H}_i \end{pmatrix}$$

— $g = 1$: $\mathcal{H}_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $g = 2$: $\mathcal{H} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$

$\tilde{\theta}^A = \mathcal{H} \circ \theta^A$ is called the ***dual theta structure*** of θ^A.

Evaluation in the Theta Model ([DMPR24])

Goal: evaluating a $(2,2)$-isogeny $f : A \to B$.

Evaluation in the Theta Model ([DMPR24])

Goal: evaluating a $(2,2)$-isogeny $f : A \to B$.

🔍 Briefly, if we know the theta null point of B, then we can evaluate f **unless** there exists a vanishing coordinate in the dual null point.

Given $P \in A$, the formula is

$$\theta^B(f(P)) = \mathcal{H} \circ \mathcal{C}_{\tilde{b}} \circ \mathcal{H} \circ \mathcal{S}(\theta^A(P))$$

where $\mathcal{H}$ and $\mathcal{S}$ are known maps, $\tilde{b} = \mathcal{H}(\theta^B(0))$, and $\mathcal{C}_{\tilde{b}}$ means scaling by $(1/\tilde{b_0}, 1/\tilde{b_1}, 1/\tilde{b_2}, 1/\tilde{b_3})$.

Evaluation in the Theta Model ([DMPR24])

Goal: evaluating a $(2,2)$-isogeny $f : A \to B$.

🔍 Briefly, if we know the theta null point of B, then we can evaluate f **unless** there exists a vanishing coordinate in the dual null point.

Given $P \in A$, the formula is

$$\theta^B(f(P)) = \mathcal{H} \circ \mathcal{C}_{\tilde{b}} \circ \mathcal{H} \circ \mathcal{S}(\theta^A(P))$$

where $\mathcal{H}$ and $\mathcal{S}$ are known maps, $\tilde{b} = \mathcal{H}(\theta^B(0))$, and $\mathcal{C}_{\tilde{b}}$ means scaling by $(1/\tilde{b_0}, 1/\tilde{b_1}, 1/\tilde{b_2}, 1/\tilde{b_3})$.

🔍 Rmk: We also have a similar formula for adjoint isogenies: $\theta^A(\tilde{f}(Q)) = \mathcal{C}_a \circ \mathcal{H} \circ \mathcal{S} \circ \mathcal{H}(\theta^B(Q))$.

Gluing Isogeny

The special case happens at gluing isogenies.

This problem was solved in [DMPR24] by assuming an additional knowledge: $\theta(P + T)$ where T is a 'suitable' 4-torsion point.

Main reason: transformation formula ensures that T swaps the coordinates, and therefore we can find the missing coordinate hidden by the vanishing coordinate.

Gluing Isogeny

The special case happens at gluing isogenies.

This problem was solved in [DMPR24] by assuming an additional knowledge: $\theta(P+T)$ where T is a 'suitable' 4-torsion point.

Main reason: transformation formula ensures that T swaps the coordinates, and therefore we can find the missing coordinate hidden by the vanishing coordinate.

Note that the additional information is not trivial even if one has $\theta(T)$: we need $\theta(P)$, $\theta(T)$ and $\theta(P-T)$ to compute $\theta(P+T)$.

In our case, we can find this additional information efficiently, so we can evaluate all kinds of isogenies.

Random Walk — ThetaCGL ([KMM+25])

$$E \times E \to \cdots \to J \to \cdots,$$

where J is irreducible.

Random Walk — ThetaCGL ([KMM+25])

$$E \times E \to \cdots \to J \to \cdots,$$

where J is irreducible. We walk on the good $(2,2)$-isogeny graph by using *ThetaCGL hash function*. Very briefly, one could determine a good $(2,2)$-isogeny by choosing three bits.

Input: $\theta^A(0)$ and $s \in \{0,1\}^3$

Output: $\theta^B(0)$ where B is $(2,2)$-isogenous to A

The Lucky Moment

We know how to walk on the good $(2, 2)$-isogeny graph, but when could we stop?

The Lucky Moment

We know how to walk on the good $(2,2)$-isogeny graph, but when could we stop?

Lemma [Dup06]

Let $\left(a_{\binom{i}{j}}\right)$ be the even ($\langle i,j\rangle = 0$) level-4 theta null point of a p.p. abelian surface A. When exactly one a_i vanishes, A is reducible. Moreover, the corresponding level-2 theta structure is the product one if and only if $a_{\binom{11}{11}} = 0$.

