Fast computation of higher dimensional isogenies for cryptographic applications

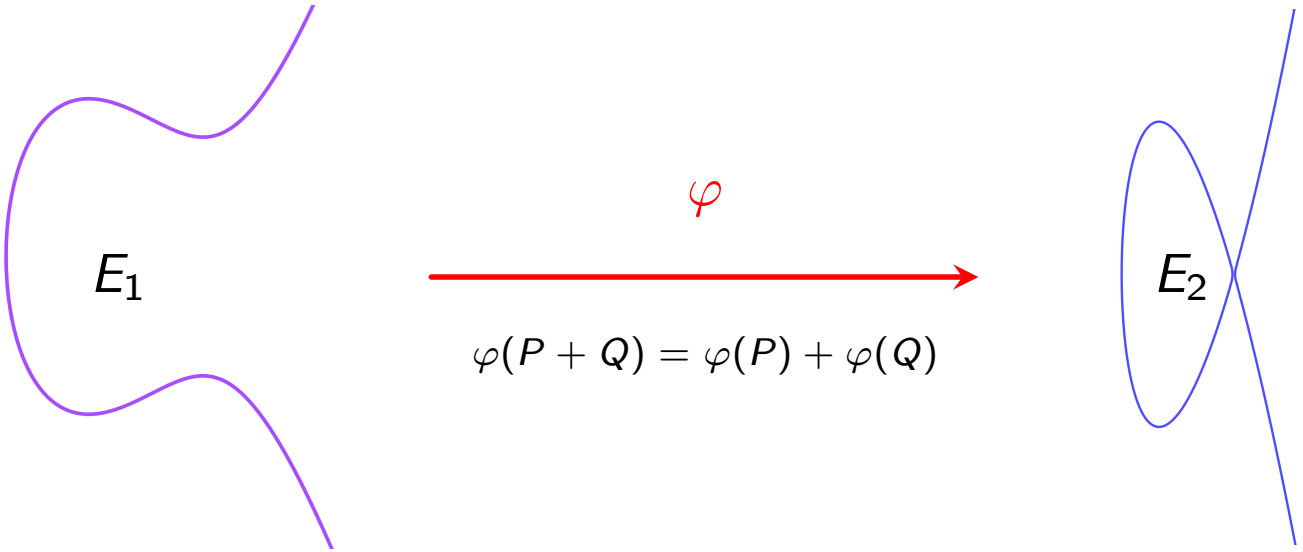
Pierrick Dartois

Joint work with Luciano Maino, Giacomo Pope and Damien Robert

21 November 2024

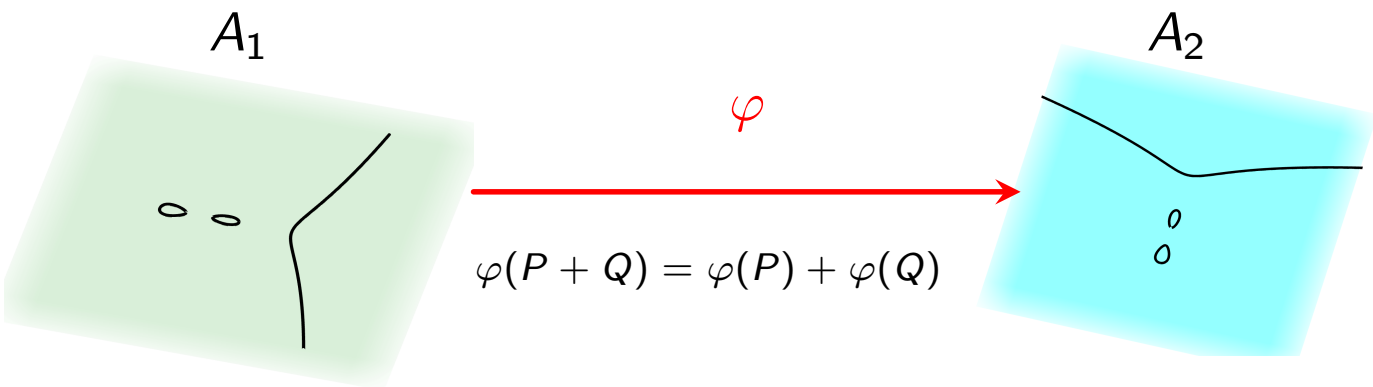
Isogenies between elliptic curves

Between elliptic curves, isogenies are non-zero morphisms of algebraic groups.



Isogenies between abelian varieties

- Abelian varieties are projective abelian group varieties, generalizing elliptic curves.
- Between abelian varieties, isogenies are morphisms which are surjective and of finite kernel.



Why (higher dimensional) isogenies matter

- Quantum computers jeopardize current public key cryptography (RSA, discrete logarithms...).
- Isogenies are used in quantum-resistant cryptographic protocols.

Why (higher dimensional) isogenies matter

- Quantum computers jeopardize current public key cryptography (RSA, discrete logarithms...).
- Isogenies are used in quantum-resistant cryptographic protocols.

Why higher dimensions?

Why (higher dimensional) isogenies matter

- Quantum computers jeopardize current public key cryptography (RSA, discrete logarithms...).
- Isogenies are used in quantum-resistant cryptographic protocols.

Why higher dimensions?

- Isogenies of dimensions 2, 4 (or 8) were used to break the isogeny-based protocol SIDH (NIST candidate).
- Higher dimensional isogenies are used as an interpolation tool.

Why (higher dimensional) isogenies matter

- Quantum computers jeopardize current public key cryptography (RSA, discrete logarithms...).
- Isogenies are used in quantum-resistant cryptographic protocols.

Why higher dimensions?

- Isogenies of dimensions 2, 4 (or 8) were used to break the isogeny-based protocol SIDH (NIST candidate).
- Higher dimensional isogenies are used as an interpolation tool.
- They also have been used constructively in several protocols (FESTA/QFESTA, SQIsignHD/2D/Prime, Scallop-HD, IS-CUBE, 3D hash function...).
- We need fast implementations.

Previous works and our contribution

Goal: Compute 2^e-isogenies in dimension $g \geq 2$.
[If f is a 2^e-isogeny in dimension g, then $\#\ker(f) = 2^{eg}$.]

Previous works and our contribution

Goal: Compute 2^e-isogenies in dimension $g \geq 2$.
[If f is a 2^e-isogeny in dimension g, then $\#\ker(f) = 2^{eg}$.]

State of the art:

- Several algorithms and implementations to compute 2^e-isogenies in dimension 2 with different models: Richelot [Smi06], Jacobian and Kummer [Kun24].
- Algorithms to compute ℓ^e-isogenies in any dimension $g \geq 2$ with theta coordinates of level n coprime with ℓ (n^g coordinates) [LR12; LR15; LR22]. Slow implementation in Magma (AVisogenies).

Previous works and our contribution

Goal: Compute 2^e-isogenies in dimension $g \geq 2$.
[If f is a 2^e-isogeny in dimension g, then $\#\ker(f) = 2^{eg}$.]

State of the art:

- Several algorithms and implementations to compute 2^e-isogenies in dimension 2 with different models: Richelot [Smi06], Jacobian and Kummer [Kun24].
- Algorithms to compute ℓ^e-isogenies in any dimension $g \geq 2$ with theta coordinates of level n coprime with ℓ (n^g coordinates) [LR12; LR15; LR22]. Slow implementation in Magma (AVisogenies).

Our contribution:

- An algorithm to compute 2^e-isogenies in any dimension $g \geq 2$ with theta coordinates of level 2 (2^g coordinates).
- Fastest implementation in dimension 2.
- Fast implementation in dimension 4.

The theory of theta functions

Line bundles

Notations:

- k: algebraically closed field.
- A: abelian variety defined over k.
- $g := \dim(A)$.

- A **line bundle** $\mathcal{L}$ on A is a locally free sheaf of $\mathcal{O}_A$-modules of rank 1.
- Line bundles on A form a group for the tensor product.
- Isomorphism classes of line bundles form the Picard group $\mathrm{Pic}(A)$.
- $\mathrm{Pic}(A) \cong \{\text{divisors on } A \text{ modulo principal divisors}\}$.

Polarisations

- Let:
$$\mathrm{Pic}^0(A) = \{[\mathcal{L}] \in \mathrm{Pic}(A) \mid \forall a \in A(k), \quad t_a^*\mathcal{L} \cong \mathcal{L}\}$$
- $\mathrm{Pic}^0(A) \cong \widehat{A}(k)$ (k-rational points of $\widehat{A}$).
- If $\mathcal{L}$ is a line bundle on A, consider:
$$\begin{array}{rcl} \varphi_{\mathcal{L}} : A & \longrightarrow & \widehat{A} \\ x \in A(k) & \longmapsto & [t_x^*\mathcal{L} \otimes \mathcal{L}^{-1}] \in \mathrm{Pic}^0(A) \end{array}$$
- When $K(\mathcal{L}) := \ker(\varphi_{\mathcal{L}})$ is finite, $\varphi_{\mathcal{L}}$ is an isogeny and we say that:
  - $\mathcal{L}$ is **ample**.
  - $\varphi_{\mathcal{L}}$ is a **polarisation** of A.
  - $(A, \mathcal{L})$ is a **polarized abelian variety**.
- When $\varphi_{\mathcal{L}}$ is an isomorphism, $(A, \mathcal{L})$ is a principally polarised abelian variety (PPAV).

Projective coordinates on polarised abelian varieties

- We are looking for systems of coordinates on $(A, \mathcal{L})$.
- **Idea:** Take global sections $s_0, \cdots, s_n \in \Gamma(A, \mathcal{L})$ that generate $\mathcal{L}$ (i.e. that generate $\mathcal{L}$ locally everywhere) and define:

$$\begin{array}{ccc} A & \longrightarrow & \mathbb{P}_k^n \\ x & \longmapsto & "(s_0(x) : \cdots : s_n(x))" \end{array}$$

- Those sections are coordinates when the above map is an embedding.

