What you need to know about higher dimensional isogenies

Pierrick Dartois

2025, September 12

1. A simplified theory of theta structures
2. Computing 2-isogeny chains in any dimension
3. The 2-dimensional case
4. Tutorial: how to break SIDH in 4D

A simplified theory of theta structures

Definition: symplectic isomorphism

- Let A/k be a PPAV of dimension g.
- If $n \nmid \mathrm{char}(k)$, then $A[n] \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$.
- A *symplectic isomorphism* $\varphi : (\mathbb{Z}/n\mathbb{Z})^g \times \widehat{(\mathbb{Z}/n\mathbb{Z})^g} \xrightarrow{\sim} A[n]$ is a group isomorphism satisfying:

$$\forall x, y \in (\mathbb{Z}/n\mathbb{Z})^g \times \widehat{(\mathbb{Z}/n\mathbb{Z})^g}, \quad e_n(\varphi(x), \varphi(y)) = e_n(x, y),$$

where the first pairing is the Weil-pairing and the second one is given by:

$$\forall (i, \chi), (i', \chi') \in (\mathbb{Z}/n\mathbb{Z})^g \times \widehat{(\mathbb{Z}/n\mathbb{Z})^g}, \quad e_n((i, \chi), (i', \chi')) = \chi'(i)\chi(i')^{-1}.$$

- Such a symplectic isomorphism is determined by a (ζ-)*symplectic basis* $(S_1, \cdots, S_g, T_1, \cdots, T_g)$ of $A[n]$ *i.e.* a basis such that:

$$\forall 1 \leq i, j \leq g, \quad e_n(S_i, S_j) = e_n(T_i, T_j) = 1 \quad \text{and} \quad e_n(S_i, T_j) = \zeta^{\delta_{i,j}},$$

where ζ is a primitive n-th root of unity.

Definition: theta structure

Definition (Mumford, Duparc)

Let A be a PPAV of dimension g. A *(symmetric) theta structure* of level n is a map

$$\begin{array}{rcl} \Theta(n): A & \longrightarrow & \mathbb{P}^{n^g-1} \\ x & \longmapsto & (\theta_i(x))_{i\in(\mathbb{Z}/n\mathbb{Z})^g} \end{array}$$

along with a symplectic isomorphism:

$$\overline{\Theta}(n):(\mathbb{Z}/n\mathbb{Z})^g\times\widehat{(\mathbb{Z}/n\mathbb{Z})^g}\overset{\sim}{\longrightarrow}A[n]$$

satisfying the *theta group action relation*:

$$\theta_i(x+\overline{\Theta}(n)(j,\chi))=\chi(i+j)^{-1}\theta_{i+j}(x),$$

for all $x\in A$, $i,j\in(\mathbb{Z}/n\mathbb{Z})^g$ and $\chi\in\widehat{(\mathbb{Z}/n\mathbb{Z})^g}$.

Properties of theta structures

Theta structures are induced by symplectic isomorphisms

Theorem (Mumford, 1966)

A level n theta structure $(\Theta(n), \overline{\Theta}(n))$ on a PPAV A is fully determined by a symplectic isomorphism $\overline{\Theta}(2n) : (\mathbb{Z}/2n\mathbb{Z})^g \times (\widehat{\mathbb{Z}/2n\mathbb{Z}})^g \xrightarrow{\sim} A[2n]$ inducing $\overline{\Theta}(n)$ i.e. by a symplectic basis of $A[2n]$ inducing $\overline{\Theta}(n)$.

Theta structures and theta null points:

- When $4|n$, the *marked AV* (PPAV and theta structure) $(A, \Theta(n), \overline{\Theta}(n))$ is determined by the *theta null point* $(\theta_i(0_A))_i$.
- In other cases, we still use the theta null point as a representative of a marked AV.
- This is enough for arithmetic operations.

