Computing higher dimensional isogenies in the Theta model

Pierrick Dartois

Joint work with Damien Robert, Luciano Maino and Giacomo Pope

23 January 2024

CANARI

Why the Theta model?

d-isogenies and the dual isogeny in higher dimension

Definition (d-isogeny)

Let $\varphi : (A, \lambda_A) \longrightarrow (B, \lambda_B)$ be an isogeny between two principally polarized abelian varieties (PPAV). We define:

- $\widetilde{\varphi} := \lambda_A^{-1} \circ \widehat{\varphi} \circ \lambda_B : B \longrightarrow A$.

$$B \xrightarrow{\lambda_B} \widehat{B} \xrightarrow{\widehat{\varphi}} \widehat{A} \xrightarrow{\lambda_A^{-1}} A$$

- We say that φ is a <u>d-isogeny</u> if $\widetilde{\varphi} \circ \varphi = [d]_A$.

Kani's embedding lemma

Definition (isogeny diamond)

An (a, b)-isogeny diamond is a commutative diagram s.t.:

$$\begin{array}{ccc} A' & \xrightarrow{\varphi'} & B' \\ \uparrow{\scriptstyle \psi} & & \uparrow{\scriptstyle \psi'} \\ A & \xrightarrow{\varphi} & B \end{array}$$

where φ, φ' are a-isogenies and ψ, ψ' are b-isogenies.

Lemma (Kani)

Consider the (a, b)-isogeny diamond on the left. Then:

- $F : A \times B' \longrightarrow B \times A'$,

$$F := \begin{pmatrix} \varphi & \widetilde{\psi}' \\ -\psi & \widetilde{\varphi}' \end{pmatrix}$$

  is a d-isogeny with $d = a + b$.

- *If $a \wedge b = 1$, then*

$$\ker(F) = \{(\widetilde{\varphi}(x), \psi'(x)) \mid x \in B[d]\}.$$

Applications of Kani's lemma

Why Kani's lemma? It provides an algorithm to evaluate everywhere a non-smooth degree isogeny φ given its values on some torsion points.

Applications:

- Polynomial time attack against SIDH.
- New algorithms for the Deuring correspondence (in dimension 2 and 4).
- New primitives: signatures (SQIsignHD), encryption (FESTA), VRF...

The limits of state of the art techniques

State of the art:

- Fast algorithms in dimension 1 (for smooth degree isogenies).
- Isogenies in the Jacobian model suitable for dimension 2 and 3 (e.g. Richelot), but slow.
- ℓ-isogenies in the Theta model at level n coprime with ℓ (n^g coordinates in dimension g), not optimized.

Question: How fast can the Theta model be when $\ell = n = 2$? Suitable for constructive applications?

Introduction to Theta coordinates

Line bundles

Notations:

- k: algebraically closed field.
- A: abelian variety defined over k.

- 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 $\mathrm{Pic}(A)$.
- $\mathrm{Pic}(A) \cong \{$divisors on A modulo principal divisors$\}$.

Polarizations

- 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 **polarization** of A.
  - $(A, \mathcal{L})$ is a **polarized abelian variety**.

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** $\rho_{\mathcal{L}} : (x, \phi_x) \longmapsto x$.
- $G(\mathcal{L})$ 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.
- $K(\delta) := K_1(\delta) \oplus K_2(\delta)$ 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 $K_1(\delta) \longrightarrow k^*$].

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

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

  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* $K_i(\mathcal{L}) = \overline{\Theta}_{\mathcal{L}}(K_i(\delta)) \xrightarrow{\sim} \widetilde{K}_i(\mathcal{L}) \subset G(\mathcal{L})$.

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 $(\alpha, x, \chi) \in \mathcal{H}(\delta)$.

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 $G(\mathcal{L})$.

