Fast computation of higher dimensional 2^e-isogenies with theta coordinates

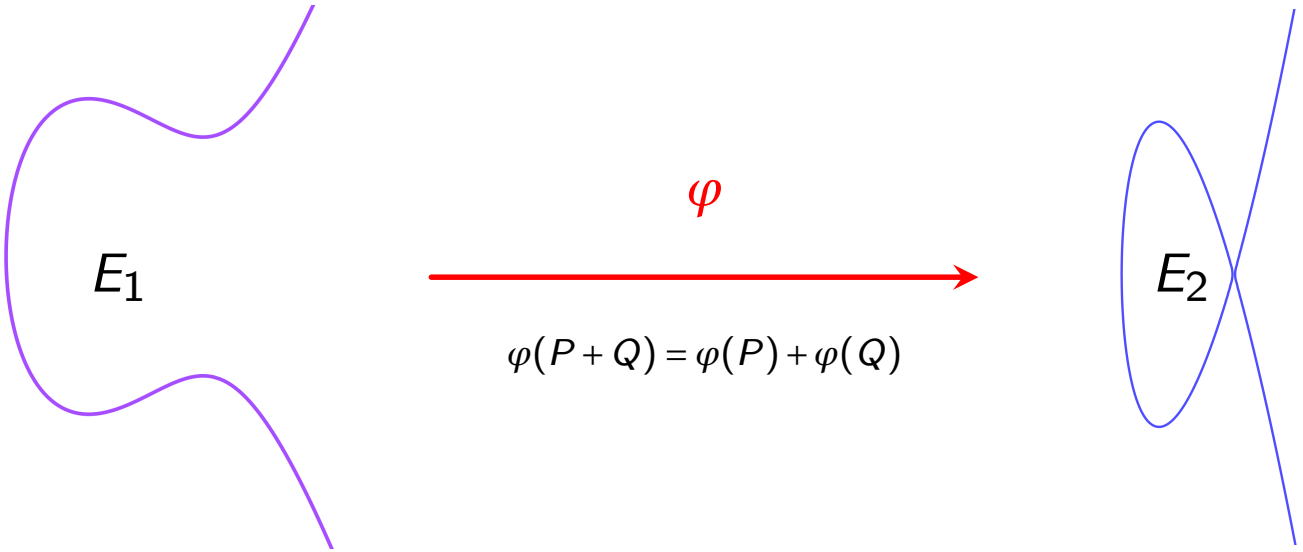
Pierrick Dartois

Joint work with Luciano Maino, Giacomo Pope and Damien Robert

May 16 2025

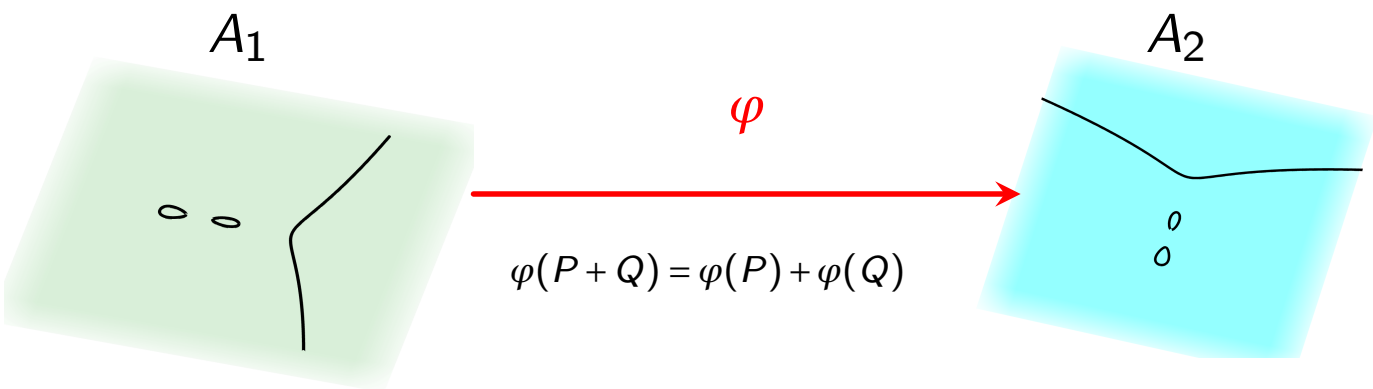
Isogenies between elliptic curves

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.