Theta structures of level 2

Theorem

Let $(A,\Theta(n),\overline{\Theta}(n))$ be a marked AV of level n and dimension g. Then:

1. *[Mum74] If $n \geq 3$, then $\Theta(n) : A \hookrightarrow \mathbb{P}^{n^g-1}$ is an embedding.*
2. *[BL04] If $n = 2$ and A is not a product, then $\Theta(2)$ defines an embedding $A/\pm \hookrightarrow \mathbb{P}^{2^g-1}$.*
3. *[BL04] If $n = 2$ and $A \simeq A_1 \times \cdots \times A_m$, then $\Theta(2)$ defines an embedding*
$$A_1/\pm \times \cdots \times A_m/\pm \hookrightarrow \mathbb{P}^{2^g-1}.$$

Computing 2-isogeny chains in any dimension

d-isogenies between PPAVs

- Let $f:(A,\lambda_A)\longrightarrow(B,\lambda_B)$ be an isogeny between PPAVs.
- Then we define its *polarised dual* $\widetilde{f}:(B,\lambda_B)\longrightarrow(A,\lambda_A)$ as the composition:

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

- f is a *d-isogeny* if $\widetilde{f}\circ f=[d]_A$.
- This is automatically true in dimension one but not always in dimensions ≥ 2.

Our goal

Goal: Given the kernel $K \subset A[2^e]$ of a 2^e-isogeny between PPAVs $f : A \longrightarrow B$, compute f in level 2 theta coordinates:

$$(\theta_i^A(x))_{i \in (\mathbb{Z}/2\mathbb{Z})^g} \longmapsto (\theta_i^B(f(x)))_{i \in (\mathbb{Z}/2\mathbb{Z})^g}$$

Method:

- Decompose f as a chain of 2-isogenies:

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

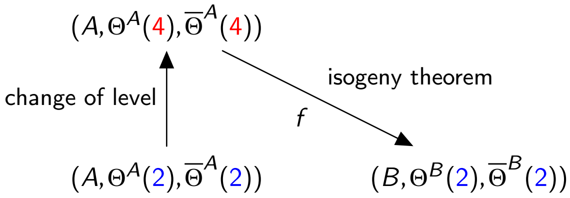
- Compute every 2-isogeny iteratively, using:

$$\ker(f_i) = [2^{e-i}] f_{i-1} \circ \cdots \circ f_1(\ker(f)).$$

Technicality: We need more torsion $K \subset A[2^{e+2}]$ above the kernel.

Computing a 2-isogeny: change of level

- Let $f : A \longrightarrow B$ be a 2-isogeny.



- The level 4 theta structure $(A, \Theta^A(4), \overline{\Theta}^A(4))$ is induced by a symplectic basis of $A[8]$.
- For that reason, we need 8-torsion points $T_1, \cdots, T_g$ such that $\ker(f) = \langle [4]T_1, \cdots, [4]T_g \rangle$ to compute f.
- With this data, we compute the codomain theta-null point $(\theta_i(0_B))_i$.

2-isogeny evaluation algorithm

A very simple isogeny evaluation algorithm:

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

where:

- $H : (x_i)_i \longmapsto \left(\sum_{i\in(\mathbb{Z}/2\mathbb{Z})^g}(-1)^{\langle i|j\rangle}x_i\right)_j$ (Hadamard).
- $S : (x_i)_i \longmapsto (x_i^2)_i$.
- $(x_i)_i \star (y_i)_i := (x_i y_i)_i$.
- $(\widetilde{\theta}_i^B(0_B))_i = H((\theta_i^B(0_B))_i)$ (dual theta null point).

Issues with the first 2-isogeny in the chain

Usually, the first isogeny of the chain is a *gluing* $f : A_1 \times A_2 \longrightarrow B$.

