A Combinatorial Perspective on Theta Structures

Applications in Superglue

Max Duparc

EPFL

SQIparty at Lleida: May 15, 2025

The challenge of Isogeny Based Cryptography

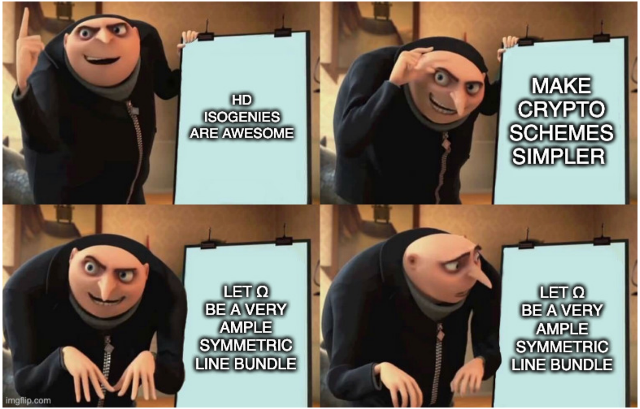

Figure: An outsider perspective on current Isogeny Based Cryptography

The combinatorial perspective

You can get a practical understanding of HD varieties & isogenies without scheme theory !

- Can infer most interesting properties from *theta structures*.
- Is it simpler ?
  - NO !!
  - More accessible. (Just ugly linear algebra).
- You should get a good toolbox to use Kani's Lemma:

$$\prod_i^g E_i \xrightarrow{(2^n,\cdots,2^n)} \prod_i^g E_i'$$

The combinatorial perspective

You can get a practical understanding of HD varieties & isogenies without scheme theory !

- Can infer most interesting properties from *theta structures*.
- Is it simpler ?
  - NO !!
  - More accessible. (Just ugly linear algebra).
- You should get a good toolbox to use Kani's Lemma:

$$\prod_i^g E_i \xrightarrow{(2^n,\cdots,2^n)} \prod_i^g E_i'$$

The combinatorial perspective

You can get a practical understanding of HD varieties & isogenies without scheme theory !

- Can infer most interesting properties from *theta structures*.
- Is it simpler ?
  - NO !!
  - More accessible. (Just ugly linear algebra).

- You should get a good toolbox to use Kani's Lemma:

$$\prod_i^g E_i \xrightarrow{(2^n,\cdots,2^n)} \prod_i^g E_i'$$

The combinatorial perspective

You can get a practical understanding of HD varieties & isogenies without scheme theory !

- Can infer most interesting properties from *theta structures*.
- Is it simpler ?
  - NO !!
  - More accessible. (Just ugly linear algebra).

- You should get a good toolbox to use Kani's Lemma:

$$\prod_i^g E_i \xrightarrow{(2^n,\cdots,2^n)} \prod_i^g E_i'$$

The combinatorial perspective

You can get a practical understanding of HD varieties & isogenies without scheme theory !

- Can infer most interesting properties from *theta structures*.
- Is it simpler ?
  - NO !!
  - More accessible. (Just ugly linear algebra).

- You should get a good toolbox to use Kani's Lemma:

$$\begin{tikzcd} \prod_i^g E_i \arrow[r] \arrow[rrrrrr, bend left, "{(2^n,\cdots,2^n)}"] & A_1 \arrow[r] & A_2 \arrow[r] & \cdots \arrow[r] & A_{n-2} \arrow[r] & A_{n-1} \arrow[r] & \prod_i^g E_i' \end{tikzcd}$$

Table of Contents

Reminder: Elliptic curves

Definition (Elliptic curve)

An *elliptic curve* E is an abelian variety of dimension 1 given by the zeros locus of a homogeneous polynomial.

$$E : zy^2 = x^3 + Ax^2z + xz^2 = x(x - \alpha z)(x - \alpha^{-1}z)$$

We have that $E[N] \cong \mathbb{Z}_N^2$ and their exists a *non-degenerate*, *bilinear*, and *alternating* Weil pairing.

$$e_N : E[N] \times E[N] \longrightarrow \mathbb{S}^1$$

- *non-degenerate:* $\exists P, Q$ s.t. $e_N(P, Q) \neq 1$
- *bilinear:* $e_N(P_1 + P_2, Q) = e_N(P_1, Q) \cdot e_N(P_2, Q)$
- *alternating:* $e_N(P, Q) = e_N(Q, P)^{-1}$

Reminder: Elliptic curves

Definition (Elliptic curve)

An *elliptic curve* E is an abelian variety of dimension 1 given by the zeros locus of a homogeneous polynomial.

$$E : zy^2 = x^3 + Ax^2z + xz^2 = x(x - \alpha z)(x - \alpha^{-1}z)$$

We have that $E[N] \cong \mathbb{Z}_N^2$ and their exists a *non-degenerate*, *bilinear*, and *alternating* Weil pairing.

$$e_N : E[N] \times E[N] \longrightarrow \mathbb{S}^1$$

- *non-degenerate:* $\exists P, Q$ s.t. $e_N(P, Q) \neq 1$
- *bilinear:* $e_N(P_1 + P_2, Q) = e_N(P_1, Q) \cdot e_N(P_2, Q)$
- *alternating:* $e_N(P, Q) = e_N(Q, P)^{-1}$

Abelian varieties

Definition (Abelian variety)

An *Abelian variety* A of dimension g given by the zeros locus of some homogeneous polynomials.
We have that $A[N] \cong \mathbb{Z}_N^{2g}$ and their is a *non-degenerate*, *bilinear*, and *alternating* Weil pairing.

$$e_N : A[N] \times A[N] \longrightarrow \mathbb{S}^1$$

- Weil Pairing is no longer trivial.

- A *symplectic structure* of $A[N]$ is an isomorphism $\pi : A[N] \cong \mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}$ compatible with the Weil pairing.

$$\pi(P) = (x_P, \widehat{x_P}) \text{ and } e_N(P, Q) = \omega^{(\widehat{x_Q} \cdot x_P) - (\widehat{x_P} \cdot x_Q)}$$

with ω is a primitive N-th root of unity.

Definition (Symplectic basis)

A *symplectic basis* of $A[N]$ is a basis $\{S_1, ..., S_g, T_1, ..., T_g\}$ such that:

$$e_N(S_i, S_j) = e_N(T_i, T_j) = 1, \quad e_N(S_i, T_j) = \omega^{\delta_{ij}}$$

Abelian varieties

Definition (Abelian variety)

An *Abelian variety* A of dimension g given by the zeros locus of some homogeneous polynomials. We have that $A[N] \cong \mathbb{Z}_N^{2g}$ and their is a *non-degenerate*, *bilinear*, and *alternating* Weil pairing.

$$e_N : A[N] \times A[N] \longrightarrow \mathbb{S}^1$$

- Weil Pairing is no longer trivial.

- A *symplectic structure* of $A[N]$ is an isomorphism $\pi : A[N] \cong \mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}$ compatible with the Weil pairing.

$$\pi(P) = (x_P, \widehat{x_P}) \text{ and } e_N(P, Q) = \omega^{(\widehat{x_Q} \cdot x_P) - (\widehat{x_P} \cdot x_Q)}$$

  with ω is a primitive N-th root of unity.

Definition (Symplectic basis)

A *symplectic basis* of $A[N]$ is a basis $\{S_1, \ldots, S_g, T_1, \ldots, T_g\}$ such that:

$$e_N(S_i, S_j) = e_N(T_i, T_j) = 1, \quad e_N(S_i, T_j) = \omega^{\delta_{ij}}$$

Abelian varieties

Definition (Abelian variety)

An *Abelian variety* A of dimension g given by the zeros locus of some homogeneous polynomials. We have that $A[N] \cong \mathbb{Z}_N^{2g}$ and their is a *non-degenerate*, *bilinear*, and *alternating* Weil pairing.

$$e_N : A[N] \times A[N] \longrightarrow \mathbb{S}^1$$

- Weil Pairing is no longer trivial.

- A *symplectic structure* of $A[N]$ is an isomorphism $\pi : A[N] \cong \mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}$ compatible with the Weil pairing.

$$\pi(P) = (x_P, \widehat{x_P}) \text{ and } e_N(P,Q) = \omega^{(\widehat{x_Q}\cdot x_P)-(\widehat{x_P}\cdot x_Q)}$$

with ω is a primitive N-th root of unity.

Definition (Symplectic basis)

A *symplectic basis* of $A[N]$ is a basis $\{S_1, \dots, S_g, T_1, \dots, T_g\}$ such that:

$$e_N(S_i, S_j) = e_N(T_i, T_j) = 1, \quad e_N(S_i, T_j) = \omega^{\delta_{ij}}$$

Abelian varieties

Definition (Abelian variety)

An *Abelian variety* A of dimension g given by the zeros locus of some homogeneous polynomials. We have that $A[N] \cong \mathbb{Z}_N^{2g}$ and their is a *non-degenerate*, *bilinear*, and *alternating* Weil pairing.

$$e_N : A[N] \times A[N] \longrightarrow \mathbb{S}^1$$

- Weil Pairing is no longer trivial.

- A *symplectic structure* of $A[N]$ is an isomorphism $\pi : A[N] \cong \mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}$ compatible with the Weil pairing.

$$\pi(P) = (x_P, \widehat{x_P}) \text{ and } e_N(P, Q) = \omega^{(\widehat{x_Q} \cdot x_P) - (\widehat{x_P} \cdot x_Q)}$$

with ω is a primitive N-th root of unity.

Definition (Symplectic basis)

A *symplectic basis* of $A[N]$ is a basis $\{S_1, ..., S_g, T_1, ..., T_g\}$ such that:

$$e_N(S_i, S_j) = e_N(T_i, T_j) = 1, \quad e_N(S_i, T_j) = \omega^{\delta_{ij}}$$

Abelian varieties

Definition (Abelian variety)

An *Abelian variety* A of dimension g given by the zeros locus of some homogeneous polynomials. We have that $A[N] \cong \mathbb{Z}_N^{2g}$ and their is a *non-degenerate*, *bilinear*, and *alternating* Weil pairing.

$$e_N : A[N] \times A[N] \longrightarrow \mathbb{S}^1$$

- Weil Pairing is no longer trivial.

