The rabbit hole of theta stucture and their constructive applications

Max Duparc

Virginia Tech Collaboration Workshop: July 5, 2026

Today's Program

- Cryptographic interest in Abelian varieties is old.

Today's Program

- Cryptographic interest in Abelian varieties is old.
  - Elliptic curves [Mil86]

Today's Program

- Cryptographic interest in Abelian varieties is old.
  - Elliptic curves [Mil86]
  - Abelian varitieties of dim 2+ [Can87].

Today's Program

- Cryptographic interest in Abelian varieties is old.
  - Elliptic curves [Mil86]
  - Abelian varitieties of dim 2+ [Can87].
- HD was never mainstream **until 2022** (SIKE attacks).

Today's Program

- Cryptographic interest in Abelian varieties is old.
  - Elliptic curves [Mil86]
  - Abelian varitieties of dim 2+ [Can87].
- HD was never mainstream **until 2022** (SIKE attacks).
- In **2026**, it is everywhere in isogeny based cryptography
  - Fast arithmetic.
  - Fast isogenies.

Today's Program

- Cryptographic interest in Abelian varieties is old.
  - Elliptic curves [Mil86]
  - Abelian varitieties of dim 2+ [Can87].
- HD was never mainstream **until 2022** (SIKE attacks).
- In **2026**, it is everywhere in isogeny based cryptography
  - Fast arithmetic.
  - Fast isogenies.
- Thanks to **theta structures**.

Today's Program

- Cryptographic interest in Abelian varieties is old.
  - Elliptic curves [Mil86]
  - Abelian varitieties of dim 2+ [Can87].
- HD was never mainstream **until 2022** (SIKE attacks).
- In **2026**, it is everywhere in isogeny based cryptography
  - Fast arithmetic.
  - Fast isogenies.
- Thanks to **theta structures**.
  - Let's explore this rabbit hole !

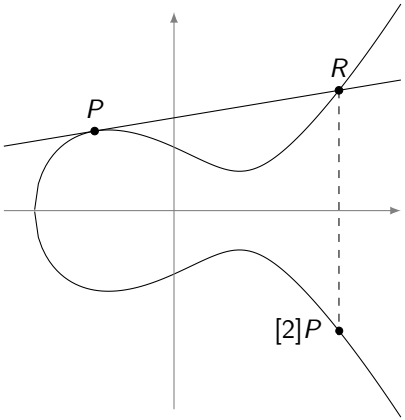
Elliptic curves

Let $\mathbb{F}_q$ be our basis field.

- *Weierstrass equations*:

$$E : y^2 = x^3 + Ax + B$$

with $4A^3 + 27B^2 \neq 0$.



Elliptic curves

Let $\mathbb{F}_q$ be our basis field.

- *Weierstrass equations*:

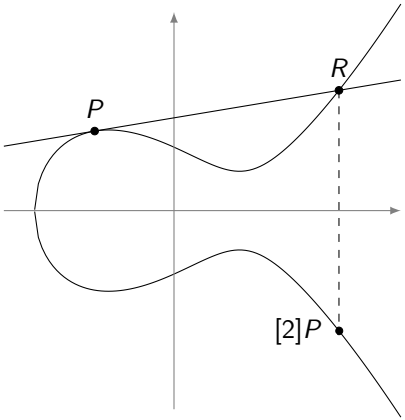
$$E : y^2 = x^3 + Ax + B$$

with $4A^3 + 27B^2 \neq 0$.

- *j-invariant*:

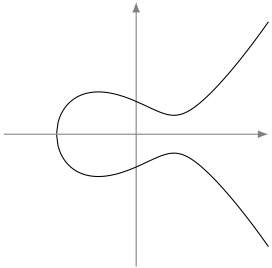
$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}$$

characterises isomorphism classes.

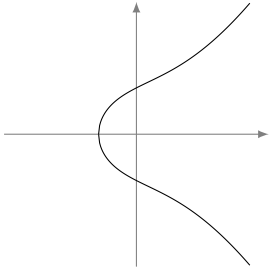


Isogenies

- Surjective group morphism between elliptic curves.



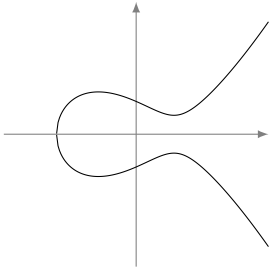
$E : y^2 = x^3 - 3x + 3$



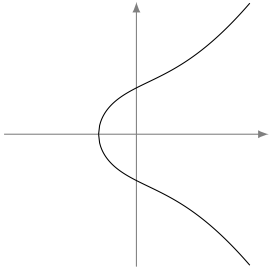
$E' : y^2 = x^3 + 5x + 6$

Isogenies

- Surjective group morphism between elliptic curves.