The algebraic theory of theta functions

Line bundles

Notations:

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

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

Polarisations

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

Projective coordinates on polarised abelian varieties

- We are looking for systems of coordinates on $(A, \mathscr{L})$.
- Assume that $\mathscr{L}$ is **generated by global sections** $s_0, \cdots, s_n \in \Gamma(A, \mathscr{L})$ *i.e.* that $s_{0,x}, \cdots, s_{n,x}$ generate $\mathscr{L}_x$ for all $x \in A$.

Projective coordinates on polarised abelian varieties

- We are looking for systems of coordinates on $(A, \mathscr{L})$.
- Assume that $\mathscr{L}$ is **generated by global sections** $s_0, \cdots, s_n \in \Gamma(A, \mathscr{L})$ *i.e.* that $s_{0,x}, \cdots, s_{n,x}$ generate $\mathscr{L}_x$ for all $x \in A$.
- **Idea:** Take such global sections $s_0, \cdots, s_n \in \Gamma(A, \mathscr{L})$. They define a map:

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

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

Projective coordinates on polarised abelian varieties

- We are looking for systems of coordinates on $(A, \mathscr{L})$.
- Assume that $\mathscr{L}$ is **generated by global sections** $s_0, \cdots, s_n \in \Gamma(A, \mathscr{L})$ *i.e.* that $s_{0,x}, \cdots, s_{n,x}$ generate $\mathscr{L}_x$ for all $x \in A$.
- **Idea:** Take such global sections $s_0, \cdots, s_n \in \Gamma(A, \mathscr{L})$. They define a map:

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

- These sections are coordinates when the above map is an embedding.
- Theta functions form a family of global sections of $\Gamma(A, \mathscr{L})$ with "good arithmetic properties".

The theta group

- Let $\mathscr{L}$ be a line bundle on A generated by global sections.

The theta group

- Let $\mathscr{L}$ be a line bundle on A generated by global sections.
- We define:
$$K(\mathscr{L}) := \{x \in A \mid t_x^* \mathscr{L} \simeq \mathscr{L}\}.$$
- Assume that $K(\mathscr{L})$ is finite so that $\varphi_{\mathscr{L}} : A \longrightarrow \widehat{A}$ is a polarisation.

The theta group

- Let $\mathscr{L}$ be a line bundle on A generated by global sections.
- We define:
$$K(\mathscr{L}) := \{x \in A \mid t_x^* \mathscr{L} \simeq \mathscr{L}\}.$$
- Assume that $K(\mathscr{L})$ is finite so that $\varphi_{\mathscr{L}} : A \longrightarrow \widehat{A}$ is a polarisation.
- The **theta group** of $\mathscr{L}$ is given by:
$$G(\mathscr{L}) := \{(x, \phi_x) \mid x \in K(\mathscr{L}),\ \phi_x : \mathscr{L} \xrightarrow{\sim} t_x^* \mathscr{L}\}.$$

The theta group

- Let $\mathscr{L}$ be a line bundle on A generated by global sections.
- We define:
$$K(\mathscr{L}) := \{x \in A \mid t_x^* \mathscr{L} \simeq \mathscr{L}\}.$$
- Assume that $K(\mathscr{L})$ is finite so that $\varphi_{\mathscr{L}} : A \longrightarrow \widehat{A}$ is a polarisation.
- The **theta group** of $\mathscr{L}$ is given by:
$$G(\mathscr{L}) := \{(x, \phi_x) \mid x \in K(\mathscr{L}),\ \phi_x : \mathscr{L} \xrightarrow{\sim} t_x^* \mathscr{L}\}.$$
- Given $(x, \phi_x), (y, \phi_y) \in G(\mathscr{L})$, the composition:
$$\mathscr{L} \xrightarrow{\phi_x} t_x^* \mathscr{L} \xrightarrow{t_x^* \phi_y} t_x^* t_y^* \mathscr{L} = t_{x+y}^* \mathscr{L},$$
defines the product:
$$(x, \phi_x) \cdot (y, \phi_y) = (x + y, t_x^* \phi_y \circ \phi_x).$$
- This defines a (non-commutative) group law on $G(\mathscr{L})$.

The commutator pairing

- There is an exact sequence:

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

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

The commutator pairing

- There is an exact sequence:

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

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

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

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

Action of the Theta group

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

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

Theorem (Mumford, 1966)

This action defines an irreducible representation of $G(\mathscr{L})$:

$$G(\mathscr{L}) \hookrightarrow GL(\Gamma(A, \mathscr{L})).$$

All irreducible representations of $G(\mathscr{L})$ on which k^* acts naturally are isomorphic.

Symplectic decompositions

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

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

  where $K_1(\mathscr{L})$ and $K_2(\mathscr{L})$ are maximal isotropic subgroups.
- $e_{\mathscr{L}}$ induces an isomorphism $K_2(\mathscr{L}) \cong \widehat{K_1(\mathscr{L})} = \mathrm{Hom}(K_1(\mathscr{L}), k^*)$.