Projective coordinates on polarised abelian varieties

- We are looking for systems of coordinates on $(A, \mathcal{L})$.
- **Idea:** Take global sections $s_0, \cdots, s_n \in \Gamma(A, \mathcal{L})$ that generate $\mathcal{L}$ (i.e. that generate $\mathcal{L}$ locally everywhere) and define:

$$\begin{array}{ccc} A & \longrightarrow & \mathbb{P}_k^n \\ x & \longmapsto & "(s_0(x) : \cdots : s_n(x))" \end{array}$$

- Those sections are coordinates when the above map is an embedding.

- Theta functions form a family of global sections of $\Gamma(A, \mathcal{L})$ with "good arithmetic properties".

The theta group

- Let $\mathcal{L}$ be an ample line bundle on A.
- Then, for every $x \in K(\mathcal{L}) = \ker(\varphi_{\mathcal{L}})$, there is an isomorphism $\phi_x : \mathcal{L} \xrightarrow{\sim} t_x^*\mathcal{L}$.
- Given $x, y \in K(\mathcal{L})$, we can consider the isomorphism:

$$\mathcal{L} \xrightarrow{\phi_x} t_x^*\mathcal{L} \xrightarrow{t_x^*\phi_y} t_x^* t_y^* \mathcal{L} = t_{x+y}^*\mathcal{L}.$$

- This defines a group structure on:

$$G(\mathcal{L}) = \{(x, \phi_x) \mid x \in K(\mathcal{L}) \text{ and } \phi_x : \mathcal{L} \xrightarrow{\sim} t_x^*\mathcal{L}\},$$

given by $(x, \phi_x) \cdot (y, \phi_y) = (x + y, t_x^*\phi_y \circ \phi_x)$.

- $G(\mathcal{L})$ is called the **theta group** of $\mathcal{L}$.

The commutator pairing

- There is an exact sequence:

$$1 \longrightarrow k^* \longrightarrow G(\mathcal{L}) \longrightarrow K(\mathcal{L}) \longrightarrow 0,$$

where the first arrow is $\lambda \longmapsto (0, \lambda \mathrm{id}_{\mathcal{L}})$ and the last arrow is the forgetful map $\rho_{\mathcal{L}} : (x, \phi_x) \longmapsto x$.

The commutator pairing

- There is an exact sequence:

$$1 \longrightarrow k^* \longrightarrow G(\mathcal{L}) \longrightarrow K(\mathcal{L}) \longrightarrow 0,$$

  where the first arrow is $\lambda \longmapsto (0, \lambda \mathrm{id}_{\mathcal{L}})$ and the last arrow is the forgetful map $\rho_{\mathcal{L}} : (x, \phi_x) \longmapsto x$.
- $G(\mathcal{L})$ does not commute and we measure the commutativity defect via the **commutator pairing**.
- Let $x, y \in K(\mathcal{L})$ and $\widetilde{x}, \widetilde{y} \in G(\mathcal{L})$ be lifts of x, y. Define:

$$e_{\mathcal{L}}(x, y) := \widetilde{x} \cdot \widetilde{y} \cdot \widetilde{x}^{-1} \cdot \widetilde{y}^{-1} \in k^*.$$

  as the **commutator pairing** of x and y.
- $e_{\mathcal{L}} : K(\mathcal{L}) \times K(\mathcal{L}) \longrightarrow k^*$ is a non-degenerate skew-symmetric bilinear map.

Symplectic decomposition

- A subgroup $K \subset K(\mathcal{L})$ is **isotropic** if $e_{\mathcal{L}}(x, y) = 1$ for all $x, y \in K$.
- $K(\mathcal{L})$ induces a **symplectic decomposition**:

$$K(\mathcal{L}) = K_1(\mathcal{L}) \oplus K_2(\mathcal{L}),$$

where $K_1(\mathcal{L})$ and $K_2(\mathcal{L})$ are maximal isotropic subgroups.

- The map:

$$y \in K_2(\mathcal{L}) \longmapsto e_{\mathcal{L}}(., y) \in \widehat{K_1(\mathcal{L})} = \mathrm{Hom}(K_1(\mathcal{L}), k^*)$$

is an isomorphism $K_2(\mathcal{L}) \cong \widehat{K_1(\mathcal{L})}$.

Symplectic decomposition

- There exists a unique tuple of integers $\delta = (d_1, \cdots, d_g)$ such that:
  - $d_1 | \cdots | d_g$ and $g = \dim(A)$;
  - $K_1(\mathcal{L}) \cong K_1(\delta)$ and $K_2(\mathcal{L}) \cong K_2(\delta)$.

  Where:

$$K_1(\delta) := \prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z} \quad \text{and} \quad K_2(\delta) := \widehat{K}_1(\delta) = \mathrm{Hom}(K_1(\delta), k^*).$$

- We say that $\mathcal{L}$ has **type** δ.

Symplectic decomposition

- There exists a unique tuple of integers $\delta = (d_1, \cdots, d_g)$ such that:
  - $d_1 | \cdots | d_g$ and $g = \dim(A)$;
  - $K_1(\mathcal{L}) \cong K_1(\delta)$ and $K_2(\mathcal{L}) \cong K_2(\delta)$.

  Where:

$$K_1(\delta) := \prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z} \quad \text{and} \quad K_2(\delta) := \widehat{K}_1(\delta) = \mathrm{Hom}(K_1(\delta), k^*).$$

- We say that $\mathcal{L}$ has **type** δ.
- $K(\delta) := K_1(\delta) \oplus K_2(\delta)$ can be equipped with a pairing $e_\delta : K(\delta) \times K(\delta) \longrightarrow k^*$.

Symplectic decomposition

- There exists a unique tuple of integers $\delta = (d_1, \cdots, d_g)$ such that:
  - $d_1 | \cdots | d_g$ and $g = \dim(A)$;
  - $K_1(\mathcal{L}) \cong K_1(\delta)$ and $K_2(\mathcal{L}) \cong K_2(\delta)$.

  Where:

$$K_1(\delta) := \prod_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z} \quad \text{and} \quad K_2(\delta) := \widehat{K}_1(\delta) = \mathrm{Hom}(K_1(\delta), k^*).$$

- We say that $\mathcal{L}$ has **type** δ.
- $K(\delta) := K_1(\delta) \oplus K_2(\delta)$ can be equipped with a pairing $e_\delta : K(\delta) \times K(\delta) \longrightarrow k^*$.
- There always exists a symplectic isomorphism $\sigma : K(\delta) \xrightarrow{\sim} K(\mathcal{L})$:

$$\forall x, y \in K(\delta), \quad e_{\mathcal{L}}(\sigma(x), \sigma(y)) = e_\delta(x, y).$$

- The $K_i(\mathcal{L}) := \sigma(K_i(\delta))$ form a symplectic decomposition of $K(\mathcal{L})$.

Theta structures

- We define the **Heisenberg group** as $\mathcal{H}(\delta) := k^* \times K(\delta)$, with the group law:

$$(\alpha, x, \chi) \cdot (\beta, x', \chi') := (\alpha\beta\chi'(x), x + x', \chi\chi').$$

[Recall that $K(\delta) = K_1(\delta) \oplus K_2(\delta)$ with $K_2(\delta) = \mathrm{Hom}(K_1(\delta), k^*)$, so χ, χ' are homorphisms $K_1(\delta) \longrightarrow k^*$].

Theta structures

- We define the **Heisenberg group** as $\mathcal{H}(\delta) := k^* \times K(\delta)$, with the group law:

$$(\alpha, x, \chi) \cdot (\beta, x', \chi') := (\alpha\beta\chi'(x), x + x', \chi\chi').$$

[Recall that $K(\delta) = K_1(\delta) \oplus K_2(\delta)$ with $K_2(\delta) = \mathrm{Hom}(K_1(\delta), k^*)$, so χ, χ' are homorphisms $K_1(\delta) \longrightarrow k^*$].

- A **Theta structure** is an isomorphism $\Theta_{\mathcal{L}} : \mathcal{H}(\delta) \xrightarrow{\sim} G(\mathcal{L})$ inducing an isomorphism of exact sequences:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & k^* & \longrightarrow & \mathcal{H}(\delta) & \longrightarrow & K(\delta) & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle \Theta_{\mathcal{L}}} & & \downarrow{\scriptstyle \overline{\Theta}_{\mathcal{L}}} & & \\
1 & \longrightarrow & k^* & \longrightarrow & G(\mathcal{L}) & \longrightarrow & K(\mathcal{L}) & \longrightarrow & 0
\end{array}$$

In particular, $\overline{\Theta}_{\mathcal{L}} : K(\delta) \xrightarrow{\sim} K(\mathcal{L})$ is symplectic.

Theta structures

Proposition

Theta structures always exist and are in bijection with triples $(\overline{\Theta}_{\mathcal{L}}, s_1, s_2)$, *where:*

- $\overline{\Theta}_{\mathcal{L}}$ *is a symplectic isomorphism* $K(\delta) \xrightarrow{\sim} K(\mathcal{L})$;
- s_i *are sections* $K_i(\Theta_{\mathcal{L}}) = \overline{\Theta}_{\mathcal{L}}(K_i(\delta)) \xrightarrow{\sim} \widetilde{K}_i(\mathcal{L}) \subset G(\mathcal{L})$.

Action of the Heisenberg group

- Let $V(\delta)$ be the space of functions $K_1(\delta) \longrightarrow k$.
- $\mathcal{H}(\delta)$ acts on $V(\delta)$ as follows:

$$(\alpha, x, \chi) \cdot f : y \longmapsto \alpha\chi(y)^{-1} f(y - x),$$

for all $f \in V(\delta)$ and $(\alpha, x, \chi) \in \mathcal{H}(\delta)$.