$E : y^2 = x^3 - 3x + 3$



$E' : y^2 = x^3 + 5x + 6$

$$\phi : (x, y) \to \left(\frac{x^2 + 6x + 1}{x - 7}, \frac{x^2 - x - 4}{(x - 7)^2} y \right) \text{ in } \mathbb{F}_{13}$$

Isogenies

$$\phi \leftrightsquigarrow \ker(\phi)$$

Isogenies are characterised by their kernel !

Isogenies

$$\phi \leftrightsquigarrow \ker(\phi)$$

Isogenies are characterised by their kernel !

- The *degree*: $\deg(\phi) = |\ker(\phi)| < \infty$.

Isogenies

$$\phi \leftrightsquigarrow \ker(\phi)$$

Isogenies are characterised by their kernel !

- The *degree*: $\deg(\phi) = |\ker(\phi)| < \infty$.

Isogenies

$$\phi \leftrightsquigarrow \ker(\phi)$$

Isogenies are characterised by their kernel !

- The *degree*: $\deg(\phi) = |\ker(\phi)| < \infty$.
- Given $\ker(\phi)$, computing ϕ takes $O(\deg(\phi))$.

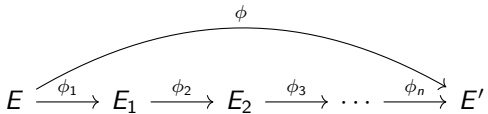
Isogenies

$$\phi \leftrightsquigarrow \ker(\phi)$$

Isogenies are characterised by their kernel !

- The *degree*: $\deg(\phi) = |\ker(\phi)| < \infty$.

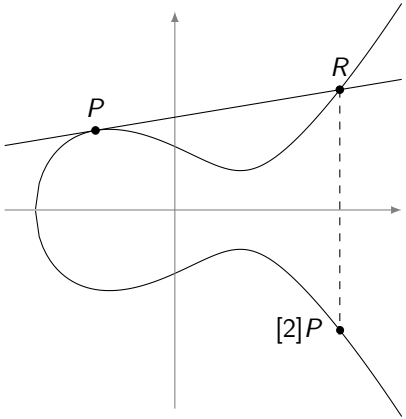
- Given $\ker(\phi)$, computing ϕ takes $O(\deg(\phi))$.
- Let $\deg(\phi) = \ell^n$. Can compute it in $O\big(n \log(n) \ell\big)$



Abelian Varieties

E

- Abelian varieties of dim 1.
- $E[N] \cong \mathbb{Z}_N^2$
- isogeny $\phi : E \to E'$ with finite kernel.
- $\deg(\phi) = |\ker(\phi)|$.

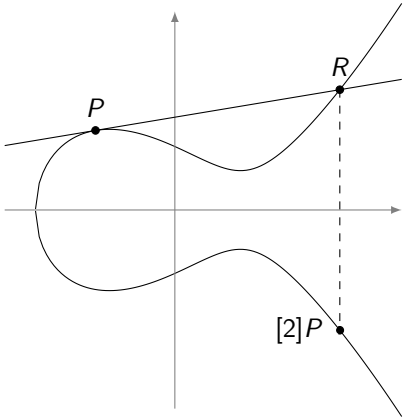


Abelian Varieties

$$(E, e^E)$$

- Abelian varieties of dim 1.
- $E[N] \cong \mathbb{Z}_N^2$
- isogeny $\phi : E \to E'$ with finite kernel.
- $\deg(\phi) = |\ker(\phi)|$.
- Alternating compatible non-degenerate pairing

$$\forall N \in \mathbb{N}, \quad e_N^E : E[N] \times E[N] \longrightarrow \mu_N$$

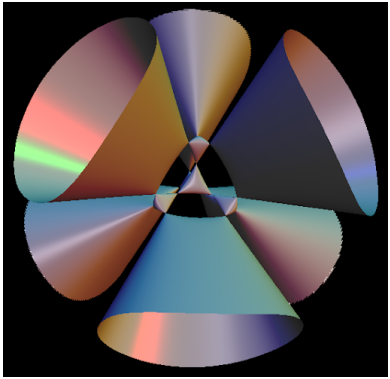


Abelian Varieties

$$(A, e^A)$$

- Abelian varieties of dim g.
- $A[N] \cong \mathbb{Z}_N^{2g}$
- isogeny $\phi : A \to A'$ with finite max isotropic* kernel. $(e^A|_{\ker(f)^2} \equiv 1)$.
- $\deg(\phi) = |\ker(\phi)|^g$.
- Alternating compatible non-degenerate pairing

$$\forall N \in \mathbb{N}, \quad e_N^A : A[N] \times A[N] \longrightarrow \mu_N$$



The HD revolution

Isogeny interpolation

$$\phi : E \to E' \text{of degree } q \xrightarrow{\text{interpolate}} \Phi : A \to A' \text{ of degree } 2^\ell \text{ and dimension } g$$

The HD revolution

Isogeny interpolation

$$\phi : E \to E' \text{of degree } q \xrightarrow{\text{interpolate}} \Phi : A \to A' \text{ of degree } 2^\ell \text{ and dimension } g$$

- Based on 30 years old lemma [Kan97].
- g varies depending on use.