Symplectic decompositions

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

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

  where $K_1(\mathscr{L})$ and $K_2(\mathscr{L})$ are maximal isotropic subgroups.
- $e_{\mathscr{L}}$ induces an isomorphism $K_2(\mathscr{L}) \cong \widehat{K_1(\mathscr{L})} = \mathrm{Hom}(K_1(\mathscr{L}), k^*)$.
- There exists a unique tuple of integers $\delta = (d_1, \cdots, d_g)$ such that:
  - $d_1 | \cdots | d_g$ and $g = \dim(A)$;
  - $K_1(\mathscr{L}) \simeq K_1(\delta)$ and $K_2(\mathscr{L}) \simeq K_2(\delta)$.

  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 $\mathscr{L}$ has **type** δ.

The Heisenberg group

- Let $K(\delta) := K_1(\delta) \times K_2(\delta)$.
- We define the **Heisenberg group** as $\mathscr{H}(\delta) := k^* \times K(\delta)$, with the group law:

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

The Heisenberg group

- Let $K(\delta) := K_1(\delta) \times K_2(\delta)$.
- We define the **Heisenberg group** as $\mathscr{H}(\delta) := k^* \times K(\delta)$, with the group law:

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

- Similarly, we define a commutator pairing $e_\delta : K(\delta) \times K(\delta) \longrightarrow k^*$.

The Heisenberg group

- Let $K(\delta) := K_1(\delta) \times K_2(\delta)$.
- We define the **Heisenberg group** as $\mathscr{H}(\delta) := k^* \times K(\delta)$, with the group law:

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

- Similarly, we define a commutator pairing $e_\delta : K(\delta) \times K(\delta) \longrightarrow k^*$.
- There always exists a **symplectic isomorphism** $\phi : K(\delta) \xrightarrow{\sim} K(\mathscr{L})$:

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

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

Theta structures

- The Heisenberg group is isomorphic to the theta group.
- A **Theta structure** is an isomorphism $\Theta_{\mathscr{L}} : \mathscr{H}(\delta) \xrightarrow{\sim} G(\mathscr{L})$ inducing an isomorphism of exact sequences:

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

  In particular, $\overline{\Theta}_{\mathscr{L}} : K(\delta) \xrightarrow{\sim} K(\mathscr{L})$ is a symplectic isomorphism.
- **Slogan:** "A theta structure is a symplectic isomorphism with lifting information."

Action of the Heisenberg group

- Let $V(\delta)$ be the space of functions $K_1(\delta) \longrightarrow k$.
- $\mathscr{H}(\delta)$ 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 $(\alpha, x, \chi) \in \mathscr{H}(\delta)$.

Action of the Heisenberg group

- Let $V(\delta)$ be the space of functions $K_1(\delta) \longrightarrow k$.
- $\mathscr{H}(\delta)$ 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 $(\alpha, x, \chi) \in \mathscr{H}(\delta)$.
- This defines an irreducible representation $\mathscr{H}(\delta) \hookrightarrow GL(V(\delta))$.

Action of the Theta group

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

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

Theorem (Mumford, 1966)

This action defines an irreducible representation of $G(\mathscr{L})$:

$$G(\mathscr{L}) \longrightarrow GL(\Gamma(A, \mathscr{L})).$$

All irreducible representations of $G(\mathscr{L})$ on which k^* acts naturally are isomorphic.

Action of the Theta group

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

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

Theorem (Mumford, 1966)

This action defines an irreducible representation of $G(\mathscr{L})$:

$$G(\mathscr{L}) \longrightarrow GL(\Gamma(A,\mathscr{L})).$$

All irreducible representations of $G(\mathscr{L})$ on which k^* acts naturally are isomorphic.

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

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

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

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

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

Theta structures of level n

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

Theta structures of level n

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

Theorem (Mumford, 1974)

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

Theorem (Birkenhake, Lange, 2004)

*When $n = 2$ and $(A, \varphi_{\mathscr{L}})$ is not a product, the map $K_A \longrightarrow \mathbb{P}_k^{2^g}$ induced by theta functions $(\theta_i^{\mathscr{L}})_{i \in (\mathbb{Z}/2\mathbb{Z})^g}$ is an embedding, where $K_A := A/\pm$ is the **Kummer variety** associated to A.*

Theta structures of level n

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

Theorem (Mumford, 1974)

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

Theorem (Birkenhake, Lange, 2004)

*When $n = 2$ and $(A, \varphi_{\mathscr{L}})$ is not a product, the map $K_A \longrightarrow \mathbb{P}_k^{2^g}$ induced by theta functions $(\theta_i^{\mathscr{L}})_{i \in (\mathbb{Z}/2\mathbb{Z})^g}$ 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).