We have a formula to calculate the squares of level-4 theta coordinates from level-2 theta coordinates.

Table of Contents

Our Idea

Given two supersingular E and E', we consider $E \times E'$.

Our Idea

Given two supersingular E and E', we consider $E \times E'$. We are able to construct $f : E \times E' \to \mathrm{Jac}(C_1) := A$ (later).

Our Idea

Given two supersingular E and E', we consider $E \times E'$. We are able to construct $f : E \times E' \to \mathrm{Jac}(C_1) := A$ (later).

If we have a 'suitable' splitting isogeny $g : A \to E_1 \times E_2$. Then Kani's lemma connects $\Phi := g \circ f$ with the commutative diagram:

$$\begin{array}{ccc} E & \xrightarrow{\phi_1} & E_1 \\ {\scriptstyle \phi_2}\downarrow & & \downarrow{\scriptstyle \psi_2} \\ E_2 & \xrightarrow{\psi_1} & E' \end{array} \qquad \Phi = \begin{pmatrix} \phi_1 & \hat{\psi}_2 \\ -\phi_2 & \hat{\psi}_1 \end{pmatrix}$$

Our Idea

Given two supersingular E and E', we consider $E \times E'$. We are able to construct $f : E \times E' \to \mathrm{Jac}(C_1) := A$ (later).

If we have a 'suitable' splitting isogeny $g : A \to E_1 \times E_2$. Then Kani's lemma connects $\Phi := g \circ f$ with the commutative diagram:

$$\begin{array}{ccc} E & \xrightarrow{\phi_1} & E_1 \\ {\scriptstyle \phi_2}\downarrow & & \downarrow{\scriptstyle \psi_2} \\ E_2 & \xrightarrow{\psi_1} & E' \end{array} \qquad \Phi = \begin{pmatrix} \phi_1 & \hat{\psi}_2 \\ -\phi_2 & \hat{\psi}_1 \end{pmatrix}$$

There is a map $\psi_2 \circ \phi_1 : E \to E'$!

Our Idea

Given two supersingular E and E', we consider $E \times E'$. We are able to construct $f : E \times E' \to \mathrm{Jac}(C_1) := A$ (later).

If we have a 'suitable' splitting isogeny $g : A \to E_1 \times E_2$. Then Kani's lemma connects $\Phi := g \circ f$ with the commutative diagram:

$$\begin{array}{ccc} E & \xrightarrow{\phi_1} & E_1 \\ {\scriptstyle \phi_2}\downarrow & & \downarrow{\scriptstyle \psi_2} \\ E_2 & \xrightarrow{\psi_1} & E' \end{array} \qquad \Phi = \begin{pmatrix} \phi_1 & \hat{\psi}_2 \\ -\phi_2 & \hat{\psi}_1 \end{pmatrix}$$

There is a map $\psi_2 \circ \phi_1 : E \to E'$!

In particular, if we consider $E \times E$, then $\psi_2 \circ \phi_1 : E \to E$!!

Our Idea

Given two supersingular E and E', we consider $E \times E'$. We are able to construct $f : E \times E' \to \mathrm{Jac}(C_1) := A$ (later).

If we have a 'suitable' splitting isogeny $g : A \to E_1 \times E_2$. Then Kani's lemma connects $\Phi := g \circ f$ with the commutative diagram:

$$\begin{array}{ccc} E & \xrightarrow{\phi_1} & E_1 \\ {\scriptstyle \phi_2}\downarrow & & \downarrow{\scriptstyle \psi_2} \\ E_2 & \xrightarrow{\psi_1} & E' \end{array} \qquad \Phi = \begin{pmatrix} \phi_1 & \hat{\psi}_2 \\ -\phi_2 & \hat{\psi}_1 \end{pmatrix}$$

There is a map $\psi_2 \circ \phi_1 : E \to E'$!

In particular, if we consider $E \times E$, then $\psi_2 \circ \phi_1 : E \to E$!!

What does "suitable" mean?

Suitable Oracle

`GoodSplitting`: Given a map $\phi\colon A \to B$ where B is irreducible, find a good (w.r.t. ϕ) splitting $\psi\colon B \to E_1 \times E_2$.

Suitable Oracle

`GoodSplitting`: Given a map $\phi\colon A \to B$ where B is irreducible, find a good (w.r.t. ϕ) splitting $\psi\colon B \to E_1 \times E_2$.

