A tale of groups and rabbits: efficient 4-dimensional isogeny computations for cryptographic group actions

Pierrick Dartois

2026, March 6

Overview of my contributions involved in this presentation

On the efficient class group action from isogenies:

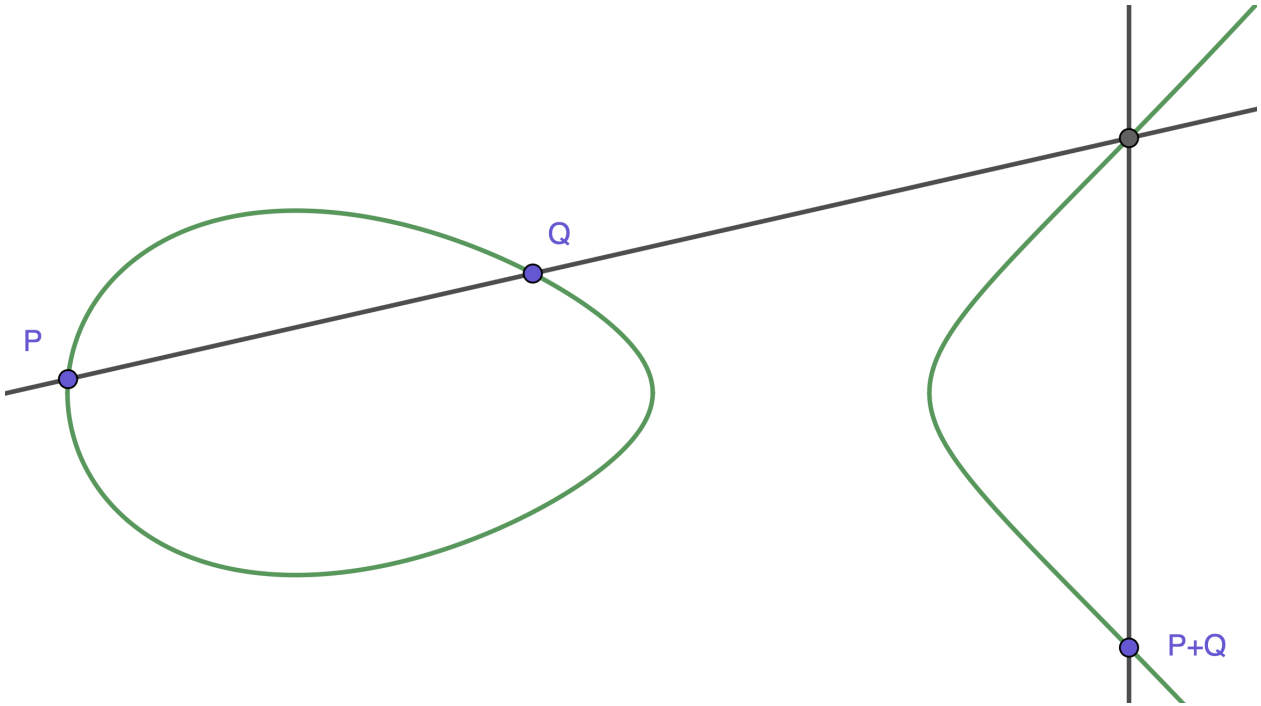
- *qt-Pegasis: Simpler and Faster Effective Class Group Actions*, with Jonathan Komada Eriksen, Riccardo Invernizzi and Frederik Vercauteren. Accepted at EUROCRYPT 2026.

On 4-dimensional isogeny computations:

- *Fast computation of 2-isogenies in dimension 4 and cryptographic applications*, single author, Journal of Algebra, 2025.
- *Chasing Rabbits Through Hypercubes: Better algorithms for higher dimensional 2-isogeny computations*, with Max Duparc, preprint, 2026.

Welcome to isogenyland

Elliptic curves

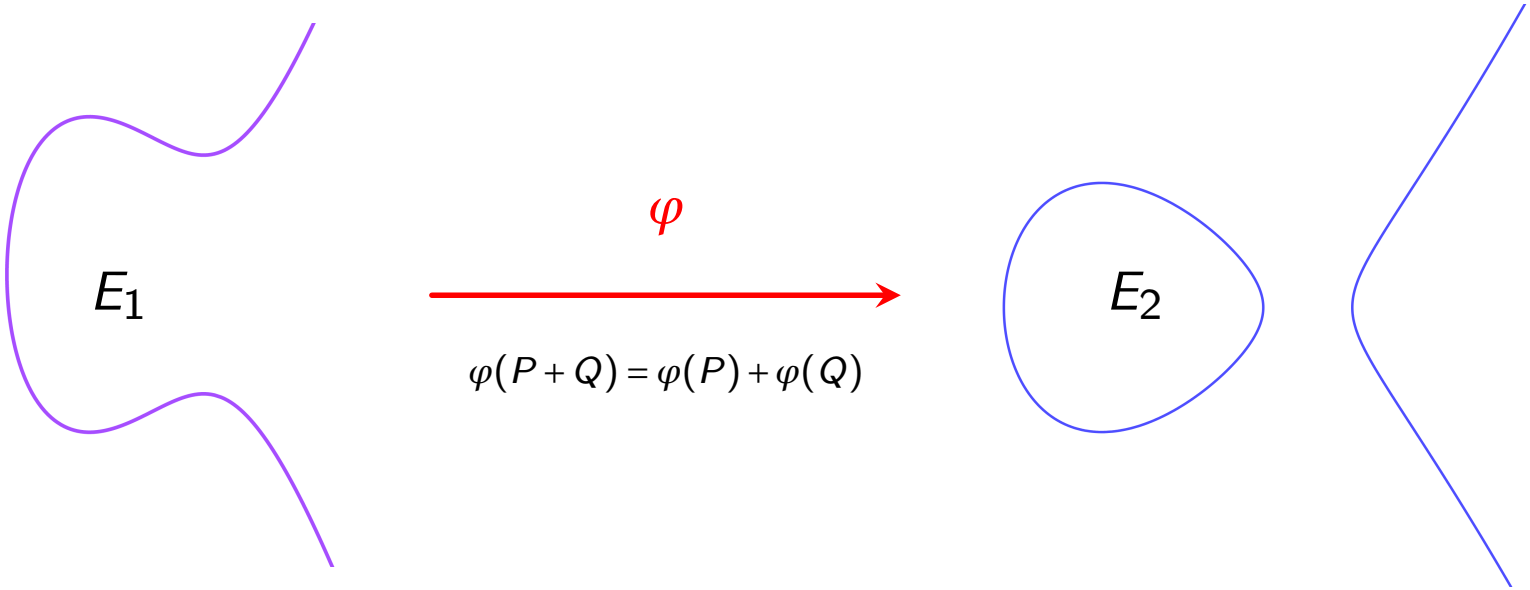


- An elliptic curve $E/\mathbb{F}_q$ is defined by:

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_q$$

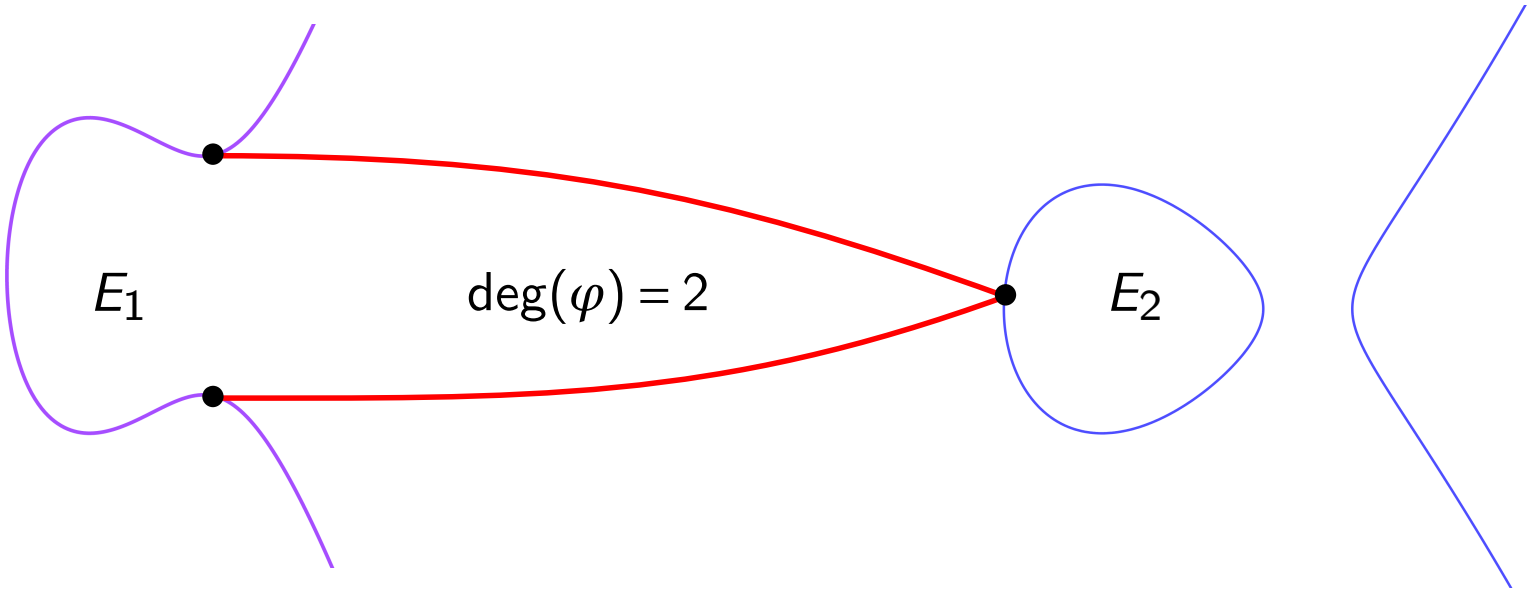
  with point at infinity 0_E.
- E is equipped with a commutative group law.