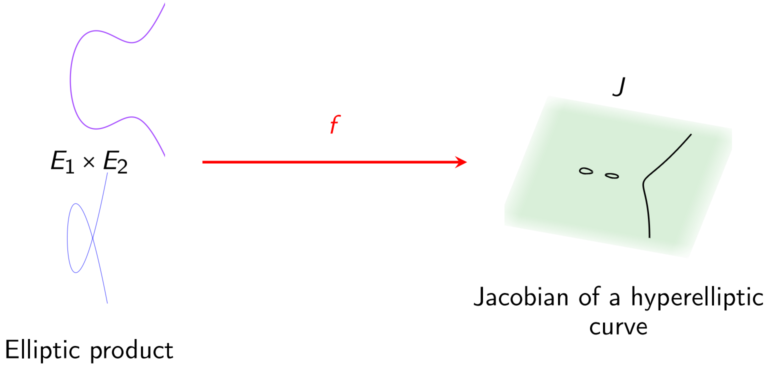


Figure: A gluing isogeny in dimension 2

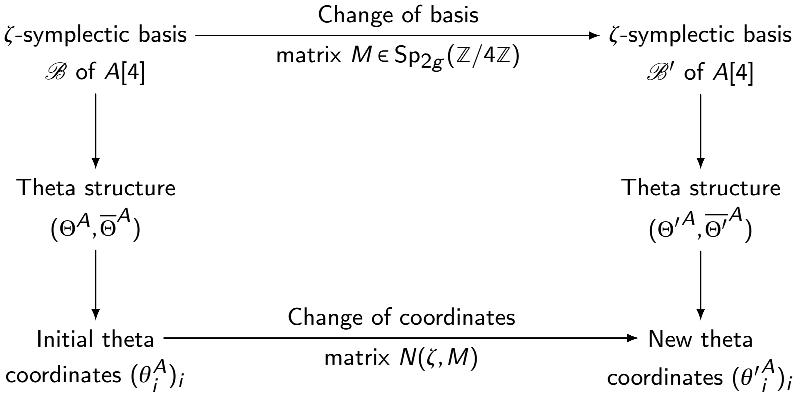
Issues with the first 2-isogeny in the chain

Issue 1:

- The starting domain theta structure $\Theta^{A_1\times A_2}$ is the product $\Theta^{A_1}\times\Theta^{A_2}$:
$$\theta_{i,j}^{A_1\times A_2}(x,y)=\theta_i^{A_1}(x)\cdot\theta_j^{A_2}(y).$$
- The isogeny formulas only work when
$$\overline{\Theta}^{A_1\times A_2}(\{0\}\times\widehat{(\mathbb{Z}/2\mathbb{Z})^g})=\ker(f).$$
- This is usually not the case when $\Theta^{A_1\times A_2}=\Theta^{A_1}\times\Theta^{A_2}$.

Solution 1: Compute a new theta structure $\Theta'^{A_1\times A_2}$ such that
$$\overline{\Theta'}^{A_1\times A_2}(\{0\}\times\widehat{(\mathbb{Z}/2\mathbb{Z})^g})=\ker(f).$$

Change of coordinate formulas



*ζ is a primitive 4-th root of unity given by the Weil-pairings of symplectic basis.

The right choice of theta structure

Definition

Let $f : A \longrightarrow B$ be a d-isogeny and $\mathscr{B} := (S_1, \cdots, S_g, T_1, \cdots, T_g)$ be a ζ-symplectic basis of $A[4d]$. We say that $\mathscr{B}$ and its associated theta structure are **adapted** to f if:

$$\ker(f) = \langle [4]T_1, \cdots, [4]T_g \rangle.$$

Theorem

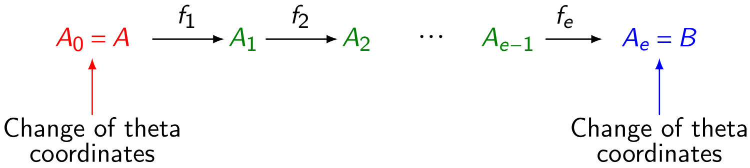
If $\mathscr{B}$ is adapted to f, then the theta structure induced on its codomain B is induced by the ζ^d-symplectic basis of $B[4]$:

$$f_*(\mathscr{B}) := ([d]f(S_1), \cdots, [d]f(S_g), f(T_1), \cdots, f(T_g)).$$

We call it the theta structure induced by f and $\mathscr{B}$.

The right choice of theta structure propagates

- When there is only one gluing isogeny, only 2 change of theta structures are needed



- Change of theta structure on A:

  Initial (product) theta structure Θ_A ⟶ Theta structure Θ'_A adapted to f_1 induced by $[2^e]\mathscr{B}$

- Change of theta structure on B:

  Theta structure Θ_B induced by $f_*(\mathscr{B})$ ⟶ Final (product) Theta structure Θ'_B

Evaluating a gluing 2-isogeny

Issue 2:

- The evaluation algorithm:

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

  no longer works because the $\widetilde{\theta}_i^B(0_B)$ may vanish.

- Why? 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.

Solution 2: Using x and translates $x + T$ where $[2]T \in \ker(f)$, we can evaluate $f(x)$.

The 2-dimensional case

A 2-dimensional 2-isogeny chain

Goal: compute a 2^e-isogeny $F : E_1 \times E_2 \longrightarrow E_3 \times E_4$ between elliptic products (obtained via Kani's lemma, *e.g.* in SQIsign).

