Superglue: Fast formulae for $(2,2)$-gluing isogenies

Max Duparc

Asiacrypt 2025: Melbourne

This talk is about ✈️

HD isogenies are everywhere in isogeny based crypto

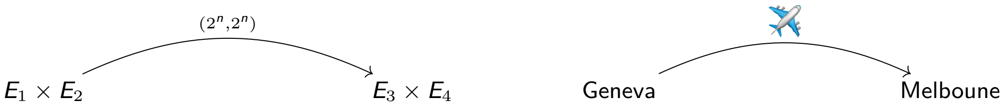
This talk is about ✈️

HD isogenies are everywhere in isogeny based crypto

$$E_1 \times E_2 \xrightarrow{(2^n,2^n)} E_3 \times E_4$$

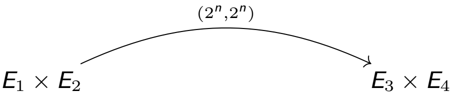
This talk is about ✈️

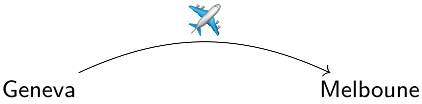
HD isogenies are everywhere in isogeny based crypto



This talk is about ✈️

HD isogenies are everywhere in isogeny based crypto





- The first step is the slowest.
  - Be at airport 3h before take off.

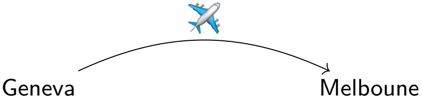
This talk is about ✈️

HD isogenies are everywhere in isogeny based crypto

$$E_1 \times E_2 \xrightarrow{(2^n,2^n)} E_3 \times E_4$$

$$E_1 \times E_2 \xrightarrow{(2,2)} A_1 \xrightarrow{(2,2)} \cdots \xrightarrow{(2,2)} A_{n-1} \xrightarrow{(2,2)} E_3 \times E_4$$

- The first step is the slowest.
- ▶ Gluing isogeny.



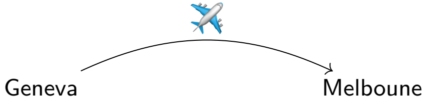
- The first step is the slowest.
- ▶ Be at airport 3h before take off.

This talk is about ✈️

HD isogenies are everywhere in isogeny based crypto

$$E_1 \times E_2 \xrightarrow{(2,2)} A_1 \xrightarrow{(2,2)} \cdots \xrightarrow{(2,2)} A_{n-1} \xrightarrow{(2,2)} E_3 \times E_4$$

$$E_1 \times E_2 \xrightarrow{(2^n,2^n)} E_3 \times E_4$$



- The first step is the slowest.
  - Gluing isogeny.

- The first step is the slowest.
  - Be at airport 3h before take off.

This work

Construct a "fast line" for isogenies.

What happens at the airport ?

φ

What happens at the airport ?

✈️

We fly using *aiplanes* !

φ

We "fly" using *theta structures* !

$$\theta^A : A_{/\pm 1} \longrightarrow \mathbb{P}^3$$

What happens at the airport ?

✈️

We fly using *aiplanes* !

1. Pass TSA.

φ

We "fly" using *theta structures* !

$$\theta^A : A_{/\pm 1} \longrightarrow \mathbb{P}^3$$

1. Sanity check your input.

What happens at the airport ?

✈️

We fly using *aiplanes* !

1. Pass TSA.
2. Get into the right ✈️.

φ

We “fly” using *theta structures* !

$$\theta^A : A_{/\pm 1} \longrightarrow \mathbb{P}^3$$

1. Sanity check your input.
2. Construct the good theta structure.

What happens at the airport ?

✈️

We fly using *aiplanes* !

1. Pass TSA.
2. Get into the right ✈️.
3. Go to the runway.

φ

We "fly" using *theta structures* !

$$\theta^A : A_{/\pm 1} \longrightarrow \mathbb{P}^3$$

1. Sanity check your input.
2. Construct the good theta structure.
3. Compute your codomain.

What happens at the airport ?