- A *symplectic structure* of $A[N]$ is an isomorphism $\pi : A[N] \cong \mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}$ compatible with the Weil pairing.

$$\pi(P) = (x_P, \widehat{x_P}) \text{ and } e_N(P, Q) = \omega^{(\widehat{x_Q} \cdot x_P) - (\widehat{x_P} \cdot x_Q)}$$

with ω is a primitive N-th root of unity.

Definition (Symplectic basis)

A *symplectic basis* of $A[N]$ is a basis $\{S_1, \ldots, S_g, T_1, \ldots, T_g\}$ such that:

$$e_N(S_i, S_j) = e_N(T_i, T_j) = 1, \quad e_N(S_i, T_j) = \omega^{\delta_{ij}}$$

Theta structures

Definition (Theta structure)

Let A be an Abelian variety of dimension g. A (level 2 symmetric) *theta structure* is a morphism into the *Kummer variety* $\mathcal{K}_A$:

$$\theta^A : A_{/\pm 1} \longrightarrow \mathcal{K}_A \subseteq \mathbb{P}^{2^g - 1}$$

that is compatible with a symplectic basis on $A[2]$: For all $X \in A[2]$ with $\pi(X) = (x, \widehat{x})$:

$$\theta_i^A(P + X) = (-1)^{\widehat{x} \cdot i} \theta_{i+x}^A(P)$$

- $\theta^A(0)$ the *theta null point* characterises A up to isomorphism.
- Several valid solutions for one symplectic basis over $A[2]$.
  - [Mum66] Fix one when considering symplectic basis over $A[4]$.

Theta structures

Definition (Theta structure)

Let A be an Abelian variety of dimension g. A (level 2 symmetric) *theta structure* is a morphism into the *Kummer variety* $\mathcal{K}_A$:

$$\theta^A : A_{/\pm 1} \longrightarrow \mathcal{K}_A \subseteq \mathbb{P}^{2^g - 1}$$

that is compatible with a symplectic basis on $A[2]$: For all $X \in A[2]$ with $\pi(X) = (x, \widehat{x})$:

$$\theta_i^A(P + X) = (-1)^{\widehat{x} \cdot i} \theta_{i+x}^A(P)$$

- $\theta^A(0)$ the *theta null point* characterises A up to isomorphism.
- Several valid solutions for one symplectic basis over $A[2]$.
  - [Mum66] Fix one when considering symplectic basis over $A[4]$.

Theta structures

Definition (Theta structure)

Let A be an Abelian variety of dimension g. A (level 2 symmetric) *theta structure* is a morphism into the *Kummer variety* $\mathcal{K}_A$:

$$\theta^A : A_{/\pm 1} \longrightarrow \mathcal{K}_A \subseteq \mathbb{P}^{2^g-1}$$

that is compatible with a symplectic basis on $A[2]$: For all $X \in A[2]$ with $\pi(X) = (x, \widehat{x})$:

$$\theta_i^A(P+X) = (-1)^{\widehat{x}\cdot i}\theta_{i+x}^A(P)$$

- $\theta^A(0)$ the *theta null point* characterises A up to isomorphism.
- Several valid solutions for one symplectic basis over $A[2]$.
  - [Mum66] Fix one when considering symplectic basis over $A[4]$.

Theta structures

Definition (Theta structure)

Let A be an Abelian variety of dimension g. A (level 2 symmetric) *theta structure* is a morphism into the *Kummer variety* $\mathcal{K}_A$:

$$\theta^A : A_{/\pm 1} \longrightarrow \mathcal{K}_A \subseteq \mathbb{P}^{2^g - 1}$$

that is compatible with a symplectic basis on $A[2]$: For all $X \in A[2]$ with $\pi(X) = (x, \widehat{x})$:

$$\theta_i^A(P + X) = (-1)^{\widehat{x} \cdot i} \theta_{i+x}^A(P)$$

- $\theta^A(0)$ the *theta null point* characterises A up to isomorphism.
- Several valid solutions for one symplectic basis over $A[2]$.
    - [Mum66] Fix one when considering symplectic basis over $A[4]$.

Theta structure on Elliptic Curves

Definition (Symmetric elements)

Given $T \in E[4]$, we define the *symmetric element* $\mathfrak{g}_T$ as the symmetry such that $\mathfrak{g}_T \cdot \binom{x_T}{z_T} = \binom{x_T}{z_T}$.

$$\forall X \in E, \; X + [2]T = \mathfrak{g}_T \cdot X$$

Let $\langle S, T \rangle$ be a (symplectic) basis of $E[4]$. Let $\theta_i(P) = \theta_i \cdot \binom{x_P}{z_Q}$:

$$\theta_i \text{ such that } \begin{cases} \theta_i \cdot \mathfrak{g}_T & = (-1)^i \theta_i \\ \theta_i \cdot \mathfrak{g}_S & = \theta_{i+1} \end{cases} \Longrightarrow \begin{cases} \theta_0 & = [\mathfrak{g}_0 + \mathfrak{g}_T]_{0,-} \\ \theta_1 & = \theta_0 \cdot \mathfrak{g}_S \end{cases}$$

Theta structure on Elliptic Curves

Definition (Symmetric elements)

Given $T \in E[4]$, we define the *symmetric element* $\mathfrak{g}_T$ as the symmetry such that $\mathfrak{g}_T \cdot \binom{x_T}{z_T} = \binom{x_T}{z_T}$.

$$\forall X \in E,\ X + [2]T = \mathfrak{g}_T \cdot X$$

Let $\langle S, T \rangle$ be a (symplectic) basis of $E[4]$. Let $\theta_i(P) = \theta_i \cdot \binom{x_P}{z_Q}$:

$$\theta_i \text{ such that } \begin{cases} \theta_i \cdot \mathfrak{g}_T & = (-1)^i \theta_i \\ \theta_i \cdot \mathfrak{g}_S & = \theta_{i+1} \end{cases} \implies \begin{cases} \theta_0 & = [\mathfrak{g}_0 + \mathfrak{g}_T]_{0,-} \\ \theta_1 & = \theta_0 \cdot \mathfrak{g}_S \end{cases}$$

Theta structure on Elliptic Curves

Definition (Symmetric elements)

Given $T \in E[4]$, we define the *symmetric element* $\mathfrak{g}_T$ as the symmetry such that $\mathfrak{g}_T \cdot \binom{x_T}{z_T} = \binom{x_T}{z_T}$.

$$\forall X \in E,\ X + [2]T = \mathfrak{g}_T \cdot X$$

Let $\langle S, T \rangle$ be a (symplectic) basis of $E[4]$. Let $\theta_i(P) = \theta_i \cdot \binom{x_P}{z_Q}$:

$$\theta_i \text{ such that } \begin{cases} \theta_i \cdot \mathfrak{g}_T & = (-1)^i \theta_i \\ \theta_i \cdot \mathfrak{g}_S & = \theta_{i+1} \end{cases} \implies \begin{cases} \theta_0 & = [\mathfrak{g}_0 + \mathfrak{g}_T]_{0,-} \\ \theta_1 & = \theta_0 \cdot \mathfrak{g}_S \end{cases}$$

Theta structure on Elliptic Curves

Definition (Symmetric elements)

Given $T \in E[4]$, we define the *symmetric element* $\mathfrak{g}_T$ as the symmetry such that $\mathfrak{g}_T \cdot \binom{x_T}{z_T} = \binom{x_T}{z_T}$.

$$\forall X \in E,\ X + [2]T = \mathfrak{g}_T \cdot X$$

Let $\langle S, T \rangle$ be a (symplectic) basis of $E[4]$. Let $\theta_i(P) = \theta_i \cdot \binom{x_P}{z_Q}$:

$$\theta_i \text{ such that } \begin{cases} \theta_i \cdot \mathfrak{g}_T & = (-1)^i \theta_i \\ \theta_i \cdot \mathfrak{g}_S & = \theta_{i+1} \end{cases} \implies \begin{cases} \theta_0 & = [\mathfrak{g}_0 + \mathfrak{g}_T]_{0,-} \\ \theta_1 & = \theta_0 \cdot \mathfrak{g}_S \end{cases}$$

Structure of symmetric elements

- You can generalise symmetric element to $\prod_{i=1}^{g} E_i$ using tensor product.
  - Ex: For $\langle S_1, S_2\rangle \oplus \langle T_1, T_2\rangle = (E_1 \times E_2)[4]$

$$\theta_i \text{ such that } \begin{cases} \theta_i \cdot \mathfrak{g}_{T_1} & = (-1)^{01\cdot i}\theta_i \\ \theta_i \cdot \mathfrak{g}_{T_2} & = (-1)^{10\cdot i}\theta_i \\ \theta_i \cdot \mathfrak{g}_{S_1} & = \theta_{i+01} \\ \theta_i \cdot \mathfrak{g}_{S_2} & = \theta_{i+10} \end{cases} \implies \begin{cases} \theta_{00} & = [(\mathfrak{g}_0 + \mathfrak{g}_{T_1})(\mathfrak{g}_0 + \mathfrak{g}_{T_2})]_{0,-} \\ \theta_{01} & = \theta_{00} \cdot \mathfrak{g}_{S_1} \\ \theta_{10} & = \theta_{00} \cdot \mathfrak{g}_{S_2} \\ \theta_{11} & = \theta_{01} \cdot \mathfrak{g}_{S_2} \end{cases}$$

with $\mathfrak{g}_P = \mathfrak{g}_{P_1} \otimes \mathfrak{g}_{P_2}$

- Symmetric elements have a structure inherited from Pauli's X, Y, Z matrices.
  - Anti-commutativity: $\mathfrak{g}_X \cdot \mathfrak{g}_Y = -\mathfrak{g}_Y \mathfrak{g}_X$
  - Quaternionic structure: $\mathfrak{g}_X \cdot \mathfrak{g}_Y = \pm \mathbf{i} \cdot \mathfrak{g}_{X+Y}$