Isogenies



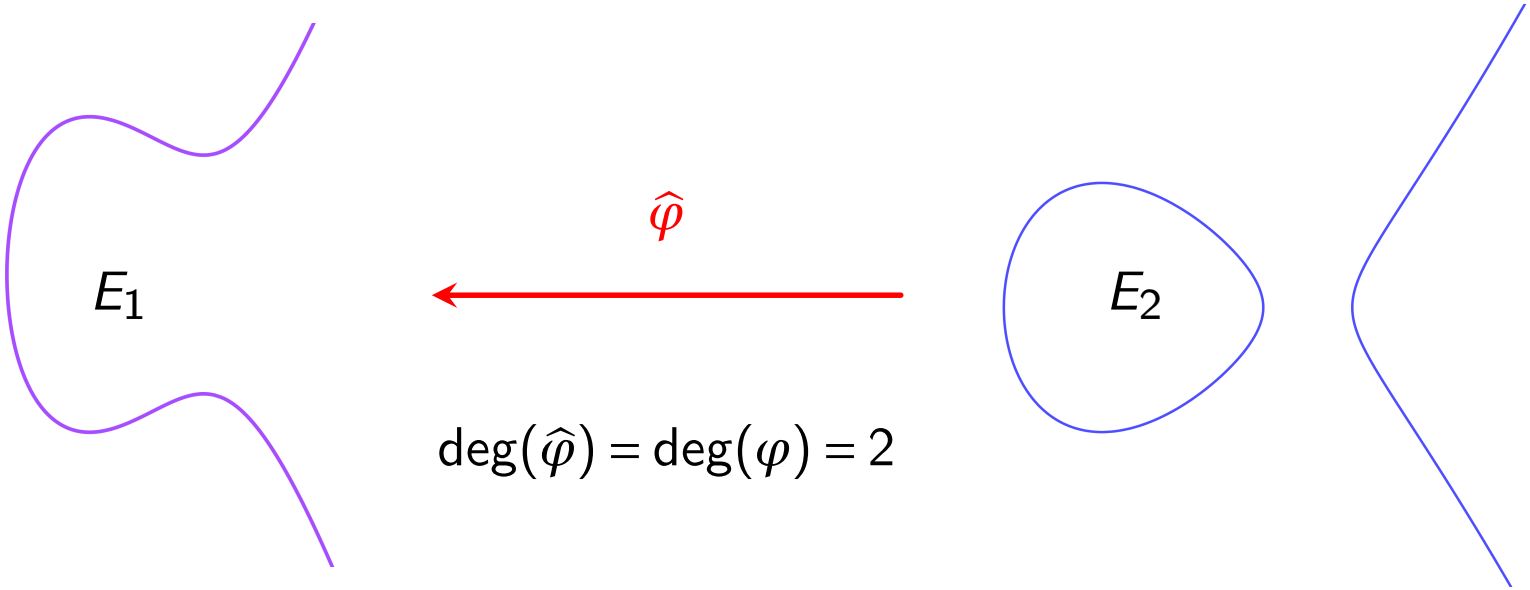
$$\varphi(x,y)=\left(\frac{p(x)}{q(x)},y\frac{r(x)}{s(x)}\right)$$

Isogenies - degree



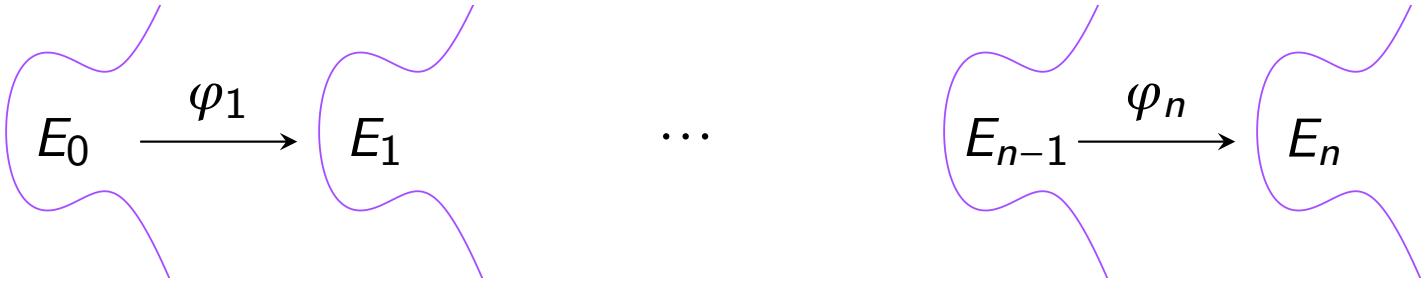
An isogeny of degree n is called an *n-isogeny*.

Isogenies - the dual isogeny



An n-isogeny φ satisfies $\widehat{\varphi} \circ \varphi = [n]$.

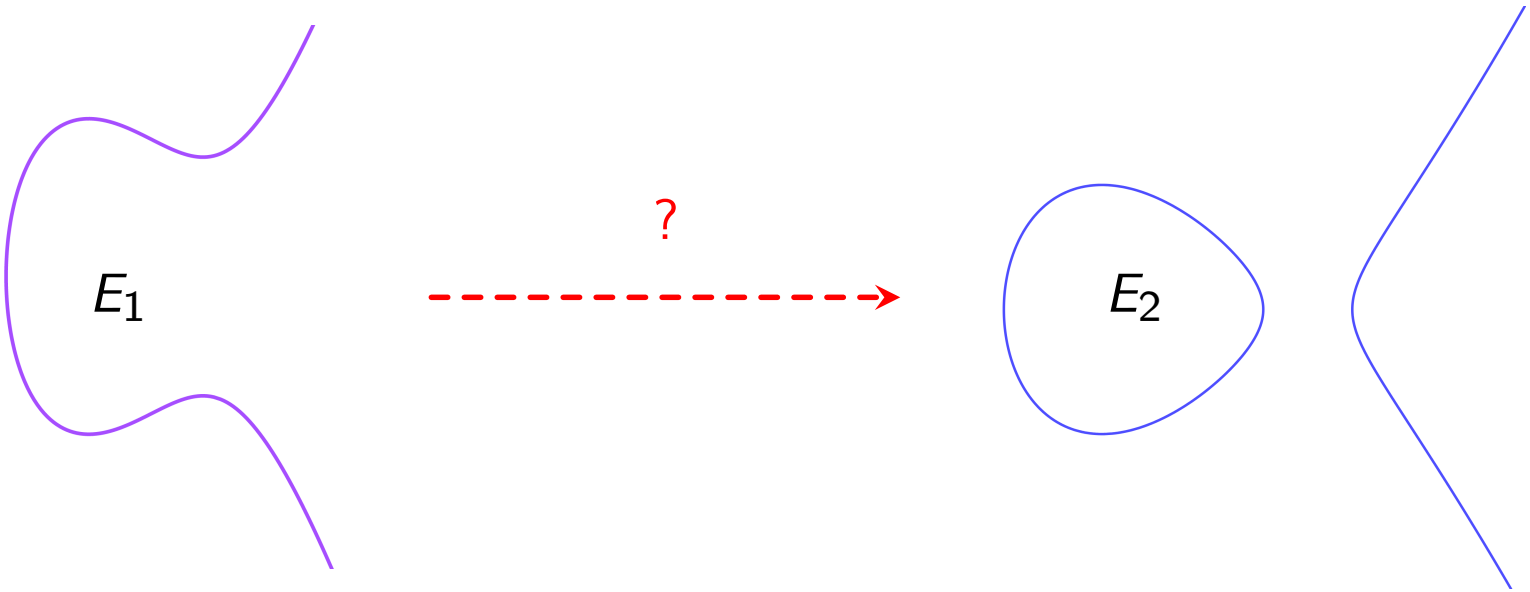
Isogeny chains



$$\deg(\varphi_n \circ \cdots \circ \varphi_1) = \prod_{i=1}^{n} \deg(\varphi_i)$$

Why are isogenies interesting in cryptography?

The isogeny problem: Given two elliptic curves $E_1, E_2/\mathbb{F}_q$, find an isogeny $E_1 \longrightarrow E_2$.



This problem is assumed to be hard for both classical and quantum computers.

What does it mean to "compute" an isogeny?