The theta null point

- The **theta null point** $(\theta_i(0_A))_i$ is of special interest.

Theorem (Mumford, 1966)

*When $4|\delta$, the theta null point $(\theta_i(0_A))_i$ entirely determines $(A, \mathscr{L}, \Theta_{\mathscr{L}})$, as it determines the **Riemann relations** relating theta coordinates in the projective space.*

The theta null point

- The **theta null point** $(\theta_i(0_A))_i$ is of special interest.

Theorem (Mumford, 1966)

*When $4|\delta$, the theta null point $(\theta_i(0_A))_i$ entirely determines $(A, \mathscr{L}, \Theta_{\mathscr{L}})$, as it determines the **Riemann relations** relating theta coordinates in the projective space.*

- In practice, even at level 2 ($\delta = (2, \cdots, 2)$), we use $(\theta_i(0_A))_i$ to represent the Kummer variety.

The theta null point

- The **theta null point** $(\theta_i(0_A))_i$ is of special interest.

Theorem (Mumford, 1966)

*When $4|\delta$, the theta null point $(\theta_i(0_A))_i$ entirely determines $(A, \mathscr{L}, \Theta_{\mathscr{L}})$, as it determines the **Riemann relations** relating theta coordinates in the projective space.*

- In practice, even at level 2 ($\delta = (2, \cdots, 2)$), we use $(\theta_i(0_A))_i$ to represent the Kummer variety.
- Unlike in most algebraic geometry studies, we do not look at abelian varieties as Jacobians or by their equations. We use their theta null point to do arithmetic.

Change of level formulas and isogeny computations

The isogeny theorem

Definition

A **polarised isogeny** $f : (A, \mathscr{L}) \longrightarrow (B, \mathscr{M})$ satisfies $f^*\mathscr{M} \simeq \mathscr{L}$. If f is such an isogeny, then we have:

- $\widehat{f} \circ \varphi_{\mathscr{M}} \circ f = \varphi_{\mathscr{L}}$.
- $K := \ker(f) \subset K(\mathscr{L})$ is an isotropic subgroup.

The isogeny theorem

Definition

A **polarised isogeny** $f : (A, \mathscr{L}) \longrightarrow (B, \mathscr{M})$ satisfies $f^*\mathscr{M} \simeq \mathscr{L}$. If f is such an isogeny, then we have:

- $\widehat{f} \circ \varphi_{\mathscr{M}} \circ f = \varphi_{\mathscr{L}}$.
- $K := \ker(f) \subset K(\mathscr{L})$ is an isotropic subgroup.

Theorem (Mumford, 1966 and Robert, 2010)

*Let $f : (A, \mathscr{L}) \longrightarrow (B, \mathscr{M})$ be a polarised isogeny and $\Theta_{\mathscr{L}}$ and $\Theta_{\mathscr{M}}$ be **compatible** theta-structures on $G(\mathscr{L})$ and $G(\mathscr{M})$.*
Then, there exists $\lambda \in k^*$ such that for all $i \in K_1(\delta_{\mathscr{M}})$,

$$f^*\theta_i^{\mathscr{M}} = \lambda \sum_{j \in \Sigma(\overline{\Theta}_{\mathscr{L}}, \overline{\Theta}_{\mathscr{M}})} \theta_j^{\mathscr{L}},$$

with $\Sigma(\overline{\Theta}_{\mathscr{L}}, \overline{\Theta}_{\mathscr{M}}) \subseteq K_1(\delta_{\mathscr{L}})$.

Our goal

- Let $(A, \mathscr{L}_0)$ and $(B, \mathscr{M}_0)$ be a principally polarised abelian varieties (PPAVs).
- A d-**isogeny** is a polarised isogeny $f : (A, \mathscr{L}_0^d) \longrightarrow (B, \mathscr{M}_0)$ *i.e.* such that $f^* \mathscr{M}_0 \simeq \mathscr{L}_0^d$.
- Then, we have:
$$\widehat{f} \circ \varphi_{\mathscr{M}_0} \circ f = \varphi_{\mathscr{L}_0^d} = [d] \varphi_{\mathscr{L}_0}$$
- And $K = \ker(f) \subseteq K(\mathscr{L}_0^d) = A[d]$.