✈️

We fly using *aiplanes* !

1. Pass TSA.
2. Get into the right ✈️.
3. Go to the runway.
4. Lift off.

φ

We "fly" using *theta structures* !

$$\theta^A : A_{/\pm 1} \longrightarrow \mathbb{P}^3$$

1. Sanity check your input.
2. Construct the good theta structure.
3. Compute your codomain.
4. Evaluate $\Phi : E_1 \times E_2 \longrightarrow A_1$.

What happens at the airport ?

✈️

We fly using *aiplanes* !

1. Pass TSA.
2. Get into the right ✈️.
3. Go to the runway.
4. Lift off.

φ

We "fly" using *theta structures* !

$$\theta^A : A_{/\pm 1} \longrightarrow \mathbb{P}^3$$

1. Sanity check your input.
2. Construct the good theta structure.
3. Compute your codomain.
4. Evaluate $\Phi : E_1 \times E_2 \longrightarrow A_1$.

This work

Improved 2. to 4.

The speed-up

Algo	**Previous gluing**	**This work**
ComputeTheta	$100\mathbf{M} + 8\mathbf{S} + 4\mathbf{I} + 49\mathbf{a}$	$38\mathbf{M} + 7\mathbf{S} + 34\mathbf{a}$
GluingCodomain	$179\mathbf{M} + 24\mathbf{S} + 5\mathbf{I} + 113\mathbf{a}$	$94\mathbf{M} + 23\mathbf{S} + 82\mathbf{a}$
GluingEval	$45\mathbf{M} + 8\mathbf{S} + 1\mathbf{I} + 48\mathbf{a}$	$26\mathbf{M} + 2\mathbf{S} + 26\mathbf{a}$
GluingEvalSpecial	$22\mathbf{M} + 4\mathbf{S} + 28\mathbf{a}$	$19\mathbf{M} + 4\mathbf{S} + 18\mathbf{a}$

Table: Cost comparison between old gluing and this work

The speed-up

Algo	**Previous gluing**	**This work**
ComputeTheta	$100\mathbf{M} + 8\mathbf{S} + 4\mathbf{I} + 49\mathbf{a}$	$38\mathbf{M} + 7\mathbf{S} + 34\mathbf{a}$
GluingCodomain	$179\mathbf{M} + 24\mathbf{S} + 5\mathbf{I} + 113\mathbf{a}$	$94\mathbf{M} + 23\mathbf{S} + 82\mathbf{a}$
GluingEval	$45\mathbf{M} + 8\mathbf{S} + 1\mathbf{I} + 48\mathbf{a}$	$26\mathbf{M} + 2\mathbf{S} + 26\mathbf{a}$
GluingEvalSpecial	$22\mathbf{M} + 4\mathbf{S} + 28\mathbf{a}$	$19\mathbf{M} + 4\mathbf{S} + 18\mathbf{a}$

Table: Cost comparison between old gluing and this work

$\log(p) = 256$	**Previously**	**This work**
Gluing	51μs	20μs
$(2^{126}, 2^{126})$	861μs	832μs

Table: Speed-up on Rust implementation

Theta structures

Theta structures are linear algebra !!

Theta structures

Theta structures are linear algebra !!

$$\theta^{E_1 \times E_2} : E_1 \times E_2 \longrightarrow \mathbb{P}^3 \quad \rightsquigarrow \quad \Theta^{E_1 \times E_2} \in \mathsf{PGL}_4(\mathbb{F}_q)$$

Theta structures

Theta structures are linear algebra !!

$$\theta^{E_1 \times E_2} : E_1 \times E_2 \longrightarrow \mathbb{P}^3 \quad \rightsquigarrow \quad \Theta^{E_1 \times E_2} \in \mathsf{PGL}_4(\mathbb{F}_q)$$

Symplectic basis

$$A[2] = \langle S_1, S_2; T_1, T_2 \rangle \text{ with } e_2(S_1, S_2) = e_N(T_1, T_2) = 1, \quad e_2(S_i, T_j) = (-1)^{\delta_{ij}}$$