Definition (Efficient representation)

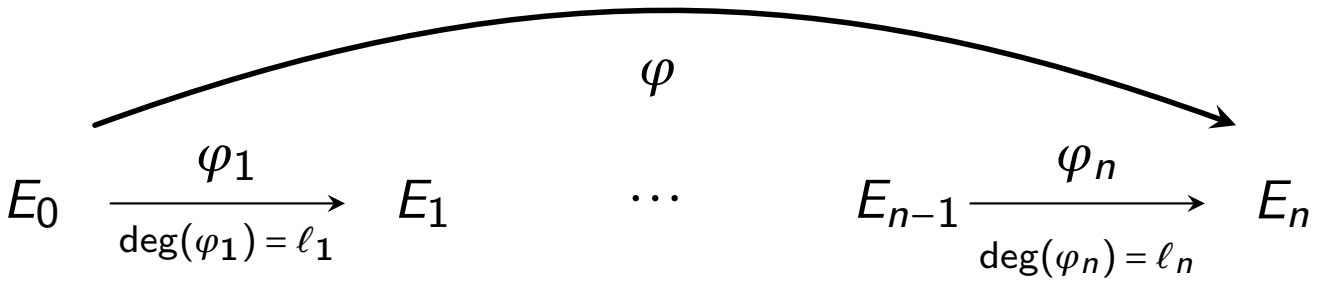
Let $\varphi : E \longrightarrow E'$ be a d-isogeny over $\mathbb{F}_q$. An efficient representation of φ with respect to an algorithm $\mathscr{A}$ is some data $D_\varphi \in \{0,1\}^*$ such that:

1. D_φ has size $\text{poly}(\log(d), \log(q))$.
2. For all $P \in E(\mathbb{F}_{q^k})$, $\mathscr{A}(D_\varphi, P)$ returns $\varphi(P)$ in time $\text{poly}(\log(d), k\log(q))$.

What does it mean to "compute" an isogeny?

Examples of efficient representations:

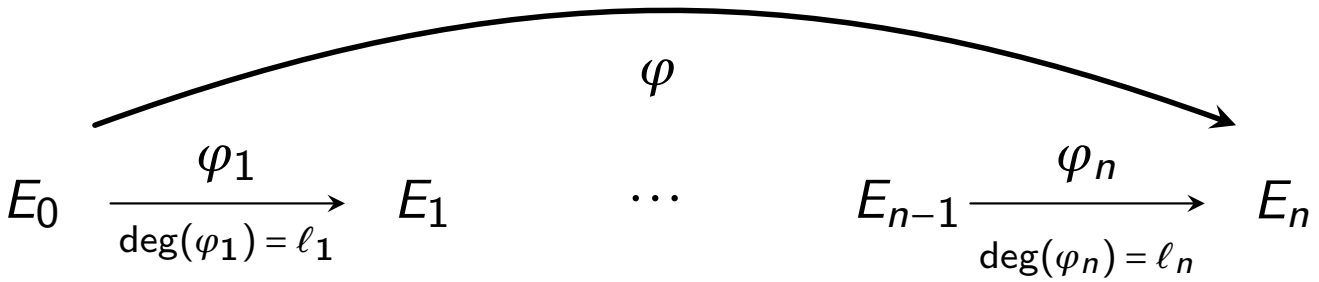
- If $\deg(\varphi) = \prod_{i=1}^{r} \ell_i$, a chain of isogenies:



What does it mean to "compute" an isogeny?

Examples of efficient representations:

- If $\deg(\varphi) = \prod_{i=1}^{r} \ell_i$, a chain of isogenies:

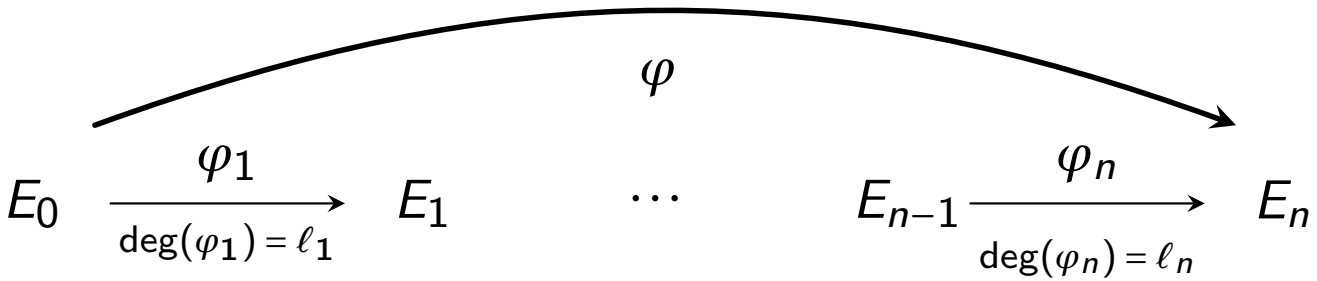


- If $\deg(\varphi)$ is smooth, a generator $P \in E(\mathbb{F}_q)$ s.t. $\ker(\varphi) = \langle P \rangle$ (Vélu).

What does it mean to "compute" an isogeny?

Examples of efficient representations:

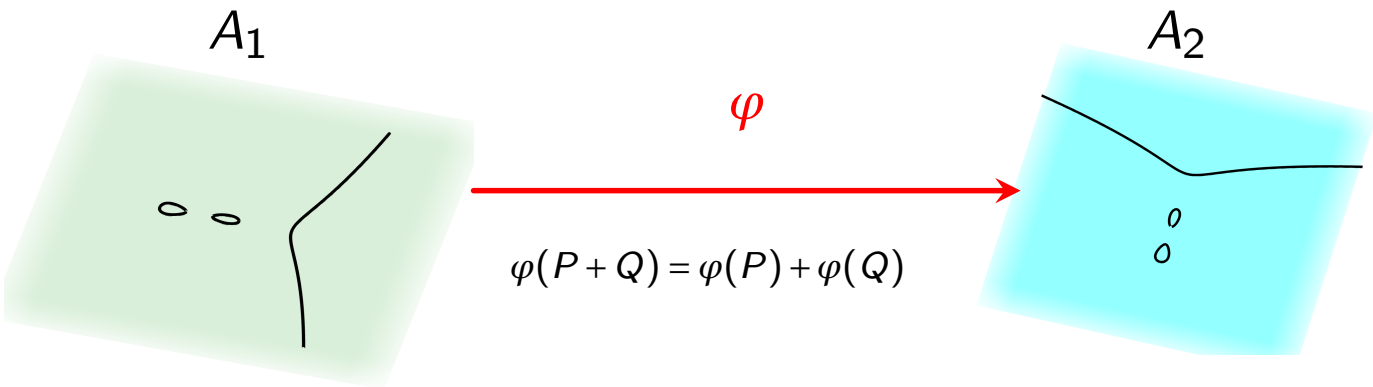
- If $\deg(\varphi) = \prod_{i=1}^{r} \ell_i$, a chain of isogenies:



- If $\deg(\varphi)$ is smooth, a generator $P \in E(\mathbb{F}_q)$ s.t. $\ker(\varphi) = \langle P \rangle$ (Vélu).
- **New:** If $\deg(\varphi) < 2^e$ is odd and $E[2^e] = \langle P, Q \rangle$, the image points $(\varphi(P), \varphi(Q))$ (higher dimensional interpolation).

Isogenies between abelian varieties

- Abelian varieties are projective abelian group varieties, generalizing elliptic curves.
- Between abelian varieties, isogenies are morphisms which are surjective and of finite kernel.



An isogeny between abelian surfaces

n-isogenies in higher dimension and their degree

- Let $\varphi : A \longrightarrow B$ be an isogeny between principally polarised abelian varieties (PPAVs).
- Then there exists a *contragradient isogeny* $\widetilde{\varphi} : B \longrightarrow A$ with $\deg(\varphi) = \deg(\widetilde{\varphi})$.

n-isogenies in higher dimension and their degree

- Let $\varphi : A \longrightarrow B$ be an isogeny between principally polarised abelian varieties (PPAVs).
- Then there exists a *contragradient isogeny* $\widetilde{\varphi} : B \longrightarrow A$ with $\deg(\varphi) = \deg(\widetilde{\varphi})$.
- φ is an n-isogeny if $\widetilde{\varphi} \circ \varphi = [n]$.

n-isogenies in higher dimension and their degree

- Let $\varphi : A \longrightarrow B$ be an isogeny between principally polarised abelian varieties (PPAVs).
- Then there exists a *contragradient isogeny* $\widetilde{\varphi} : B \longrightarrow A$ with $\deg(\varphi) = \deg(\widetilde{\varphi})$.
- φ is an n-isogeny if $\widetilde{\varphi} \circ \varphi = [n]$.
- ⚠ True between elliptic curves but not a general fact.
- ⚠ n-isogenies have degree n^g (with $g = \dim(A) = \dim(B)$).

The Endomorphism ring

Definition (Endomorphism ring)

$$\mathrm{End}(E) = \{0\} \cup \{\text{Isogenies } \varphi : E \longrightarrow E\}$$

Defines a ring for the addition and composition of isogenies.

The Endomorphism ring

Definition (Endomorphism ring)

$$\mathrm{End}(E) = \{0\} \cup \{\text{Isogenies } \varphi : E \longrightarrow E\}$$

Defines a ring for the addition and composition of isogenies.