Action of the Heisenberg group

- Let $V(\delta)$ be the space of functions $K_1(\delta) \longrightarrow k$.
- $\mathcal{H}(\delta)$ acts on $V(\delta)$ as follows:

$$(\alpha, x, \chi) \cdot f : y \longmapsto \alpha\chi(y)^{-1} f(y - x),$$

for all $f \in V(\delta)$ and $(\alpha, x, \chi) \in \mathcal{H}(\delta)$.

Theorem (Mumford, 1966)

Every irreducible representation of $\mathcal{H}(\delta)$ on which k^* acts naturally is isomorphic to $V(\delta)$.

Action of the Theta group

- $G(\mathcal{L})$ acts on the space of global sections $\Gamma(A, \mathcal{L})$ as follows:

$$\forall s \in \Gamma(A, \mathcal{L}), (x, \phi_x) \in G(\mathcal{L}), \quad (x, \phi_x) \cdot s = t^*_{-x}(\phi_x(s)).$$

Theorem (Mumford, 1966)

$\Gamma(A, \mathcal{L})$ is an irreducible representation of $G(\mathcal{L})$.

Action of the Theta group

- $G(\mathcal{L})$ acts on the space of global sections $\Gamma(A, \mathcal{L})$ as follows:

$$\forall s \in \Gamma(A, \mathcal{L}), (x, \phi_x) \in G(\mathcal{L}), \quad (x, \phi_x) \cdot s = t^*_{-x}(\phi_x(s)).$$

Theorem (Mumford, 1966)

$\Gamma(A, \mathcal{L})$ is an irreducible representation of $G(\mathcal{L})$.

- Hence, if $\mathcal{L}$ has type δ, there exists an isomorphism of representations $\beta : V(\delta) \xrightarrow{\sim} \Gamma(A, \mathcal{L})$:

$$\forall v \in V(\delta), h \in \mathcal{H}(\delta), \quad \beta(h \cdot v) = \Theta_{\mathcal{L}}(h) \cdot \beta(v).$$

- β is unique up to a multiplicative constant (by Shur's lemma).

Theta functions

- Consider the basis of $V(\delta)$ given by Kronecker functions:

$$\delta_i : j \in K_1(\delta) \longmapsto \delta_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

  for all $i \in K_1(\delta)$.
- Then the $\theta_i^{\mathcal{L}} := \beta(\delta_i)$ form the basis of **theta functions** on $(A, \mathcal{L}, \Theta_{\mathcal{L}})$.
- This basis is defined up to a multiplicative constant.

Theta functions

- Consider the basis of $V(\delta)$ given by Kronecker functions:

$$\delta_i : j \in K_1(\delta) \longmapsto \delta_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

  for all $i \in K_1(\delta)$.
- Then the $\theta_i^{\mathcal{L}} := \beta(\delta_i)$ form the basis of **theta functions** on $(A, \mathcal{L}, \Theta_{\mathcal{L}})$.
- This basis is defined up to a multiplicative constant.
- It defines a projective map:

$$\begin{array}{ccc} A & \longrightarrow & \mathbb{P}_k^{d_1 \cdots d_g - 1} \\ x & \longmapsto & (\theta_i^{\mathcal{L}}(x))_{i \in K_1(\delta)} \end{array}$$

Theta functions

- Consider the basis of $V(\delta)$ given by Kronecker functions:

$$\delta_i : j \in K_1(\delta) \longmapsto \delta_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

  for all $i \in K_1(\delta)$.
- Then the $\theta_i^{\mathcal{L}} := \beta(\delta_i)$ form the basis of **theta functions** on $(A, \mathcal{L}, \Theta_{\mathcal{L}})$.
- This basis is defined up to a multiplicative constant.
- It defines a projective map:

$$\begin{array}{ccc} A & \longrightarrow & \mathbb{P}_k^{d_1 \cdots d_g - 1} \\ x & \longmapsto & (\theta_i^{\mathcal{L}}(x))_{i \in K_1(\delta)} \end{array}$$

- **Main advantage of theta functions:** the action $G(\mathcal{L}) \curvearrowright \Gamma(A, \mathcal{L})$ yields nice formulas on theta functions.

Theta structures of level n

- When $\mathcal{L}$ is of type $\delta = (n, \cdots, n)$, we say $\mathcal{L}$ has **level** n.
- Then $K(\mathcal{L}) = A[n]$ and there are n^g theta functions $(\theta_i^{\mathcal{L}})_{i \in (\mathbb{Z}/n\mathbb{Z})^g}$.

Theta structures of level n

- When $\mathcal{L}$ is of type $\delta = (n, \cdots, n)$, we say $\mathcal{L}$ has **level** n.
- Then $K(\mathcal{L}) = A[n]$ and there are n^g theta functions $(\theta_i^{\mathcal{L}})_{i \in (\mathbb{Z}/n\mathbb{Z})^g}$.

Theorem (Mumford, 1974)

When $n \geq 3$, the map $A \longrightarrow \mathbb{P}_k^{n^g}$ induced by theta functions $(\theta_i^{\mathcal{L}})_{i \in (\mathbb{Z}/n\mathbb{Z})^g}$ is an embedding.

Theorem (Birkenhake, Lange, 2004)

*When $n = 2$, the map $K_A \longrightarrow \mathbb{P}_k^{2^g}$ induced by theta functions $(\theta_i^{\mathcal{L}})_{i \in (\mathbb{Z}/2\mathbb{Z})^g}$ is an embedding, where $K_A := A/\pm$ is the **Kummer variety** associated to A.*

Theta structures of level n

- When $\mathcal{L}$ is of type $\delta = (n, \cdots, n)$, we say $\mathcal{L}$ has **level** n.
- Then $K(\mathcal{L}) = A[n]$ and there are n^g theta functions $(\theta_i^{\mathcal{L}})_{i \in (\mathbb{Z}/n\mathbb{Z})^g}$.

Theorem (Mumford, 1974)

When $n \geq 3$, the map $A \longrightarrow \mathbb{P}_k^{n^g}$ induced by theta functions $(\theta_i^{\mathcal{L}})_{i \in (\mathbb{Z}/n\mathbb{Z})^g}$ is an embedding.

Theorem (Birkenhake, Lange, 2004)

*When $n = 2$, the map $K_A \longrightarrow \mathbb{P}_k^{2^g}$ induced by theta functions $(\theta_i^{\mathcal{L}})_{i \in (\mathbb{Z}/2\mathbb{Z})^g}$ is an embedding, where $K_A := A/\pm$ is the **Kummer variety** associated to A.*

- $n = 2$ gives the minimal number of coordinates (2^g on the Kummer variety).

Computing isogenies with theta coordinates

Polarised isogenies

Definition

A **polarised isogeny** $f : (A, \mathcal{L}) \longrightarrow (B, \mathcal{M})$ satisfies $f^*\mathcal{M} \cong \mathcal{L}$.

If f is such an isogeny, then we have:

- $\widehat{f} \circ \varphi_{\mathcal{M}} \circ f = \varphi_{\mathcal{L}}$.
- $f^{-1}(K(\mathcal{M})) \subseteq K(\mathcal{L})$. The type $\delta_{\mathcal{L}}$ is "bigger" than $\delta_{\mathcal{M}}$.
- $K := \ker(f) \subset K(\mathcal{L})$ is an isotropic subgroup ($e_{\mathcal{L}|K\times K} = 1$).

Descent theory

- Let $f : (A, \mathcal{L}) \longrightarrow (B, \mathcal{M})$ be a polarised isogeny ($f^*\mathcal{M} \cong \mathcal{L}$).
- Given an isomorphism $\alpha : f^*\mathcal{M} \xrightarrow{\sim} \mathcal{L}$, define a **level subgroup**:

$$\widetilde{K} := \{(x, t_x^*\alpha \circ \alpha^{-1}) \mid x \in K\}.$$

- $\widetilde{K} \simeq K$ lifts K in $G(\mathcal{L})$.
- And α induces an isomorphism $\alpha_f : Z(\widetilde{K})/\widetilde{K} \xrightarrow{\sim} G(\mathcal{M})$.

Theorem (Grothendieck)

There is a one to one correspondence between couples (f, α) and level subgroups $\widetilde{K} \subset G(\mathcal{L})$.

Compatible Theta structures

Definition

Two theta-structures $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{M}}$ on $G(\mathcal{L})$ and $G(\mathcal{M})$ respectively are **compatible** when:

- $\widetilde{K} = (\widetilde{K} \cap \widetilde{K}_1(\Theta_{\mathcal{L}})) \oplus (\widetilde{K} \cap \widetilde{K}_2(\Theta_{\mathcal{L}}))$.
- α_f maps $Z(\widetilde{K}) \cap \widetilde{K}_i(\Theta_{\mathcal{L}})$ to $\widetilde{K}_i(\Theta_{\mathcal{M}})$ for $i \in \{1, 2\}$.

- Write $K = K_1 \oplus K_2$ with $K_i \subseteq K_i(\Theta_{\mathcal{L}})$ for $i \in \{1, 2\}$.
- Let $K^{\perp} = \{x \in K(\mathcal{L}) \mid \forall y \in K, \quad e_{\mathcal{L}}(x, y) = 1\}$.
- Write $K^{\perp} = K^{\perp,1} \oplus K^{\perp,2}$ with $K^{\perp,i} \subseteq K_i(\Theta_{\mathcal{L}})$ for $i \in \{1, 2\}$.

Proposition (Mumford, 1966)

There is a one to one correspondence between theta-structures $\Theta_{\mathcal{M}}$ on $G(\mathcal{M})$ compatible with $\Theta_{\mathcal{L}}$ and isomorphisms $\sigma : K^{\perp,1}/K_1 \xrightarrow{\sim} K_1(\delta_{\mathcal{M}})$.