The HD revolution

Isogeny interpolation

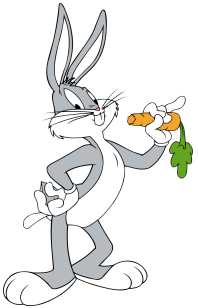
$$\phi : E \to E' \text{of degree } q \xrightarrow{\text{interpolate}} \Phi : A \to A' \text{ of degree } 2^\ell \text{ and dimension } g$$

- Based on 30 years old lemma [Kan97].
- g varies depending on use.

- We need fast arithmetic and isogenies on Abelian varieties.

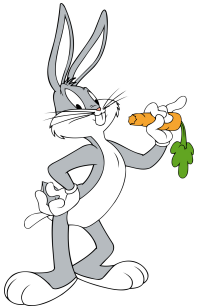
What's up, doc?

- Precursor works: [LR10, LR12].



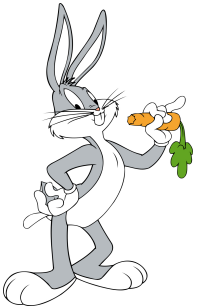
What's up, doc?

- Precursor works: [LR10, LR12].
- dim 2:
  - [DMPR24]: Fast and constant time dim 2 implementation.
  - [Dup25]: Improvement on gluing.
  - *ongoing*: Further tricks to make $(2, 2)$-isogenies faster.



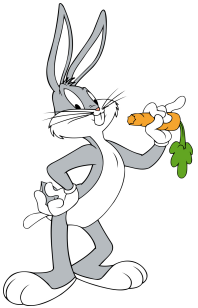
What's up, doc?

- Precursor works: [LR10, LR12].
- dim 2:
  - [DMPR24]: Fast and constant time dim 2 implementation.
  - [Dup25]: Improvement on gluing.
  - *ongoing*: Further tricks to make $(2,2)$-isogenies faster.
- generic dim:
  - [Dar24]: Generalisation of [DMPR24].
  - [DD26]: **Making it cryptographic.**



What's up, doc?

- Precursor works: [LR10, LR12].
- dim 2:
  - [DMPR24]: Fast and constant time dim 2 implementation.
  - [Dup25]: Improvement on gluing.
  - *ongoing*: Further tricks to make $(2,2)$-isogenies faster.
- generic dim:
  - [Dar24]: Generalisation of [DMPR24].
  - [DD26]: **Making it cryptographic.**



We now have all tools to compute fast HD isogenies (of degree 2^ℓ).

Symplectic form

- Theta structures are old [Mum66].
- They are representation of $A[N] \cong \mathbb{Z}_N^{2g}$ compatible with e^A.

Symplectic form

- Theta structures are old [Mum66].
- They are representation of $A[N] \cong \mathbb{Z}_N^{2g}$ compatible with e^A.

Symplectic representation

- Using $\widehat{\mathbb{Z}_N^g} = \{\chi : \mathbb{Z}_N^g \longrightarrow \mu_N\}$ the dual of $\mathbb{Z}_N^g$[a], let:

$$\epsilon : \left(\mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}\right)^2 \longrightarrow \mu_N, \quad \text{s.t.} \quad \epsilon\big((x_1,\chi_1),(x_2,\chi_2)\big) = \chi_2(x_1)\cdot\chi_1(x_2)^{-1}$$

[a] $\chi_i(-) \leftrightsquigarrow \zeta^{\langle x_i|-\rangle}$ for ζ a primitive N-root of unity and $x_i \in \mathbb{Z}_N^g$.

Symplectic form

- Theta structures are old [Mum66].
- They are representation of $A[N] \cong \mathbb{Z}_N^{2g}$ compatible with e^A.

Symplectic representation

- Using $\widehat{\mathbb{Z}_N^g} = \{\chi : \mathbb{Z}_N^g \longrightarrow \mu_N\}$ the dual of $\mathbb{Z}_N^g$[a], let:

$$\epsilon : \left(\mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}\right)^2 \longrightarrow \mu_N, \quad \text{s.t.} \quad \epsilon\big((x_1,\chi_1),(x_2,\chi_2)\big) = \chi_2(x_1)\cdot\chi_1(x_2)^{-1}$$

- **Symplectic representation** of $A[N]$:

$$\mu : (A[N], e_A) \xrightarrow{\cong} (\mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}, \epsilon)$$

[a] $\chi_i(-) \leftrightsquigarrow \zeta^{\langle x_i|-\rangle}$ for ζ a primitive N-root of unity and $x_i \in \mathbb{Z}_N^g$.

Symplectic form

- Theta structures are old [Mum66].
- They are representation of $A[N] \cong \mathbb{Z}_N^{2g}$ compatible with e^A.