Structure of symmetric elements

- You can generalise symmetric element to $\prod_{i=1}^{g} E_i$ using tensor product.
  - Ex: For $\langle S_1, S_2 \rangle \oplus \langle T_1, T_2 \rangle = (E_1 \times E_2)[4]$

$$\theta_i \text{ such that } \begin{cases} \theta_i \cdot \mathfrak{g}_{T_1} & = (-1)^{01\cdot i}\theta_i \\ \theta_i \cdot \mathfrak{g}_{T_2} & = (-1)^{10\cdot i}\theta_i \\ \theta_i \cdot \mathfrak{g}_{S_1} & = \theta_{i+01} \\ \theta_i \cdot \mathfrak{g}_{S_2} & = \theta_{i+10} \end{cases} \implies \begin{cases} \theta_{00} & = [(\mathfrak{g}_0 + \mathfrak{g}_{T_1})(\mathfrak{g}_0 + \mathfrak{g}_{T_2})]_{0,-} \\ \theta_{01} & = \theta_{00} \cdot \mathfrak{g}_{S_1} \\ \theta_{10} & = \theta_{00} \cdot \mathfrak{g}_{S_2} \\ \theta_{11} & = \theta_{01} \cdot \mathfrak{g}_{S_2} \end{cases}$$

with $\mathfrak{g}_P = \mathfrak{g}_{P_1} \otimes \mathfrak{g}_{P_2}$

- Symmetric elements have a structure inherited from Pauli's X, Y, Z matrices.
  - Anti-commutativity: $\mathfrak{g}_X \cdot \mathfrak{g}_Y = -\mathfrak{g}_Y \mathfrak{g}_X$
  - Quaternionic structure: $\mathfrak{g}_X \cdot \mathfrak{g}_Y = \pm \mathbf{i} \cdot \mathfrak{g}_{X+Y}$

Structure of symmetric elements

- You can generalise symmetric element to $\prod_{i=1}^{g} E_i$ using tensor product.
  - Ex: For $\langle S_1, S_2\rangle \oplus \langle T_1, T_2\rangle = (E_1 \times E_2)[4]$

$$\theta_i \text{ such that } \begin{cases} \theta_i \cdot \mathfrak{g}_{T_1} & = (-1)^{01\cdot i}\theta_i \\ \theta_i \cdot \mathfrak{g}_{T_2} & = (-1)^{10\cdot i}\theta_i \\ \theta_i \cdot \mathfrak{g}_{S_1} & = \theta_{i+01} \\ \theta_i \cdot \mathfrak{g}_{S_2} & = \theta_{i+10} \end{cases} \implies \begin{cases} \theta_{00} & = [(\mathfrak{g}_0 + \mathfrak{g}_{T_1})(\mathfrak{g}_0 + \mathfrak{g}_{T_2})]_{0,-} \\ \theta_{01} & = \theta_{00} \cdot \mathfrak{g}_{S_1} \\ \theta_{10} & = \theta_{00} \cdot \mathfrak{g}_{S_2} \\ \theta_{11} & = \theta_{01} \cdot \mathfrak{g}_{S_2} \end{cases}$$

with $\mathfrak{g}_P = \mathfrak{g}_{P_1} \otimes \mathfrak{g}_{P_2}$

- Symmetric elements have a structure inherited from Pauli's X, Y, Z matrices.
  - Anti-commutativity: $\mathfrak{g}_X \cdot \mathfrak{g}_Y = -\mathfrak{g}_Y\mathfrak{g}_X$
  - Quaternionic structure: $\mathfrak{g}_X \cdot \mathfrak{g}_Y = \pm\mathbf{i} \cdot \mathfrak{g}_{X+Y}$

Structure of symmetric elements

- You can generalise symmetric element to $\prod_{i=1}^{g} E_i$ using tensor product.
    - Ex: For $\langle S_1, S_2\rangle \oplus \langle T_1, T_2\rangle = (E_1 \times E_2)[4]$

$$\theta_i \text{ such that } \begin{cases} \theta_i \cdot \mathfrak{g}_{T_1} & = (-1)^{01\cdot i}\theta_i \\ \theta_i \cdot \mathfrak{g}_{T_2} & = (-1)^{10\cdot i}\theta_i \\ \theta_i \cdot \mathfrak{g}_{S_1} & = \theta_{i+01} \\ \theta_i \cdot \mathfrak{g}_{S_2} & = \theta_{i+10} \end{cases} \implies \begin{cases} \theta_{00} & = [(\mathfrak{g}_0 + \mathfrak{g}_{T_1})(\mathfrak{g}_0 + \mathfrak{g}_{T_2})]_{0,-} \\ \theta_{01} & = \theta_{00} \cdot \mathfrak{g}_{S_1} \\ \theta_{10} & = \theta_{00} \cdot \mathfrak{g}_{S_2} \\ \theta_{11} & = \theta_{01} \cdot \mathfrak{g}_{S_2} \end{cases}$$

with $\mathfrak{g}_P = \mathfrak{g}_{P_1} \otimes \mathfrak{g}_{P_2}$

- Symmetric elements have a structure inherited from Pauli's X, Y, Z matrices.
    - Anti-commutativity: $\mathfrak{g}_X \cdot \mathfrak{g}_Y = -\mathfrak{g}_Y \mathfrak{g}_X$
    - Quaternionic structure: $\mathfrak{g}_X \cdot \mathfrak{g}_Y = \pm \mathbf{i} \cdot \mathfrak{g}_{X+Y}$

Structure of $E[4]$

$$
\begin{tikzcd}
 & & (1:1) \arrow[dr] & & (1:-1) \arrow[dl] & & \\
(a+b:a-b) \arrow[dr] & & & (0:1)=C \arrow[d] & & & (a+\mathbf{i}b:a-\mathbf{i}b) \arrow[dl] \\
 & (a^2+b^2:a^2-b^2) \arrow[rr] & & (1:0) & & (a^2-b^2:a^2+b^2) \arrow[ll] & \\
(a-b:a+b) \arrow[ur] & & & & & & (a-\mathbf{i}b:a+\mathbf{i}b) \arrow[ul]
\end{tikzcd}
$$

Figure: Structure of $E[4]$ over the Kummer line.

$$\mathfrak{g}_{(1:\pm1)} = \pm X$$

$$\mathfrak{g}_{(a\pm b:a\mp b)} = \pm\frac{1}{2ab}\left((a^2+b^2)Z - \mathbf{i}(a^2-b^2)Y\right)$$

$$\mathfrak{g}_{(a\pm ib:a\mp ib)} = \mp\frac{1}{2ab}\left(\mathbf{i}(a^2-b^2)Z + (a^2+b^2)Y\right)$$

Structure of $E[4]$

$$\begin{tikzcd}
 & (1:1) \arrow[dr] & & (1:-1) \arrow[dl] & \\
(a+b:a-b) \arrow[dr] & & (0:1)=C \arrow[d] & & (a+\mathbf{i}b:a-\mathbf{i}b) \arrow[dl] \\
 & (a^2+b^2:a^2-b^2) \arrow[r] & (1:0) & (a^2-b^2:a^2+b^2) \arrow[l] & \\
(a-b:a+b) \arrow[ur] & & & & (a-\mathbf{i}b:a+\mathbf{i}b) \arrow[ul]
\end{tikzcd}$$

Figure: Structure of $E[4]$ over the Kummer line.

$$\begin{aligned}
\mathfrak{g}_{(1:\pm 1)} &= \pm X \\
\mathfrak{g}_{(a\pm b:a\mp b)} &= \pm\frac{1}{2ab}\left((a^2+b^2)Z - \mathbf{i}(a^2-b^2)Y\right) \\
\mathfrak{g}_{(a\pm ib:a\mp ib)} &= \mp\frac{1}{2ab}\left(\mathbf{i}(a^2-b^2)Z + (a^2+b^2)Y\right)
\end{aligned}$$

Lookup table for theta structure on EC

$$\mathcal{B}_1 = \langle (a+b : a-b), (1:1) \rangle \implies \theta^{\mathcal{B}_1} = \begin{pmatrix} b & b \\ a & -a \end{pmatrix}$$

$$\mathcal{B}_2 = \langle (a+b : a-b), (1:-1) \rangle \implies \theta^{\mathcal{B}_2} = \begin{pmatrix} a & -a \\ b & b \end{pmatrix} = \text{the theta model}$$

$$\mathcal{B}_3 = \langle (1:1), (a+b : a-b) \rangle \implies \theta^{\mathcal{B}_3} = \begin{pmatrix} a+b & b-a \\ b-a & a+b \end{pmatrix}$$

$$\mathcal{B}_4 = \langle (1:-1), (a+b : a-b) \rangle \implies \theta^{\mathcal{B}_4} = \begin{pmatrix} a+b & b-a \\ a-b & -a-b \end{pmatrix}$$

$$\mathcal{B}_5 = \langle (a+b : a-b), (a+\mathbf{i}b : a-\mathbf{i}b) \rangle \implies \theta^{\mathcal{B}_5} = \begin{pmatrix} a+b & -(a-b) \\ -\mathbf{i}(a-b) & \mathbf{i}(a+b) \end{pmatrix}$$

$$\mathcal{B}_6 = \langle (a+b : a-b), (a-\mathbf{i}b : a+\mathbf{i}b) \rangle \implies \theta^{\mathcal{B}_6} = \begin{pmatrix} a+b & -(a-b) \\ \mathbf{i}(a-b) & -\mathbf{i}(a+b) \end{pmatrix}$$

Table: List of the change of basis matrix of the different theta structures depending on the basis of $E[4]$.

$$\mathcal{B}_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \mathcal{B}_1 \iff \theta^{\mathcal{B}_3} = \mathcal{H}(\theta^{\mathcal{B}_1}) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \theta^{\mathcal{B}_1}$$