Theorem (Deuring)

Let $E/\mathbb{F}_q$ ($p = \mathrm{char}(\mathbb{F}_q)$). Then $\mathrm{End}(E)$ is either isomorphic to:

- *An order in a quadratic imaginary field. We say that E is **ordinary**.*
- *A maximal order in a quaternion algebra. We say that E is **supersingular**.*

Ordinary vs. supersingular

- An **order** is a lattice with a ring structure.
- If E is ordinary, $\mathrm{End}(E) \simeq \mathbb{Z} \oplus \mathbb{Z}\alpha$ has rank 2 and is commutative.
- If E is supersingular, $\mathrm{End}(E) \simeq \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\gamma$ has rank 4 and is not commutative.

Ordinary vs. supersingular

- An **order** is a lattice with a ring structure.
- If E is ordinary, $\mathrm{End}(E) \simeq \mathbb{Z} \oplus \mathbb{Z}\alpha$ has rank 2 and is commutative.
- If E is supersingular, $\mathrm{End}(E) \simeq \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\beta \oplus \mathbb{Z}\gamma$ has rank 4 and is not commutative.

Why supersingular curves/isogenies are more efficient:

- If $E/\mathbb{F}_{p^n}$ is supersingular, it is isomorphic to $E'/\mathbb{F}_{p^2}$.
- If we choose p so that $N | p+1$, we can ensure $E[N] \subseteq E(\mathbb{F}_{p^2})$.

Efficient cryptographic group action from isogenies

Complex multiplication and ideal action

Definition

Let $\mathfrak{O}$ be a quadratic imaginary order and E be an ordinary elliptic curve. We say that E has **complex multiplication (CM)** by $\mathfrak{O}$ when $\mathrm{End}(E) \simeq \mathfrak{O}$.

Complex multiplication and ideal action

Definition

Let $\mathfrak{O}$ be a quadratic imaginary order and E be an ordinary elliptic curve. We say that E has **complex multiplication (CM)** by $\mathfrak{O}$ when $\mathrm{End}(E) \simeq \mathfrak{O}$.

- An ideal $\mathfrak{a} \subseteq \mathfrak{O}$ corresponds to an isogeny $\varphi_\mathfrak{a} : E \to \mathfrak{a} \cdot E$.
- $\mathfrak{a} \cdot E$ also has CM by $\mathfrak{O}$.
- If $\mathfrak{a} = \alpha\mathfrak{O}$ is principal, then $\varphi_\mathfrak{a}$ is an endomorphism $E \to \mathfrak{a} \cdot E \simeq E$.

Complex multiplication and ideal action

Definition

Let $\mathfrak{O}$ be a quadratic imaginary order and E be an ordinary elliptic curve. We say that E has **complex multiplication (CM)** by $\mathfrak{O}$ when $\mathrm{End}(E) \simeq \mathfrak{O}$.

- An ideal $\mathfrak{a} \subseteq \mathfrak{O}$ corresponds to an isogeny $\varphi_\mathfrak{a} : E \to \mathfrak{a} \cdot E$.
- $\mathfrak{a} \cdot E$ also has CM by $\mathfrak{O}$.
- If $\mathfrak{a} = \alpha\mathfrak{O}$ is principal, then $\varphi_\mathfrak{a}$ is an endomorphism $E \to \mathfrak{a} \cdot E \simeq E$.

Theorem

This defines a group action of the ideal class group of $\mathfrak{O}$:

$$\mathrm{Cl}(\mathfrak{O}) = \{\textit{Invertible ideals } \mathfrak{a} \subseteq \mathfrak{O}\}/\{\textit{Principal ideals } \alpha\mathfrak{O}\}$$

on the elliptic curves with CM by $\mathfrak{O}$. This action is free and transitive.

Ideal class group action on ordinary curves

$\mathfrak{O}$-ideals	Curves with CM by $\mathfrak{O}$ and isogenies
Ideal $\mathfrak{a} \subseteq \mathfrak{O}$	$\varphi_{\mathfrak{a}} : E \longrightarrow E_{\mathfrak{a}} := \mathfrak{a} \cdot E$
$\alpha\mathfrak{O}$	$[\alpha] : E \longrightarrow E$
$\mathfrak{b} \sim \mathfrak{a}$	$\mathfrak{a} \cdot E \simeq \mathfrak{b} \cdot E$
$\overline{\mathfrak{a}}$	$\widehat{\varphi}_{\mathfrak{a}}$
$\mathfrak{a}\mathfrak{b}$	$\varphi_{\mathfrak{b}} \circ \varphi_{\mathfrak{a}}$
$N(\mathfrak{a})$	$\deg(\varphi_{\mathfrak{a}})$

Ideal class group action on supersingular curves [CK20]

- **Issue:** Ordinary isogenies are slow to compute. So is the ideal class group action.

Ideal class group action on supersingular curves [CK20]

- **Issue:** Ordinary isogenies are slow to compute. So is the ideal class group action.
- **Solution:** Work with supersingular curves instead! [CLMPR18; CK20]

Ideal class group action on supersingular curves [CK20]

- **Issue:** Ordinary isogenies are slow to compute. So is the ideal class group action.
- **Solution:** Work with supersingular curves instead! [CLMPR18; CK20]
- Let $\mathfrak{O}$ be a quadratic imaginary order.
- A (primitively) $\mathfrak{O}$-*oriented* curve is a supersingular elliptic curve $E/\overline{\mathbb{F}}_p$ with a maximal embedding

$$\iota : \mathfrak{O} \hookrightarrow \mathrm{End}(E).$$

Ideal class group action on supersingular curves [CK20]

- **Issue:** Ordinary isogenies are slow to compute. So is the ideal class group action.
- **Solution:** Work with supersingular curves instead! [CLMPR18; CK20]
- Let $\mathfrak{O}$ be a quadratic imaginary order.
- A (primitively) $\mathfrak{O}$-*oriented* curve is a supersingular elliptic curve $E/\overline{\mathbb{F}}_p$ with a maximal embedding

$$\iota : \mathfrak{O} \hookrightarrow \mathrm{End}(E).$$

Theorem (Belding, Colò, Kohel)

$\mathrm{Cl}(\mathfrak{O})$ *acts freely on* $\mathfrak{O}$*-oriented curves and admits at most two orbits.*

Example: orientation defined by the Frobenius [CLMPR18]

- Let $E/\mathbb{F}_p$ supersingular and

  $$\pi_p : (x, y) \in E \longmapsto (x^p, y^p) \in E$$

  be its **Frobenius endomorphism**.

Example: orientation defined by the Frobenius [CLMPR18]

- Let $E/\mathbb{F}_p$ supersingular and

  $$\pi_p : (x, y) \in E \longmapsto (x^p, y^p) \in E$$

  be its **Frobenius endomorphism**.

- Then $\pi_p \circ \pi_p = [-p]$ so π_p defines an embedding $\mathbb{Z}[\sqrt{-p}] \hookrightarrow \mathrm{End}(E)$.

- E is either oriented by:
  - $\mathbb{Z}[\sqrt{-p}]$ (floor).
  - $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ (surface).

Example: orientation defined by the Frobenius [CLMPR18]

- Let $E/\mathbb{F}_p$ supersingular and

  $$\pi_p : (x, y) \in E \longmapsto (x^p, y^p) \in E$$

  be its **Frobenius endomorphism**.
- Then $\pi_p \circ \pi_p = [-p]$ so π_p defines an embedding $\mathbb{Z}[\sqrt{-p}] \hookrightarrow \mathrm{End}(E)$.
- E is either oriented by:
  - $\mathbb{Z}[\sqrt{-p}]$ (floor).
  - $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ (surface).
- Common setting in isogeny based cryptography.

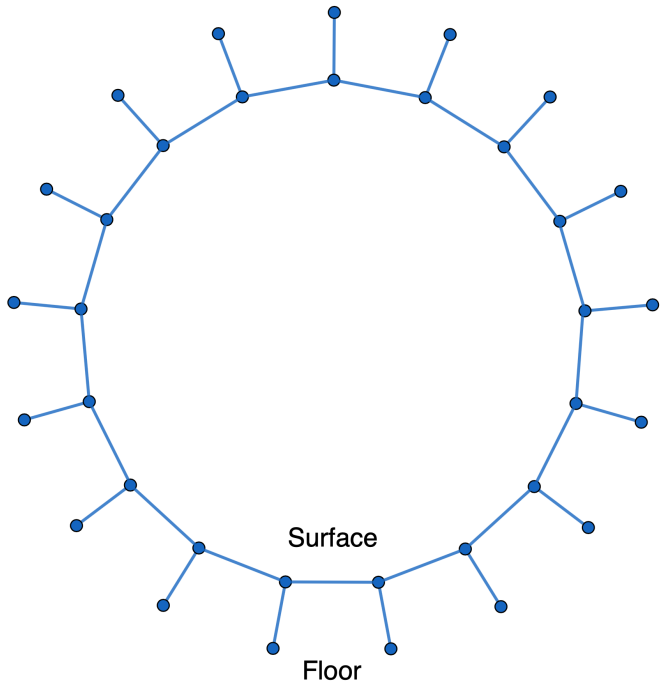


Figure: 2-isogeny volcano containing supersingular curves over $\mathbb{F}_{383}$. Segments represent 2-isogenies.