Theta structures

Theta structures are linear algebra !!

$$\theta^{E_1 \times E_2} : E_1 \times E_2 \longrightarrow \mathbb{P}^3 \quad \rightsquigarrow \quad \Theta^{E_1 \times E_2} \in \mathrm{PGL}_4(\mathbb{F}_q)$$

Symplectic basis

$$A[2] = \langle S_1, S_2; T_1, T_2 \rangle \text{ with } e_2(S_1, S_2) = e_N(T_1, T_2) = 1, \quad e_2(S_i, T_j) = (-1)^{\delta_{ij}}$$

- Theta structure are linear combinations of *translation maps* $\mathfrak{g}_X$ for $X \in A[2]$.

$$\text{Row-wise: } \begin{cases} \Theta_i \cdot \mathfrak{g}_{T_1} & = (-1)^{01 \cdot i} \Theta_i \\ \Theta_i \cdot \mathfrak{g}_{T_2} & = (-1)^{10 \cdot i} \Theta_i \\ \Theta_i \cdot \mathfrak{g}_{S_1} & = \Theta_{i+01} \\ \Theta_i \cdot \mathfrak{g}_{S_2} & = \Theta_{i+10} \end{cases}$$

Theta structures

Theta structures are linear algebra !!

$$\theta^{E_1 \times E_2} : E_1 \times E_2 \longrightarrow \mathbb{P}^3 \quad \leftrightsquigarrow \quad \Theta^{E_1 \times E_2} \in \mathrm{PGL}_4(\mathbb{F}_q)$$

Symplectic basis

$$A[2] = \langle S_1, S_2; T_1, T_2 \rangle \text{ with } e_2(S_1, S_2) = e_N(T_1, T_2) = 1, \quad e_2(S_i, T_j) = (-1)^{\delta_{ij}}$$

- Theta structure are linear combinations of *translation maps* $\mathfrak{g}_X$ for $X \in A[2]$.

$$\text{Row-wise: } \begin{cases} \Theta_i \cdot \mathfrak{g}_{T_1} & = (-1)^{01 \cdot i} \Theta_i \\ \Theta_i \cdot \mathfrak{g}_{T_2} & = (-1)^{10 \cdot i} \Theta_i \\ \Theta_i \cdot \mathfrak{g}_{S_1} & = \Theta_{i+01} \\ \Theta_i \cdot \mathfrak{g}_{S_2} & = \Theta_{i+10} \end{cases} \Longrightarrow \begin{cases} \Theta_{00} & = [(\mathfrak{g}_0 + \mathfrak{g}_{T_1})(\mathfrak{g}_0 + \mathfrak{g}_{T_2})]_{0,*} \\ \Theta_{01} & = \Theta_{00} \cdot \mathfrak{g}_{S_1} \\ \Theta_{10} & = \Theta_{00} \cdot \mathfrak{g}_{S_2} \\ \Theta_{11} & = \Theta_{01} \cdot \mathfrak{g}_{S_2} \end{cases}$$

Theta structures

Theta structures are linear algebra !!

$$\theta^{E_1\times E_2} : E_1 \times E_2 \longrightarrow \mathbb{P}^3 \quad \rightsquigarrow \quad \Theta^{E_1\times E_2} \in \mathrm{PGL}_4(\mathbb{F}_q)$$

Symplectic basis

$$A[2] = \langle S_1, S_2; T_1, T_2\rangle \text{ with } e_2(S_1, S_2) = e_N(T_1, T_2) = 1, \quad e_2(S_i, T_j) = (-1)^{\delta_{ij}}$$

- Theta structure are linear combinations of *translation maps* $\mathfrak{g}_X$ for $X \in A[2]$.