Symplectic representation

- Using $\widehat{\mathbb{Z}_N^g} = \{\chi : \mathbb{Z}_N^g \longrightarrow \mu_N\}$ the dual of $\mathbb{Z}_N^g$[a], let:

$$\epsilon : \left(\mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}\right)^2 \longrightarrow \mu_N, \quad \text{s.t.} \quad \epsilon\big((x_1, \chi_1), (x_2, \chi_2)\big) = \chi_2(x_1) \cdot \chi_1(x_2)^{-1}$$

- **Symplectic representation** of $A[N]$:

$$\mu : (A[N], e_A) \xrightarrow{\cong} (\mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}, \epsilon)$$

- Equivalent to **symplectic basis** $\mathcal{B}_\mu := \{S_1, \dots, S_g, T_1, \dots, T_g\}$:

$$e_A(S_i, S_j) = e_A(T_i, T_j) = 1, \quad e_A(S_i, T_j) = \zeta^{\delta_{i,j}}$$

[a] $\chi_i(-) \rightsquigarrow \zeta^{\langle x_i | - \rangle}$ for ζ a primitive N-root of unity and $x_i \in \mathbb{Z}_N^g$.

Theta structures

Definition

1. A symplectic representation $\mu_A : A[N] \xrightarrow{\cong} \mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}$;

Theta structures

Definition

1. A symplectic representation $\mu_A : A[N] \xrightarrow{\cong} \mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}$;
2. A map

$$\begin{array}{rccc} \theta^A : & A & \longrightarrow & \mathbb{P}_k^{N^g-1} \\ & P & \longrightarrow & \left(\theta_i^A(P)\right)_{i\in\mathbb{Z}_N^g} \end{array}$$

Theta structures

Definition

1. A symplectic representation $\mu_A : A[N] \xrightarrow{\cong} \mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}$;
2. A map

$$\begin{aligned} \theta^A : A &\longrightarrow \mathbb{P}_k^{N^g-1} \\ P &\longrightarrow \left(\theta_i^A(P)\right)_{i\in\mathbb{Z}_N^g} \end{aligned}$$

satisfying the *theta group action relation*:

$$\forall P \in A, Q \in A[N] \text{ with } \mu_A(Q) = (x_Q, \chi_Q) : \quad \theta_j^A(P+Q) = \chi_Q(j)^{-1}\theta_{j+x_Q}^A(P)$$

Theta structures

Definition

1. A symplectic representation $\mu_A : A[N] \xrightarrow{\cong} \mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}$;
2. A map

$$\begin{array}{rccc} \theta^A : & A & \longrightarrow & \mathbb{P}_k^{N^g-1} \\ & P & \longrightarrow & \left(\theta_i^A(P)\right)_{i\in\mathbb{Z}_N^g} \end{array}$$

satisfying the *theta group action relation*:

$$\forall P \in A, Q \in A[N] \text{ with } \mu_A(Q) = (x_Q, \chi_Q) : \quad \theta_j^A(P+Q) = \chi_Q(j)^{-1}\theta_{j+x_Q}^A(P)$$

- Mainly interested in $N = 2$:
  - $\theta^A(0)$ characterises A (up to isomorphism).
  - It is *symmetric*: (i.e. $\theta^A(-P) = \theta^A(P)$).

Theta structure symmetries

- Theta structure have a lot of self-similarities:

Theta structure symmetries

- Theta structure have a lot of self-similarities:

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

Theta structure symmetries

- Theta structure have a lot of self-similarities:

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

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

	0	T_1	T_2	$T_1 + T_2$
0	$-$	$(x:0:y:0)$	$(x:y:0:0)$	$(x:0:0:y)$
S_1	$(x:x:y:y)$	$(x:\mathbf{i}x:y:\mathbf{i}y)$	$(x:x:y:-y)$	$(x:\mathbf{i}x:y:-\mathbf{i}y)$
S_2	$(x:y:x:y)$	$(x:y:x:-y)$	$(x:y:\mathbf{i}x:-\mathbf{i}y)$	$(x:y:-\mathbf{i}x:\mathbf{i}y)$
$S_1 + S_2$	$(x:y:y:x)$	$(x:y:-\mathbf{i}y:\mathbf{i}x)$	$(x:y:\mathbf{i}y:\mathbf{i}x)$	$(x:y:-y:x)$

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

Computation

Notation:

$$(x_i)_i \odot (y_i)_i = (x_i y_i)_i$$
$$(x_i)_i^{\odot n} = (x_i^n)_i \text{ for } n \in \mathbb{Z}.$$

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

Computation

Notation:

$$(x_i)_i \odot (y_i)_i = (x_i y_i)_i$$
$$(x_i)_i^{\odot n} = (x_i^n)_i \text{ for } n \in \mathbb{Z}.$$

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

[Mum66]: The isogeny formula

Let $f : A \to B$ by a 2-isogeny, then:

$$\mathcal{H}\left(\theta^A(P+Q) \odot \theta^A(P-Q)\right) = \mathcal{H}\big(\theta^B(f(P))\big) \odot \mathcal{H}\big(\theta^B(f(Q))\big)$$