Lookup table for theta structure on EC

$$\mathcal{B}_1 = \langle (a+b : a-b), (1:1) \rangle \implies \theta^{\mathcal{B}_1} = \begin{pmatrix} b & b \\ a & -a \end{pmatrix}$$

$$\mathcal{B}_2 = \langle (a+b : a-b), (1:-1) \rangle \implies \theta^{\mathcal{B}_2} = \begin{pmatrix} a & -a \\ b & b \end{pmatrix} = \text{the theta model}$$

$$\mathcal{B}_3 = \langle (1:1), (a+b : a-b) \rangle \implies \theta^{\mathcal{B}_3} = \begin{pmatrix} a+b & b-a \\ b-a & a+b \end{pmatrix}$$

$$\mathcal{B}_4 = \langle (1:-1), (a+b : a-b) \rangle \implies \theta^{\mathcal{B}_4} = \begin{pmatrix} a+b & b-a \\ a-b & -a-b \end{pmatrix}$$

$$\mathcal{B}_5 = \langle (a+b : a-b), (a+\mathbf{i}b : a-\mathbf{i}b) \rangle \implies \theta^{\mathcal{B}_5} = \begin{pmatrix} a+b & -(a-b) \\ -\mathbf{i}(a-b) & \mathbf{i}(a+b) \end{pmatrix}$$

$$\mathcal{B}_6 = \langle (a+b : a-b), (a-\mathbf{i}b : a+\mathbf{i}b) \rangle \implies \theta^{\mathcal{B}_6} = \begin{pmatrix} a+b & -(a-b) \\ \mathbf{i}(a-b) & -\mathbf{i}(a+b) \end{pmatrix}$$

Table: List of the change of basis matrix of the different theta structures depending on the basis of $E[4]$.

$$\mathcal{B}_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \mathcal{B}_1 \iff \theta^{\mathcal{B}_3} = \mathcal{H}(\theta^{\mathcal{B}_1}) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \theta^{\mathcal{B}_1}$$

Table of Contents

Theta structure[2]

- Theta structure have a lot of .self-similarities:

$$P \in A[2] \implies \theta_i^A(P) = (-1)^{\widehat{x}\cdot i}\theta_{i+x}^A(0) \text{ with } \pi(P) = (x, \widehat{x})$$

$$P \in A[4] \implies \theta^A(P) \text{ is fixed by the action of } [2]P$$

	0	T_1	T_2	$T_1 + T_2$
0	$-$	$(x:0:y:0)$	$(x:y:0:0)$	$(x:0:0:y)$
S_1	$(x:x:y:y)$	$(x:ix:y:iy)$	$(x:x:y:-y)$	$(x:ix:y:-iy)$
S_2	$(x:y:x:y)$	$(x:y:x:-y)$	$(x:y:ix:-iy)$	$(x:y:-ix:iy)$
$S_1 + S_2$	$(x:y:y:x)$	$(x:y:-iy:ix)$	$(x:y:iy:ix)$	$(x:y:-y:x)$

Table: Structure of $\theta^A(P)$ depending on the position of $[2]P \in A[2]$

Theta structure[2]

- Theta structure have a lot of .self-similarities:

$$P \in A[2] \implies \theta_i^A(P) = (-1)^{\widehat{x}\cdot i}\theta_{i+x}^A(0) \text{ with } \pi(P) = (x, \widehat{x})$$

$$P \in A[4] \implies \theta^A(P) \text{ is fixed by the action of } [2]P$$

	0	T_1	T_2	$T_1 + T_2$
0	$-$	$(x:0:y:0)$	$(x:y:0:0)$	$(x:0:0:y)$
S_1	$(x:x:y:y)$	$(x:ix:y:iy)$	$(x:x:y:-y)$	$(x:ix:y:-iy)$
S_2	$(x:y:x:y)$	$(x:y:x:-y)$	$(x:y:ix:-iy)$	$(x:y:-ix:iy)$
$S_1 + S_2$	$(x:y:y:x)$	$(x:y:-iy:ix)$	$(x:y:iy:ix)$	$(x:y:-y:x)$

Table: Structure of $\theta^A(P)$ depending on the position of $[2]P \in A[2]$

Theta structure[2]

- Theta structure have a lot of .self-similarities:

$$P \in A[2] \implies \theta_i^A(P) = (-1)^{\widehat{x}\cdot i}\theta_{i+x}^A(0) \text{ with } \pi(P) = (x, \widehat{x})$$

$$P \in A[4] \implies \theta^A(P) \text{ is fixed by the action of } [2]P$$

	0	T_1	T_2	$T_1 + T_2$
0	$-$	$(x:0:y:0)$	$(x:y:0:0)$	$(x:0:0:y)$
S_1	$(x:x:y:y)$	$(x:ix:y:iy)$	$(x:x:y:-y)$	$(x:ix:y:-iy)$
S_2	$(x:y:x:y)$	$(x:y:x:-y)$	$(x:y:ix:-iy)$	$(x:y:-ix:iy)$
$S_1 + S_2$	$(x:y:y:x)$	$(x:y:-iy:ix)$	$(x:y:iy:ix)$	$(x:y:-y:x)$

Table: Structure of $\theta^A(P)$ depending on the position of $[2]P \in A[2]$

Riemann positions

Theorem: Riemann positions

Let $P_1, \cdots, P_4 \in \mathbb{F}_q$ such that $\sum P_i = [2]P$ and $P_i' = P - P_i$. Then,

$$\mathcal{H}\Big(\theta^A(P_1) \odot \theta^A(P_2)\Big) \odot \mathcal{H}\Big(\theta^A(P_3) \odot \theta^A(P_4)\Big) = \mathcal{H}\Big(\theta^A(P_1') \odot \theta^A(P_2')\Big) \odot \mathcal{H}\Big(\theta^A(P_3') \odot \theta^A(P_4')\Big)$$

- It is a differential addition mechanism:

$$\mathcal{H}\left(\theta^A(P+Q) \odot \theta^A(P-Q)\right) \odot \mathcal{H}\left(\theta^A(0)^{\odot 2}\right) = \mathcal{H}\left(\theta^A(P)^{\odot 2}\right) \odot \mathcal{H}\left(\theta^A(Q)^{\odot 2}\right)$$

- It is a triple addition mechanism:

$$\mathcal{H}\left(\theta^A(P+Q+R) \odot \theta^A(P)\right) \odot \mathcal{H}\left(\theta^A(Q) \odot \theta^A(R)\right) = \mathcal{H}\left(\theta^A(0) \odot \theta^A(Q+R)\right) \odot \mathcal{H}\left(\theta^A(P+R) \odot \theta^A(P+Q)\right)$$

Riemann positions

Theorem: Riemann positions

Let $P_1, \cdots, P_4 \in \mathbb{F}_q$ such that $\sum P_i = [2]P$ and $P_i' = P - P_i$. Then,

$$\mathcal{H}\Big(\theta^A(P_1) \odot \theta^A(P_2)\Big) \odot \mathcal{H}\Big(\theta^A(P_3) \odot \theta^A(P_4)\Big) = \mathcal{H}\Big(\theta^A(P_1') \odot \theta^A(P_2')\Big) \odot \mathcal{H}\Big(\theta^A(P_3') \odot \theta^A(P_4')\Big)$$

- It is a differential addition mechanism:

$$\mathcal{H}\left(\theta^A(P+Q) \odot \theta^A(P-Q)\right) \odot \mathcal{H}\left(\theta^A(0)^{\odot 2}\right) = \mathcal{H}\left(\theta^A(P)^{\odot 2}\right) \odot \mathcal{H}\left(\theta^A(Q)^{\odot 2}\right)$$

- It is a triple addition mechanism:

$$\mathcal{H}\left(\theta^A(P+Q+R) \odot \theta^A(P)\right) \odot \mathcal{H}\left(\theta^A(Q) \odot \theta^A(R)\right) = \mathcal{H}\left(\theta^A(0) \odot \theta^A(Q+R)\right) \odot \mathcal{H}\left(\theta^A(P+R) \odot \theta^A(P+Q)\right)$$

Riemann positions

Theorem: Riemann positions

Let $P_1, \cdots, P_4 \in \mathbb{F}_q$ such that $\sum P_i = [2]P$ and $P_i' = P - P_i$. Then,

$$\mathcal{H}\Big(\theta^A(P_1) \odot \theta^A(P_2)\Big) \odot \mathcal{H}\Big(\theta^A(P_3) \odot \theta^A(P_4)\Big) = \mathcal{H}\Big(\theta^A(P_1') \odot \theta^A(P_2')\Big) \odot \mathcal{H}\Big(\theta^A(P_3') \odot \theta^A(P_4')\Big)$$

- It is a differential addition mechanism:

$$\mathcal{H}\left(\theta^A(P+Q) \odot \theta^A(P-Q)\right) \odot \mathcal{H}\left(\theta^A(0)^{\odot 2}\right) = \mathcal{H}\left(\theta^A(P)^{\odot 2}\right) \odot \mathcal{H}\left(\theta^A(Q)^{\odot 2}\right)$$

- It is a triple addition mechanism:

$$\mathcal{H}\left(\theta^A(P+Q+R) \odot \theta^A(P)\right) \odot \mathcal{H}\left(\theta^A(Q) \odot \theta^A(R)\right) = \mathcal{H}\left(\theta^A(0) \odot \theta^A(Q+R)\right) \odot \mathcal{H}\left(\theta^A(P+R) \odot \theta^A(P+Q)\right)$$

Riemann positions

Theorem: Riemann positions

Let $P_1, \cdots, P_4 \in \mathbb{F}_q$ such that $\sum P_i = [2]P$ and $P_i' = P - P_i$. Then,

$$\mathcal{H}\Big(\theta^A(P_1) \odot \theta^A(P_2)\Big) \odot \mathcal{H}\Big(\theta^A(P_3) \odot \theta^A(P_4)\Big) = \mathcal{H}\Big(\theta^A(P_1') \odot \theta^A(P_2')\Big) \odot \mathcal{H}\Big(\theta^A(P_3') \odot \theta^A(P_4')\Big)$$

- It is a differential addition mechanism:

$$\mathcal{H}\left(\theta^A(P+Q) \odot \theta^A(P-Q)\right) \odot \mathcal{H}\left(\theta^A(0)^{\odot 2}\right) = \mathcal{H}\left(\theta^A(P)^{\odot 2}\right) \odot \mathcal{H}\left(\theta^A(Q)^{\odot 2}\right)$$