- 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.
- It defines a projective map:

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

Action of the Heisenberg group and Theta functions

- β "transfers" the Heisenberg group action to Theta functions.
- This way, we easily obtain formulas:

$$\Theta_{\mathcal{L}}(\alpha, j, \chi) \cdot \theta_i^{\mathcal{L}} = \beta((\alpha, j, \chi) \cdot \delta_i) = \alpha\chi(i+j)^{-1}\theta_{i+j}^{\mathcal{L}}.$$

- In particular, we can obtain the $\theta_i^{\mathcal{L}}$ from $\theta_0^{\mathcal{L}}$:

$$\forall i \in K_1(\delta), \quad \Theta_{\mathcal{L}}(1, i, 1) \cdot \theta_0^{\mathcal{L}} = \theta_i^{\mathcal{L}}.$$

- Besides, $K_2(\delta)$ stabilizes $\theta_0^{\mathcal{L}}$:

$$\forall \chi \in K_2(\delta), \quad \Theta_{\mathcal{L}}(1, 0, \chi) \cdot \theta_0^{\mathcal{L}} = \theta_0^{\mathcal{L}}.$$

Action of a maximal level subgroup

- Let $K \subseteq K(\mathcal{L})$.
- A **level subgroup** lying above K is a subgroup $\widetilde{K} \subset G(\mathcal{L})$ isomorphic to K via the forgetful map $(x, \phi_x) \longmapsto x$.
- K admits a level subgroup if and only if K is isotropic ($e_{\mathcal{L}}(x, y) = 1$ for all $x, y \in K$).

Proposition (Mumford, 1966)

Let $\widetilde{K} \subset G(\mathcal{L})$ be a maximal level subgroup. Then the subspace of $\Gamma(A, \mathcal{L})$ stabilized by the action of $\widetilde{K}$ has dimension 1 over k.

- In particular, $\theta_0^{\mathcal{L}}$ is the only function up to a constant to be stabilized by $\widetilde{K}_2(\mathcal{L})$.

Heisenberg group automorphisms and base change formulas

- **Heisenberg group automorphisms** are automorphisms of $\mathcal{H}(\delta)$ fixing k^*.
- They induce new theta structures $\Theta'_{\mathcal{L}} = \Theta_{\mathcal{L}} \circ \psi$.

Proposition (Robert, 2010)

Consider basis of theta functions $(\theta_i)_i$ and $(\theta'_i)_i$ associated to $\Theta_{\mathcal{L}}$ and $\Theta'_{\mathcal{L}} = \Theta_{\mathcal{L}} \circ \psi$ respectively.
Then, there exists $i_0 \in K_1(\delta)$ and $\lambda \in k^*$ such that:

$$\theta'_0 = \lambda \sum_{\chi \in K_2(\delta)} \Theta_{\mathcal{L}}(\delta) \circ \psi(1, 0, \chi) \cdot \theta_{i_0}.$$

The θ'_i are then given by $\theta'_i = \Theta_{\mathcal{L}} \circ \psi(1, i, 1) \cdot \theta'_0$.

Descent theory

- Consider an isogeny $f : (A, \mathcal{L}) \longrightarrow (B, \mathcal{M})$ $(f^*\mathcal{M} \cong \mathcal{L})$.
- Let $K := \ker(f)$. Then $K \subset K(\mathcal{L})$ is an isotropic subgroup.
- Given an isomorphism $\alpha : f^*\mathcal{M} \xrightarrow{\sim} \mathcal{L}$, define a level subgroup:

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

- Then, 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 triples $(f, \alpha, \mathcal{M})$ 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:

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

- Write $K = K_1 \oplus K_2$ with $K_i \subseteq K_i(\mathcal{L})$ 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 $K^{\perp,i} \subseteq K_i(\mathcal{L})$ 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 $i \in K_1(\delta_{\mathcal{M}})$,