Computation

Notation:

$$(x_i)_i \odot (y_i)_i = (x_i y_i)_i$$
$$(x_i)_i^{\odot n} = (x_i^n)_i \text{ for } n \in \mathbb{Z}.$$

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

[Mum66]: The isogeny formula

Let $f : A \to B$ by a 2-isogeny, then:

$$\mathcal{H}\left(\theta^A(P+Q) \odot \theta^A(P-Q)\right) = \mathcal{H}\big(\theta^B(f(P))\big) \odot \mathcal{H}\big(\theta^B(f(Q))\big)$$

Computation

Notation:

$$(x_i)_i \odot (y_i)_i = (x_i y_i)_i$$
$$(x_i)_i^{\odot n} = (x_i^n)_i \text{ for } n \in \mathbb{Z}.$$

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

[Mum66]: The isogeny formula

Let $f : A \to B$ by a 2-isogeny, then:

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

- [Gau07] Gives a fast (differential) arithmetic on A.

Computing Isogenies

$$\prod^{g} E_i = A_0 \xrightarrow{\quad f \quad} A_e$$

Computing Isogenies

$$\prod^{g} E_i = A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \xrightarrow{f_3} \cdots \xrightarrow{f_{e-2}} A_{e-2} \xrightarrow{f_{e-1}} A_{e-1} \xrightarrow{f_e} A_e, \qquad A_0 \xrightarrow{f} A_e$$

Computing Isogenies

$$\prod^{g} E_i = A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \xrightarrow{f_3} \cdots \xrightarrow{f_{e-2}} A_{e-2} \xrightarrow{f_{e-1}} A_{e-1} \xrightarrow{f_e} A_e, \qquad A_0 \xrightarrow{f} A_e$$

- Building block: $\theta^A(P) \xrightarrow{f_i} \theta^B(f_i(P))$:

Computing Isogenies

$$\prod^g E_i = A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \xrightarrow{f_3} \cdots \xrightarrow{f_{e-2}} A_{e-2} \xrightarrow{f_{e-1}} A_{e-1} \xrightarrow{f_e} A_e, \qquad A_0 \xrightarrow{f} A_e$$

- Building block: $\theta^A(P) \xrightarrow{f_i} \theta^B(f_i(P))$:

$$\theta^A(P) \xrightarrow{S} \theta^A(P)^{\odot 2} \xrightarrow{\mathcal{H}} \mathcal{H}(\theta^A(P)^{\odot 2}) \xrightarrow{\odot \mathcal{H}\left(\theta^B(0_B)\right)^{\odot -1}} \widetilde{\theta}^B(f(P)) \xrightarrow{\mathcal{H}} \theta^B(f(P)).$$

Computing Isogenies

$$\prod^g E_i = A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \xrightarrow{f_3} \cdots \xrightarrow{f_{e-2}} A_{e-2} \xrightarrow{f_{e-1}} A_{e-1} \xrightarrow{f_e} A_e, \qquad A_0 \xrightarrow{f} A_e$$

- Building block: $\theta^A(P) \xrightarrow{f_i} \theta^B(f_i(P))$:

$$\theta^A(P) \xrightarrow{S} \theta^A(P)^{\odot 2} \xrightarrow{\mathcal{H}} \mathcal{H}(\theta^A(P)^{\odot 2}) \xrightarrow{\odot \mathcal{H}\left(\theta^B(0_B)\right)^{\odot -1}} \widetilde{\theta}^B(f(P)) \xrightarrow{\mathcal{H}} \theta^B(f(P)).$$

- Bottleneck: computing $\mathcal{H}\left(\theta^B(0_B)\right)^{\odot -1}$?

Computing the inverse dual theta null point

$$\mathcal{B} \subseteq \ker(f)$$

Computing the inverse dual theta null point

$$\mathcal{B} \subseteq \ker(f) \iff (\pi_{\mathbf{i},j})_{\mathbf{i}\in\mathbb{Z}_2^g,\mathcal{B}} \text{ system of equations}$$

Computing the inverse dual theta null point

$$\mathcal{B} \subseteq \ker(f) \iff (\pi_{\mathbf{i},j})_{\mathbf{i}\in\mathbb{Z}_2^g,\mathcal{B}} \text{ system of equations} \iff \text{a graph } \mathcal{G}.$$

Computing the inverse dual theta null point

$$\mathcal{B} \subseteq \ker(f) \iff (\pi_{\mathbf{i},j})_{\mathbf{i}\in\mathbb{Z}_{2^g},\mathcal{B}} \text{ system of equations} \iff \text{a graph } \mathcal{G}.$$

[DD26] Theorem I

$$\theta^{\odot -1}(0) \text{ computable} \iff \mathcal{G} \text{ is connected.}$$

Computing the inverse dual theta null point

$$\mathcal{B} \subseteq \ker(f) \iff (\pi_{\mathbf{i},j})_{\mathbf{i}\in\mathbb{Z}_{2^g},\mathcal{B}} \text{ system of equations} \iff \text{a graph } \mathcal{G}.$$