The isogeny theorem

Theorem (Mumford, 1966 and Robert, 2010)

Let $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{M}}$ be compatible theta-structures on $G(\mathcal{L})$ and $G(\mathcal{M})$ respectively and let $\sigma : K^{\perp,1}/K_1 \xrightarrow{\sim} K_1(\delta_{\mathcal{M}})$ be the isomorphism induced by $\Theta_{\mathcal{M}}$.
Then, there exists $\lambda \in k^*$ such that for all $i \in K_1(\delta_{\mathcal{M}})$,

$$f^*\theta_i^{\mathcal{M}} = \lambda \sum_{j \in \overline{\Theta}_{\mathcal{L}}^{-1}(\sigma^{-1}(\{i\}))} \theta_j^{\mathcal{L}}.$$

Our goal

- Let $(A, \mathcal{L}_0)$ and $(B, \mathcal{M}_0)$ be a principally polarised abelian varieties (PPAVs).
- An n-**isogeny** is a polarised isogeny $f : (A, \mathcal{L}_0^n) \longrightarrow (B, \mathcal{M}_0)$ i.e. such that $f^* \mathcal{M}_0 \simeq \mathcal{L}_0^n$.
- Then, we have:

$$\widehat{f} \circ \varphi_{\mathcal{M}_0} \circ f = \varphi_{\mathcal{L}_0^n} = [n] \varphi_{\mathcal{L}_0}$$

- And $K = \ker(f) \subseteq K(\mathcal{L}_0^n) = A[n]$.

Our goal

- Let $(A, \mathcal{L}_0)$ and $(B, \mathcal{M}_0)$ be a principally polarised abelian varieties (PPAVs).
- An n-**isogeny** is a polarised isogeny $f : (A, \mathcal{L}_0^n) \longrightarrow (B, \mathcal{M}_0)$ i.e. such that $f^*\mathcal{M}_0 \simeq \mathcal{L}_0^n$.
- Then, we have:

$$\widehat{f} \circ \varphi_{\mathcal{M}_0} \circ f = \varphi_{\mathcal{L}_0^n} = [n]\varphi_{\mathcal{L}_0}$$

- And $K = \ker(f) \subseteq K(\mathcal{L}_0^n) = A[n]$.

Goal: When $n = 2^e$, given $K \subset A[2^e]$, compute f in level 2 theta coordinates:

$$(\theta_i^{\mathcal{L}_0^{\mathbf{2}}}(x))_{i \in (\mathbb{Z}/2\mathbb{Z})^g} \longmapsto (\theta_i^{\mathcal{M}_0^{\mathbf{2}}}(f(x)))_{i \in (\mathbb{Z}/2\mathbb{Z})^g}$$

Our goal

- Let $(A, \mathcal{L}_0)$ and $(B, \mathcal{M}_0)$ be a principally polarised abelian varieties (PPAVs).
- An n-**isogeny** is a polarised isogeny $f : (A, \mathcal{L}_0^n) \longrightarrow (B, \mathcal{M}_0)$ i.e. such that $f^*\mathcal{M}_0 \simeq \mathcal{L}_0^n$.
- Then, we have:

$$\widehat{f} \circ \varphi_{\mathcal{M}_\mathbf{0}} \circ f = \varphi_{\mathcal{L}_\mathbf{0}^n} = [n]\varphi_{\mathcal{L}_\mathbf{0}}$$

- And $K = \ker(f) \subseteq K(\mathcal{L}_0^n) = A[n]$.

Goal: When $n = 2^e$, given $K \subset A[2^e]$, compute f in level 2 theta coordinates:

$$(\theta_i^{\mathcal{L}_\mathbf{0}^\mathbf{2}}(x))_{i\in(\mathbb{Z}/2\mathbb{Z})^g} \longmapsto (\theta_i^{\mathcal{M}_\mathbf{0}^\mathbf{2}}(f(x)))_{i\in(\mathbb{Z}/2\mathbb{Z})^g}$$

Technicality: We shall need $K' \subset A[2^{e+2}]$ maximal isotropic such that $[4]K' = K$.

Decomposing the problem

f can be decomposed as a chain:

$$A_0 = A \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \quad \cdots \quad A_{e-1} \xrightarrow{f_e} A_e = B$$

where $f_i : (A_{i-1}, \mathcal{L}_{i-1}^2) \longrightarrow (A_i, \mathcal{L}_i)$ is a 2-isogeny between PPAVs of kernel $[2^{e-i}]f_{i-1} \circ \cdots \circ f_1(K)$ for all $i \in [\![1 \ ; \ e]\!]$.

Decomposing the problem

f can be decomposed as a chain:

$$A_0 = A \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \quad \cdots \quad A_{e-1} \xrightarrow{f_e} A_e = B$$

where $f_i : (A_{i-1}, \mathcal{L}_{i-1}^2) \longrightarrow (A_i, \mathcal{L}_i)$ is a 2-isogeny between PPAVs of kernel $[2^{e-i}]f_{i-1} \circ \cdots \circ f_1(K)$ for all $i \in [\![1 \ ; \ e]\!]$.

New goal: Let $f : (A, \mathcal{L}_0^2) \longrightarrow (B, \mathcal{M}_0)$ be a 2-isogeny between PPAVs. Given $K = \ker(f) \subset A[2]$, compute f in level 2 theta coordinates:

$$(\theta_i^{\mathcal{L}_{\mathbf{0}}^{\mathbf{2}}}(x))_{i \in (\mathbb{Z}/2\mathbb{Z})^g} \longmapsto (\theta_i^{\mathcal{M}_{\mathbf{0}}^{\mathbf{2}}}(f(x)))_{i \in (\mathbb{Z}/2\mathbb{Z})^g}$$

Decomposing the problem

f can be decomposed as a chain:

$$A_0 = A \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \quad \cdots \quad A_{e-1} \xrightarrow{f_e} A_e = B$$

where $f_i : (A_{i-1}, \mathcal{L}_{i-1}^2) \longrightarrow (A_i, \mathcal{L}_i)$ is a 2-isogeny between PPAVs of kernel $[2^{e-i}]f_{i-1} \circ \cdots \circ f_1(K)$ for all $i \in [\![1 \ ; \ e]\!]$.

New goal: Let $f : (A, \mathcal{L}_0^2) \longrightarrow (B, \mathcal{M}_0)$ be a 2-isogeny between PPAVs. Given $K = \ker(f) \subset A[2]$, compute f in level 2 theta coordinates:

$$(\theta_i^{\mathcal{L}_0^{\mathbf{2}}}(x))_{i \in (\mathbb{Z}/2\mathbb{Z})^g} \longmapsto (\theta_i^{\mathcal{M}_0^{\mathbf{2}}}(f(x)))_{i \in (\mathbb{Z}/2\mathbb{Z})^g}$$

New technicality: We shall need $K' \subset A[8]$ maximal isotropic such that $[4]K' = K$.

Applying the isogeny theorem

- Let $f : (A, \mathcal{L}_0^2) \longrightarrow (B, \mathcal{M}_0)$ be a 2-isogeny between PPAVs.
- f is also a polarised isogeny $(A, \mathcal{L}^2) \longrightarrow (B, \mathcal{M})$ where $\mathcal{L} := \mathcal{L}_0^2$ and $\mathcal{M} := \mathcal{M}_0^2$ are of level 2.

Applying the isogeny theorem

- Let $f : (A, \mathcal{L}_0^2) \longrightarrow (B, \mathcal{M}_0)$ be a 2-isogeny between PPAVs.
- f is also a polarised isogeny $(A, \mathcal{L}^2) \longrightarrow (B, \mathcal{M})$ where $\mathcal{L} := \mathcal{L}_0^2$ and $\mathcal{M} := \mathcal{M}_0^2$ are of level 2.

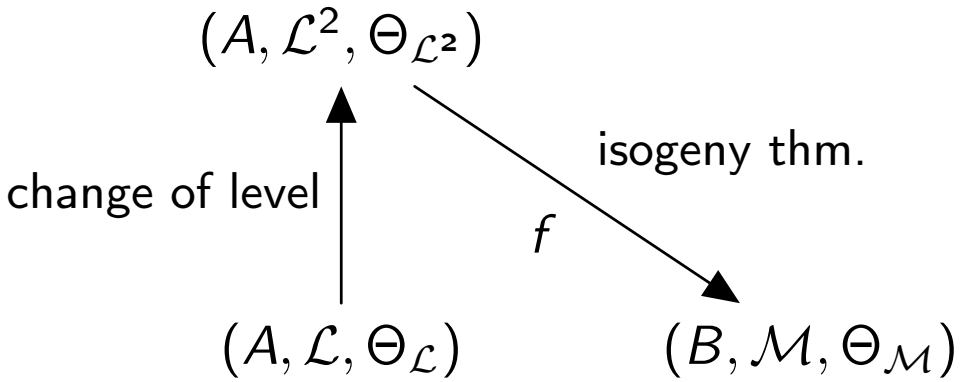
Corollary (of the isogeny theorem)

Assume $K = K_2(\Theta_{\mathcal{L}})$. Then we can choose compatible theta structures $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{M}}$ such that:

$$\forall i \in (\mathbb{Z}/2\mathbb{Z})^g, \quad f^* \theta_i^{\mathcal{M}} = \theta_{2i}^{\mathcal{L}^2} \quad \text{i.e.} \quad \theta_i^{\mathcal{M}}(f(x)) = \theta_{2i}^{\mathcal{L}^2}(x)$$

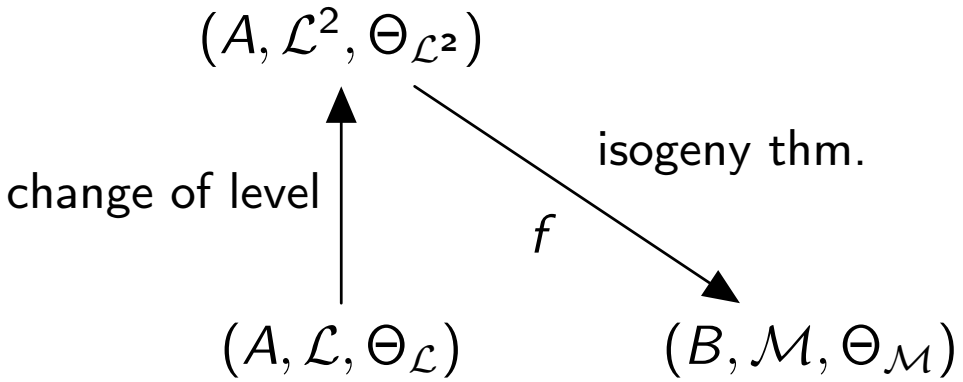
Problem: We know $(\theta_i^{\mathcal{L}}(x))_i$ but not $(\theta_{2i}^{\mathcal{L}^2}(x))_i$.