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

Computing isogenies with Theta coordinates

Computing 2-isogenies in the Theta model

- Let $f : A \longrightarrow B$ is a 2-isogeny $\widetilde{f} \circ f = [2]$.
- Consider line bundles $\mathcal{L}$ and $\mathcal{M}$ on A and B of type $\underline{2} = (2, \cdots, 2)$.
- We say that $\mathcal{L}$ and $\mathcal{M}$ are of **level 2**.
- This minimizes the number of coordinates to 2^g.
- But the map:

$$\begin{array}{rcl} A(k) & \longrightarrow & \mathbb{P}^{2^g-1}(k) \\ x & \longmapsto & (\theta_i^{\mathcal{L}}(x))_{i \in K_1(\underline{2})} \end{array}$$

  is not an embedding. It defines an embedding of the **Kummer variety** $A/\pm$.

Goal: compute $(\theta_i^{\mathcal{M}}(f(x)))_i$ knowing $(\theta_i^{\mathcal{L}}(x))_i$.

Case $K = K_2(\underline{2})$

- **Idea:** Reduce to the case when there is only one element in the sum:

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

- Let $\mathcal{L}$ and $\mathcal{M}$ be line bundles of level 2 on A and B such that $f^*\mathcal{M} \cong \mathcal{L}^2$.
- Assume that $K = K_2(\mathcal{L})$.
- Then, we can choose $\Theta_{\mathcal{M}}$ so that for all $i \in K_1(\underline{2})$,

$$f^*\theta_i^{\mathcal{M}} = \theta_{2i}^{\mathcal{L}^2}.$$

[$\mathcal{L}^2$ is of level 4 (i.e. of type $\underline{4}$).]

- **Problem:** Obtain the $\theta_{2i}^{\mathcal{L}^2}$ from the $\theta_i^{\mathcal{L}}$.

Symmetric Theta structures

- Let $\mathcal{L}$ be a line bundle of type δ on A.
- $\mathcal{L}$ is **symmetric** if $[-1]^*\mathcal{L} \cong \mathcal{L}$.
- $\mathcal{L}$ is **totally symmetric** if there exists a line bundle $\mathcal{M}$ on A such that $\mathcal{L} \cong \mathcal{M}^2$.
- Consider the automorphism δ_{-1} of $G(\mathcal{L})$ fitting into:

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

- Let D_{-1} be its analogue in $\mathcal{H}(\delta)$.
- A theta-structure $\Theta_{\mathcal{L}}$ is **symmetric** if $\Theta_{\mathcal{L}} \circ D_{-1} = \delta_{-1} \circ \Theta_{\mathcal{L}}$.

Compatible symmetric Theta structures

- Let $\mathcal{L}$ be a totally symmetric line bundle on A.
- Let $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{L}^2}$ be symmetric theta-structures on $G(\mathcal{L})$ and $G(\mathcal{L}^2)$ respectively.
- Consider the maps $\varepsilon_2 : G(\mathcal{L}) \longrightarrow G(\mathcal{L}^2)$ and $\eta_2 : G(\mathcal{L}^2) \longrightarrow G(\mathcal{L})$:

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

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

Compatible symmetric Theta structures

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

Theorem (Mumford, 1966)

- *Every symmetric theta-structure $\Theta_{\mathcal{L}^2}$ on $G(\mathcal{L}^2)$ induces a unique symmetric theta-structure $\Theta_{\mathcal{L}}$ on $G(\mathcal{L})$ that is compatible with $\Theta_{\mathcal{L}^2}$.*
- *The resulting theta-structure $\Theta_{\mathcal{L}}$ on $G(\mathcal{L})$ only depends on the symplectic isomorphism $\overline{\Theta}_{\mathcal{L}^2} : K(2\delta) \xrightarrow{\sim} K(\mathcal{L}^2)$.*
- *Every symmetric theta-structure on $G(\mathcal{L})$ is induced by a symmetric theta-structure on $G(\mathcal{L}^2)$, or equivalently, by a symplectic isomorphism $K(2\delta) \xrightarrow{\sim} K(\mathcal{L}^2)$.*

Addition and duplication formulas

Let $\Theta_{\mathcal{L}}$ and $\Theta_{\mathcal{L}^2}$ be compatible symmetric theta structures on $G(\mathcal{L})$ and $G(\mathcal{L}^2)$.