Okay, "good" looks good, but why?

Suitable Oracle

`GoodSplitting`: Given a map $\phi\colon A \to B$ where B is irreducible, find a good (w.r.t. ϕ) splitting $\psi\colon B \to E_1 \times E_2$.

Okay, "good" looks good, but why?

1. Kani's lemma works on (N, N)-product isogenies.

Suitable Oracle

`GoodSplitting`: Given a map $\phi\colon A \to B$ where B is irreducible, find a good (w.r.t. ϕ) splitting $\psi\colon B \to E_1 \times E_2$.

Okay, "good" looks good, but why?

1. Kani's lemma works on (N, N)-product isogenies.
2. If we only consider the plain `Splitting` oracle, we might obtain some 'terrible' splittings,

Suitable Oracle

`GoodSplitting`: Given a map $\phi\colon A \to B$ where B is irreducible, find a good (w.r.t. ϕ) splitting $\psi\colon B \to E_1 \times E_2$.

Okay, "good" looks good, but why?

1. Kani's lemma works on (N, N)-product isogenies.
2. If we only consider the plain `Splitting` oracle, we might obtain some 'terrible' splittings, for example, the 'smartest' oracle:

$$\begin{pmatrix} [N] & 0 \\ 0 & [N] \end{pmatrix} : E \times E' \underset{\tilde{f}_1}{\overset{f_1}{\rightleftarrows}} \mathrm{Jac}(C)$$

Suitable Oracle

`GoodSplitting`: Given a map $\phi\colon A \to B$ where B is irreducible, find a good (w.r.t. ϕ) splitting $\psi\colon B \to E_1 \times E_2$.

Okay, "good" looks good, but why?

1. Kani's lemma works on (N, N)-product isogenies.
2. If we only consider the plain `Splitting` oracle, we might obtain some 'terrible' splittings, for example, the 'smartest' oracle:

$$\begin{pmatrix} [N] & 0 \\ 0 & [N] \end{pmatrix} : E \times E' \overset{f_1}{\underset{\tilde{f}_1}{\rightleftarrows}} \mathrm{Jac}(C)$$

3. In isogeny-based constructions, we like chains of good isogenies; otherwise, there might exist attacks, e.g., the collision attack [FT19] on the first 2-dimensional CGL hash function.

Goal

Recall that we know:

(1) The method to seek a good splitting.

(2) Evaluating a chain of good $(2,2)$-isogenies with a special care of the gluing.

$$E \times E' \longrightarrow \cdots \overset{\text{where}}{\longrightarrow} \mathrm{Jac}(C_1) \longrightarrow \cdots$$

It remains to locate the gluing.

Where is the gluing?

We can force the first isogeny to be a gluing by the following lemma.

Where is the gluing?

We can force the first isogeny to be a gluing by the following lemma.

Lemma

Let $\theta^{E\times E'}(0) = (a_0 : a_1 : a_2 : a_3)$ be the theta null point of $E \times E'$ in the product structure. By applying the symplectic transformation

$$\sigma = \begin{pmatrix} 1 & 1 & 1 & -1 \\ -i & i & -i & -i \\ 1 & -1 & -1 & -1 \\ -i & -i & i & -i \end{pmatrix}$$

the codomain from the radical formula is irreducible if one of the following holds:
(1) $E \not\cong E'$
(2) $j(E) = j(E') \notin \{0, 1728\}$ and $\theta^E(0) = \theta^{E'}(0)$.

Note that the automorphism σ is the same for any starting $E \times E'$.

$$E \times E' \xrightarrow{\sim} (E \times E')_\sigma \to A \to \cdots$$

Computational Reason

We use the following facts: Given $E \times E'$ and $f : E \times E' \to B$

(1) We exactly know the symplectic transformation converting the structure to the product one. More precisely, we know how to validly move the vanishing coordinates to $\binom{11}{11}$.

(2) The level-2 theta coordinates of dual null point of B is the first four coordinates of the level-4 coordinates of the theta null point of the domain.

So we can locate a gluing by constructing a special case: Using the converse of (1), we know the valid matrix σ converting $\binom{11}{11}$ to $\binom{00}{00}$.

If we are fortunate enough...

Assume we have found $F\colon E \times E' \to E_1 \times E_2$.