Our goal

- Let $(A, \mathscr{L}_0)$ and $(B, \mathscr{M}_0)$ be a principally polarised abelian varieties (PPAVs).
- A d-**isogeny** is a polarised isogeny $f : (A, \mathscr{L}_0^d) \longrightarrow (B, \mathscr{M}_0)$ *i.e.* such that $f^* \mathscr{M}_0 \simeq \mathscr{L}_0^d$.
- Then, we have:
$$\widehat{f} \circ \varphi_{\mathscr{M}_0} \circ f = \varphi_{\mathscr{L}_0^d} = [d] \varphi_{\mathscr{L}_0}$$
- And $K = \ker(f) \subseteq K(\mathscr{L}_0^d) = A[d]$.

State of the art [LR12; LR15; LR22]: When n and d are coprime, given $K \subset A[d]$, compute f in level n theta coordinates:

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

Our goal

- Let $(A, \mathscr{L}_0)$ and $(B, \mathscr{M}_0)$ be a principally polarised abelian varieties (PPAVs).
- A d-**isogeny** is a polarised isogeny $f : (A, \mathscr{L}_0^d) \longrightarrow (B, \mathscr{M}_0)$ *i.e.* such that $f^* \mathscr{M}_0 \simeq \mathscr{L}_0^d$.
- Then, we have:
$$\widehat{f} \circ \varphi_{\mathscr{M}_0} \circ f = \varphi_{\mathscr{L}_0^d} = [d] \varphi_{\mathscr{L}_0}$$
- And $K = \ker(f) \subseteq K(\mathscr{L}_0^d) = A[d]$.

State of the art [LR12; LR15; LR22]: When n and d are coprime, given $K \subset A[d]$, compute f in level n theta coordinates:

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

Our goal: Treat the case $n = 2$ and $d = 2^e$ (cryptographically relevant).

Applying the isogeny theorem

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

Applying the isogeny theorem

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

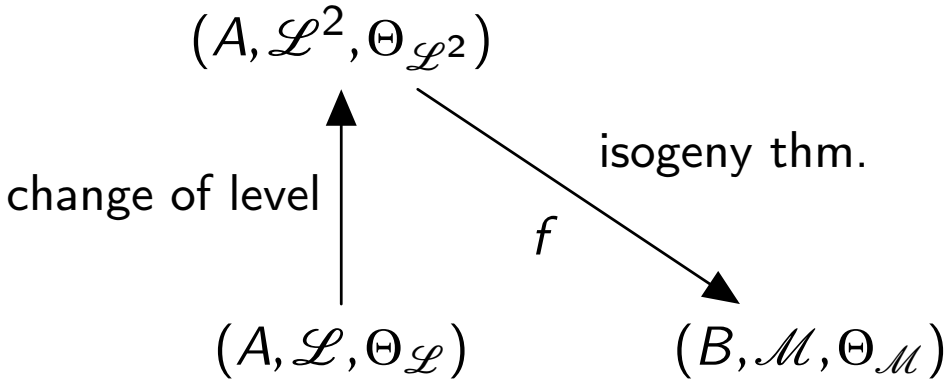
Corollary (of the isogeny theorem)

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

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

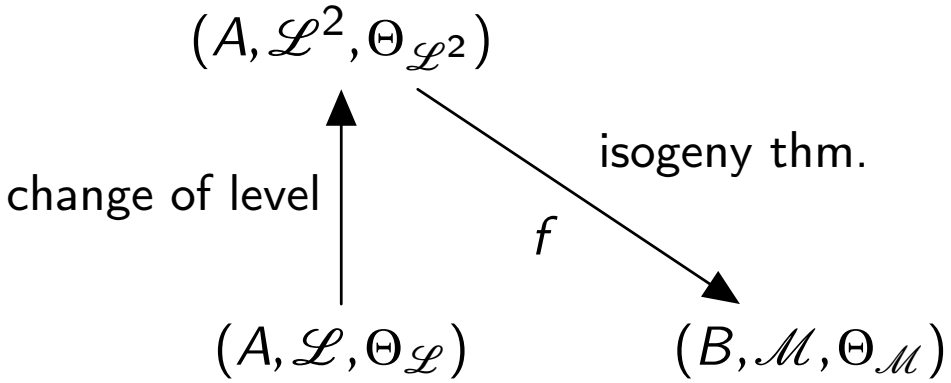
Problem: We know $(\theta_i^{\mathscr{L}}(x))_i$ but not $(\theta_{2i}^{\mathscr{L}^2}(x))_i$.