Change of level



Goal: Change of level $(A, \mathcal{L}, \Theta_{\mathcal{L}}) \longrightarrow (A, \mathcal{L}^2, \Theta_{\mathcal{L}^2})$.

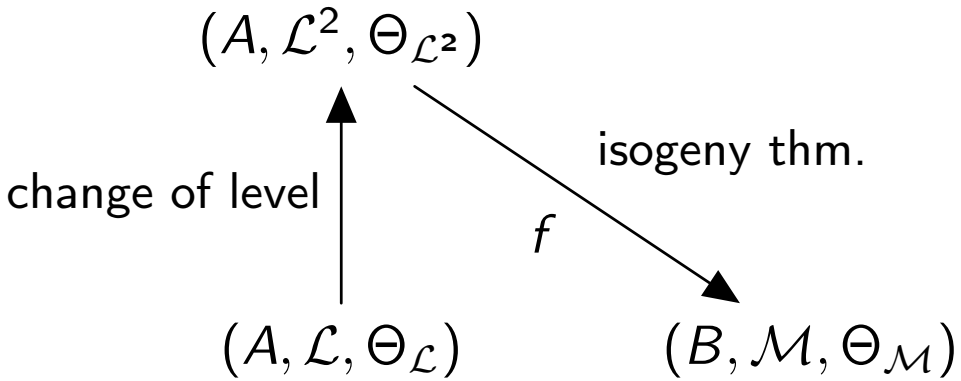
Change of level



Goal: Change of level $(A, \mathcal{L}, \Theta_{\mathcal{L}}) \longrightarrow (A, \mathcal{L}^2, \Theta_{\mathcal{L}^2})$.

- We have some compatibility condition between $(A, \mathcal{L}^2, \Theta_{\mathcal{L}^2})$ and $(B, \mathcal{M}, \Theta_{\mathcal{M}})$.
- What compatibility condition do we have between $(A, \mathcal{L}, \Theta_{\mathcal{L}})$ and $(A, \mathcal{L}^2, \Theta_{\mathcal{L}^2})$?

Change of level



Goal: Change of level $(A, \mathcal{L}, \Theta_{\mathcal{L}}) \longrightarrow (A, \mathcal{L}^2, \Theta_{\mathcal{L}^2})$.

- We have some compatibility condition between $(A, \mathcal{L}^2, \Theta_{\mathcal{L}^2})$ and $(B, \mathcal{M}, \Theta_{\mathcal{M}})$.
- What compatibility condition do we have between $(A, \mathcal{L}, \Theta_{\mathcal{L}})$ and $(A, \mathcal{L}^2, \Theta_{\mathcal{L}^2})$?
- First, $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{L}^2}$ have to be **symmetric** (then $\Theta_{\mathcal{M}}$ is symmetric).

Symmetric theta structures

Definition

A theta-structure $\Theta_{\mathcal{L}}$ is **symmetric** if $\Theta_{\mathcal{L}} \circ D_{-1} = \delta_{-1} \circ \Theta_{\mathcal{L}}$, where $D_{-1} \in \mathrm{Aut}(\mathcal{H}(\delta))$ and $\delta_{-1} \in \mathrm{Aut}(G(\mathcal{L}))$ are maps that lift $[-1] : x \longrightarrow -x$.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & k^* & \longrightarrow & G(\mathcal{L}) & \longrightarrow & K(\mathcal{L}) & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle \delta_{-1}} & & \downarrow{\scriptstyle [-1]} & & \\
1 & \longrightarrow & k^* & \longrightarrow & G(\mathcal{L}) & \longrightarrow & K(\mathcal{L}) & \longrightarrow & 0
\end{array}$$

$$\begin{array}{ccccccccc}
1 & \longrightarrow & k^* & \longrightarrow & \mathcal{H}(\delta) & \longrightarrow & K(\delta) & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle D_{-1}} & & \downarrow{\scriptstyle [-1]} & & \\
1 & \longrightarrow & k^* & \longrightarrow & \mathcal{H}(\delta) & \longrightarrow & K(\delta) & \longrightarrow & 0
\end{array}$$

Compatible symmetric theta structures

- Consider $\varepsilon_2 : G(\mathcal{L}) \longrightarrow G(\mathcal{L}^2)$ and $\eta_2 : G(\mathcal{L}^2) \longrightarrow G(\mathcal{L})$:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & k^* & \longrightarrow & G(\mathcal{L}) & \xrightarrow{\rho_{\mathcal{L}}} & K(\mathcal{L}) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \lambda\mapsto\lambda^2} & & \downarrow{\scriptstyle \varepsilon_2} & & \downarrow & & \\
1 & \longrightarrow & k^* & \longrightarrow & G(\mathcal{L}^2) & \xrightarrow{\rho_{\mathcal{L}^2}} & K(\mathcal{L}^2) & \longrightarrow & 0
\end{array}$$

$$\begin{array}{ccccccccc}
1 & \longrightarrow & k^* & \longrightarrow & G(\mathcal{L}^2) & \xrightarrow{\rho_{\mathcal{L}^2}} & K(\mathcal{L}^2) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \lambda\mapsto\lambda^2} & & \downarrow{\scriptstyle \eta_2} & & \downarrow{\scriptstyle [2]} & & \\
1 & \longrightarrow & k^* & \longrightarrow & G(\mathcal{L}) & \xrightarrow{\rho_{\mathcal{L}}} & K(\mathcal{L}) & \longrightarrow & 0
\end{array}$$

- Let $E_2 : \mathcal{H}(\delta) \longrightarrow \mathcal{H}(2\delta)$ and $H_2 : \mathcal{H}(2\delta) \longrightarrow \mathcal{H}(\delta)$ their Heisenberg group analogues.
- We say that symmetric theta structures $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{L}^2}$ are **compatible** if $\Theta_{\mathcal{L}^2} \circ E_2 = \varepsilon_2 \circ \Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{L}} \circ H_2 = \eta_2 \circ \Theta_{\mathcal{L}^2}$.

Differential addition and duplication formulas

For all $\chi \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g$ and $i \in K_1(2\delta)$, define:

$$U^{\mathcal{L}^2}_{\chi,i} := \sum_{t \in (\mathbb{Z}/2\mathbb{Z})^g} \chi(t)\theta^{\mathcal{L}^2}_{i+t\delta}$$

Theorem (Mumford, 1966 and Robert, 2010)

Assume $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{L}^2}$ are symmetric and compatible. Let $x, y \in A$. Then there exists $\lambda_1, \lambda_2 \in k^*$ such that for all $i, j \in K_1(2\delta)$ such that $i \equiv j \mod 2$ and $\chi \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g$, we have:

$$\theta^{\mathcal{L}}_{(i+j)/2}(x+y)\theta^{\mathcal{L}}_{(i-j)/2}(x-y) = \lambda_1 \sum_{\chi \in (\widehat{\mathbb{Z}/2\mathbb{Z}})^g} U^{\mathcal{L}^2}_{\chi,i}(x)U^{\mathcal{L}^2}_{\chi,j}(y)$$

$$U^{\mathcal{L}^2}_{\chi,i}(x)U^{\mathcal{L}^2}_{\chi,j}(y) = \lambda_2 \sum_{t \in (\mathbb{Z}/2\mathbb{Z})^g} \chi(t)\theta^{\mathcal{L}}_{(i+j+t\delta)/2}(x+y)\theta^{\mathcal{L}}_{(i-j+t\delta)/2}(x-y).$$

Differential addition and duplication formulas

These formulas yield:

- A change of level algorithm to evaluate f:

$$(\theta_i^{\mathcal{L}}(x))_i \longmapsto (\theta_{2i}^{\mathcal{L}^2}(x))_i = (\theta_i^{\mathcal{M}}(f(x)))_i.$$

Differential addition and duplication formulas

These formulas yield:

- A change of level algorithm to evaluate f:

$$(\theta_i^{\mathcal{L}}(x))_i \longmapsto (\theta_{2i}^{\mathcal{L}^2}(x))_i = (\theta_i^{\mathcal{M}}(f(x)))_i.$$

But also:

- A duplication algorithm $(\theta_i^{\mathcal{L}}(x))_i \longmapsto (\theta_i^{\mathcal{L}}(2x))_i$ (useful for isogeny chain computations).
- A differential addition algorithm:

$$(\theta_i^{\mathcal{L}}(x))_i, (\theta_i^{\mathcal{L}}(y))_i, (\theta_i^{\mathcal{L}}(x-y))_i \longmapsto (\theta_i^{\mathcal{L}}(x+y))_i.$$

Evaluation algorithm

Proposition (D., Maino, Pope, Robert, 2023)

For all $x \in A$,

$$(\widetilde{\theta}_i^{\mathcal{M}}(f(x)))_i \star (\widetilde{\theta}_i^{\mathcal{M}}(0_B))_i = H \circ S((\theta_i^{\mathcal{L}}(x))_i),$$

where $(\widetilde{\theta}_i^{\mathcal{M}}(x))_i := H((\theta_i^{\mathcal{M}}(x))_i)$ and:

- *H is the **Hadamard** operator: $(x_i)_i \longmapsto \left(\sum_{i \in (\mathbb{Z}/2\mathbb{Z})^g} (-1)^{\langle i|j \rangle} x_i\right)_j$.*
- *S is the **squaring** operator $(x_i)_i \longmapsto (x_i^2)_i$.*
- *$\star$ is the **multiplication** operator $(x_i)_i, (y_i)_i \longmapsto (x_i y_i)_i$.*