$$\text{Row-wise: } \begin{cases} \Theta_i \cdot \mathfrak{g}_{T_1} & = (-1)^{01\cdot i}\Theta_i \\ \Theta_i \cdot \mathfrak{g}_{T_2} & = (-1)^{10\cdot i}\Theta_i \\ \Theta_i \cdot \mathfrak{g}_{S_1} & = \Theta_{i+01} \\ \Theta_i \cdot \mathfrak{g}_{S_2} & = \Theta_{i+10} \end{cases} \Longrightarrow \begin{cases} \Theta_{00} & = [(\mathfrak{g}_0 + \mathfrak{g}_{T_1})(\mathfrak{g}_0 + \mathfrak{g}_{T_2})]_{0,*} \\ \Theta_{01} & = \Theta_{00} \cdot \mathfrak{g}_{S_1} \\ \Theta_{10} & = \Theta_{00} \cdot \mathfrak{g}_{S_2} \\ \Theta_{11} & = \Theta_{01} \cdot \mathfrak{g}_{S_2} \end{cases}$$

- Compatibility problem between $\mathfrak{g}_X$ and addition.

Building consistently ?

$$\theta^A$$

- Combination of $\mathfrak{g}_X$.

✈️

- Combination of engines, wings, wires ...

Building consistently ?

$$\theta^A$$

- Combination of $\mathfrak{g}_X$.

✈️

- Combination of engines, wings, wires ...
- Solution: Vertical integration.

Building consistently ?

$$\theta^A$$

- Combination of $\mathfrak{g}_X$.
- Solution: Vertical integration.

✈️

- Combination of engines, wings, wires ...
- Solution: Vertical integration.

Building consistently ?

θ^A

- Combination of $\mathfrak{g}_X$.
- Solution: Vertical integration.

✈️

- Combination of engines, wings, wires ...
- Solution: Vertical integration.

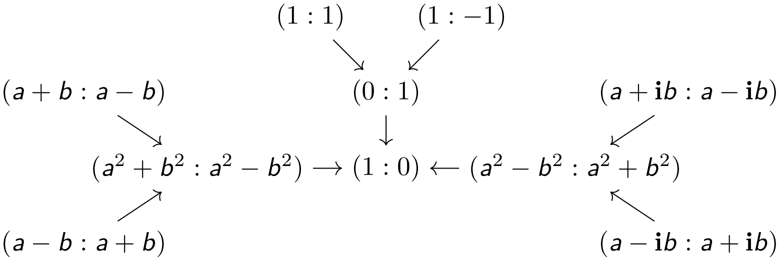


Figure: Structure of $E[4]_{/\pm 1}$ on Montgomery curves

Gluing evaluation

- We have our plane $\Theta^{E_1 \times E_2}$. How do we fly ?

$$E_1 \times E_2 \xrightarrow{\Phi_1} A_1$$

Gluing evaluation

- We have our plane $\Theta^{E_1 \times E_2}$. How do we fly ?

$$E_1 \times E_2 \xrightarrow{\Phi_1} A_1$$

$$\begin{pmatrix} x_i \\ z_i \end{pmatrix} \sim P_i \in E_{i/\pm 1}$$

$$\mathcal{H} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$\odot, \otimes$ Hadamard/Kronecker product

Gluing evaluation

- We have our plane $\Theta^{E_1 \times E_2}$. How do we fly ?

$$E_1 \times E_2 \xrightarrow{\Phi_1} A_1$$

$$\begin{pmatrix} x_i \\ z_i \end{pmatrix} \sim P_i \in E_{i/\pm 1}$$

$$\mathcal{H} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$\odot, \otimes$ Hadamard/Kronecker product

- We use the *duplication formula* !

$$\mathcal{H}\Big(\theta^{A_1}(\Phi_1(P_1, P_2))\Big) \odot \mathcal{H}\left(\theta^{A_1}(0)\right) = \mathcal{H}\Big((\Theta^{E_1 \times E_2} \cdot (P_1 \otimes P_2)) \odot (\Theta^{E_1 \times E_2} \cdot (P_1 \otimes P_2))\Big)$$

Gluing evaluation

- We have our plane $\Theta^{E_1 \times E_2}$. How do we fly ?