Theorem (Robert, 2010)

For all $x, y \in A(k)$, and all $i, j \in K_1(\delta)$,

$$\theta_i^{\mathcal{L}}(x+y)\theta_j^{\mathcal{L}}(x-y) = \sum_{\begin{cases} u,v \in K_1(2\delta) \\ u+v=2i \\ u-v=2j \end{cases}} \theta_u^{\mathcal{L}^2}(x)\theta_v^{\mathcal{L}^2}(y)$$

Definition (Dual Theta coordinates)

For all $\chi \in K_2(\underline{2}) = (\widehat{\mathbb{Z}/2\mathbb{Z}})^g$ and $i \in K_1(2\delta)$, define:

$$U_{\chi,i}^{\mathcal{L}^2} := \sum_{t \in K_1(\underline{2})} \chi(t)\theta_{i+t\delta}^{\mathcal{L}^2}$$

Addition and duplication formulas (with dual coordinates)

Theorem (Robert, 2010)

Let $x, y \in A(k)$. Then there exists $\lambda_1, \lambda_2 \in k^*$ such that for all $i, j \in K_1(2\delta)$ such that $i \equiv j \mod \delta$, we have:

$$\theta^{\mathcal{L}}_{i+j}(x+y)\theta^{\mathcal{L}}_{i-j}(x-y) = \lambda_1 \sum_{\chi \in K_2(\underline{2})} U^{\mathcal{L}^2}_{\chi,i}(x)U^{\mathcal{L}^2}_{\chi,j}(y)$$

$$U^{\mathcal{L}^2}_{\chi,i}(x)U^{\mathcal{L}^2}_{\chi,j}(y) = \lambda_2 \sum_{t \in K_1(\underline{2})} \chi(t)\theta^{\mathcal{L}}_{i+j+t\delta/2}(x+y)\theta^{\mathcal{L}}_{i-j+t\delta/2}(x-y).$$

With these formulas, we can:

- Compute the $\theta^{\mathcal{L}}_{i+j}(x+y)$, knowing the $\theta^{\mathcal{L}}_i(x)$, $\theta^{\mathcal{L}}_i(y)$, $\theta^{\mathcal{L}}_i(x-y)$ and $\theta^{\mathcal{L}}_i(0)$ (**differential addition**).
- Compute the $\theta^{\mathcal{L}}_{i+j}(2x)$, knowing the $\theta^{\mathcal{L}}_i(x)$ and $\theta^{\mathcal{L}}_i(0)$ (**doubling**).
- Derive our isogeny formula...

Back to isogeny formulas (case $K = K_2(\underline{2})$)

Recall that:

- $f : (A, \mathcal{L}^2) \longrightarrow (B, \mathcal{M})$ is a 2-isogeny.
- $\mathcal{L}$ is of type $\delta = \underline{2} = (2, \cdots, 2)$.
- $K = K_2(\mathcal{L})$.
- For all $i \in K_1(\underline{2})$,
$$f^*\theta_i^{\mathcal{M}} = \theta_{2i}^{\mathcal{L}^2}.$$
- We want to express the $\theta_{2i}^{\mathcal{L}^2}$.
- The duplication formulas ensure that:
$$U_{\chi,0}^{\mathcal{L}^2}(x)U_{\chi,0}^{\mathcal{L}^2}(0_A) = \sum_{t \in K_1(\underline{2})} \chi(t)\theta_t^{\mathcal{L}}(x)^2.$$

Back to isogeny formulas (case $K = K_2(\underline{2})$)

Proposition (Robert, 2023)

We have:

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

where:

- *H is the **Hadamard** operator:* $(x_i)_i \longmapsto \left(\sum_{i \in K_1(\underline{2})} (-1)^{\langle i | j \rangle} x_i\right)_j$.
- *S is the **squaring** operator* $(x_i)_i \longmapsto (x_i^2)_i$.