[DD26] Theorem I

$$\theta^{\odot -1}(0) \text{ computable} \iff \mathcal{G} \text{ is connected.}$$

[DD26] Theorem II

$$\text{From } \mathcal{T} \subseteq \mathcal{G} \text{ spanning tree} \implies \text{formulae for } \theta^{\odot -1}(0).$$

Computing the inverse dual theta null point

$$\mathcal{B} \subseteq \ker(f) \iff (\pi_{\mathbf{i},j})_{\mathbf{i}\in\mathbb{Z}_2^g,\mathcal{B}} \text{ system of equations} \iff \text{a graph } \mathcal{G}.$$

[DD26] Theorem I

$$\theta^{\odot -1}(0) \text{ computable} \iff \mathcal{G} \text{ is connected.}$$

[DD26] Theorem II

$$\text{From } \mathcal{T} \subseteq \mathcal{G} \text{ spanning tree} \implies \text{formulae for } \theta^{\odot -1}(0).$$

- For generic isogenies of dim g, $\mathcal{G}$ is a hypercube.
  - Need good spanning tree of hypercubes.

A good spanning tree on hypercube

A good spanning tree on hypercube

- Gray paths on hypercubes H_g.

$$\eta : [2^g] \xrightarrow{\cong} H_g$$

$$\eta(i) := i \oplus (i \gg 1)$$

A good spanning tree on hypercube

- Gray paths on hypercubes H_g.

$$\eta : [2^g] \xrightarrow{\cong} H_g$$

$$\eta(i) := i \oplus (i \gg 1)$$

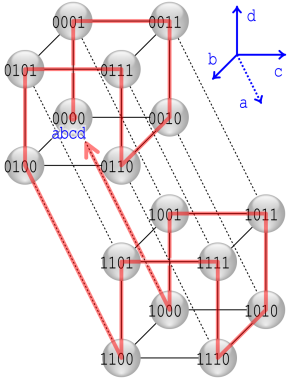


Figure: Gray code in a H_4

A good spanning tree on hypercube

- Gray paths on hypercubes H_g.

$$\eta : [2^g] \xrightarrow{\cong} H_g$$

$$\eta(i) := i \oplus (i \gg 1)$$

$$x^{-1}_{\eta(i)} = \left(\prod_{j=0}^{i-1} \pi_{\eta(j),s_j} \right) \cdot \left(\prod_{j=i}^{2^g-2} \pi_{\eta(j+1),s_j} \right)$$

with $s_i := \eta(i+1) - \eta(i)$.

Consequence

2x faster & constant time.

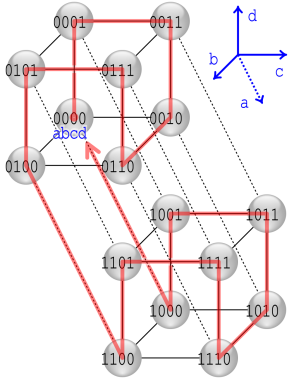


Figure: Gray code in a H_4

Exotic case: Gluing

$$\underbrace{(\overset{g}{\prod} E_i = A_0) \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2}_{\textit{Gluing}} \underbrace{\xrightarrow{f_2} \cdots \xrightarrow{f^{e-1}} A_{e-1} \xrightarrow{f_e} A_e}_{\text{generic}}$$

Exotic case: Gluing

$$\underbrace{(\prod^{g} E_i = A_0) \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2}_{\textit{Gluing}} \underbrace{\xrightarrow{f_2} \cdots \xrightarrow{f^{e-1}} A_{e-1} \xrightarrow{f_e} A_e}_{\text{generic}}$$

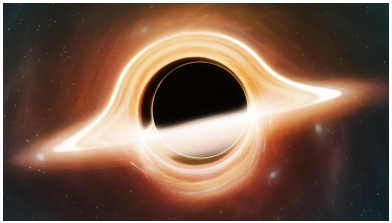


Figure: Artist view of a gluing isogeny

Exotic case: Gluing

$$\underbrace{(\overset{g}{\prod} E_i = A_0) \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2}_{\textit{Gluing}} \underbrace{\xrightarrow{f_2} \cdots \xrightarrow{f^{e-1}} A_{e-1} \xrightarrow{f_e} A_e}_{\text{generic}}$$

Gluing is:

- Full of technicality.
- The hardest part of the implementation.

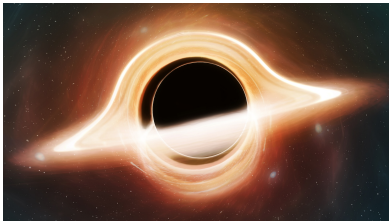


Figure: Artist view of a gluing isogeny

Exotic case: Gluing

$$\underbrace{(\overset{g}{\prod} E_i = A_0) \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2}_{\textit{Gluing}} \underbrace{\xrightarrow{f_2} \cdots \xrightarrow{f^{e-1}} A_{e-1} \xrightarrow{f_e} A_e}_{\text{generic}}$$

Gluing is:

- Full of technicality.
- The hardest part of the implementation.
- Computable thanks to [DD26] !