$$E_1 \times E_2 \xrightarrow{\Phi_1} A_1$$

$$\begin{pmatrix} x_i \\ z_i \end{pmatrix} \sim P_i \in E_{i/\pm 1}$$

$$\mathcal{H} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$\odot, \otimes$ Hadamard/Kronecker product

- We use the *duplication formula* !

$$\mathcal{H}\Big(\theta^{A_1}(\Phi_1(P_1, P_2))\Big) \odot \mathcal{H}\left(\theta^{A_1}(0)\right) = \mathcal{H}\Big(\left(\Theta^{E_1 \times E_2} \cdot (P_1 \otimes P_2)\right) \odot \left(\Theta^{E_1 \times E_2} \cdot (P_1 \otimes P_2)\right)\Big)$$

- For gluing, $\mathcal{H}(\theta^{A_1}(0))$ has zeros coefficients.

$$E_{1/\pm 1} \times E_{2/\pm 1} \xrightarrow{\Phi_1} A_{1/\pm 1}$$

Gluing evaluation

$$\theta^A$$

- Problem: Undesired zeros.

✈️

- Problem: Need long runway to takeoff.

[0]With $P = (P_1, P_2)$, $Q = (Q_1, Q_2)$

Gluing evaluation

$$\theta^A$$

- Problem: Undesired zeros.

✈️

- Problem: Need long runway to takeoff.
- Solution: Activate afterburner!

[0] With $P = (P_1, P_2)$, $Q = (Q_1, Q_2)$

Gluing evaluation

θ^A

✈️

- Problem: Undesired zeros.
- Solution: Use *generalised* duplication formula!

- Problem: Need long runway to takeoff.
- Solution: Activate afterburner!

$$\mathcal{H}\Big(\theta^{A_1}(\Phi_1(P))\Big) \odot \mathcal{H}\Big(\theta^{A_1}(\Phi_1(Q))\Big) = \mathcal{H}\Big((\Theta^{E_1\times E_2}\cdot(P+Q)) \odot (\Theta^{E_1\times E_2}\cdot(P-Q))\Big)$$

[0]With $P = (P_1, P_2)$, $Q = (Q_1, Q_2)$

Gluing evaluation

θ^A

✈️

- Problem: Undesired zeros.
- Solution: Use *generalised* duplication formula!

- Problem: Need long runway to takeoff.
- Solution: Activate afterburner!

$$\mathcal{H}\Big(\theta^{A_1}(\Phi_1(P))\Big) \odot \mathcal{H}\Big(\theta^{A_1}(\Phi_1(Q))\Big) = \mathcal{H}\Big((\Theta^{E_1 \times E_2} \cdot (P+Q)) \odot (\Theta^{E_1 \times E_2} \cdot (P-Q))\Big)$$

- Works because:
  - Good Q are free.
  - Deceptively cheap to compute.

[0] With $P = (P_1, P_2)$, $Q = (Q_1, Q_2)$

Barycentric coordinates

Barycentric coordinates

$P, Q \in E$, let $(u : v : w) \in \mathbb{P}^3$ such that $(P \pm Q)_{/\pm 1} = (u \pm v : w)$

Barycentric coordinates

Barycentric coordinates

$P, Q \in E$, let $(u : v : w) \in \mathbb{P}^3$ such that $(P \pm Q)_{/\pm 1} = (u \pm v : w)$

- Easy to compute thanks to *differential algebra* on E.

Gluing formula

$$(\Theta^{E_1 \times E_2} \cdot (P+Q)) \odot (\Theta^{E_1 \times E_2} \cdot (P-Q)) =$$