With the special care of the first step:
We can evaluate $F = \begin{pmatrix} \phi_1 & \hat{\psi}_2 \\ -\phi_2 & \hat{\psi}_1 \end{pmatrix}$ at a given $(P, Q) \in E \times E$ by the isogeny formula — especially at $(P, 0)$.
We can evaluate $\tilde{F} = \begin{pmatrix} \hat{\phi}_1 & -\phi_2 \\ \psi_2 & \psi_1 \end{pmatrix}$ at a given $(P', Q') \in E_1 \times E_2$ by the isogeny formula — especially at $(\phi_1(P), 0)$.

Therefore, we can extract $\psi_2 \circ \phi_1$.

If we are fortunate enough...

Assume we have found $F\colon E \times E' \to E_1 \times E_2$.

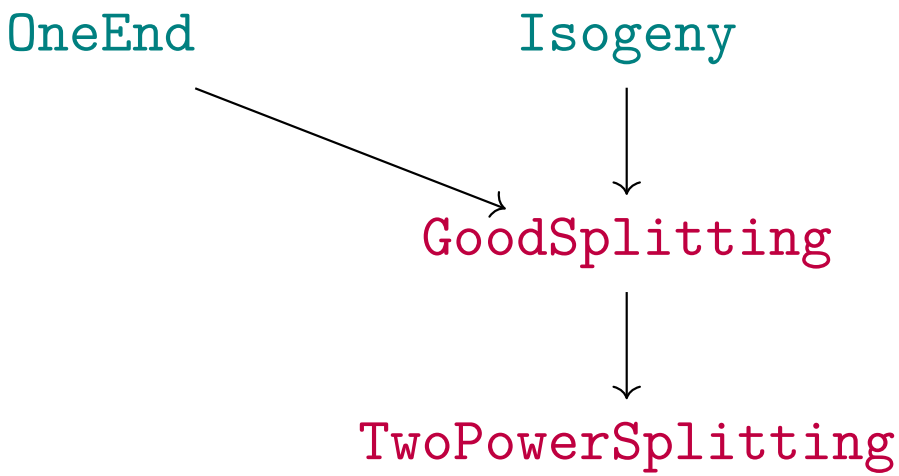
With the special care of the first step:
We can evaluate $F = \begin{pmatrix} \phi_1 & \hat{\psi}_2 \\ -\phi_2 & \hat{\psi}_1 \end{pmatrix}$ at a given $(P, Q) \in E \times E$ by the isogeny formula — especially at $(P, 0)$.
We can evaluate $\tilde{F} = \begin{pmatrix} \hat{\phi}_1 & -\phi_2 \\ \psi_2 & \psi_1 \end{pmatrix}$ at a given $(P', Q') \in E_1 \times E_2$ by the isogeny formula — especially at $(\phi_1(P), 0)$.

Therefore, we can extract $\psi_2 \circ \phi_1$.

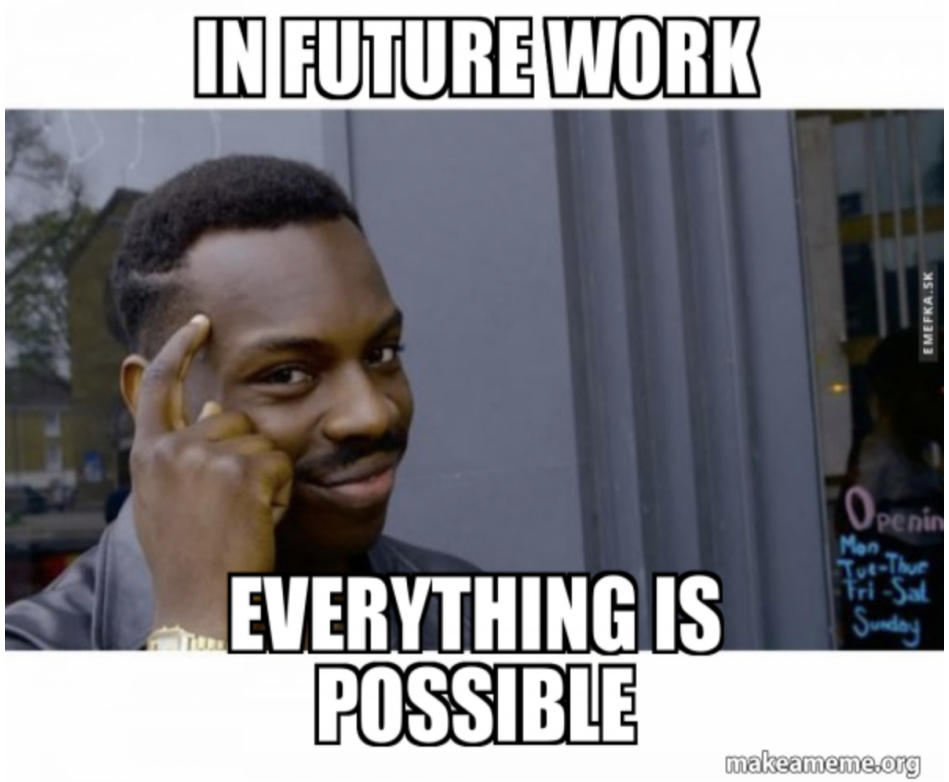
RMK: The degree of the extracted endomorphism (or isogeny) is of the form $\deg \phi_1(2^s - \deg \phi_1)$ where s is the length of the splitting. Note that it is usually non-smooth.