We can decompose F into a chain of 2-isogenies:

$$E_1 \times E_2 \xrightarrow[\text{gluing}]{f_1} A_1 \xrightarrow{f_2} A_2 \quad \cdots \quad A_{e-1} \xrightarrow[\text{splitting}]{f_e} E_3 \times E_4$$

Two cases:

- We know $T_1, T_2 \in (E_1 \times E_2)[2^{e+2}]$ forming an isotropic subgroup such that $\ker(F) = \langle [4]T_1, [4]T_2 \rangle$.
- We only know $T_1, T_2 \in (E_1 \times E_2)[2^e]$ such that $\ker(F) = \langle T_1, T_2 \rangle$.

Step 1: change of coordinates

Step 1: from Montgomery $(x:z)$-coordinates to theta coordinates adapted to f_1.

- **Method 1:** successive change of coordinates [Dar25, § 6.5.1]

$$\begin{array}{ccccc} (x_1:z_1),(x_2:z_2) & \longrightarrow & \Theta_{E_1}\times\Theta_{E_2} & \longrightarrow & \Theta'_{E_1\times E_2} \\ (x_1x_2:x_1z_2:z_1x_2:z_1z_2) & \xrightarrow[\text{linear}]{} & & & (\theta'_{00}:\theta'_{10}:\theta'_{01}:\theta'_{11}) \end{array}$$

- **Method 2:** direct theta group action on global sections *a.k.a.* Damien Robert's method [DMPR23] (see also [Dup25])

$$\begin{array}{ccc} (x_1:z_1),(x_2:z_2) & \xrightarrow{\text{theta group action}} & \Theta'_{E_1\times E_2} \\ (x_1x_2:x_1z_2:z_1x_2:z_1z_2) & \xrightarrow[\text{linear}]{} & (\theta'_{00}:\theta'_{10}:\theta'_{01}:\theta'_{11}) \end{array}$$

Step 2: gluing isogeny $f_1 : E_1 \times E_2 \longrightarrow A_1$

- By generic algorithms, we obtain the dual codomain theta null point $(\alpha, \beta, \gamma, \delta)$.
- Its last coordinate is always $\delta = 0$.

- Generic evaluation algorithm would require to divide by $\delta = 0$.
- Instead, we use x and $x + T$ with $[2]T \in \ker(f_1)$ to evaluate $f_1(x)$.

- See Superglue algorithms for new formulas exploiting symmetries [Dup25].

Completing the chain computation

Assumption: we are given $T_1, T_2 \in (E_1 \times E_2)[2^{e+2}]$ forming an isotropic subgroup such that $\ker(F) = \langle [4]T_1, [4]T_2 \rangle$.

Step 4: For all $i \geq 2$, compute each generic 2-isogeny $f_i : A_{i-1} \longrightarrow A_i$ from the evaluation of:

$$([2^{e-i}]f_{i-1} \circ \cdots f_1(T_1), [2^{e-i}]f_{i-1} \circ \cdots f_1(T_2))$$

Step 5: Compute the splitting change of theta coordinates on $E_3 \times E_4$ induced by a choice of basis (S_1, S_2, T_1, T_2) adapted to F.

Square root computations needed

Assumption: we are only given $T_1, T_2 \in (E_1 \times E_2)[2^e]$ such that $\ker(F) = \langle T_1, T_2 \rangle$.

Step 4: For all $2 \leq i \leq e-2$, compute each generic 2-isogeny $f_i : A_{i-1} \longrightarrow A_i$ from the evaluation of:

$$([2^{e-i-2}]f_{i-1} \circ \cdots f_1(T_1), [2^{e-i-2}]f_{i-1} \circ \cdots f_1(T_2))$$

Step 5: Compute the 2-isogeny $f_{e-1} : A_{e-2} \longrightarrow A_{e-1}$ from $f_{e-2} \circ \cdots f_1(T_1)$ and 2 square roots.

Step 6: Compute the 2-isogeny $f_e : A_{e-1} \longrightarrow A_e$ using 3 square roots.

How to split with incomplete torsion

Assumption: we are only given $T_1, T_2 \in (E_1 \times E_2)[2^e]$ such that $\ker(F) = \langle T_1, T_2 \rangle$.

Step 7: Recovering a product theta structure on $B := E_3 \times E_4$.