Evaluation algorithm

Proposition (D., Maino, Pope, Robert, 2023)

For all $x \in A$,

$$(\widetilde{\theta}_i^{\mathcal{M}}(f(x)))_i \star (\widetilde{\theta}_i^{\mathcal{M}}(0_B))_i = H \circ S((\theta_i^{\mathcal{L}}(x))_i),$$

where $(\widetilde{\theta}_i^{\mathcal{M}}(x))_i := H((\theta_i^{\mathcal{M}}(x))_i)$ and:

- *H is the **Hadamard** operator: $(x_i)_i \longmapsto \left(\sum_{i \in (\mathbb{Z}/2\mathbb{Z})^g} (-1)^{\langle i|j \rangle} x_i\right)_j$.*
- *S is the **squaring** operator $(x_i)_i \longmapsto (x_i^2)_i$.*
- *$\star$ is the **multiplication** operator $(x_i)_i, (y_i)_i \longmapsto (x_i y_i)_i$.*

A straightforward algorithm follows:

$$(\theta_i^{\mathcal{L}}(x))_i \xrightarrow{H} * \xrightarrow{S} * \xrightarrow{\star(1/\widetilde{\theta}_i^{\mathcal{M}}(0_B))_i} * \xrightarrow{H} (\theta_i^{\mathcal{M}}(f(x)))_i$$

Evaluation algorithm

Proposition (D., Maino, Pope, Robert, 2023)

For all $x \in A$,

$$(\widetilde{\theta}_i^{\mathcal{M}}(f(x)))_i \star (\widetilde{\theta}_i^{\mathcal{M}}(0_B))_i = H \circ S((\theta_i^{\mathcal{L}}(x))_i),$$

where $(\widetilde{\theta}_i^{\mathcal{M}}(x))_i := H((\theta_i^{\mathcal{M}}(x))_i)$ and:

- *H is the **Hadamard** operator: $(x_i)_i \longmapsto \left(\sum_{i \in (\mathbb{Z}/2\mathbb{Z})^g} (-1)^{\langle i|j \rangle} x_i\right)_j$.*
- *S is the **squaring** operator $(x_i)_i \longmapsto (x_i^2)_i$.*
- *$\star$ is the **multiplication** operator $(x_i)_i, (y_i)_i \longmapsto (x_i y_i)_i$.*

A straightforward algorithm follows:

$$(\theta_i^{\mathcal{L}}(x))_i \xrightarrow{H} * \xrightarrow{S} * \xrightarrow{\star(1/\widetilde{\theta}_i^{\mathcal{M}}(0_B))_i} * \xrightarrow{H} (\theta_i^{\mathcal{M}}(f(x)))_i$$

Problem: We don't know the dual theta null point $(\widetilde{\theta}_i^{\mathcal{M}}(0_B))_i$.

Computing the codomain theta null point

Proposition (D., Maino, Pope, Robert, 2023)

Let $(T_1, \cdots, T_g)$ *forming a maximal isotropic subgroup of* $A[8]$ *such that* $K = \langle [4]T_1, \cdots, [4]T_g \rangle$.
Then, for all $l \in [\![1\ ;\ g]\!]$ *and* $i \in (\mathbb{Z}/2\mathbb{Z})^g$,

$$\widetilde{\theta}^{\mathcal{M}}_{i+e_l}(0_B) \cdot H \circ S((\theta^{\mathcal{L}}_j(T_l))_j)_i = \widetilde{\theta}^{\mathcal{M}}_i(0_B) \cdot H \circ S((\theta^{\mathcal{L}}_j(T_l))_j)_{i+e_l},$$

where $e_l = (0, \cdots, 1, \cdots, 0)$ *with* 1 *at the* l*-th position.*

Computing the codomain theta null point: $g = 2$

- Let (T_1, T_2) form an isotropic subgroup of $A[8]$ such that $K = \langle [4]T_1, [4]T_2 \rangle$.
- Let $(\alpha : \beta : \gamma : \delta)$ be the dual theta null point.
- Then, by the previous Proposition:

$$H \circ S(\theta_{00}(T_1), \theta_{10}(T_1), \theta_{01}(T_1), \theta_{11}(T_1)) = (x\alpha, x\beta, y\gamma, y\delta)$$

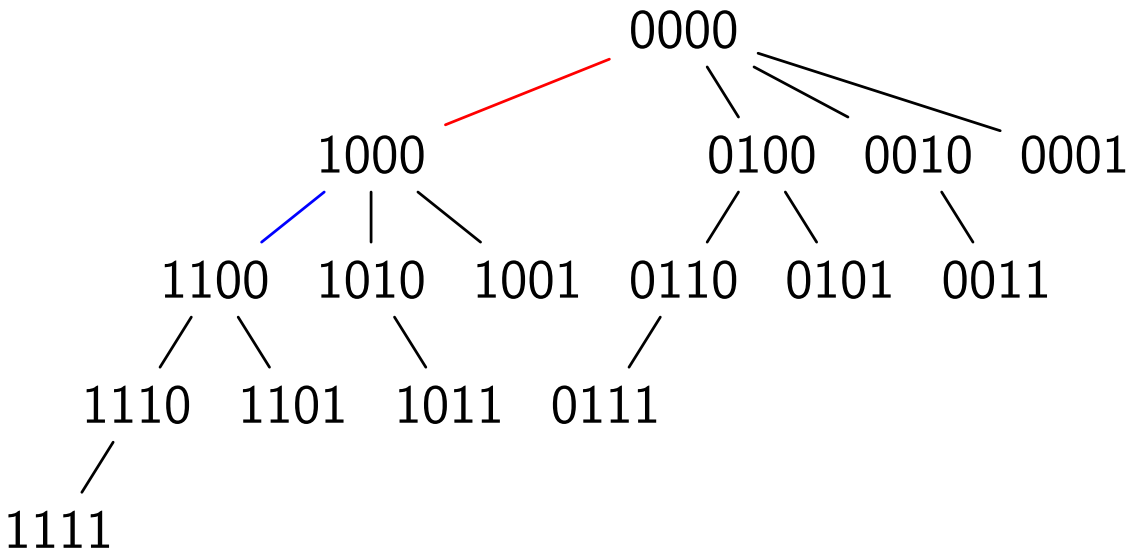
$$H \circ S(\theta_{00}(T_2), \theta_{10}(T_2), \theta_{01}(T_2), \theta_{11}(T_2)) = (z\alpha, t\beta, z\gamma, t\delta)$$

- We can the compute $(1 : \beta/\alpha : \gamma/\alpha : \delta/\alpha)$ as follows:

$$\frac{\beta}{\alpha} = \frac{x\beta}{x\alpha}, \quad \frac{\gamma}{\alpha} = \frac{z\gamma}{z\alpha}, \quad \frac{\delta}{\alpha} = \frac{y\delta}{y\gamma} \cdot \frac{\gamma}{\alpha}$$

Computing the codomain theta null point: $g = 4$

Example: dimension $g = 4$.

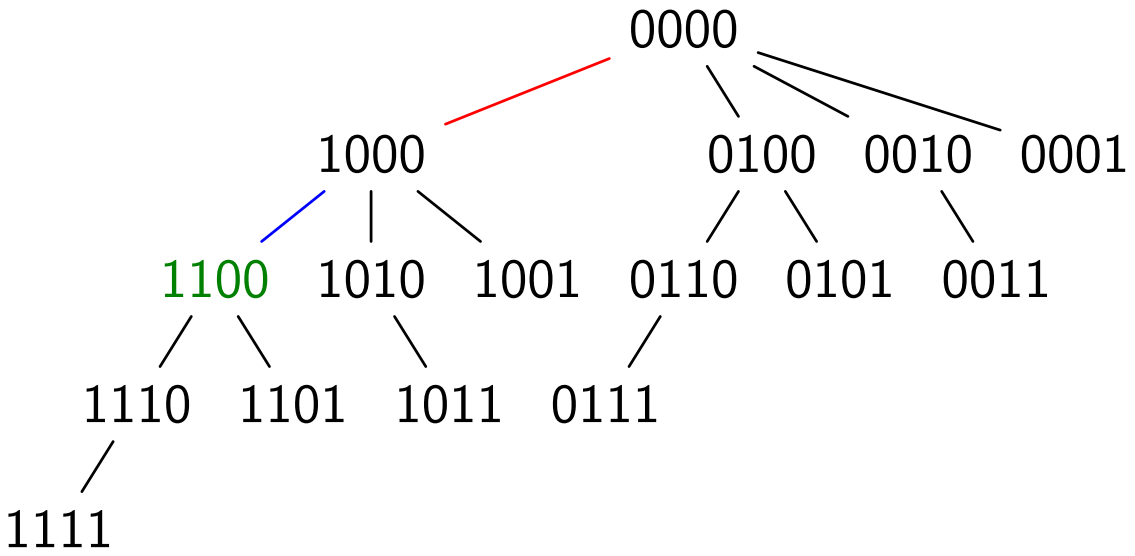


We have:

$$\frac{\widetilde{\theta}^{\mathcal{M}}_{1000}(0_B)}{\widetilde{\theta}^{\mathcal{M}}_{0000}(0_B)} = \frac{H \circ S((\theta^{\mathcal{L}}_i(T_1))_i)_{1000}}{H \circ S((\theta^{\mathcal{L}}_i(T_1))_i)_{0000}}, \quad \frac{\widetilde{\theta}^{\mathcal{M}}_{1100}(0_B)}{\widetilde{\theta}^{\mathcal{M}}_{1000}(0_B)} = \frac{H \circ S((\theta^{\mathcal{L}}_i(T_2))_i)_{1100}}{H \circ S((\theta^{\mathcal{L}}_i(T_2))_i)_{1000}}$$

Computing the codomain theta null point: $g = 4$

Example: dimension $g = 4$.