Change of level



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

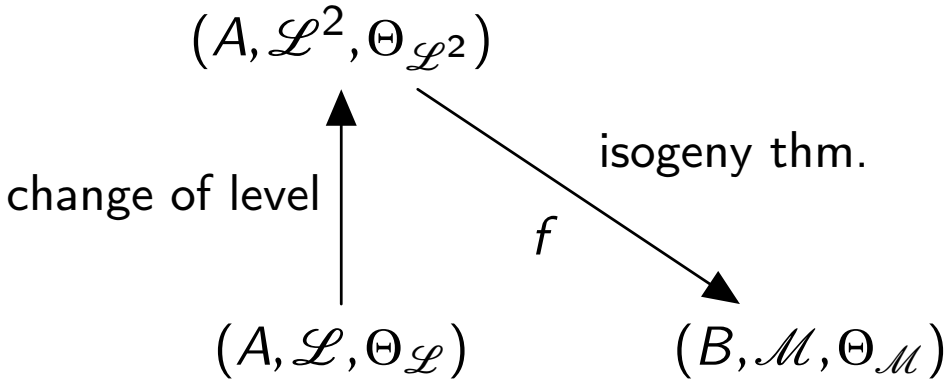
Change of level



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

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

Change of level



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

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

Symmetric theta structures

Definition

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

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

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

Compatible symmetric theta structures

Two symmetric theta structures $\Theta_{\mathscr{L}}$ of $G(\mathscr{L})$ and $\Theta_{\mathscr{L}^2}$ of $G(\mathscr{L}^2)$ are **compatible** if the following diagrams commute:

$$\begin{array}{ccc} \mathscr{H}(2\delta) & \xrightarrow{\Theta_{\mathscr{L}^2}} & G(\mathscr{L}^2) \\ \uparrow{\scriptstyle E_2} & & \uparrow{\scriptstyle \varepsilon_2} \\ \mathscr{H}(\delta) & \xrightarrow{\Theta_{\mathscr{L}}} & G(\mathscr{L}) \end{array} \qquad \begin{array}{ccc} \mathscr{H}(2\delta) & \xrightarrow{\Theta_{\mathscr{L}^2}} & G(\mathscr{L}^2) \\ \downarrow{\scriptstyle H_2} & & \downarrow{\scriptstyle \eta_2} \\ \mathscr{H}(\delta) & \xrightarrow{\Theta_{\mathscr{L}}} & G(\mathscr{L}) \end{array}$$

Differential addition and duplication formulas

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

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

Theorem (Mumford, 1966 and Robert, 2010)

Assume $\Theta_{\mathscr{L}}$ and $\Theta_{\mathscr{L}^2}$ 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 $i \equiv j \bmod 2$ and $\chi \in \widehat{(\mathbb{Z}/2\mathbb{Z})^g}$, we have:

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

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

Differential addition and duplication formulas

These formulas yield:

- A change of level algorithm to evaluate f:

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

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

⚠ We need 8-torsion points above the kernel.

- In dimensions 2 and 3, these can be avoided at the expense of square root computations.

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.*

Why we need change of coordinate formulas

Corollary (of the isogeny theorem)

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

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

Why we need change of coordinate formulas

Corollary (of the isogeny theorem)

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

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

Issue: The domain theta structure $\Theta_{\mathscr{L}}$ we are given may not satisfy $K = K_2(\overline{\Theta}_{\mathscr{L}})$.

Why we need change of coordinate formulas

Corollary (of the isogeny theorem)

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

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

Issue: The domain theta structure $\Theta_{\mathscr{L}}$ we are given may not satisfy $K = K_2(\overline{\Theta}_{\mathscr{L}})$.

Solution: Change the theta structure and compute the associated change of theta coordinates.

Sym. theta structures and symplectic basis (Mumford, 1966)

$$\{ \text{ Symmetric theta structures } \Theta_{\mathscr{L}^2} \text{ on } G(\mathscr{L}^2) \}$$

$$\downarrow$$

$$\left\{ \text{ Symplectic isomorphisms } \overline{\Theta}_{\mathscr{L}^2} : K(2\delta) \longrightarrow K(\mathscr{L}^2) \right\}$$

$$\downarrow\uparrow$$

$$\{ \text{ Symplectic basis of } K(\mathscr{L}^2) \}$$

$$\downarrow$$

$$\{ \text{ Symmetric theta structures } \Theta_{\mathscr{L}} \text{ on } G(\mathscr{L}) \}$$

Symplectic basis

- Assume $\mathscr{L}$ is of level n (*e.g.* $\mathscr{L} = \mathscr{L}_0^n$).
- What is a symplectic basis of $K(\mathscr{L}^2) = A[2n]$?