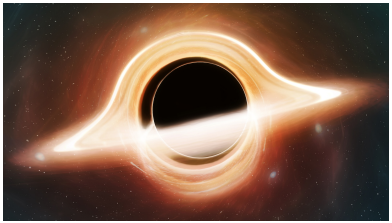


Figure: Artist view of a gluing isogeny

Rabbits of qt-Pegasis

In qt-Pegasis, gluing graphs G are rabbits !

Rabbits of qt-Pegasis

In qt-Pegasis, gluing graphs G are rabbits !

Rabbit classification lemma

Figure: A rabbit

Rabbits of qt-Pegasis

In qt-Pegasis, gluing graphs G are rabbits !

Rabbit classification lemma

1. There are 32 rabbits, identical except for their fur colour, of which there are four.

Figure: A rabbit

Rabbits of qt-Pegasis

In qt-Pegasis, gluing graphs G are rabbits !

Rabbit classification lemma

1. There are 32 rabbits, identical except for their fur colour, of which there are four.
2. Can dye rabbits into another colour through bit-swapping the indices.

Figure: A rabbit

Rabbits of qt-Pegasis

In qt-Pegasis, gluing graphs G are rabbits !

Rabbit classification lemma

1. There are 32 rabbits, identical except for their fur colour, of which there are four.
2. Can dye rabbits into another colour through bit-swapping the indices.
3. Rabbits are satiated when feed 5 carrots.

Figure: A rabbit

Rabbits of qt-Pegasis

In qt-Pegasis, gluing graphs G are rabbits !

Rabbit classification lemma

1. There are 32 rabbits, identical except for their fur colour, of which there are four.
2. Can dye rabbits into another colour through bit-swapping the indices.
3. Rabbits are satiated when feed 5 carrots.
4. Every rabbit has a skeleton that forms a Hamiltonian path in his body, with two ears on top.

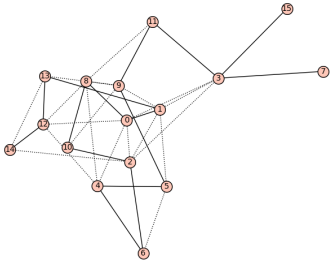


Figure: A rabbit

Rabbits of qt-Pegasis

In qt-Pegasis, gluing graphs G are rabbits !

Rabbit classification lemma

1. There are 32 rabbits, identical except for their fur colour, of which there are four.
2. Can dye rabbits into another colour through bit-swapping the indices.
3. Rabbits are satiated when feed 5 carrots.
4. Every rabbit has a skeleton that forms a Hamiltonian path in his body, with two ears on top.

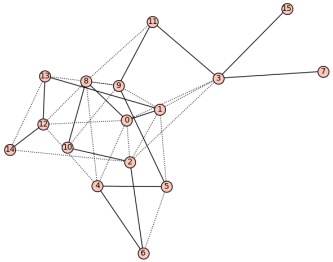


Figure: A rabbit

- Almost as fast as generic case.
- Using **many** others technical tricks, can make constant time gluing for qt-Pegasis.
  - Base of the *PQarrot* crypto-suite.

Exotic case: Special varieties

On some special Abelian varieties, theta structures have extra symmetries:

- e.g. Scholten construction.
- e.g. Fourfold of Weil-type (dim 4).

Exotic case: Special varieties

On some special Abelian varieties, theta structures have extra symmetries:

- e.g. Scholten construction.
- e.g. Fourfold of Weil-type (dim 4).

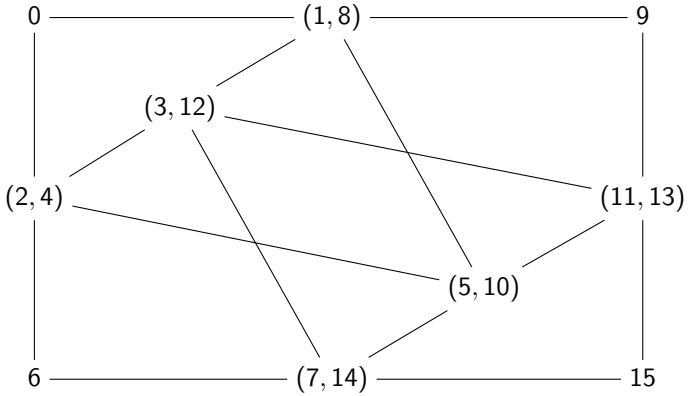


Figure: Graphs abelian fourfold of Weil type

Exotic case: Special varieties

On some special Abelian varieties, theta structures have extra symmetries:

- e.g. Scholten construction.
- e.g. Fourfold of Weil-type (dim 4).

Consequence

Can compute isogenies (and arithmetic) faster !