Reductions

We formally proved the reductions from `OneEnd` (resp. `Isogeny`) to `TwoPowerSplitting` and `GoodSplitting`: it remains to show the induced map is non-scalar (resp. non-zero).



Current/Future Works



1. Removing the 'good' restriction.
2. Connecting the splitting problems with other two-dimensional problems.
3. Studying the splitting problems themselves.

Finally, we find OneEnd — the ~~One~~End.

— A random photo I took, just to fill the void

Thank you!
Questions or Comments?

— ?

References I


Craig Costello and Benjamin Smith, *The Supersingular Isogeny Problem in Genus 2 and Beyond*, Post-Quantum Cryptography (Cham) (Jintai Ding and Jean-Pierre Tillich, eds.), Springer International Publishing, 2020, pp. 151–168.


Pierrick Dartois, Luciano Maino, Giacomo Pope, and Damien Robert, *An algorithmic approach to (2, 2)-isogenies in the theta model and applications to isogeny-based cryptography*, International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2024, pp. 304–338.


Régis Dupont, *Moyenne arithmético-géométrique, suites de borchardt et applications*, Ph.D. thesis, École polytechnique, 2006.


E. V. Flynn and Yan Bo Ti, *Genus Two Isogeny Cryptography*, Post-Quantum Cryptography (Cham) (Jintai Ding and Rainer Steinwandt, eds.), Springer International Publishing, 2019, pp. 286–306.


Sabrina Kunzweiler, Luciano Maino, Tomoki Moriya, Christophe Petit, Giacomo Pope, Damien Robert, Miha Stopar, and Yan Bo Ti, *Radical 2-isogenies and cryptographic hash functions in dimensions 1, 2 and 3*, IACR International Conference on Public-Key Cryptography, Springer, 2025, pp. 265–299.

References II

Arthur Herlédan Le Merdy and Benjamin Wesolowski, *Unconditional foundations for supersingular isogeny-based cryptography*, Cryptology ePrint Archive, Paper 2025/271, 2025.

Aurel Page and Benjamin Wesolowski, *The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent*, Advances in Cryptology – EUROCRYPT 2024 (Cham) (Marc Joye and Gregor Leander, eds.), Springer Nature Switzerland, 2024, pp. 388–417.

Supplement: OneEnd to TwoPowerSplitting

Step 1: If the endomorphism $\psi_2 \circ \phi_1 : E \to E$ is a constant. By analyzing the matrix form and the kernels in detail, one can show that F is of the form $\begin{pmatrix} \phi_1 & \pm\phi_1 \\ -\phi_2 & \pm\phi_2 \end{pmatrix}$.

Step 2: Recall that an isogeny is defined by its kernel up to isomorphism. Consider $\left(\begin{smallmatrix} 1 & 1 \\ -1 & 1 \end{smallmatrix}\right) : E^2 \to E^2$, if a $(2,2)$-isogeny $f : E \times E \to A$ has kernel $\{(P,P) \mid P \in E[2]\}$, then $A \cong E \times E$. In particular, it's reducible.

Step 3: Assume $\psi_2 \circ \phi_1$ is a constant, then $\forall\, P \in E[2]$, $F((P,P)) = 0$ by Step 1. However, it means the first codomain is isomorphic to $E \times E$ which contradicts the fact that f_1 is a gluing.