- It is a triple addition mechanism:

$$\mathcal{H}\left(\theta^A(P+Q+R) \odot \theta^A(P)\right) \odot \mathcal{H}\left(\theta^A(Q) \odot \theta^A(R)\right) = \mathcal{H}\left(\theta^A(0) \odot \theta^A(Q+R)\right) \odot \mathcal{H}\left(\theta^A(P+R) \odot \theta^A(P+Q)\right)$$

Isogenies and theta structure

Theorem: Duplication Formula

Let $K = \langle T_1, \cdots, T_g \rangle \subset A[2]$ and $\Phi : A \to B$ the $(\overbrace{2, \cdots, 2}^{g \text{ times}})$ isogeny with $\ker(\Phi) = K$. We then have the *Duplication Formula*:

$$\mathcal{H}\Big(\theta^A(P+Q) \odot \theta^A(P-Q)\Big) = \widetilde{\theta}^B(\Phi(P)) \odot \widetilde{\theta}^B(\Phi(Q))$$

$$\begin{tikzcd} E_0 \times E_1 \arrow[r, bend left, "(2^n{,}2^n)"] & E_2 \times E_3 \end{tikzcd}$$

Isogenies and theta structure

Theorem: Duplication Formula

Let $K = \langle T_1, \cdots, T_g \rangle \subset A[2]$ and $\Phi : A \to B$ the $(\overbrace{2, \cdots, 2}^{g \text{ times}})$ isogeny with $\ker(\Phi) = K$. We then have the *Duplication Formula*:

$$\mathcal{H}\Big(\theta^A(P+Q) \odot \theta^A(P-Q)\Big) = \widetilde{\theta}^B(\Phi(P)) \odot \widetilde{\theta}^B(\Phi(Q))$$

$$\begin{tikzcd}
E_0 \times E_1 \arrow[r] \arrow[rrrrrr, bend left, "{(2^n,2^n)}"] & J_1 \arrow[r] & J_2 \arrow[r] & \cdots \arrow[r] & J_{n-2} \arrow[r] & J_{n-1} \arrow[r] & E_2 \times E_3
\end{tikzcd}$$

Isogenies and theta structure

Theorem: Duplication Formula

Let $K = \langle T_1, \cdots, T_g \rangle \subset A[2]$ and $\Phi : A \to B$ the $(\overbrace{2, \cdots, 2}^{g \text{ times}})$ isogeny with $\ker(\Phi) = K$. We then have the *Duplication Formula*:

$$\mathcal{H}\Big(\theta^A(P+Q) \odot \theta^A(P-Q)\Big) = \widetilde{\theta}^B(\Phi(P)) \odot \widetilde{\theta}^B(\Phi(Q))$$

$$\begin{tikzcd}
E_0 \times E_1 \arrow[r] \arrow[d] \arrow[dr, "1"] \arrow[rrrrrr, bend left, "{(2^n,2^n)}"] & J_1 \arrow[r] \arrow[d, "\theta^{J_1}"] & J_2 \arrow[r] & \cdots \arrow[r] & J_{n-2} \arrow[r] & J_{n-1} \arrow[r] & E_2 \times E_3 \\
\mathcal{K}_{E_0} \times \mathcal{K}_{E_1} \arrow[r] & \mathcal{K}_{J_1} & & & & &
\end{tikzcd}$$

Isogenies and theta structure

Theorem: Duplication Formula

Let $K = \langle T_1, \cdots, T_g \rangle \subset A[2]$ and $\Phi : A \to B$ the $(\overbrace{2, \cdots, 2}^{g \text{ times}})$ isogeny with $\ker(\Phi) = K$. We then have the *Duplication Formula*:

$$\mathcal{H}\Big(\theta^A(P+Q) \odot \theta^A(P-Q)\Big) = \widetilde{\theta}^B(\Phi(P)) \odot \widetilde{\theta}^B(\Phi(Q))$$

$$\begin{tikzcd}
E_0 \times E_1 \arrow[r] \arrow[d] \arrow[dr, "1"] \arrow[rrrrrr, bend left, "{(2^n,2^n)}"] & J_1 \arrow[r] \arrow[d, "\theta^{J_1}"] & J_2 \arrow[r] \arrow[d, "\theta^{J_2}"] & \cdots \arrow[r] & J_{n-2} \arrow[r] \arrow[d, "\theta^{J_{n-2}}"'] & J_{n-1} \arrow[r] \arrow[d, "\theta^{J_{n-1}}"'] & E_2 \times E_3 \\
\mathcal{K}_{E_0} \times \mathcal{K}_{E_1} \arrow[r] & \mathcal{K}_{J_1} \arrow[r] & \mathcal{K}_{J_2} \arrow[r] & \cdots \arrow[r, "2"] & \mathcal{K}_{J_{n-2}} \arrow[r] & \mathcal{K}_{J_{n-1}} &
\end{tikzcd}$$

Isogenies and theta structure

Theorem: Duplication Formula

Let $K = \langle T_1, \cdots, T_g \rangle \subset A[2]$ and $\Phi : A \to B$ the $(\overbrace{2, \cdots, 2}^{g \text{ times}})$ isogeny with $\ker(\Phi) = K$. We then have the *Duplication Formula*:

$$\mathcal{H}\Big(\theta^A(P+Q) \odot \theta^A(P-Q)\Big) = \widetilde{\theta}^B(\Phi(P)) \odot \widetilde{\theta}^B(\Phi(Q))$$

$$\begin{tikzcd}
E_0 \times E_1 \arrow[r] \arrow[d] \arrow[dr, "1"] \arrow[rrrrrr, bend left, "{(2^n,2^n)}"] & J_1 \arrow[r] \arrow[d, "\theta^{J_1}"] & J_2 \arrow[r] \arrow[d, "\theta^{J_2}"] & \cdots \arrow[r] & J_{n-2} \arrow[r] \arrow[d, "\theta^{J_{n-2}}"'] & J_{n-1} \arrow[r] \arrow[d, "\theta^{J_{n-1}}"'] & E_2 \times E_3 \\
\mathcal{K}_{E_0} \times \mathcal{K}_{E_1} \arrow[r] & \mathcal{K}_{J_1} \arrow[r] & \mathcal{K}_{J_2} \arrow[r] & \cdots \arrow[r, "2"] & \mathcal{K}_{J_{n-2}} \arrow[r] & \mathcal{K}_{J_{n-1}} \arrow[r] \arrow[ur, "3"] & \mathcal{K}_{E_2} \times \mathcal{K}_{E_3} \arrow[u]
\end{tikzcd}$$

Table of Contents

Quizz on gluing

$$\Phi : E_1 \times E_2 \to J_1$$

$$\mathcal{H}\left(\theta^{E_1 \times E_2}(P+Q) \odot \theta^{E_1 \times E_2}(P-Q)\right) = \widetilde{\theta}^{J_1}(\Phi(P)) \odot \widetilde{\theta}^{J_1}(\Phi(Q))$$

Quizz on gluing

$$\Phi : E_1 \times E_2 \to J_1$$

$$\mathcal{H}\left(\theta^{E_1 \times E_2}(P+Q) \odot \theta^{E_1 \times E_2}(P-Q)\right) = \widetilde{\theta}^{J_1}\left(\Phi(P)\right) \odot \widetilde{\theta}^{J_1}\left(\Phi(Q)\right)$$

Quizz on gluing

$$\Phi : E_1 \times E_2 \to J_1$$

$$\mathcal{H}\Big(\theta^{E_1 \times E_2}(P+Q) \odot \theta^{E_1 \times E_2}(P-Q)\Big) = \widetilde{\theta}^{J_1}(\Phi(P)) \odot \widetilde{\theta}^{J_1}(\Phi(Q))$$

$$\theta^{E_1 \times E_2}(X) = \mathbf{M}(X_1 \otimes X_2) = \begin{pmatrix} \mathbf{M}_{0,0} & \mathbf{M}_{0,1} & \mathbf{M}_{0,2} & \mathbf{M}_{0,3} \\ \mathbf{M}_{1,0} & \mathbf{M}_{1,1} & \mathbf{M}_{1,2} & \mathbf{M}_{1,3} \\ \mathbf{M}_{2,0} & \mathbf{M}_{2,1} & \mathbf{M}_{2,2} & \mathbf{M}_{2,3} \\ \mathbf{M}_{3,0} & \mathbf{M}_{3,1} & \mathbf{M}_{3,2} & \mathbf{M}_{3,3} \end{pmatrix} \begin{pmatrix} x_1 x_2 \\ x_1 z_2 \\ z_1 x_2 \\ z_1 z_2 \end{pmatrix}$$

- How many components of $\mathbf{M}$ do we need to compute Φ ?

Quizz on gluing

$$\Phi : E_1 \times E_2 \to J_1$$

$$\mathcal{H}\left(\theta^{E_1 \times E_2}(P+Q) \odot \theta^{E_1 \times E_2}(P-Q)\right) = \widetilde{\theta}^{J_1}(\Phi(P)) \odot \widetilde{\theta}^{J_1}(\Phi(Q))$$

$$\theta^{E_1 \times E_2}(X) = \mathbf{M}(X_1 \otimes X_2) = \begin{pmatrix} \mathbf{M}_{0,0} & \mathbf{M}_{0,1} & \mathbf{M}_{0,2} & \mathbf{M}_{0,3} \\ \mathbf{M}_{1,0} & \cancel{\mathbf{M}_{1,1}} & \cancel{\mathbf{M}_{1,2}} & \cancel{\mathbf{M}_{1,3}} \\ \mathbf{M}_{2,0} & \cancel{\mathbf{M}_{2,1}} & \cancel{\mathbf{M}_{2,2}} & \cancel{\mathbf{M}_{2,3}} \\ \cancel{\mathbf{M}_{3,0}} & \cancel{\mathbf{M}_{3,1}} & \cancel{\mathbf{M}_{3,2}} & \cancel{\mathbf{M}_{3,3}} \end{pmatrix}$$

- Answer: **6.33** !
- Done by using the self-similarities of theta structure.