Symplectic basis

- Assume $\mathscr{L}$ is of level n (*e.g.* $\mathscr{L} = \mathscr{L}_0^n$).
- What is a symplectic basis of $K(\mathscr{L}^2) = A[2n]$?

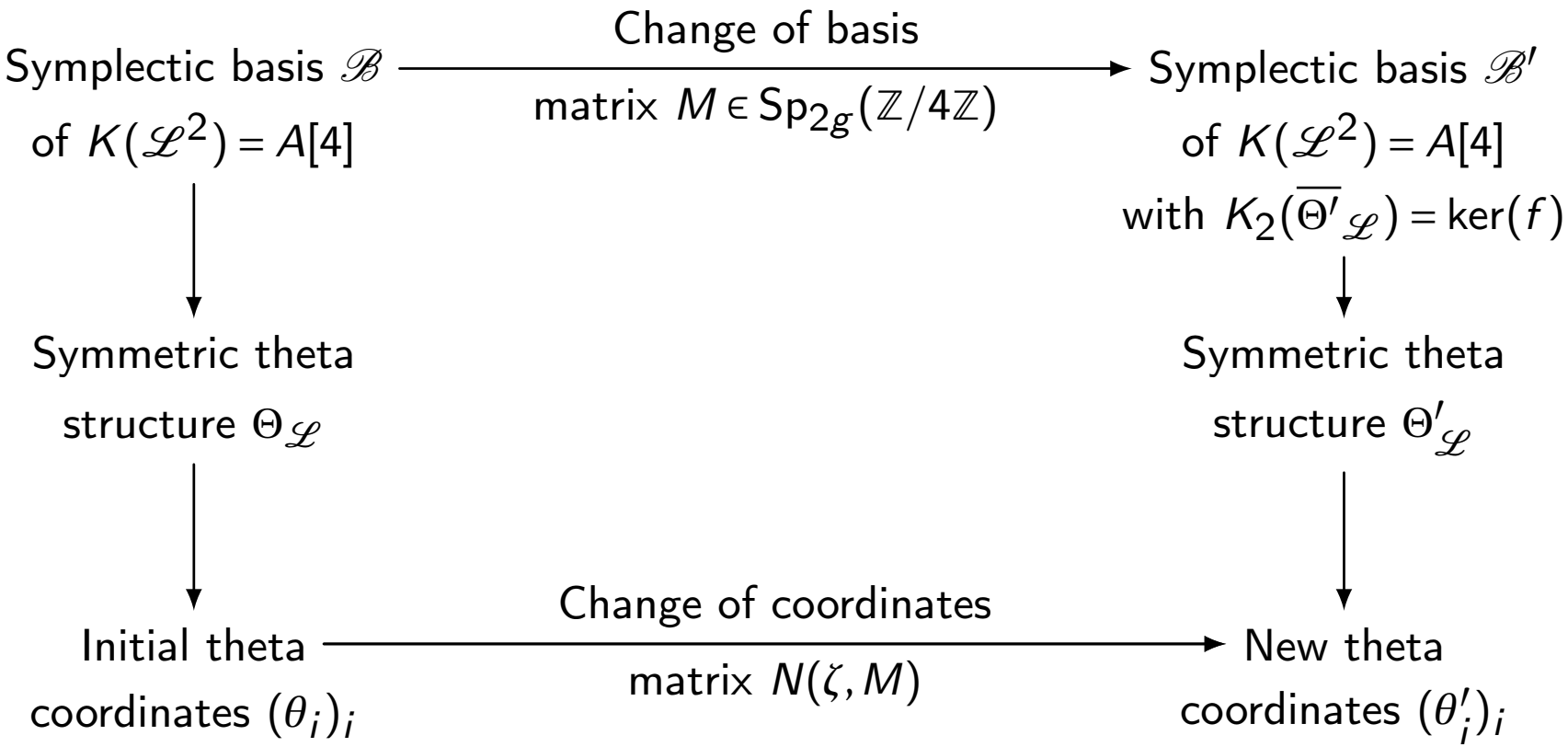
Definition

Let $\zeta \in k^*$ be a primitive $2n$-th root of unity.
A ζ-**symplectic** basis of $K(\mathscr{L}^2) = A[2n]$ is a basis $(x_1, \cdots, x_g, y_1, \cdots, y_g)$ such that:

- $\forall 1 \leq i,j \leq g, \quad e_{\mathscr{L}^2}(x_i, x_j) = e_{\mathscr{L}^2}(y_i, y_j) = 1;$
- $\forall 1 \leq i,j \leq g, \quad e_{\mathscr{L}^2}(x_i, y_j) = \zeta^{\delta_{i,j}}.$

Then $K_1(\mathscr{L}^2) := \langle x_1, \cdots, x_g \rangle$ and $K_2(\mathscr{L}^2) := \langle y_1, \cdots, y_g \rangle$ form a symplectic decomposition of $K(\mathscr{L}^2)$.