Cryptographic group action

The action of $\mathrm{Cl}(\mathfrak{O})$ is a **cryptographic group action*** because it is:

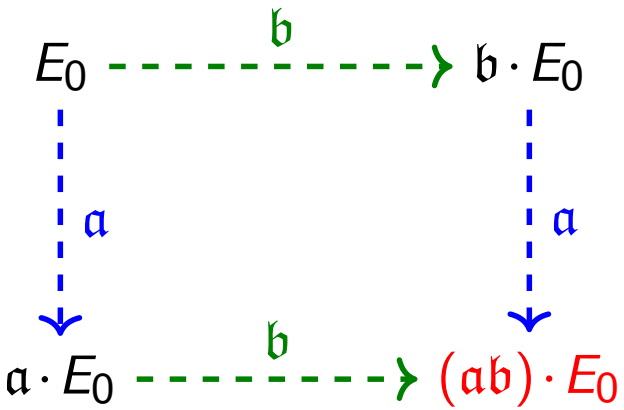
1. Commutative, free and transitive.
2. **Easy to compute**: $\mathfrak{a} \cdot E$ can be computed in polynomial time* given $\mathfrak{a} \subseteq \mathfrak{O}$ and E, $\mathfrak{O}$-oriented.
3. **One way**: given E and $\mathfrak{a} \cdot E$, $[\mathfrak{a}] \in \mathrm{Cl}(\mathfrak{O})$ is hard to find.

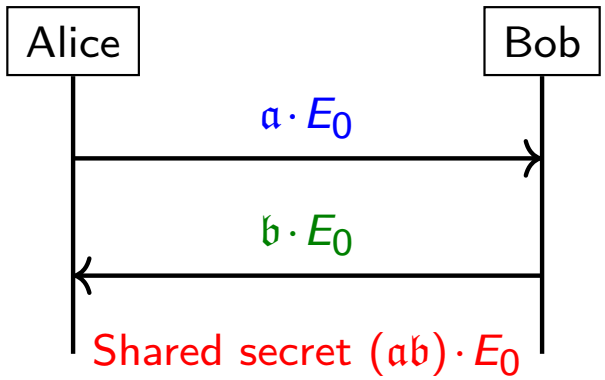
Cryptographic group action

The action of $\mathrm{Cl}(\mathfrak{O})$ is a **cryptographic group action*** because it is:

1. Commutative, free and transitive.
2. **Easy to compute**: $\mathfrak{a} \cdot E$ can be computed in polynomial time* given $\mathfrak{a} \subseteq \mathfrak{O}$ and E, $\mathfrak{O}$-oriented.
3. **One way**: given E and $\mathfrak{a} \cdot E$, $[\mathfrak{a}] \in \mathrm{Cl}(\mathfrak{O})$ is hard to find.

Application: Diffie-Hellman key exchange



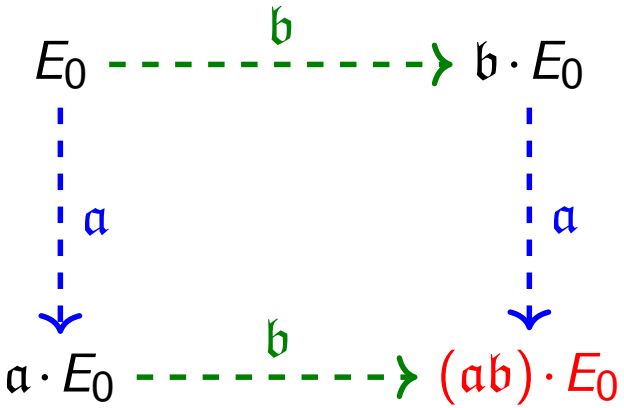


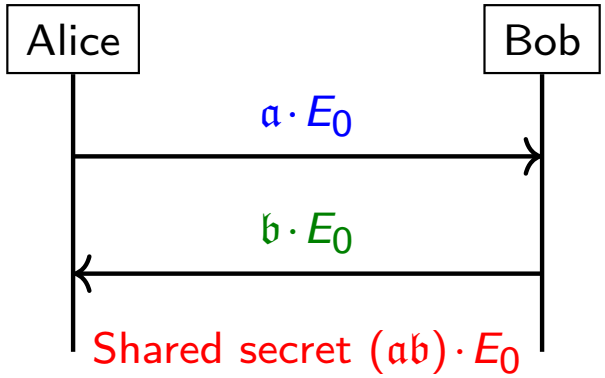
Cryptographic group action

The action of $\mathrm{Cl}(\mathfrak{O})$ is a ~~**cryptographic group action***~~ because it is:

1. Commutative, free and transitive.
2. ~~**Easy to compute**: $\mathfrak{a} \cdot E$ can be computed in polynomial time* given $\mathfrak{a} \subseteq \mathfrak{O}$ and E, $\mathfrak{O}$-oriented.~~
3. **One way**: given E and $\mathfrak{a} \cdot E$, $[\mathfrak{a}] \in \mathrm{Cl}(\mathfrak{O})$ is hard to find.

Application: Diffie-Hellman key exchange





Restricted cryptographic group action

- With standard techniques, we only knew how to compute the action by small norm ideals $\mathfrak{l}_1, \cdots, \mathfrak{l}_t$ and their products:

$$\left(\prod_{i=1}^{t} \mathfrak{l}_i^{e_i} \right) \cdot E$$

Restricted cryptographic group action

- With standard techniques, we only knew how to compute the action by small norm ideals $\mathfrak{l}_1, \cdots, \mathfrak{l}_t$ and their products:

$$\left(\prod_{i=1}^{t} \mathfrak{l}_i^{e_i}\right) \cdot E$$

- It is hard to sample classes of the form $[\prod_{i=1}^{t} \mathfrak{l}_i^{e_i}] \in \mathrm{Cl}(\mathfrak{O})$ uniformly at random.
- ⚠ Restricts some cryptographic applications as parameters grow to resist quantum attacks (Kuperberg [Kup05]).

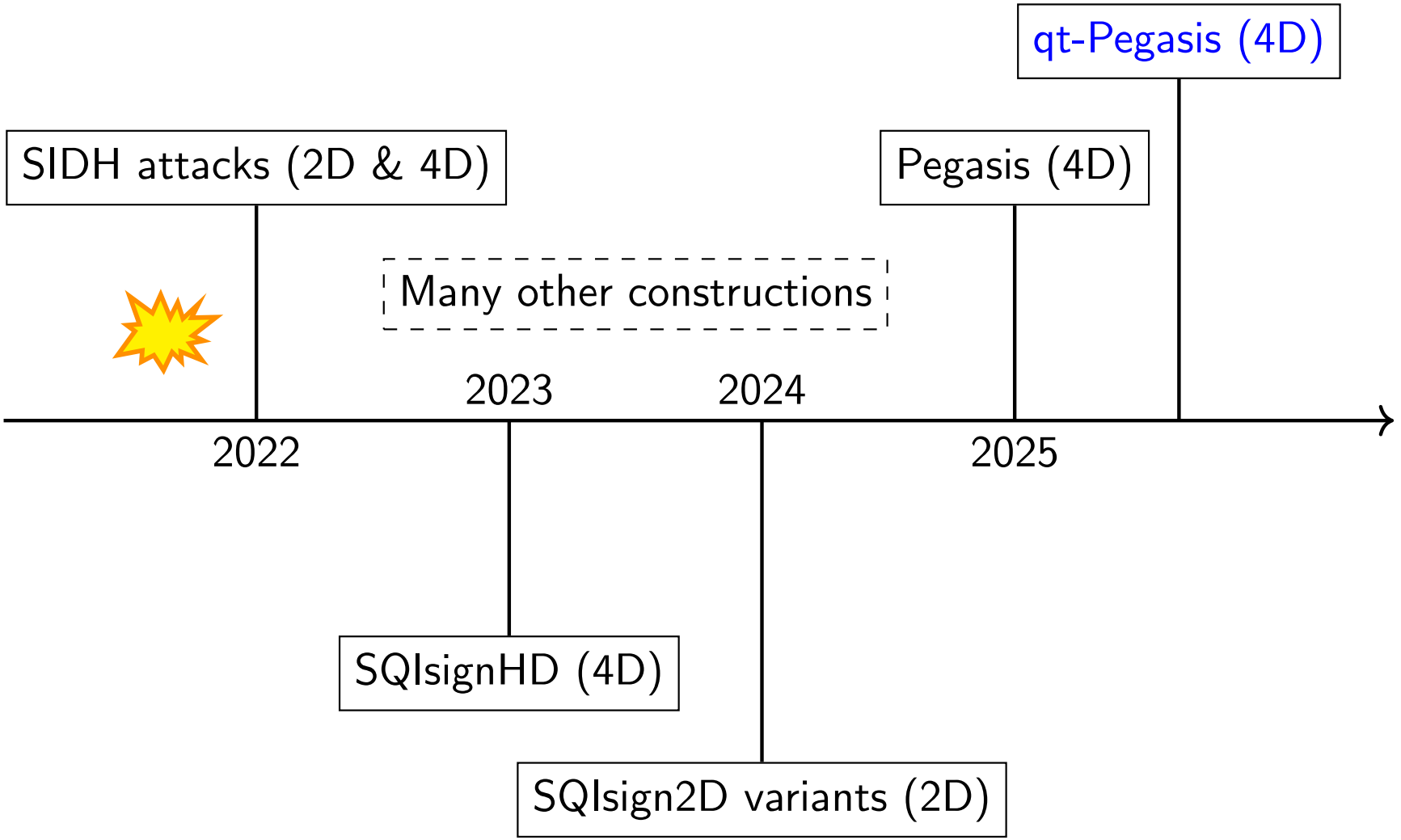
Restricted cryptographic group action

- With standard techniques, we only knew how to compute the action by small norm ideals $\mathfrak{l}_1, \cdots, \mathfrak{l}_t$ and their products:

$$\left(\prod_{i=1}^{t} \mathfrak{l}_i^{e_i}\right) \cdot E$$

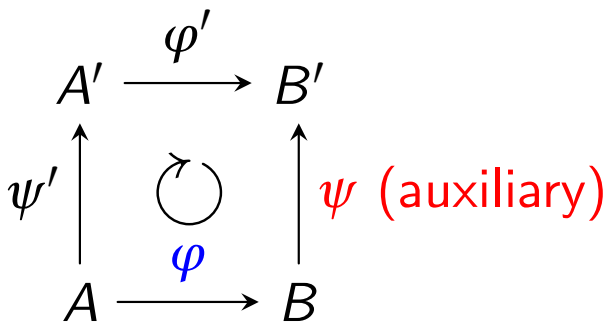
- It is hard to sample classes of the form $[\prod_{i=1}^{t} \mathfrak{l}_i^{e_i}] \in \mathrm{Cl}(\mathfrak{O})$ uniformly at random.
- ⚠ Restricts some cryptographic applications as parameters grow to resist quantum attacks (Kuperberg [Kup05]).
- Need to unrestrict the action by computing the action by $\mathfrak{a} \subseteq \mathfrak{O}$ of any norm.

The HD revolution



Kani's lemma [Kan97]

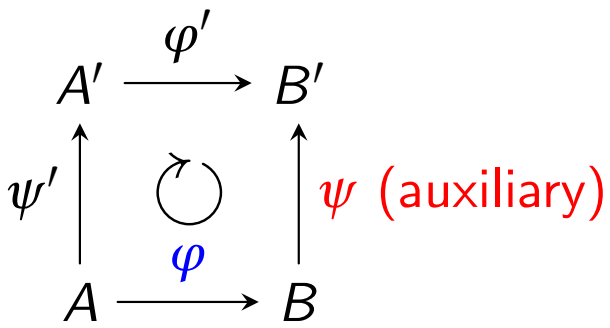
- Consider the commutative diagram:



where φ and φ' are q-isogenies and ψ and ψ' are r-isogenies.

Kani's lemma [Kan97]

- Consider the commutative diagram:



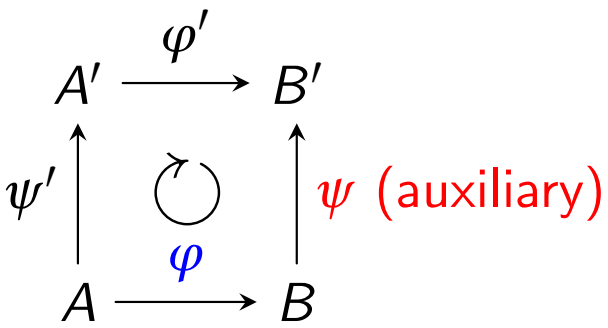
  where φ and φ' are q-isogenies and ψ and ψ' are r-isogenies.
- Assume that $\gcd(q, r) = 1$ and $q + r = 2^e$.
- Then

$$F := \begin{pmatrix} \varphi & \widehat{\psi} \\ -\psi' & \widehat{\varphi'} \end{pmatrix} : A \times B' \longrightarrow B \times A'$$

  is a 2^e-isogeny, i.e. $\widetilde{\Phi} \circ \Phi = [2^e]$.

Kani's lemma [Kan97]

- Consider the commutative diagram:



  where φ and φ' are q-isogenies and ψ and ψ' are r-isogenies.
- Assume that $\gcd(q, r) = 1$ and $q + r = 2^e$.
- Then

$$F := \begin{pmatrix} \varphi & \widehat{\psi} \\ -\psi' & \widehat{\varphi'} \end{pmatrix} : A \times B' \longrightarrow B \times A'$$

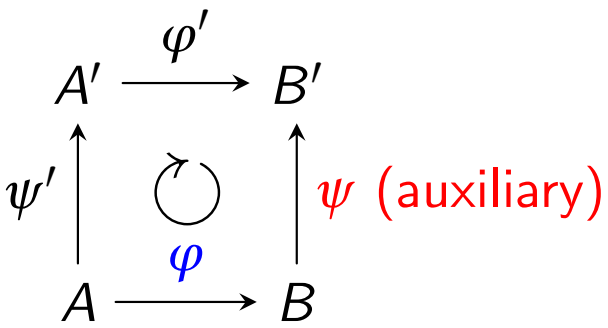
  is a 2^e-isogeny, i.e. $\widetilde{\Phi} \circ \Phi = [2^e]$.
- Its kernel is:

$$\ker(F) = \{([q]P, \psi \circ \varphi(P)) \mid P \in A[2^e]\},$$

  so F can be computed from q and $\psi \circ \varphi(A[2^e])$.

Kani's lemma [Kan97]

- Consider the commutative diagram:



  where φ and φ' are q-isogenies and ψ and ψ' are r-isogenies.
- Assume that $\gcd(q,r)=1$ and $q+r=2^e$.
- Then

$$F := \begin{pmatrix} \varphi & \widehat{\psi} \\ -\psi' & \widehat{\varphi'} \end{pmatrix} : A \times B' \longrightarrow B \times A'$$

  is a 2^e-isogeny, i.e. $\widetilde{\Phi} \circ \Phi = [2^e]$.
- Its kernel is:

$$\ker(F) = \{([q]P, \psi \circ \varphi(P)) \mid P \in A[2^e]\},$$

  so F can be computed from q and $\psi \circ \varphi(A[2^e])$.
- F **efficiently represents** φ:

$$F(P,0) = (\varphi(P), -\psi'(P)).$$

The Clapoti method [PR23]

Clapoti: CLass group Action in POlynomial TIme.

Goal: Given an $\mathfrak{O}$-oriented curve E and **any** ideal $\mathfrak{a} \subseteq \mathfrak{O}$, compute $E_\mathfrak{a} := \mathfrak{a} \cdot E$.

The Clapoti method [PR23]

Clapoti: CLass group Action in POlynomial TIme.

Goal: Given an $\mathfrak{O}$-oriented curve E and **any** ideal $\mathfrak{a} \subseteq \mathfrak{O}$, compute $E_\mathfrak{a} := \mathfrak{a} \cdot E$.

- **Step 1:** Solve a norm equation:

$$\sum_i u_i N(\mathfrak{b}_i) = 2^e \quad (\star)$$

  involving equivalent ideals $\mathfrak{b}_i \sim \mathfrak{a}$ and $u_i \in \mathbb{N}^*$.
- **Step 2:** Use the solution to $(\star)$ and Kani's lemma [Kan97] to compute a higher dimensional 2^e-isogeny F.
- **Step 3:** Extract $E_\mathfrak{a}$ from the codomain of F.

qt-Pegasis [DEIV25]

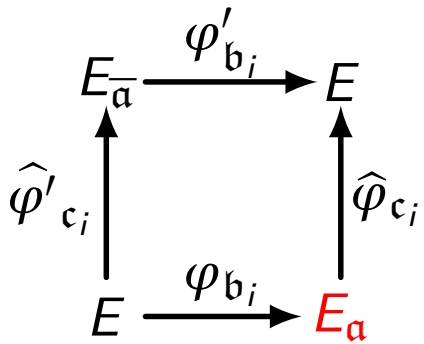
- **Step 1:** Find $\mathfrak{b}_1, \mathfrak{c}_1, \mathfrak{b}_2, \mathfrak{c}_2 \sim \mathfrak{a}$ such that

$$N(\mathfrak{b}_1) + N(\mathfrak{c}_1) + N(\mathfrak{b}_2) + N(\mathfrak{c}_2) = 2^e$$

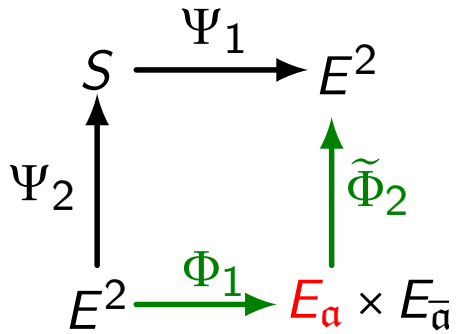
with $N(\mathfrak{b}_i)$ odd and $N(\mathfrak{c}_i)$ even.