- We try several change of theta coordinates.
- 10 tries at most are necessary.
- We try several change of theta coordinates until:

$$\widetilde{\theta}^B_{11,11}(0_B) := \sum_{t_1, t_2 \in \mathbb{Z}/2\mathbb{Z}} (-1)^{t_1+t_2} \theta^B_{t_1+1, t_2+1}(0_B) \theta^B_{t_1, t_2}(0_B)$$

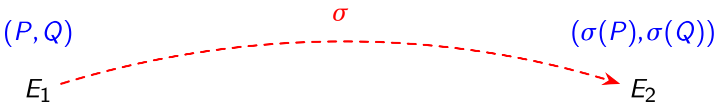
is zero.

Tutorial: how to break SIDH in 4D

The interpolation problem

Problem

Let $\sigma : E_1 \longrightarrow E_2$ be a q-isogeny and (P, Q) be a basis of $E_1[2^f]$.
Given $P, Q, \sigma(P), \sigma(Q)$ and q, evaluate σ anywhere in polynomial time.



A solution from Kani's lemma

- Find $a_1, a_2 \in \mathbb{Z}$ and $e+4 \leq 2f$ such that $q + a_1^2 + a_2^2 = 2^e$.
- Consider the 4-dimensional 2^e-isogeny:

$$F := \begin{pmatrix} a_1 & a_2 & \widehat{\sigma} & 0 \\ -a_2 & a_1 & 0 & \widehat{\sigma} \\ -\sigma & 0 & a_1 & -a_2 \\ 0 & -\sigma & a_2 & a_1 \end{pmatrix} \in \mathrm{End}(E_1^2 \times E_2^2).$$

- Its kernel is given by:

$$\ker(F) = \{([a_1]R - [a_2]S, [a_2]R + [a_1]S, \sigma(R), \sigma(S)) \mid R, S \in E_1[2^e]\}.$$

- From $e, a_1, a_2, P, Q, \sigma(P), \sigma(Q)$, one can compute F.
- Then for all $P \in E_1$:

$$F(P,0,0,0) = ([a_1]P, -[a_2]P, -\sigma(P), 0).$$

Do we have enough torsion?

- If $f \geq e+2$, we can directly compute $T_1, \cdots, T_4 \in (E_1^2 \times E_2^2)[2^{e+2}]$ such that $\ker(F) = \langle [4]T_1, \cdots, [4]T_4 \rangle$.
- But this is not the case in practice...

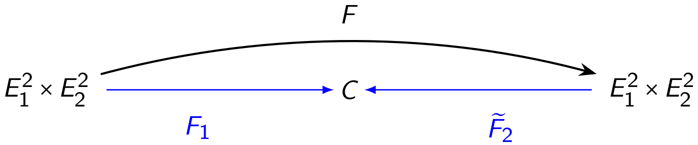
- If $e/2 + 2 \leq f < e+2$, we divide F in two parts.
- Let $e := e_1 + e_2$ such that $e_i + 2 \leq f$.

$$E_1^2 \times E_2^2 \xrightarrow{\quad F \quad} E_1^2 \times E_2^2$$

Do we have enough torsion?

- If $f \geq e+2$, we can directly compute $T_1, \cdots, T_4 \in (E_1^2 \times E_2^2)[2^{e+2}]$ such that $\ker(F) = \langle [4]T_1, \cdots, [4]T_4 \rangle$.
- But this is not the case in practice...

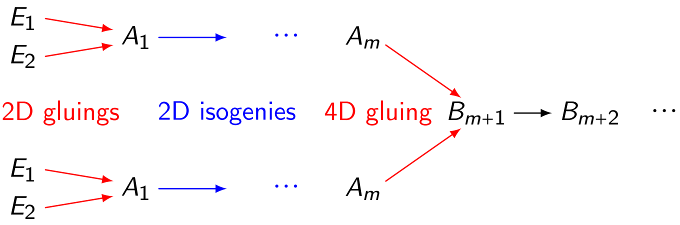
- If $e/2+2 \leq f < e+2$, we divide F in two parts.
- Let $e := e_1 + e_2$ such that $e_i + 2 \leq f$.



- Consider 2^{e_i}-isogenies F_i such that $F := F_2 \circ F_1$.
- We use $e_1, e_2, a_1, a_2, P, Q, \sigma(P), \sigma(Q)$ to compute F_1 and $\widetilde{F}_2$ and then $F := \widetilde{\widetilde{F}}_2 \circ F_1$.