Computing the duplication formula

$$\Phi : E_1 \times E_2 \to J_1$$

$$\mathcal{H}\left(\theta^{E_1 \times E_2}(P+Q) \odot \theta^{E_1 \times E_2}(P-Q)\right) = \widetilde{\theta}^{J_1}\left(\Phi(P)\right) \odot \widetilde{\theta}^{J_1}\left(\Phi(Q)\right)$$

$$\theta^{E_1 \times E_2}(P+Q) \odot \theta^{E_1 \times E_2}(P-Q) = \left(\mathbf{M} \cdot (P^1_{\oplus} \otimes P^2_{\oplus})\right) \odot \left(\mathbf{M} \cdot (P^1_{\ominus} \otimes P^2_{\ominus})\right)$$

Computing the duplication formula

$$\Phi : E_1 \times E_2 \to J_1$$

$$\mathcal{H}\Big(\theta^{E_1 \times E_2}(P+Q) \odot \theta^{E_1 \times E_2}(P-Q)\Big) = \widetilde{\theta}^{J_1}(\Phi(P)) \odot \widetilde{\theta}^{J_1}(\Phi(Q))$$

$$\theta^{E_1 \times E_2}(P+Q) \odot \theta^{E_1 \times E_2}(P-Q) = \Big(\mathbf{M}\vec{u}\Big)^{\odot 2} - \Big(\mathbf{M}\vec{v}\Big)^{\odot 2}$$

$$\vec{u} = \begin{pmatrix} u_1 u_2 + v_1 v_2 \\ u_1 w_2 \\ w_1 u_2 \\ w_1 w_2 \end{pmatrix} \qquad \vec{v} = \begin{pmatrix} v_1 u_2 + u_1 v_2 \\ v_1 w_2 \\ w_1 v_2 \\ 0 \end{pmatrix}$$

Using $(u_i \mp v_i : w_i) = P_i \pm Q_i$.

Computing the duplication formula

$$\Phi : E_1 \times E_2 \to J_1$$

$$\mathcal{H}\Big(\theta^{E_1\times E_2}(P+Q) \odot \theta^{E_1\times E_2}(P-Q)\Big) = \widetilde{\theta}^{J_1}(\Phi(P)) \odot \widetilde{\theta}^{J_1}(\Phi(Q))$$

$$\begin{aligned}
\theta^{E_1\times E_2}(P+Q) \odot \theta^{E_1\times E_2}(P-Q) = {} & [\mathbf{M}_0\mathbf{M}_0](u_1^2 - v_1^2)(u_2^2 - v_2^2) + [\mathbf{M}_1\mathbf{M}_1]w_2^2(u_1^2 - v_1^2) \\
& + [\mathbf{M}_2\mathbf{M}_2]w_1^2(u_2^2 - v_2^2) + [\mathbf{M}_3\mathbf{M}_3]w_1^2 w_2^2 \\
& + 2[\mathbf{M}_0\mathbf{M}_1]u_2 w_2(u_1^2 - v_1^2) + 2[\mathbf{M}_2\mathbf{M}_3]u_2 w_2 w_1^2 \\
& + 2[\mathbf{M}_0\mathbf{M}_2]u_1 w_1(u_2^2 - v_2^2) + 2[\mathbf{M}_1\mathbf{M}_3]u_1 w_1 w_2^2 \\
& + 2[\mathbf{M}_0\mathbf{M}_3 + \mathbf{M}_1\mathbf{M}_2]u_1 u_2 w_1 w_2 \\
& + 2[\mathbf{M}_0\mathbf{M}_3 - \mathbf{M}_1\mathbf{M}_2]v_1 v_2 w_1 w_2
\end{aligned}$$

Using $(u_i \mp v_i : w_i) = P_i \pm Q_i$.

Computing the duplication formula

$$\Phi : E_1 \times E_2 \to J_1$$

$$\mathcal{H}\Big(\theta^{E_1\times E_2}(P+Q) \odot \theta^{E_1\times E_2}(P-Q)\Big) = \widetilde{\theta}^{J_1}(\Phi(P)) \odot \widetilde{\theta}^{J_1}(\Phi(Q))$$

$$\begin{aligned}
\mathcal{H}\left(\theta^{E_1\times E_2}(P+Q) \odot \theta^{E_1\times E_2}(P-Q)\right) = {} & [\widetilde{\mathbf{M}_0\mathbf{M}_0}](u_1^2 - v_1^2)(u_2^2 - v_2^2) + [\widetilde{\mathbf{M}_1\mathbf{M}_1}]w_2^2(u_1^2 - v_1^2) \\
& + [\widetilde{\mathbf{M}_2\mathbf{M}_2}]w_1^2(u_2^2 - v_2^2) + [\widetilde{\mathbf{M}_3\mathbf{M}_3}]w_1^2 w_2^2 \\
& + 2[\widetilde{\mathbf{M}_0\mathbf{M}_1}]u_2 w_2(u_1^2 - v_1^2) + 2[\widetilde{\mathbf{M}_2\mathbf{M}_3}]u_2 w_2 w_1^2 \\
& + 2[\widetilde{\mathbf{M}_0\mathbf{M}_2}]u_1 w_1(u_2^2 - v_2^2) + 2[\widetilde{\mathbf{M}_1\mathbf{M}_3}]u_1 w_1 w_2^2 \\
& + 2[\widetilde{\mathbf{M}_0\mathbf{M}_3} + \widetilde{\mathbf{M}_1\mathbf{M}_2}]u_1 u_2 w_1 w_2 \\
& + 2[\widetilde{\mathbf{M}_0\mathbf{M}_3} - \widetilde{\mathbf{M}_1\mathbf{M}_2}]v_1 v_2 w_1 w_2
\end{aligned}$$

Using $(u_i \mp v_i : w_i) = P_i \pm Q_i$.

Overview of Superglue

- $\mathbf{M}_i = \theta^{E_1 \times E_2}(C^{\delta_{10 \cdot i}} \otimes C^{\delta_{01 \cdot i}})$ with $C = (0 : 1)$.
- $\widetilde{\mathbf{M}_i \mathbf{M}_j}$ are couples of points in $J_1[4]$.
- Using the self-similarities of theta structures:
  - Of the 10 couples of points, we only need 4.
  - Of those 4, at least 2 are sparse.
  - The rest is retrieved from the position of $C \in \ker(\Phi)$.

▶ 9 cases yielding 9 distinct set of equations.

Overview of Superglue

- $\mathbf{M}_i = \theta^{E_1 \times E_2}(C^{\delta_{10 \cdot i}} \otimes C^{\delta_{01 \cdot i}})$ with $C = (0:1)$.
- $\widetilde{\mathbf{M}_i \mathbf{M}_j}$ are couples of points in $J_1[4]$.
- Using the self-similarities of theta structures:
  - Of the 10 couples of points, we only need 4.
  - Of those 4, at least 2 are sparse.
  - The rest is retrieved from the position of $C \in \ker(\Phi)$.

▶ 9 cases yielding 9 distinct set of equations.

Overview of Superglue

- $\mathbf{M}_i = \theta^{E_1 \times E_2}(C^{\delta_{10 \cdot i}} \otimes C^{\delta_{01 \cdot i}})$ with $C = (0 : 1)$.
- $\widetilde{\mathbf{M}_i \mathbf{M}_j}$ are couples of points in $J_1[4]$.
- Using the self-similarities of theta structures:
  - Of the 10 couples of points, we only need 4.
  - Of those 4, at least 2 are sparse.
  - The rest is retrieved from the position of $C \in \ker(\Phi)$.

▶ 9 cases yielding 9 distinct set of equations.

Overview of Superglue

- $\mathbf{M}_i = \theta^{E_1 \times E_2}(C^{\delta_{10 \cdot i}} \otimes C^{\delta_{01 \cdot i}})$ with $C = (0:1)$.
- $\widetilde{\mathbf{M}_i \mathbf{M}_j}$ are couples of points in $J_1[4]$.
- Using the self-similarities of theta structures:
  - Of the 10 couples of points, we only need 4.
  - Of those 4, at least 2 are sparse.
  - The rest is retrieved from the position of $C \in \ker(\Phi)$.

▶ 9 cases yielding 9 distinct set of equations.

Superglue formulae (Type I)

Theorem: Superglue in position 01

Let $\theta^{E_1 \times E_2}$ be a theta structure induced by the symplectic basis of $\langle (0, C), (C, 0) \rangle \oplus \langle (C, \alpha), (\beta, C) \rangle$ with $\mathbf{M}$ its change of basis matrix. For any $P, Q \in E_1 \times E_2$ we have that

$$\mathcal{H}(\theta^{E_1 \times E_2}(P + Q) \odot \theta^{E_1 \times E_2}(P - Q)) =$$

$$\begin{aligned}
&[\widetilde{\mathbf{M}_0 \mathbf{M}_0}](u_1^2 - v_1^2)(u_2^2 - v_2^2) + [\widetilde{\mathbf{M}_1 \mathbf{M}_1}] w_2^2 (u_1^2 - v_1^2) + [\widetilde{\mathbf{M}_2 \mathbf{M}_2}] w_1^2 (u_2^2 - v_2^2) + [\widetilde{\mathbf{M}_3 \mathbf{M}_3}] w_1^2 w_2^2 \\
&+ 2[\widetilde{\mathbf{M}_0 \mathbf{M}_1}] u_2 w_2 (u_1^2 - v_1^2) + 2[\widetilde{\mathbf{M}_2 \mathbf{M}_3}] u_2 w_2 w_1^2 \\
&+ 2[\widetilde{\mathbf{M}_0 \mathbf{M}_2}] u_1 w_1 (u_2^2 - v_2^2) + 2[\widetilde{\mathbf{M}_1 \mathbf{M}_3}] u_1 w_1 w_2^2 \\
&+ 2[\widetilde{\mathbf{M}_0 \mathbf{M}_3} + \widetilde{\mathbf{M}_1 \mathbf{M}_2}] u_1 u_2 w_1 w_2 + 2[\widetilde{\mathbf{M}_0 \mathbf{M}_3} - \widetilde{\mathbf{M}_1 \mathbf{M}_2}] v_1 v_2 w_1 w_2
\end{aligned}$$