- **Step 2:** Compute $F : E^4 \to E_\mathfrak{a} \times E_{\overline{\mathfrak{a}}} \times S$ given by ([Kan97] $\times 2$):

In 2D



In 4D



$$\Phi_i := \begin{pmatrix} \varphi_{\mathfrak{b}_i} & \varphi_{\mathfrak{c}_i} \\ -\widehat{\varphi}'_{\mathfrak{c}_i} & \widehat{\varphi}'_{\mathfrak{b}_i} \end{pmatrix} : E^2 \to E_\mathfrak{a} \times E_{\overline{\mathfrak{a}}} \qquad F := \begin{pmatrix} \Phi_1 & \Phi_2 \\ -\Psi_2 & \widetilde{\Psi}_1 \end{pmatrix} : E^4 \to E_\mathfrak{a} \times E_{\overline{\mathfrak{a}}} \times S$$

Comparison with state of the art

Paper	$\log_2(\lvert\Delta_{\mathfrak{O}}\rvert)$	500	1000	1500	2000	4000
SCALLOP [FFK+23]*	C++	35s	12m30s	–	–	–
SCALLOP-HD [CLP24]*	Sage	88s	19m	–	–	–
PEARL-SCALLOP [ABE+24]	C++	30s	58s	12m	–	–
KLaPoTi [PPS24]	Sage	200s	–	–	–	–
	Rust	1.95s	–	–	–	–
Pegasis [DEF+25]	Sage	1.53s	4.21s	10.5s	21.3s	122s
qt-Pegasis [DEIV25]	Sage	0.85s	2.48s	5.54s	9.69s	47.6s
	C (prelim.)	41ms	204ms	0.65s	1.45s	11.5s

Table: Comparison between (qt-)Pegasis and other effective group actions in the literature. The last 5 columns gives the timings corresponding to the different security levels, where s/m gives the number of seconds/minutes in wall-clock time. SCALLOP and SCALLOP-HD are starred because they were measured on a different hardware setup.

Down the rabbit hole of 4-dimensional isogenies

Definition: symplectic isomorphism

- Let A/k be a PPAV of dimension g.
- If $n \nmid \mathrm{char}(k)$, then $A[n] \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$.

Definition: symplectic isomorphism

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

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

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

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

Definition: theta structure

Definition (Mumford, Duparc)

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

$$\begin{aligned} \theta^{A,n} : A &\longrightarrow \mathbb{P}^{n^g-1} \\ P &\longmapsto (\theta_i^A(P))_{i\in(\mathbb{Z}/n\mathbb{Z})^g} \end{aligned}$$

along with a symplectic isomorphism (*i.e.* that respects pairings):

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

satisfying the *theta group action relation*:

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

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

The case of level $n = 2$

- We use theta structures of level $n = 2$.
- This gives the minimal number of coordinates (2^g) that is arithmetically relevant.

  NB: We drop the 2 exponent $\theta^A = \theta^{A,2}$.

The case of level $n = 2$

- We use theta structures of level $n = 2$.
- This gives the minimal number of coordinates (2^g) that is arithmetically relevant.

  NB: We drop the 2 exponent $\theta^A = \theta^{A,2}$.
- If A is not a (polarised) product, a level 2 theta structure induces an embedding of the Kummer variety:

$$\theta^A : A/\pm \hookrightarrow \mathbb{P}^{2^g-1}$$

- Points are represented up to sign: $\theta^A(P) = \theta^A(-P)$ for all $P \in A$.

The case of level $n = 2$

- We use theta structures of level $n = 2$.
- This gives the minimal number of coordinates (2^g) that is arithmetically relevant.

  NB: We drop the 2 exponent $\theta^A = \theta^{A,2}$.
- If A is not a (polarised) product, a level 2 theta structure induces an embedding of the Kummer variety:

$$\theta^A : A/\pm \hookrightarrow \mathbb{P}^{2^g-1}$$

- Points are represented up to sign: $\theta^A(P) = \theta^A(-P)$ for all $P \in A$.
- Analogue of working with $(x : z)$-coordinates over elliptic curves, *e.g.* we have differential addition formulas

$$(\theta^A(P), \theta^A(Q), \theta^A(P-Q)) \longmapsto \theta^A(P+Q).$$

Computing a 2^e-isogeny: example of qt-Pegasis

Goal: Compute a 2^e-isogeny $F : A \longrightarrow B$ when given $T_1, \cdots, T_g \in A[2^{e+2}]$ such that $\ker(F) = \langle [4]T_1, \cdots, [4]T_g \rangle$. The computation is done in level 2 theta coordinates:

$$\theta^A(P) \longmapsto \theta^B(F(P))$$

Computing a 2^e-isogeny: example of qt-Pegasis

Goal: Compute a 2^e-isogeny $F : A \longrightarrow B$ when given $T_1, \cdots, T_g \in A[2^{e+2}]$ such that $\ker(F) = \langle [4]T_1, \cdots, [4]T_g \rangle$. The computation is done in level 2 theta coordinates:

$$\theta^A(P) \longmapsto \theta^B(F(P))$$

Method (ex. qt-Pegasis, $g = 4$): Decompose F into a chain of 2-isogenies of length e:

$$A = E^4 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \quad \cdots \quad A_{e-2} \xrightarrow{f_{e-1}} A_{e-1} \xrightarrow{f_e} B = E_{\mathfrak{a}} \times E_{\overline{\mathfrak{a}}} \times S$$

Gluing — Generic isogenies — Splitting

Computing a 2^e-isogeny: example of qt-Pegasis

$$A = E^4 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \quad \cdots \quad A_{e-2} \xrightarrow{f_{e-1}} A_{e-1} \xrightarrow{f_e} B = E_{\mathfrak{a}} \times E_{\overline{\mathfrak{a}}} \times S$$

Gluing — Generic isogenies — Splitting

Steps:

1. **Gluing:** Compute the gluing $f_1 : A \to A_1$.
   Using 8-torsion points $[2^{e-1}]T_1, \cdots, [2^{e-1}]T_g$.

Computing a 2^e-isogeny: example of qt-Pegasis

$$A = E^4 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \quad \cdots \quad A_{e-2} \xrightarrow{f_{e-1}} A_{e-1} \xrightarrow{f_e} B = E_{\mathfrak{a}} \times E_{\overline{\mathfrak{a}}} \times S$$

Gluing — Generic isogenies — Splitting

Steps:

1. **Gluing:** Compute the gluing $f_1 : A \to A_1$.
   Using 8-torsion points $[2^{e-1}]T_1, \cdots, [2^{e-1}]T_g$.
2. **Generic:** Compute generic isogenies $f_i : A_{i-1} \to A_i$ $(2 \leq i \leq e)$.
   Using 8-torsion points $[2^{e-i}]f_{i-1} \circ \cdots \circ f_1(T_1, \cdots, T_g)$.

Computing a 2^e-isogeny: example of qt-Pegasis

$$A = E^4 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \quad \cdots \quad A_{e-2} \xrightarrow{f_{e-1}} A_{e-1} \xrightarrow{f_e} B = E_{\mathfrak{a}} \times E_{\overline{\mathfrak{a}}} \times S$$

Gluing — Generic isogenies — Splitting

Steps:

1. **Gluing:** Compute the gluing $f_1 : A \to A_1$.
   Using 8-torsion points $[2^{e-1}]T_1, \cdots, [2^{e-1}]T_g$.

2. **Generic:** Compute generic isogenies $f_i : A_{i-1} \to A_i$ $(2 \leq i \leq e)$.
   Using 8-torsion points $[2^{e-i}]f_{i-1} \circ \cdots \circ f_1(T_1, \cdots, T_g)$.
   $O(g \cdot e \log(e))$ point duplications and 2-isogeny evaluations needed.

Computing a 2^e-isogeny: example of qt-Pegasis

$$A = E^4 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \quad \cdots \quad A_{e-2} \xrightarrow{f_{e-1}} A_{e-1} \xrightarrow{f_e} B = E_{\mathfrak{a}} \times E_{\overline{\mathfrak{a}}} \times S$$

Gluing — Generic isogenies — Splitting

Steps:

1. **Gluing:** Compute the gluing $f_1 : A \to A_1$.
   Using 8-torsion points $[2^{e-1}]T_1, \cdots, [2^{e-1}]T_g$.

2. **Generic:** Compute generic isogenies $f_i : A_{i-1} \to A_i$ $(2 \le i \le e)$.
   Using 8-torsion points $[2^{e-i}]f_{i-1} \circ \cdots \circ f_1(T_1, \cdots, T_g)$.
   $O(g \cdot e \log(e))$ point duplications and 2-isogeny evaluations needed.

3. **Splitting:** Split the codomain B (into $E_{\mathfrak{a}} \times E_{\overline{\mathfrak{a}}} \times S$).

Computing a 2^e-isogeny: example of qt-Pegasis

$$A = E^4 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \quad \cdots \quad A_{e-2} \xrightarrow{f_{e-1}} A_{e-1} \xrightarrow{f_e} B = E_a \times E_{\overline{a}} \times S$$

Gluing — Generic isogenies — Splitting

Steps:

1. **Gluing:** Compute the gluing $f_1 : A \to A_1$.
   Using 8-torsion points $[2^{e-1}]T_1, \cdots, [2^{e-1}]T_g$.