$$\left(\begin{pmatrix} \Theta_{0,0} & \Theta_{0,1} & \Theta_{0,2} & \Theta_{0,3} \\ \Theta_{1,0} & \Theta_{1,1} & \Theta_{1,2} & \Theta_{1,3} \\ \Theta_{2,0} & \Theta_{2,1} & \Theta_{2,2} & \Theta_{2,3} \\ \Theta_{3,0} & \Theta_{3,1} & \Theta_{3,2} & \Theta_{3,3} \end{pmatrix} \cdot \begin{pmatrix} u_1 u_2 + v_1 v_2 \\ u_1 w_2 \\ w_1 u_2 \\ w_1 w_2 \end{pmatrix}\right)^{\odot 2} - \left(\begin{pmatrix} \Theta_{0,0} & \Theta_{0,1} & \Theta_{0,2} & \Theta_{0,3} \\ \Theta_{1,0} & \Theta_{1,1} & \Theta_{1,2} & \Theta_{1,3} \\ \Theta_{2,0} & \Theta_{2,1} & \Theta_{2,2} & \Theta_{2,3} \\ \Theta_{3,0} & \Theta_{3,1} & \Theta_{3,2} & \Theta_{3,3} \end{pmatrix} \cdot \begin{pmatrix} v_1 u_2 + u_1 v_2 \\ v_1 w_2 \\ w_1 v_2 \\ 0 \end{pmatrix}\right)^{\odot 2}$$

Superglue formulae

- Can go *faster*!
  - Further exploit theta structures symmetries.

Superglue formulae

- Can go *faster*!
  - Further exploit theta structures symmetries.

A superglue formula

$$\left(\Theta^{E_1\times E_2}\cdot(P+Q)\right)\odot\left(\Theta^{E_1\times E_2}\cdot(P-Q)\right)=$$

$$\left(\begin{pmatrix}\Theta_{0,0} & \Theta_{0,1} & \Theta_{0,2} & \Theta_{0,3}\\ \Theta_{1,0} & \Theta_{1,1} & \Theta_{1,2} & \Theta_{1,3}\\ \Theta_{2,0} & \Theta_{2,1} & \Theta_{2,2} & \Theta_{2,3}\\ \Theta_{3,0} & \Theta_{3,1} & \Theta_{3,2} & \Theta_{3,3}\end{pmatrix}\cdot\begin{pmatrix}u_1u_2+v_1v_2\\ u_1w_2\\ w_1u_2\\ w_1w_2\end{pmatrix}\right)^{\odot 2}-\left(\begin{pmatrix}\Theta_{0,0} & \Theta_{0,1} & \Theta_{0,2} & \Theta_{0,3}\\ \Theta_{1,0} & \Theta_{1,1} & \Theta_{1,2} & \Theta_{1,3}\\ \Theta_{2,0} & \Theta_{2,1} & \Theta_{2,2} & \Theta_{2,3}\\ \Theta_{3,0} & \Theta_{3,1} & \Theta_{3,2} & \Theta_{3,3}\end{pmatrix}\cdot\begin{pmatrix}v_1u_2+u_1v_2\\ v_1w_2\\ w_1v_2\\ 0\end{pmatrix}\right)^{\odot 2}$$

Superglue formulae

- Can go *faster*!
  - Further exploit theta structures symmetries.

A superglue formula

$$\mathcal{H}\Big(\big(\Theta^{E_1\times E_2}\cdot(P+Q)\big)\odot\big(\Theta^{E_1\times E_2}\cdot(P-Q)\big)\Big)=$$

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

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

Before coffee break

Additionally, I skated over:

- Evaluation of $(2^n, 2^n)$ isogenies on quadratic twists.
- Getting rid of modular inversions.
- Getting rid of the y-coordinate.
- All formulae are constant-time, (not branchless).

Before coffee break

Additionally, I skated over:

- Evaluation of $(2^n, 2^n)$ isogenies on quadratic twists.
- Getting rid of modular inversions.
- Getting rid of the y-coordinate.
- All formulae are constant-time, (not branchless).

eprint

Thanks for listening !

Have a safe HD isogeny back home !