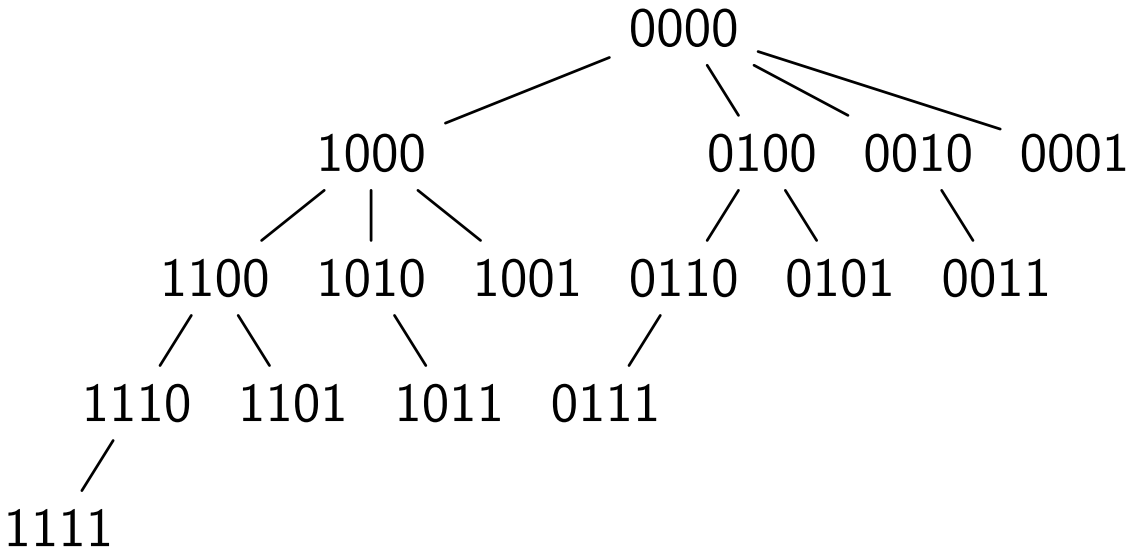


We have:

$$\frac{\widetilde{\theta}^{\mathcal{M}}_{1100}(0_B)}{\widetilde{\theta}^{\mathcal{M}}_{0000}(0_B)} = \frac{\widetilde{\theta}^{\mathcal{M}}_{1100}(0_B)}{\widetilde{\theta}^{\mathcal{M}}_{1000}(0_B)} \cdot \frac{\widetilde{\theta}^{\mathcal{M}}_{1000}(0_B)}{\widetilde{\theta}^{\mathcal{M}}_{0000}(0_B)}$$

Computing the codomain theta null point: $g = 4$

Example: dimension $g = 4$.



We finally obtain:

$$\left(1 : \frac{\widetilde{\theta}^{\mathcal{M}}_{1000}(0_B)}{\widetilde{\theta}^{\mathcal{M}}_{0000}(0_B)} : \frac{\widetilde{\theta}^{\mathcal{M}}_{1100}(0_B)}{\widetilde{\theta}^{\mathcal{M}}_{0000}(0_B)} : \frac{\widetilde{\theta}^{\mathcal{M}}_{1010}(0_B)}{\widetilde{\theta}^{\mathcal{M}}_{0000}(0_B)} : \cdots\right)$$

Zero dual theta constants

- So far, we have assumed that $\widetilde{\theta}_i^{\mathcal{M}}(0_B) \neq 0$ for all $i \in (\mathbb{Z}/2\mathbb{Z})^g$.
- Recall the evaluation algorithm:

$$(\theta_i^{\mathcal{L}}(x))_i \xrightarrow{H} * \xrightarrow{S} * \xrightarrow{\star(1/\widetilde{\theta}_i^{\mathcal{M}}(0_B))_i} * \xrightarrow{H} (\theta_i^{\mathcal{M}}(f(x)))_i$$

- What can we do when $\widetilde{\theta}_i^{\mathcal{M}}(0_B) = 0$ for some $i \in (\mathbb{Z}/2\mathbb{Z})^g$?

Zero dual theta constants

- So far, we have assumed that $\widetilde{\theta}_i^{\mathcal{M}}(0_B) \neq 0$ for all $i \in (\mathbb{Z}/2\mathbb{Z})^g$.
- Recall the evaluation algorithm:

$$(\theta_i^{\mathcal{L}}(x))_i \xrightarrow{H} * \xrightarrow{S} * \xrightarrow{\star(1/\widetilde{\theta}_i^{\mathcal{M}}(0_B))_i} * \xrightarrow{H} (\theta_i^{\mathcal{M}}(f(x)))_i$$

- What can we do when $\widetilde{\theta}_i^{\mathcal{M}}(0_B) = 0$ for some $i \in (\mathbb{Z}/2\mathbb{Z})^g$?
- We expect this to happen only during gluing steps:

$$f : A_1 \times A_2 \longrightarrow B$$

- Because level 2 theta coordinates encode points up to a sign, we are computing:

$$(\pm x, \pm y) \longmapsto \pm f(x, y)$$

- We need additional information to lift the sign indetermination.

Gluing evaluation algorithm

- When some dual theta-constants vanish, we need additional data:

$$H \circ S((\theta_i^{\mathcal{L}}(x+T))_i),$$

  for some $T \in A[4]$ such that $[2]T \in K$.
- **Idea:** Using translates $x+T$ shifts indices in the isogeny evaluation formula so that we can avoid dividing by zero.

Gluing evaluation algorithm

- When some dual theta-constants vanish, we need additional data:

$$H \circ S((\theta_i^{\mathcal{L}}(x+T))_i),$$

  for some $T \in A[4]$ such that $[2]T \in K$.
- **Idea:** Using translates $x+T$ shifts indices in the isogeny evaluation formula so that we can avoid dividing by zero.

- In dimension $g=2$, translating by $T := [2]T_1$ is sufficient.
- In dimension $g=4$, we use 2 translates $T = [2]T_1, [2]T_2$ are sufficient (conjecture).

Gluing evaluation algorithm

- When some dual theta-constants vanish, we need additional data:

$$H \circ S((\theta_i^{\mathcal{L}}(x+T))_i),$$

  for some $T \in A[4]$ such that $[2]T \in K$.
- **Idea:** Using translates $x+T$ shifts indices in the isogeny evaluation formula so that we can avoid dividing by zero.

- In dimension $g = 2$, translating by $T := [2]T_1$ is sufficient.
- In dimension $g = 4$, we use 2 translates $T = [2]T_1, [2]T_2$ are sufficient (conjecture).

- The same idea applies to codomain dual theta null point computation.

Put the kernel in the right place

- So far, we have assumed that $K = K_2(\Theta_{\mathcal{L}})$.
- This depends on the choice of theta structure $\Theta_{\mathcal{L}}$ on A and the associated system of theta coordinates $(\theta_i^{\mathcal{L}})_i$.
- **Idea:** Change the theta $\Theta'_{\mathcal{L}}$ so that $K = K_2(\Theta'_{\mathcal{L}})$.
- **Problem:** How to compute the new theta coordinates $(\theta'^{\mathcal{L}}_i)_i$?

Theta structures are determined by symplectic basis

Theorem (Mumford, 1966)

Every symmetric theta-structure on $G(\mathcal{L})$ is determined by a symplectic isomorphism $K(2\delta) \xrightarrow{\sim} K(\mathcal{L}^2)$.

Theta structures are determined by symplectic basis

Theorem (Mumford, 1966)

Every symmetric theta-structure on $G(\mathcal{L})$ is determined by a symplectic isomorphism $K(2\delta) \xrightarrow{\sim} K(\mathcal{L}^2)$.

In other words, if $\Theta_{\mathcal{L}}$ is a level 2 theta structure, then it is determined by a **symplectic basis** $(S_1, \cdots, S_g, T_1, \cdots, T_g)$ of $A[4]$.

Such a basis satisfies for some 4-th root of unity $\zeta_4 \in k^*$ and for all $I, m \in [\![1\ ;\ g]\!]$:

- $e_4(T_I, T_m) = e_4(S_I, S_m) = 1$;
- $e_4(S_I, T_m) = \zeta_4^{\delta_{I,m}}$.

Besides, $K_1(\Theta_{\mathcal{L}}) = \langle [2]S_1, \cdots, [2]S_g \rangle$ and $K_2(\Theta_{\mathcal{L}}) = \langle [2]T_1, \cdots, [2]T_g \rangle$.

Explicit change of coordinate formulas

- Let $(\theta_i^{\mathcal{L}})_i$ be the original coordinates associated to a symplectic basis $\mathcal{B} := (S_1, \cdots, T_g)$.
- Let $(\theta'^{\mathcal{L}}_i)_i$ be the new coordinates associated to a symplectic basis $\mathcal{B}' := (S'_1, \cdots, T'_g)$ with $K = \langle [2]T'_1, \cdots, [2]T'_g \rangle = K_2(\Theta'_{\mathcal{L}})$.
- Let the change of basis matrix from $\mathcal{B}$ to $\mathcal{B}' := \mathcal{B} \cdot M$:

$$M := \begin{pmatrix} A & C \\ B & D \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z}/4\mathbb{Z})$$

Theorem (D., 2024)

There exists $i_0 \in K_1(\underline{2})$ such that for all $i \in (\mathbb{Z}/2\mathbb{Z})^g$:

$$\theta'^{\mathcal{L}}_i = \lambda \sum_{j \in (\mathbb{Z}/2\mathbb{Z})^g} \zeta_4^{\langle i|j\rangle - \langle Ai+Cj+2i_0 | Bi+Dj\rangle} \theta^{\mathcal{L}}_{Ai+Cj+i_0},$$

where $\zeta_4 := e_4(S_l, T_l) = e_4(S'_l, T'_l)$ for all $l \in [\![1\ ;\ g]\!]$.

Summary: computing a 2^e-isogeny chain

Goal: Compute the 2^e-isogeny chain $f : A_0 \xrightarrow{f_1} A_1 \cdots A_{e-1} \xrightarrow{f_e} A_e$ given $K' \subset A_0[2^{e+2}]$ such that $[4]K' = \ker(f)$.