Superglue formulae (Type I)

Theorem: Superglue in position 01

Let $\theta^{E_1 \times E_2}$ be a theta structure induced by the symplectic basis of $\langle (0,C),(C,0)\rangle \oplus \langle (C,\alpha),(\beta,C)\rangle$ with $\mathbf{M}$ its change of basis matrix. For any $P, Q \in E_1 \times E_2$ we have that

$$\mathcal{H}(\theta^{E_1\times E_2}(P+Q) \odot \theta^{E_1\times E_2}(P-Q)) =$$

$$\begin{pmatrix} {\mathbf{M}_{1,0}}^2 + {\mathbf{M}_{2,0}}^2 \\ {\mathbf{M}_{0,0}}^2 - {\mathbf{M}_{1,0}}^2 \\ {\mathbf{M}_{0,0}}^2 - {\mathbf{M}_{2,0}}^2 \\ 0 \end{pmatrix} \odot \begin{pmatrix} (u_1^2 - v_1^2 + w_1^2)(u_2^2 - v_2^2 + w_2^2) \\ (u_1^2 - v_1^2 + w_1^2)(u_2^2 - v_2^2 - w_2^2) \\ (u_1^2 - v_1^2 - w_1^2)(u_2^2 - v_2^2 + w_2^2) \\ 0 \end{pmatrix} + 2u_2w_2 \begin{pmatrix} \mathbf{M}_{0,0}\mathbf{M}_{0,1} + \mathbf{M}_{0,2}\mathbf{M}_{0,3} \\ 0 \\ \mathbf{M}_{0,0}\mathbf{M}_{0,1} - \mathbf{M}_{0,2}\mathbf{M}_{0,3} \\ 0 \end{pmatrix} \odot \begin{pmatrix} u_1^2 - v_1^2 + w_1^2 \\ 0 \\ u_1^2 - v_1^2 - w_1^2 \\ 0 \end{pmatrix}$$

$$+ 2u_1w_1 \begin{pmatrix} \mathbf{M}_{0,0}\mathbf{M}_{0,2} + \mathbf{M}_{0,1}\mathbf{M}_{0,3} \\ \mathbf{M}_{0,0}\mathbf{M}_{0,2} - \mathbf{M}_{0,1}\mathbf{M}_{0,3} \\ 0 \\ 0 \end{pmatrix} \odot \begin{pmatrix} u_2^2 - v_2^2 + w_2^2 \\ u_2^2 - v_2^2 - w_2^2 \\ 0 \\ 0 \end{pmatrix} + 4w_1w_2 \begin{pmatrix} \mathbf{M}_{0,0}\mathbf{M}_{0,3} + \mathbf{M}_{0,1}\mathbf{M}_{0,3} \\ 0 \\ 0 \\ \mathbf{M}_{0,0}\mathbf{M}_{0,3} - \mathbf{M}_{0,1}\mathbf{M}_{0,3} \end{pmatrix} \odot \begin{pmatrix} u_1u_2 \\ 0 \\ 0 \\ v_1v_2 \end{pmatrix}$$

Why bother ?

Algorithms	Classic gluing	Superglue
ThetaChangeOfBasis	$113\mathbf{M} + 8\mathbf{S} + 1\mathbf{I} + 49\mathbf{a}$	$37\mathbf{M} + 7\mathbf{S} + 34\mathbf{a}$
GluingCodomain	$167\mathbf{M} + 16\mathbf{S} + 1\mathbf{I} + 105\mathbf{a}$	$98\mathbf{M} + 19\mathbf{S} + 94\mathbf{a}$
GluingEval	$40\mathbf{M} + 8\mathbf{S} + 44\mathbf{a}$	$27\mathbf{M} + 2\mathbf{S} + 24\mathbf{a}$
GluingEvalSpecial	$23\mathbf{M} + 4\mathbf{S} + 28\mathbf{a}$	$20\mathbf{M} + 4\mathbf{S} + 20\mathbf{a}$

Table: Cost comparison between classic gluing and Superglue

- Also works on quadratic twist.
- Should generalises to dimension g (*only* 3^g distinct cases to handle[1]).

- *Open question: Is it interesting for generic* $(2, 2)$ *isogenies ?*

[1] + endless fun in debugging.

Why bother ?

Algorithms	Classic gluing	Superglue
ThetaChangeOfBasis	$113\mathbf{M} + 8\mathbf{S} + 1\mathbf{I} + 49\mathbf{a}$	$37\mathbf{M} + 7\mathbf{S} + 34\mathbf{a}$
GluingCodomain	$167\mathbf{M} + 16\mathbf{S} + 1\mathbf{I} + 105\mathbf{a}$	$98\mathbf{M} + 19\mathbf{S} + 94\mathbf{a}$
GluingEval	$40\mathbf{M} + 8\mathbf{S} + 44\mathbf{a}$	$27\mathbf{M} + 2\mathbf{S} + 24\mathbf{a}$
GluingEvalSpecial	$23\mathbf{M} + 4\mathbf{S} + 28\mathbf{a}$	$20\mathbf{M} + 4\mathbf{S} + 20\mathbf{a}$

Table: Cost comparison between classic gluing and Superglue

- Also works on quadratic twist.
- Should generalises to dimension g (*only* 3^g distinct cases to handle[1]).

▶ *Open question: Is it interesting for generic* $(2,2)$ *isogenies ?*

[1] + endless fun in debugging.

Why bother ?

Algorithms	Classic gluing	Superglue
ThetaChangeOfBasis	$113\mathbf{M} + 8\mathbf{S} + 1\mathbf{I} + 49\mathbf{a}$	$37\mathbf{M} + 7\mathbf{S} + 34\mathbf{a}$
GluingCodomain	$167\mathbf{M} + 16\mathbf{S} + 1\mathbf{I} + 105\mathbf{a}$	$98\mathbf{M} + 19\mathbf{S} + 94\mathbf{a}$
GluingEval	$40\mathbf{M} + 8\mathbf{S} + 44\mathbf{a}$	$27\mathbf{M} + 2\mathbf{S} + 24\mathbf{a}$
GluingEvalSpecial	$23\mathbf{M} + 4\mathbf{S} + 28\mathbf{a}$	$20\mathbf{M} + 4\mathbf{S} + 20\mathbf{a}$

Table: Cost comparison between classic gluing and Superglue

- Also works on quadratic twist.
- Should generalises to dimension g (*only* 3^g distinct cases to handle[1]).

▸ *Open question: Is it interesting for generic* $(2,2)$ *isogenies ?*

[1] + endless fun in debugging.

Why bother ?

Algorithms	Classic gluing	Superglue
ThetaChangeOfBasis	$113\mathbf{M} + 8\mathbf{S} + 1\mathbf{I} + 49\mathbf{a}$	$37\mathbf{M} + 7\mathbf{S} + 34\mathbf{a}$
GluingCodomain	$167\mathbf{M} + 16\mathbf{S} + 1\mathbf{I} + 105\mathbf{a}$	$98\mathbf{M} + 19\mathbf{S} + 94\mathbf{a}$
GluingEval	$40\mathbf{M} + 8\mathbf{S} + 44\mathbf{a}$	$27\mathbf{M} + 2\mathbf{S} + 24\mathbf{a}$
GluingEvalSpecial	$23\mathbf{M} + 4\mathbf{S} + 28\mathbf{a}$	$20\mathbf{M} + 4\mathbf{S} + 20\mathbf{a}$

Table: Cost comparison between classic gluing and Superglue

- Also works on quadratic twist.
- Should generalises to dimension g (*only* 3^g distinct cases to handle[1]).

▶ *Open question: Is it interesting for generic* $(2,2)$ *isogenies ?*

[1] + endless fun in debugging.

The end

$$
\begin{pmatrix} {\mathbf{M}_{1,0}}^2 + {\mathbf{M}_{2,0}}^2 \\ {\mathbf{M}_{0,0}}^2 - {\mathbf{M}_{1,0}}^2 \\ {\mathbf{M}_{0,0}}^2 - {\mathbf{M}_{2,0}}^2 \\ 0 \end{pmatrix} \odot \begin{pmatrix} (u_1^2 - v_1^2 - w_1^2)(u_2^2 - v_2^2 + w_2^2) \\ (u_1^2 - v_1^2 + w_1^2)(u_2^2 - v_2^2 - w_2^2) \\ (u_1^2 - v_1^2 + w_1^2)(u_2^2 - v_2^2 + w_2^2) \\ 0 \end{pmatrix} + 2u_2 w_2 \begin{pmatrix} \mathbf{M}_{0,0}\mathbf{M}_{0,1} - \mathbf{M}_{0,2}\mathbf{M}_{0,3} \\ 0 \\ \mathbf{M}_{0,0}\mathbf{M}_{0,1} + \mathbf{M}_{0,2}\mathbf{M}_{0,3} \\ 0 \end{pmatrix} \odot \begin{pmatrix} u_1^2 - v_1^2 - w_1^2 \\ 0 \\ u_1^2 - v_1^2 + w_1^2 \\ 0 \end{pmatrix}
$$

$$
+ 2u_1 w_1 \begin{pmatrix} 0 \\ \mathbf{M}_{0,0}\mathbf{M}_{0,2} - \mathbf{M}_{0,1}\mathbf{M}_{0,3} \\ \mathbf{M}_{0,0}\mathbf{M}_{0,2} + \mathbf{M}_{0,1}\mathbf{M}_{0,3} \\ 0 \end{pmatrix} \odot \begin{pmatrix} 0 \\ u_2^2 - v_2^2 - w_2^2 \\ u_2^2 - v_2^2 + w_2^2 \\ 0 \end{pmatrix} + 4w_1 w_2 \begin{pmatrix} 0 \\ 0 \\ \mathbf{M}_{0,0}\mathbf{M}_{0,3} + \mathbf{M}_{0,1}\mathbf{M}_{0,3} \\ \mathbf{M}_{0,0}\mathbf{M}_{0,3} - \mathbf{M}_{0,1}\mathbf{M}_{0,3} \end{pmatrix} \odot \begin{pmatrix} 0 \\ 0 \\ u_1 u_2 \\ v_1 v_2 \end{pmatrix}
$$

HD isogenies are fun !!