Hence, to evaluate an isogeny, we first have to compute the dual of the codomain **theta null-point**:

$$H((\theta_i^{\mathcal{M}}(0_B))_i) = (U_{\chi,0}^{\mathcal{M}}(0_B))_\chi.$$

Evaluation algorithm (case $K = K_2(\underline{2})$)

Algorithm 1: Generic isogeny evaluation algorithm.

Data: A theta point $(\theta_i^{\mathcal{L}}(x))_i$ of A and the dual theta-null point $H((\theta_i^{\mathcal{M}}(0_B))_i)$ of B with non-vanishing coordinates.

Result: $(\theta_i^{\mathcal{L}}(f(x)))_i$.

1 Let $(D_j)_j := H((\theta_i^{\mathcal{M}}(0_B))_i)$ and precompute $C_j \longleftarrow 1/D_j$ for all $j \in K_1(\underline{2})$;

2 Compute $(Z_j)_j \longleftarrow H \circ S((\theta_i^{\mathcal{L}}(x))_i)$;

3 Compute $(Y_j)_j \longleftarrow (C_j \cdot Z_j)_j$;

4 Return $H((Y_j)_j)$;

Computing the codomain Theta null point ($K = K_2(\underline{2})$)

- Let $(T_1', \cdots, T_g')$ be a basis of $K_2(\mathcal{L}^2) \subset A[4]$.
- Let $T_i'' \in A[8]$ such that $[2]T_i'' = T_i'$ for all $i \in [\![1\ ;\ g]\!]$.
- For all $i \in [\![1\ ;\ g]\!]$, let $\chi_i : j \in K_1(\underline{2}) \longmapsto (-1)^{j_i}$.

Proposition

For all $i \in [\![1\ ;\ g]\!]$ and $\chi \in K_2(\underline{2})$,

$$U^{\mathcal{M}}_{\chi\chi_i,0}(0_B) \cdot H \circ S((\theta_j^{\mathcal{M}}(T_i''))_j)_\chi = U^{\mathcal{M}}_{\chi,0}(0_B) \cdot H \circ S((\theta_j^{\mathcal{M}}(T_i''))_j)_{\chi\chi_i}.$$

Example for $g = 2$

- Let (T_1', T_2') be a basis of $K_2(\mathcal{L}^2) \subset A[4]$.
- Let $T_i'' \in A[8]$ such that $[2]T_i'' = T_i'$ for all $i \in \{1, 2\}$.
- Let $(\alpha : \beta : \gamma : \delta)$ be the dual theta null point.
- Then, we have:

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

$$H \circ S(\theta_{00}(T_2''), \theta_{10}(T_2''), \theta_{01}(T_2''), \theta_{11}(T_2'')) = (z\alpha, t\beta, z\gamma, t\delta)$$

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

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

- What happens when $\alpha \cdot \beta \cdot \gamma \cdot \delta = 0$?
- We can still find $(\alpha : \beta : \gamma : \delta)$ but not evaluate f as easily.

Gluing isogenies

- Isogenies $A_1 \times A_2 \longrightarrow B$.
- **Example:** elliptic products.
- The dual theta constants $U^{\mathcal{M}}_{\chi,0}(0_B)$ can vanish.
- The previous evaluation algorithm requiring $1/U^{\mathcal{M}}_{\chi,0}(0_B)$ does not apply.
- This is not surprising since we work on Kummer varieties. We have to lift sign ambiguities:

$$(A_1/\pm) \times (A_2/\pm) \longrightarrow B/\pm$$

Fixing the evaluation algorithm

- In most cases, it suffices to to compute $H \circ S((\theta_i^{\mathcal{L}}(x))_i)$ to compute $(\theta_i^{\mathcal{M}}(f(x)))_i$.
- When some dual theta-constants vanish, we need additional data:

$$H \circ S((\theta_i^{\mathcal{L}}(x + T'))_i),$$

  for some $T' \in K_2(\mathcal{L}^2)$ of order 4.
- In dimension $g = 2$, translating by $T' := T_1'$ is sufficient.
- In dimension $g = 4$, we use 10 translates $T' = T_i'$ and $T' := T_i' + T_j'$ $(1 \leq i < j \leq 4)$ (could be optimized).