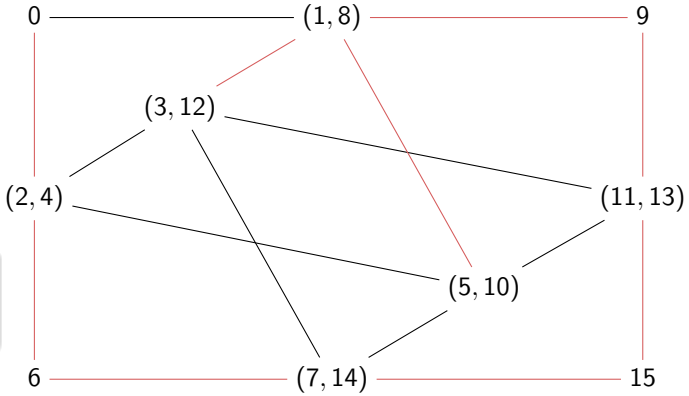


Figure: Graphs abelian fourfold of Weil type

Implementation of dim 4 chains

$\lceil \log_2(p) \rceil$	ARM (Mcycles)	X86 (Mcycles)	Timing (ms)
505	146.95	274.38	23.94
1008	871.34	1627.05	146.19
1525	3163.05	5208.81	543.01
2017	7041.82	11192.45	1222.96

Table: Performance of the C-implementation of generic 4D chain (qt-Pegasis).

Timings collected on arm 64 M4 Pro, 4.5GHz.

Implementation of dim 4 chains

$\lceil \log_2(p) \rceil$	ARM (Mcycles)	X86 (Mcycles)	Timing (ms)
505	146.95	274.38	23.94
1008	871.34	1627.05	146.19
1525	3163.05	5208.81	543.01
2017	7041.82	11192.45	1222.96

Table: Performance of the C-implementation of generic 4D chain (qt-Pegasis).

$\lceil \log_2(p) \rceil$	sk	pk	KeyGen (ms)	KeyAgrement (ms)
256	32 B	64 B	0.335	2.238
384	48 B	92 B	1.095	8.720
512	64 B	128 B	2.525	21.017

Table: Performance of the Rust implementation of 4D chain on Weil type curve (MIKE).

Timings collected on arm 64 M4 Pro, 4.5GHz.

Conclusion

Theta structure make Abelian varieties easy !

Conclusion

Theta structure make Abelian varieties easy !

1. Dim 4 chains of isogenies are constructively practical!

Conclusion

Theta structure make Abelian varieties easy !

1. Dim 4 chains of isogenies are constructively practical!
2. We have all the tools for generic dimension!

Conclusion

Theta structure make Abelian varieties easy !

1. Dim 4 chains of isogenies are constructively practical!
2. We have all the tools for generic dimension!
3. Can they be used outside isogeny based crypto ?

Conclusion

Theta structure make Abelian varieties easy !

1. Dim 4 chains of isogenies are constructively practical!
2. We have all the tools for generic dimension!
3. Can they be used outside isogeny based crypto ?

Thanks for listening !

Beware of rabbits !

References I


David G Cantor, *Computing in the jacobian of a hyperelliptic curve*, Mathematics of computation **48** (1987), no. 177, 95–101.


Pierrick Dartois, *Fast computation of 2-isogenies in dimension 4 and cryptographic applications*, Cryptology ePrint Archive, Report 2024/1180, 2024.


Pierrick Dartois and Max Duparc, *Chasing rabbits through hypercubes: Better algorithms for higher dimensional 2-isogeny computations*, Cryptology ePrint Archive, Paper 2026/114, 2026.


Pierrick Dartois, Luciano Maino, Giacomo Pope, and Damien Robert, *An algorithmic approach to (2, 2)-isogenies in the theta model and applications to isogeny-based cryptography*, ASIACRYPT 2024, Part III (Kai-Min Chung and Yu Sasaki, eds.), LNCS, vol. 15486, Springer, Singapore, December 2024, pp. 304–338.

Max Duparc, *Superglue: Fast formulae for (2,2)-gluing isogenies*, ASIACRYPT 2025, Part IV, LNCS, Springer, Singapore, December 2025, pp. 372–400.

References II

- Pierrick Gaudry, *Fast genus 2 arithmetic based on theta functions*, Journal of Mathematical Cryptology **1** (2007), no. 3, 243–265.
- Ernst Kani, *The number of curves of genus two with elliptic differentials*, Journal fur die reine und angewandte Mathematik **485** (1997), 93–122.
- David Lubicz and Damien Robert, *Efficient pairing computation with theta functions*, International Algorithmic Number Theory Symposium, Springer, 2010, pp. 251–269.
- _____, *Computing isogenies between abelian varieties*, Compositio Mathematica **148** (2012), no. 5, 1483–1515.
- Victor S. Miller, *Use of elliptic curves in cryptography*, CRYPTO'85 (Hugh C. Williams, ed.), LNCS, vol. 218, Springer, Berlin, Heidelberg, August 1986, pp. 417–426.
- David Bryant Mumford, *On the equations defining abelian varieties. i*, Inventiones mathematicae (1966).