Thank you for your attention !

- eprint 2025/736.

Type II formulae (position 00)

Theorem: Superglue in position 00

Let $\theta^{E_1 \times E_2}$ be the theta structure induced by the symplectic basis of $\langle (0,\beta),(C,0)\rangle \oplus \langle (C,C),(\alpha,\beta)\rangle$ with $\mathbf{M}$ its change of basis matrix. For any $P, Q \in E_1 \times E_2$ we have that

$$\mathcal{H}(\theta^{E_1\times E_2}(P+Q) \odot \theta^{E_1\times E_2}(P-Q)) =$$

$$\begin{pmatrix} \mathbf{M_{1,0}}^2 + \mathbf{M_{2,0}}^2 \\ \mathbf{M_{0,0}}^2 - \mathbf{M_{1,0}}^2 \\ \mathbf{M_{0,0}}^2 - \mathbf{M_{2,0}}^2 \\ 0 \end{pmatrix} \odot \begin{pmatrix} (u_1^2 - v_1^2 + w_1^2)(u_2^2 - v_2^2 + w_2^2) \\ (u_1^2 - v_1^2 + w_1^2)(u_2^2 - v_2^2 + w_2^2) \\ (u_1^2 - v_1^2 - w_1^2)(u_2^2 - v_2^2 - w_2^2) \\ 0 \end{pmatrix} + 2u_2 w_2 \begin{pmatrix} \mathbf{M_{0,0}M_{0,1}} + \mathbf{M_{1,0}M_{1,1}} \\ \mathbf{M_{0,0}M_{0,1}} - \mathbf{M_{1,0}M_{1,1}} \\ 0 \\ 0 \end{pmatrix} \odot \begin{pmatrix} u_1^2 - v_1^2 + w_1^2 \\ u_1^2 - v_1^2 + w_1^2 \\ 0 \\ 0 \end{pmatrix}$$

$$+ (-1)^{\mathbf{M}_{0,1} = -\mathbf{M}_{0,2}} \left(2u_1 w_1 \begin{pmatrix} \mathbf{M_{0,0}M_{0,1}} - \mathbf{M_{1,0}M_{1,1}} \\ \mathbf{M_{0,0}M_{0,1}} + \mathbf{M_{1,0}M_{1,1}} \\ 0 \\ 0 \end{pmatrix} \odot \begin{pmatrix} u_2^2 - v_2^2 + w_2^2 \\ u_2^2 - v_2^2 + w_2^2 \\ 0 \\ 0 \end{pmatrix} + 4w_1 w_2 \begin{pmatrix} \mathbf{M_{0,0}}^2 - \mathbf{M_{1,0}}^2 \\ \mathbf{M_{1,0}}^2 + \mathbf{M_{2,0}}^2 \\ 0 \\ \mathbf{M_{0,0}}^2 - \mathbf{M_{2,0}}^2 \end{pmatrix} \odot \begin{pmatrix} u_1 u_2 \\ u_1 u_2 \\ 0 \\ v_1 v_2 \end{pmatrix} \right)$$

columns	theta points		columns	dual theta points
$\mathbf{M}_0\mathbf{M}_0$	$\theta^{E_1\times E_2}(0,0)\theta^{E_1\times E_2}(0,0)$	$\Longleftrightarrow$	$\widetilde{\mathbf{M}_0\mathbf{M}_0}$	$\widetilde{\theta}^{J_1}(\Phi(0,0))\widetilde{\theta}^{J_1}(\Phi(0,0))$
$\mathbf{M}_1\mathbf{M}_1$	$\theta^{E_1\times E_2}(0,C)\theta^{E_1\times E_2}(0,C)$	$\Longleftrightarrow$	$\widetilde{\mathbf{M}_1\mathbf{M}_1}$	$\widetilde{\theta}^{J_1}(\Phi(0,0))\widetilde{\theta}^{J_1}(\Phi(0,C))$
$\mathbf{M}_2\mathbf{M}_2$	$\theta^{E_1\times E_2}(C,0)\theta^{E_1\times E_2}(C,0)$	$\Longleftrightarrow$	$\widetilde{\mathbf{M}_2\mathbf{M}_2}$	$\widetilde{\theta}^{J_1}(\Phi(0,0))\widetilde{\theta}^{J_1}(\Phi(C,0))$
$\mathbf{M}_3\mathbf{M}_3$	$\theta^{E_1\times E_2}(C,C)\theta^{E_1\times E_2}(C,C)$	$\Longleftrightarrow$	$\widetilde{\mathbf{M}_3\mathbf{M}_3}$	$\widetilde{\theta}^{J_1}(\Phi(0,0))\widetilde{\theta}^{J_1}(\Phi(C,C))$
$\mathbf{M}_0\mathbf{M}_1$	$\theta^{E_1\times E_2}(0,0)\theta^{E_1\times E_2}(0,C)$	$\Longleftrightarrow$	$\widetilde{\mathbf{M}_0\mathbf{M}_1}$	$\widetilde{\theta}^{J_1}(\Phi(0,C'))\widetilde{\theta}^{J_1}(\Phi(0,C'))$
$\mathbf{M}_2\mathbf{M}_3$	$\theta^{E_1\times E_2}(C,0)\theta^{E_1\times E_2}(C,C)$	$\Longleftrightarrow$	$\widetilde{\mathbf{M}_2\mathbf{M}_3}$	$\widetilde{\theta}^{J_1}(\Phi(0,C'))\widetilde{\theta}^{J_1}(\Phi(C,C'))$
$\mathbf{M}_0\mathbf{M}_2$	$\theta^{E_1\times E_2}(0,0)\theta^{E_1\times E_2}(C,0)$	$\Longleftrightarrow$	$\widetilde{\mathbf{M}_0\mathbf{M}_2}$	$\widetilde{\theta}^{J_1}(\Phi(C',0))\widetilde{\theta}^{J_1}(\Phi(C',0))$
$\mathbf{M}_1\mathbf{M}_3$	$\theta^{E_1\times E_2}(0,C)\theta^{E_1\times E_2}(C,C)$	$\Longleftrightarrow$	$\widetilde{\mathbf{M}_1\mathbf{M}_3}$	$\widetilde{\theta}^{J_1}(\Phi(C',0))\widetilde{\theta}^{J_1}(\Phi(C',C))$
$\mathbf{M}_0\mathbf{M}_3$	$\theta^{E_1\times E_2}(0,0)\theta^{E_1\times E_2}(C,C)$	$\Longleftrightarrow$	$\widetilde{\mathbf{M}_0\mathbf{M}_3}$	$\widetilde{\theta}^{J_1}(\Phi(C',C'))\widetilde{\theta}^{J_1}(\Phi(C',C'))$
$\mathbf{M}_1\mathbf{M}_2$	$\theta^{E_1\times E_2}(0,C)\theta^{E_1\times E_2}(C,0)$	$\Longleftrightarrow$	$\widetilde{\mathbf{M}_1\mathbf{M}_2}$	$\widetilde{\theta}^{J_1}(\Phi(C',C'))\widetilde{\theta}^{J_1}(\Phi(C',-C'))$

Table: Correspondence between product of columns and theta points with $C = (0:1)$ and $C' = (1:\pm 1)$.

Where are the C points

Position	**Type**	$\ker(\Phi)$	$(C,0)$	$(0,C)$	(C,C)
00	II	$\langle (C,C),(\alpha,\beta)\rangle$	S_2	S_2+T_1	T_1
01	I	$\langle (C,\beta),(\alpha,C)\rangle$	S_2	S_1	S_1+S_2
02	I	$\langle (C,\beta),(\alpha,\beta^{-1})\rangle$	S_2	$S_1+S_2+T_1$	S_1+T_1
10	I	$\langle (\alpha,C),(C,\beta)\rangle$	S_1+T_2	S_2+T_1	$S_1+S_2+T_1+T_2$
11	II	$\langle (\alpha,\beta),(C,C)\rangle$	S_1+T_2	S_1	T_2
12	I	$\langle (\alpha,\beta),(C,\beta^{-1})\rangle$	S_1+T_2	$S_1+S_2+T_1$	$S_2+T_1+T_2$
20	I	$\langle (\alpha,C),(\alpha^{-1},\beta)\rangle$	$S_1+S_2+T_2$	S_2+T_1	$S_1+T_1+T_2$
21	I	$\langle (\alpha,\beta),(\alpha^{-1},C)\rangle$	$S_1+S_2+T_2$	S_1	S_2+T_2
22	II	$\langle (\alpha,\beta),(\alpha^{-1},\beta^{-1})\rangle$	$S_1+S_2+T_2$	$S_1+S_2+T_1$	T_1+T_2

Table: Different positions of $C=(0:1)$ points in the symplectic basis depending on the kernel

Supergluing elliptic curves

- **pos** $= 0$:

$$\mathcal{H}\left(\theta^{E_1}(P+Q)\odot\theta^{E_1}(P-Q)\right) = \begin{pmatrix} b^2\left((u\pm w)^2 - v^2\right) + a^2\left((u\mp w)^2 - v^2\right) \\ 2ab(u^2 - v^2 - w^2) \end{pmatrix}$$

- **pos** $= 1$:

$$\mathcal{H}\left(\theta^{E_1}(P+Q)\odot\theta^{E_1}(P-Q)\right) = \begin{pmatrix} b^2\left((u\pm w)^2 - v^2\right) + a^2\left((u\mp w)^2 - v^2\right) \\ b^2\left((u\pm w)^2 - v^2\right) - a^2\left((u\mp w)^2 - v^2\right) \end{pmatrix}$$

- **pos** $= 2$:

$$\mathcal{H}\left(\theta^{E_1}(P+Q)\odot\theta^{E_1}(P-Q)\right) = \begin{pmatrix} 2ab(u^2 - v^2 - w^2) \\ b^2\left((u\pm w)^2 - v^2\right) + a^2\left((u\mp w)^2 - v^2\right) \end{pmatrix}$$