Summary: computing a 2^e-isogeny chain

Goal: Compute the 2^e-isogeny chain $f : A_0 \xrightarrow{f_1} A_1 \cdots A_{e-1} \xrightarrow{f_e} A_e$ given $K' \subset A_0[2^{e+2}]$ such that $[4]K' = \ker(f)$.

- Change theta coordinates on $(A_0, \mathcal{L}_0)$ to ensure that $\ker(f_1) = K_2(\Theta_{\mathcal{L}_0})$.
- Compute the dual theta null point $(\widetilde{\theta}_i^{\mathcal{L}_1}(0_1))_i$ of A_1 using $K_1' := [2^{e-1}]K'$.

Summary: computing a 2^e-isogeny chain

Goal: Compute the 2^e-isogeny chain $f : A_0 \xrightarrow{f_1} A_1 \cdots A_{e-1} \xrightarrow{f_e} A_e$ given $K' \subset A_0[2^{e+2}]$ such that $[4]K' = \ker(f)$.

- Change theta coordinates on $(A_0, \mathcal{L}_0)$ to ensure that $\ker(f_1) = K_2(\Theta_{\mathcal{L}_0})$.
- Compute the dual theta null point $(\widetilde{\theta}_i^{\mathcal{L}_1}(0_1))_i$ of A_1 using $K_1' := [2^{e-1}]K'$.
- **Good news:** We automatically have $\ker(f_2) = K_2(\Theta_{\mathcal{L}_1})$, no need to change the theta coordinates again.

- Compute $K_2' := [2^{e-2}]f_1(K')$.
- Compute the dual theta null point $(\widetilde{\theta}_i^{\mathcal{L}_2}(0_2))_i$ of A_2 using K_2'.

Summary: computing a 2^e-isogeny chain

Goal: Compute the 2^e-isogeny chain $f : A_0 \xrightarrow{f_1} A_1 \cdots A_{e-1} \xrightarrow{f_e} A_e$ given $K' \subset A_0[2^{e+2}]$ such that $[4]K' = \ker(f)$.

- Change theta coordinates on $(A_0, \mathcal{L}_0)$ to ensure that $\ker(f_1) = K_2(\Theta_{\mathcal{L}_0})$.
- Compute the dual theta null point $(\widetilde{\theta}_i^{\mathcal{L}_1}(0_1))_i$ of A_1 using $K_1' := [2^{e-1}]K'$.
- **Good news:** We automatically have $\ker(f_2) = K_2(\Theta_{\mathcal{L}_1})$, no need to change the theta coordinates again.

- Compute $K_2' := [2^{e-2}]f_1(K')$.
- Compute the dual theta null point $(\widetilde{\theta}_i^{\mathcal{L}_2}(0_2))_i$ of A_2 using K_2'.

- Proceed similarly to obtain the dual theta null point $(\widetilde{\theta}_i^{\mathcal{L}_2}(0_j))_i$ of A_j for all $j \geq 3$.

Implementations for applications

In dimension 2 [DMPR23]

Goal: Compute a 2^e-isogeny $F : E_1 \times E_2 \longrightarrow E_3 \times E_4$, given $K' \subset (E_1 \times E_2)[2^{e+2}]$ such that $[4]K' = \ker(f)$ defined over $\mathbb{F}_{p^2}$.

$$E_1 \times E_2 \xrightarrow{\text{gluing}} A_1 \longrightarrow A_2 \quad \cdots \quad A_{e-1} \xrightarrow{\text{splitting}} E_3 \times E_4$$

In dimension 2 [DMPR23]

Goal: Compute a 2^e-isogeny $F : E_1 \times E_2 \longrightarrow E_3 \times E_4$, given $K' \subset (E_1 \times E_2)[2^{e+2}]$ such that $[4]K' = \ker(f)$ defined over $\mathbb{F}_{p^2}$.

$$E_1 \times E_2 \xrightarrow{\text{gluing}} A_1 \longrightarrow A_2 \quad \cdots \quad A_{e-1} \xrightarrow{\text{splitting}} E_3 \times E_4$$

- After the splitting, a change of theta coordinates is necessary to recover $E_3 \times E_4$ as a product.

In dimension 2 [DMPR23]

Goal: Compute a 2^e-isogeny $F : E_1 \times E_2 \longrightarrow E_3 \times E_4$, given $K' \subset (E_1 \times E_2)[2^{e+2}]$ such that $[4]K' = \ker(f)$ defined over $\mathbb{F}_{p^2}$.

$$E_1 \times E_2 \xrightarrow{\text{gluing}} A_1 \longrightarrow A_2 \quad \cdots \quad A_{e-1} \xrightarrow{\text{splitting}} E_3 \times E_4$$

- After the splitting, a change of theta coordinates is necessary to recover $E_3 \times E_4$ as a product.
- If we only know $K = \ker(f) \subset (E_1 \times E_2)[2^e]$, we can still compute F at the expense of square root computations in the last two steps.

Implementation results in dimension 2 [DMPR23]

Table: Timings of a 2^e-isogeny **chain computation** in dimension 2.

$\log_2(p)$	254	381	1293
e	126	208	632
Theta Rust	**2.13 ms**	**9.05 ms**	**463 ms**
Theta SageMath	108 ms	201 ms	1225 ms
Kummer SageMath	467 ms	858 ms	5150 ms
Jacobian SageMath	760 ms	1478 ms	9196 ms
Richelot SageMath	1028 ms	1998 ms	12840 ms

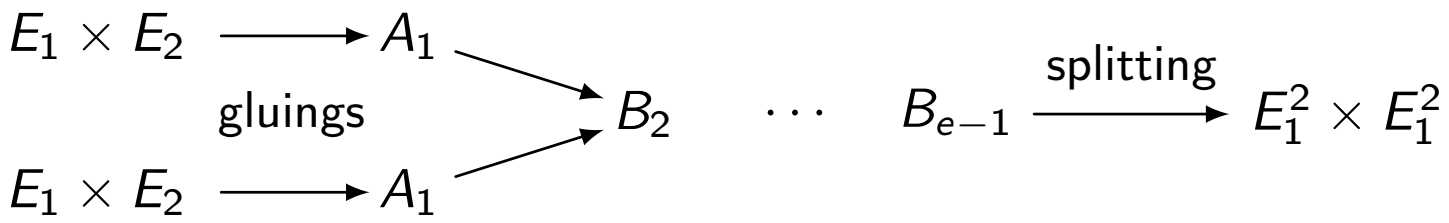
Implementation results in dimension 2 [DMPR23]

Table: Timings of a 2^e-isogeny **evaluation** in dimension 2.

$\log_2(p)$	254	381	1293
e	126	208	632
Theta Rust	**161 μs**	**411 μs**	**17.8 ms**
Theta SageMath	5.43 ms	8.68 ms	40.8 ms
Kummer SageMath	18.4 ms	31.4 ms	170 ms
Jacobian SageMath	66.7 ms	119 ms	593 ms
Richelot SageMath	114 ms	208 ms	1203 ms

In dimension 4 [Dar24]

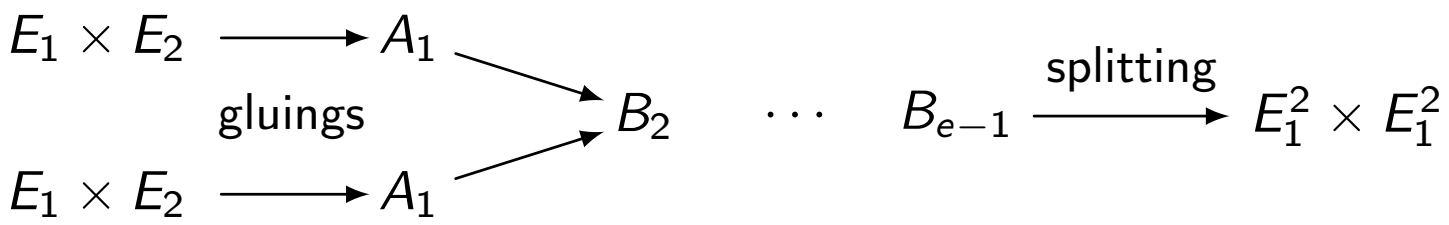
Goal: Compute a 2^e-isogeny $F : E_1^2 \times E_2^2 \longrightarrow E_1^2 \times E_2^2$, given $K' \subset (E_1^2 \times E_2^2)[2^{e+2}]$ such that $[4]K' = \ker(f)$ defined over $\mathbb{F}_{p^2}$.



- Gluings are more technical to handle than in dimension 2.

In dimension 4 [Dar24]

Goal: Compute a 2^e-isogeny $F : E_1^2 \times E_2^2 \longrightarrow E_1^2 \times E_2^2$, given $K' \subset (E_1^2 \times E_2^2)[2^{e+2}]$ such that $[4]K' = \ker(f)$ defined over $\mathbb{F}_{p^2}$.



- Gluings are more technical to handle than in dimension 2.
- We need to know K', $K = \ker(f)$ is not sufficient.

Implementation results in dimension 4 [Dar24]

Table: Timings in **SageMath** of a 2^e-isogeny chain computation and evaluation in dimension 4.

$\log_2(p)$	125	254	371
e	64	128	192
Computation	678 ms	1519 ms	2459 ms
Evaluation	25.9 ms	59.3 ms	107.7 ms

We expect an improvement by a factor 40 with a C implementation.

Thanks for listening!

P. Dartois, L. Maino, G. Pope, D. Robert. An Algorithmic Approach to (2, 2)-isogenies in the Theta Model and Applications to Isogeny-based Cryptography. Cryptology ePrint Archive, 2023. https://eprint.iacr.org/2023/1747

P. Dartois. Fast computation of 2-isogenies in dimension 4 and cryptographic applications. Cryptology ePrint Archive, 2024. https://eprint.iacr.org/2024/1180