Computing the Theta null point

Goal: Compute the codomain dual theta null point $U^{\mathcal{M}}_{\chi,0}(0_B)$ of a gluing isogeny.

- In dimension $g=2$, the $H\circ S((\theta_i^{\mathcal{L}}(T_i''))_i)$ suffice.
- In dimension $g=4$, we also need translates $H\circ S((\theta_i^{\mathcal{L}}(T_i''+T_j'))_i)$.

Why base change formulas?

- Our formulas work when $K = K_2(\mathcal{L})$.
- When $K \neq K_2(\mathcal{L})$, we have to compute a base change of Theta coordinates.
- A **symplectic basis** $(S'_1, \cdots, S'_g, T'_1, \cdots, T'_g)$ of $A[4] = K(\mathcal{L}^2)$ satisfies:

$$e_{\mathcal{L}}(S'_i, S'_j) = e_{\mathcal{L}}(T'_i, T'_j) = 1 \quad \text{and} \quad e_{\mathcal{L}}(S'_i, T'_j) = \zeta_4,$$

  with $\zeta_4^2 = -1$.
- Such a defines a symplectic isomorphism $\overline{\Theta}_{\mathcal{L}} : K(\underline{4}) \xrightarrow{\sim} K(\mathcal{L}^2)$, so it suffices to define a symmetric Theta structure $\Theta_{\mathcal{L}}$.
- We then have:

$$K_2(\mathcal{L}^2) = \overline{\Theta}_{\mathcal{L}}(K_2(\underline{4})) = \langle T'_1, \cdots, T'_g \rangle$$

- We may change of basis so that $[2]K_2(\mathcal{L}^2) = K$.

Explicit base change formulas

- A symplectic base change of $A[4]=K(\mathcal{L}^2)$ is given by a matrix:

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

- Let $(\theta_i^{\mathcal{L}})_i$ and $(\theta_i'^{\mathcal{L}})_i$ be respectively theta functions determined by basis $\mathcal{B}$ and $\mathcal{B}' := M^T\mathcal{B}$ of $A[4]$.

Theorem (D., 2023)

There exists $i_0 \in K_1(\underline{2})$ such that for all $i \in K_1(\underline{2})$:

$$\theta_i'^{\mathcal{L}} = \lambda \sum_{j\in K_1(\underline{2})} \zeta_4^{\langle i|j\rangle - \langle Ai+Cj+2i_0|Bi+Dj\rangle} \theta^{\mathcal{L}}_{Ai+Cj+i_0}.$$

Implementation results and future works

In dimension 2

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

Implementation results: $\log(p) = 254$, $n = 126$.

	Theta Rust	Theta SageMath	Richelot SageMath
Codomains	**2.85 ms**	108 ms	1028 ms
Evaluation	**161 μs**	5.43 ms	114 ms

In dimension 4

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

Implementation results: In SageMath, with $\log(p) = 256$, $n = 142$ (SQIsignHD verification).

- Codomains: **770 ms**.
- Image: **12 ms**.

Conclusion and future works

Conclusion:

- General theory to compute 2-isogenies in level 2.
- Implementation in dimension 2. Read our paper here: `https://eprint.iacr.org/2023/1747`
- Proof of concept in dimension 4 for SQIsignHD verification. Read our paper here: `https://eprint.iacr.org/2023/436`

Future works:

- Provide a robust and optimized implementation of dimension 4.
- Provide a low level implementation of dimension 4.
- Integrate dimension 2 (and 4) into SageMath, Pari GP...

Thank you for listening!