Change of coordinate formulas (D., 2024)



Computing chains of 2-isogenies

Computing a 2^e-isogeny

Input: Points $T_1, \cdots, T_g$ forming a maximal isotropic subgroup of $A[2^{e+2}]$.

Output: A 2^e-isogeny $f : (A, \mathscr{L}^{2^e}) \longrightarrow (B, \mathscr{M})$ with kernel $\langle [4]T_1, \cdots, [4]T_g \rangle$.

Computing a 2^e-isogeny

Input: Points $T_1, \cdots, T_g$ forming a maximal isotropic subgroup of $A[2^{e+2}]$.

Output: A 2^e-isogeny $f : (A, \mathscr{L}^{2^e}) \longrightarrow (B, \mathscr{M})$ with kernel $\langle [4]T_1, \cdots, [4]T_g \rangle$.

- We divide the computation into a chain of 2-isogenies:

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

Computing a 2^e-isogeny

Input: Points $T_1, \cdots, T_g$ forming a maximal isotropic subgroup of $A[2^{e+2}]$.

Output: A 2^e-isogeny $f : (A, \mathscr{L}^{2^e}) \longrightarrow (B, \mathscr{M})$ with kernel $\langle [4]T_1, \cdots, [4]T_g \rangle$.

- We divide the computation into a chain of 2-isogenies:

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

- For all $i \in [\![1 \ ; \ e]\!]$, we compute the dual theta null point $(\widetilde{\theta}_j(0_{A_i}))_j$ of A_i to obtain $f_i : A_{i-1} \longrightarrow A_i$.
- $(\widetilde{\theta}_j(0_{A_i}))_j$ is obtained from

$$[2^{e-i}]f_{i-1} \circ \cdots \circ f_1(T_1), \cdots, [2^{e-i}]f_{i-1} \circ \cdots \circ f_1(T_g).$$

Computing a 2^e-isogeny

Input: Points $T_1, \cdots, T_g$ forming a maximal isotropic subgroup of $A[2^{e+2}]$.

Output: A 2^e-isogeny $f : (A, \mathscr{L}^{2^e}) \longrightarrow (B, \mathscr{M})$ with kernel $\langle [4]T_1, \cdots, [4]T_g \rangle$.

- This involves point duplications and evaluations. Their number can be optimised with divide and conquer strategies.

Computing a 2^e-isogeny

Input: Points $T_1, \cdots, T_g$ forming a maximal isotropic subgroup of $A[2^{e+2}]$.

Output: A 2^e-isogeny $f : (A, \mathscr{L}^{2^e}) \longrightarrow (B, \mathscr{M})$ with kernel $\langle [4]T_1, \cdots, [4]T_g \rangle$.

- This involves point duplications and evaluations. Their number can be optimised with divide and conquer strategies.
- If A is a product, $f_1 : A \longrightarrow A_1$ is a gluing isogeny (and the following can also be gluings). Formulas are different.

Computing a 2^e-isogeny

Input: Points $T_1, \cdots, T_g$ forming a maximal isotropic subgroup of $A[2^{e+2}]$.

Output: A 2^e-isogeny $f : (A, \mathscr{L}^{2^e}) \longrightarrow (B, \mathscr{M})$ with kernel $\langle [4]T_1, \cdots, [4]T_g \rangle$.

- This involves point duplications and evaluations. Their number can be optimised with divide and conquer strategies.
- If A is a product, $f_1 : A \longrightarrow A_1$ is a gluing isogeny (and the following can also be gluings). Formulas are different.
- The change of theta coordinates is only needed on A to compute f_1 (or further gluings).

Computing a 2^e-isogeny

Input: Points $T_1, \cdots, T_g$ forming a maximal isotropic subgroup of $A[2^{e+2}]$.

Output: A 2^e-isogeny $f : (A, \mathscr{L}^{2^e}) \longrightarrow (B, \mathscr{M})$ with kernel $\langle [4]T_1, \cdots, [4]T_g \rangle$.

- This involves point duplications and evaluations. Their number can be optimised with divide and conquer strategies.
- If A is a product, $f_1 : A \longrightarrow A_1$ is a gluing isogeny (and the following can also be gluings). Formulas are different.
- The change of theta coordinates is only needed on A to compute f_1 (or further gluings).
- A change of theta coordinates can be needed on B if it is a product.

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

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 50 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