The first isogenies of the chain

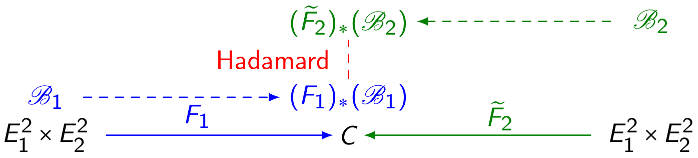
- Let $m := \max(v_2(a_1), v_2(a_2))$.
- Then the first isogenies in the 2-isogeny chain F is of the form:



- This is the same holds for both F_1 and $\widetilde{F}_2$.

Steps to compute F: adapted basis

Step 1: Build matching symplectic basis adapted to F_1 and $\widetilde{F}_2$:

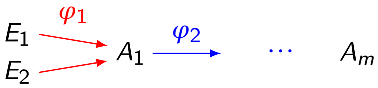


i.e. basis $\mathscr{B}_i := (S_{i,1}, \cdots, S_{i,4}, T_{i,1}, \cdots, T_{i,4})$ of $(E_1^2 \times E_2^2)[2^{e_i+2}]$ such that:

- $\ker(F_1) = \langle [4]T_{1,1}, \cdots, [4]T_{1,4} \rangle$.
- $\ker(\widetilde{F}_2) = \langle [4]T_{2,1}, \cdots, [4]T_{2,4} \rangle$.
- $[2^{e_2}]\widetilde{F}_2(S_{2,j}) = F_1(T_{1,j})$ and $\widetilde{F}_2(T_{2,j}) = -[2^{e_1}]F_1(S_{1,j})$.

Steps to compute F: computing F_1

Step 2: Compute the m starting 2-dimensional isogenies:



Step 3: Computing the change of theta coordinates:

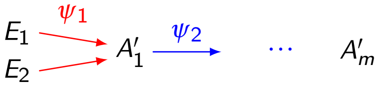
Product theta structure $\Theta_{A_m} \times \Theta_{A_m}$ induced by $\varphi_m \circ \cdots \circ \varphi_1$ $\longrightarrow$ Theta structure $\Theta_{A_m \times A_m}$ adapted to $f_{m+1} : A_m^2 \longrightarrow B_{m+1}$ induced by $\mathscr{B}_1$

Step 4: Computing the gluing isogeny $f_{m+1} : A_m^2 \longrightarrow B_{m+1}$.

Step 5: Computing the generic isogenies $f_i : B_{i-1} \longrightarrow B_i$ for all $m+2 \leq i \leq e_1$.

Steps to compute F: computing $\widetilde{F}_2$

Step 2: Compute the m starting 2-dimensional isogenies:



Step 5: Computing the change of theta coordinates:

Product theta structure $\Theta_{A'_m} \times \Theta_{A'_m}$ induced by $\psi_m \circ \cdots \circ \psi_1$ $\longrightarrow$ Theta structure $\Theta'_{A'_m \times A'_m}$ adapted to $g_{m+1} : A'^2_m \longrightarrow B'_{m+1}$ induced by $\mathscr{B}_2$

Step 6: Computing the gluing isogeny $g_{m+1} : A'^2_m \longrightarrow B'_{m+1}$.

Step 7: Computing the generic isogenies $g_i : B'_{i-1} \longrightarrow B'_i$ for all $m+2 \leq i \leq e_2$.

Steps to compute F: final matching

Step 8: Check that codomains match $B_{e_1} = B'_{e_2}$ by checking that:

$$\Theta_{B_{e_1}} = H \circ \Theta_{B'_{e_2}}.$$

Step 9: Compute $F_2 = \widetilde{g}_1 \circ \cdots \circ \widetilde{g}_{e_2}$. This is immediate by Hadamard transform: if $f : A \longrightarrow B$ is a 2-isogeny, then

$$H \circ \Theta_B(f(x)) \star H \circ \Theta_B(0_B) = H \circ S \circ \Theta_A(x)$$

becomes:

$$\Theta_A(\widetilde{f}(y)) \star \Theta_A(0_A) = H \circ S \circ H \circ \Theta_B(y).$$

Finally, $F = F_2 \circ F_1$ can be evaluated.

Conclusion and future works

- The theory is getting more accessible.
- Formulas are really practical to implement.

Future/ongoing works:

- What about odd degrees?
- Constant time algorithms.
- New gluing formulas in dimension 4.