Abelian varieties

- Elliptic curves: $E[N] \cong \mathbb{Z}_N^2$

$$e_N : E[N] \times E[N] \to \mu_N$$

- Abelian variety of dim g: $A[N] \cong \mathbb{Z}_N^{2g}$

$$e_N : A[N] \times A[N] \to \mu_N$$

Symplectic representation

$$\pi : A[N] \cong \mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}$$

$$\pi(P) = (x_P, \widehat{x_P})$$

- Compatible with e_N:

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

- Equivalent to *symplectic basis* $\{S_1, ..., S_g, T_1, ..., T_g\}$:

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

Theta structures

Theta structure

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.

columns	theta points		columns	dual theta points
$\Theta_0\Theta_0$	$\theta^{E_1\times E_2}(0,0)\theta^{E_1\times E_2}(0,0)$	$\Longleftrightarrow$	$\widetilde{\Theta_0\Theta_0}$	$\widetilde{\theta}^{A_1}(\Phi(0,0))\widetilde{\theta}^{A_1}(\Phi(0,0))$
$\Theta_1\Theta_1$	$\theta^{E_1\times E_2}(0,C)\theta^{E_1\times E_2}(0,C)$	$\Longleftrightarrow$	$\widetilde{\Theta_1\Theta_1}$	$\widetilde{\theta}^{A_1}(\Phi(0,0))\widetilde{\theta}^{A_1}(\Phi(0,C))$
$\Theta_2\Theta_2$	$\theta^{E_1\times E_2}(C,0)\theta^{E_1\times E_2}(C,0)$	$\Longleftrightarrow$	$\widetilde{\Theta_2\Theta_2}$	$\widetilde{\theta}^{A_1}(\Phi(0,0))\widetilde{\theta}^{A_1}(\Phi(C,0))$
$\Theta_3\Theta_3$	$\theta^{E_1\times E_2}(C,C)\theta^{E_1\times E_2}(C,C)$	$\Longleftrightarrow$	$\widetilde{\Theta_3\Theta_3}$	$\widetilde{\theta}^{A_1}(\Phi(0,0))\widetilde{\theta}^{A_1}(\Phi(C,C))$
$\Theta_0\Theta_1$	$\theta^{E_1\times E_2}(0,0)\theta^{E_1\times E_2}(0,C)$	$\Longleftrightarrow$	$\widetilde{\Theta_0\Theta_1}$	$\widetilde{\theta}^{A_1}(\Phi(0,C'))\widetilde{\theta}^{A_1}(\Phi(0,C'))$
$\Theta_2\Theta_3$	$\theta^{E_1\times E_2}(C,0)\theta^{E_1\times E_2}(C,C)$	$\Longleftrightarrow$	$\widetilde{\Theta_2\Theta_3}$	$\widetilde{\theta}^{A_1}(\Phi(0,C'))\widetilde{\theta}^{A_1}(\Phi(C,C'))$
$\Theta_0\Theta_2$	$\theta^{E_1\times E_2}(0,0)\theta^{E_1\times E_2}(C,0)$	$\Longleftrightarrow$	$\widetilde{\Theta_0\Theta_2}$	$\widetilde{\theta}^{A_1}(\Phi(C',0))\widetilde{\theta}^{A_1}(\Phi(C',0))$
$\Theta_1\Theta_3$	$\theta^{E_1\times E_2}(0,C)\theta^{E_1\times E_2}(C,C)$	$\Longleftrightarrow$	$\widetilde{\Theta_1\Theta_3}$	$\widetilde{\theta}^{A_1}(\Phi(C',0))\widetilde{\theta}^{A_1}(\Phi(C',C))$
$\Theta_0\Theta_3$	$\theta^{E_1\times E_2}(0,0)\theta^{E_1\times E_2}(C,C)$	$\Longleftrightarrow$	$\widetilde{\Theta_0\Theta_3}$	$\widetilde{\theta}^{A_1}(\Phi(C',C'))\widetilde{\theta}^{A_1}(\Phi(C',C'))$
$\Theta_1\Theta_2$	$\theta^{E_1\times E_2}(0,C)\theta^{E_1\times E_2}(C,0)$	$\Longleftrightarrow$	$\widetilde{\Theta_1\Theta_2}$	$\widetilde{\theta}^{A_1}(\Phi(C',C'))\widetilde{\theta}^{A_1}(\Phi(C',-C'))$

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