2. **Generic:** Compute generic isogenies $f_i : A_{i-1} \to A_i$ $(2 \leq i \leq e)$.
   Using 8-torsion points $[2^{e-i}]f_{i-1} \circ \cdots \circ f_1(T_1, \cdots, T_g)$.
   $O(g \cdot e \log(e))$ point duplications and 2-isogeny evaluations needed.

3. **Splitting:** Split the codomain B (into $E_a \times E_{\overline{a}} \times S$).

Computing a generic 2-isogeny

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

Assumptions: We are given:

Computing a generic 2-isogeny

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

Assumptions: We are given:

- A level 2 theta structure $\Theta_A := (\theta^A, \overline{\Theta}^A)$ compatible with f:

$$\overline{\Theta}^A(\{0\} \times \widehat{(\mathbb{Z}/2\mathbb{Z})^g}) = \ker(f).$$

Computing a generic 2-isogeny

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

Assumptions: We are given:

- A level 2 theta structure $\Theta_A := (\theta^A, \overline{\Theta}^A)$ compatible with f:

$$\overline{\Theta}^A(\{0\} \times \widehat{(\mathbb{Z}/2\mathbb{Z})^g}) = \ker(f).$$

- The theta coordinates $\theta^A(T_1), \cdots, \theta^A(T_g)$ of 8-torsion points such that $\ker(f) = \langle [4]T_1, \cdots, [4]T_g \rangle$.

Computing a generic 2-isogeny

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

Assumptions: We are given:

- A level 2 theta structure $\Theta_A := (\theta^A, \overline{\Theta}^A)$ compatible with f:

$$\overline{\Theta}^A(\{0\} \times \widehat{(\mathbb{Z}/2\mathbb{Z})^g}) = \ker(f).$$

- The theta coordinates $\theta^A(T_1), \cdots, \theta^A(T_g)$ of 8-torsion points such that $\ker(f) = \langle [4]T_1, \cdots, [4]T_g \rangle$.

Steps: To compute f we can:

1. From $\theta^A(T_1), \cdots, \theta^A(T_g)$, compute the codomain **theta null point** $\theta^B(0_B)$ determining* a codomain theta structure $\Theta_B := (\theta^B, \overline{\Theta}^B)$.

Computing a generic 2-isogeny

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

Assumptions: We are given:

- A level 2 theta structure $\Theta_A := (\theta^A, \overline{\Theta}^A)$ compatible with f:

$$\overline{\Theta}^A(\{0\} \times \widehat{(\mathbb{Z}/2\mathbb{Z})^g}) = \ker(f).$$

- The theta coordinates $\theta^A(T_1), \cdots, \theta^A(T_g)$ of 8-torsion points such that $\ker(f) = \langle [4]T_1, \cdots, [4]T_g \rangle$.

Steps: To compute f we can:

1. From $\theta^A(T_1), \cdots, \theta^A(T_g)$, compute the codomain **theta null point** $\theta^B(0_B)$ determining* a codomain theta structure $\Theta_B := (\theta^B, \overline{\Theta}^B)$.
2. From $\theta^B(0_B)$, we can evaluate f at any point:

$$\theta^A(P) \longmapsto \theta^B(f(P)).$$

Generic 2-isogeny - evaluation

- Consider the **Hadamard transform**:

$$H : (x_i)_{i \in (\mathbb{Z}/2\mathbb{Z})^g} \longmapsto \left(\sum_{i \in (\mathbb{Z}/2\mathbb{Z})^g} (-1)^{\langle i|j \rangle} x_i \right)_{j \in (\mathbb{Z}/2\mathbb{Z})^g}$$

  where $\langle .|. \rangle$ is the usual scalar product.

- Let $\widetilde{\theta}^B := H(\theta^B)$ be the **dual theta coordinates**.

Generic 2-isogeny - evaluation

- Consider the **Hadamard transform**:

$$H : (x_i)_{i \in (\mathbb{Z}/2\mathbb{Z})^g} \longmapsto \left(\sum_{i \in (\mathbb{Z}/2\mathbb{Z})^g} (-1)^{\langle i|j \rangle} x_i \right)_{j \in (\mathbb{Z}/2\mathbb{Z})^g}$$

  where $\langle .|. \rangle$ is the usual scalar product.

- Let $\widetilde{\theta}^B := H(\theta^B)$ be the **dual theta coordinates**.
- Consider the **dot product** $(x_i)_i \odot (y_i)_i := (x_i \cdot y_i)_i$.
- And $(x_i)_i^{\odot n} := (x_i^n)_i$ for all $n \in \mathbb{Z}$.

Generic 2-isogeny - evaluation

- Consider the **Hadamard transform**:

$$H : (x_i)_{i \in (\mathbb{Z}/2\mathbb{Z})^g} \longmapsto \left(\sum_{i \in (\mathbb{Z}/2\mathbb{Z})^g} (-1)^{\langle i|j \rangle} x_i \right)_{j \in (\mathbb{Z}/2\mathbb{Z})^g}$$

  where $\langle .|. \rangle$ is the usual scalar product.

- Let $\widetilde{\theta}^B := H(\theta^B)$ be the **dual theta coordinates**.
- Consider the **dot product** $(x_i)_i \odot (y_i)_i := (x_i \cdot y_i)_i$.
- And $(x_i)_i^{\odot n} := (x_i^n)_i$ for all $n \in \mathbb{Z}$.
- **Evaluation formula:** for all $P \in A$,

$$\widetilde{\theta}^B(0_B) \odot \widetilde{\theta}^B(f(P)) = H(\theta^A(P)^{\odot 2}).$$

Generic 2-isogeny - evaluation

- Fron the evaluation formula, we get:

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

- A very simple isogeny evaluation algorithm:

$$\theta^A(P) \xrightarrow{\bullet^{\odot 2}} * \xrightarrow{H} * \xrightarrow{\odot \widetilde{\theta}^B(0_B)^{\odot -1}} * \xrightarrow{H} \theta^B(f(P))$$

- We need to precompute the inverse codomain dual theta null point $\widetilde{\theta}^B(0_B)^{\odot -1}$.

Generic 2-isogeny - codomain computation

- Applying the evaluation formula to $P = T_m$ $(1 \leq m \leq g)$, we get:

$$\widetilde{\theta}^B(0_B) \odot \widetilde{\theta}^B(f(T_m)) = H(\theta^A(T_m)^{\odot 2}).$$

- And by standard properties of theta coordinates:

$$\forall i \in (\mathbb{Z}/2\mathbb{Z})^g, \quad \widetilde{\theta}^B_i(f(T_m)) = \widetilde{\theta}^B_{i+e_m}(f(T_m)),$$

  where $e_{m,n} = 1$ if $n = m$ and 0 otherwise.
- It follows that for all $i \in (\mathbb{Z}/2\mathbb{Z})^g$,

$$\widetilde{\theta}^B_i(0_B) \cdot H(\theta^A(T_m)^{\odot 2})_{i+e_m} = \widetilde{\theta}^B_{i+e_m}(0_B) \cdot H(\theta^A(T_m)^{\odot 2})_i.$$

Generic 2-isogeny - codomain computation

A graph theoretic problem:

- From $\widetilde{\theta}_i^B(0_B)^{-1}$, we obtain $\widetilde{\theta}_{i+e_m}^B(0_B)^{-1}$:

$$\widetilde{\theta}_{i+e_m}^B(0_B)^{-1} = \widetilde{\theta}_i^B(0_B)^{-1} \cdot \frac{H(\theta^A(T_m)^{\odot 2})_i}{H(\theta^A(T_m)^{\odot 2})_{i+e_m}},$$

whenever $H(\theta^A(T_m)^{\odot 2})_{i+e_m} \neq 0$.

Generic 2-isogeny - codomain computation

A graph theoretic problem:

- From $\widetilde{\theta}_i^B(0_B)^{-1}$, we obtain $\widetilde{\theta}_{i+e_m}^B(0_B)^{-1}$:

$$\widetilde{\theta}_{i+e_m}^B(0_B)^{-1} = \widetilde{\theta}_i^B(0_B)^{-1} \cdot \frac{H(\theta^A(T_m)^{\odot 2})_i}{H(\theta^A(T_m)^{\odot 2})_{i+e_m}},$$

  whenever $H(\theta^A(T_m)^{\odot 2})_{i+e_m} \neq 0$.

- Consider a subgraph of the hypercube of dimension g.
- Vertices: $i \in (\mathbb{Z}/2\mathbb{Z})^g$ labelled by $\widetilde{\theta}_i^B(0_B)^{-1}$.
- Edges: $(i, i+e_m)$ such that $H(\theta^A(T_m)^{\odot 2})_{i+e_m} \neq 0$ labelled by ratios.

Generic 2-isogeny - codomain computation

A graph theoretic problem:

- From $\widetilde{\theta}_i^B(0_B)^{-1}$, we obtain $\widetilde{\theta}_{i+e_m}^B(0_B)^{-1}$:

$$\widetilde{\theta}_{i+e_m}^B(0_B)^{-1} = \widetilde{\theta}_i^B(0_B)^{-1} \cdot \frac{H(\theta^A(T_m)^{\odot 2})_i}{H(\theta^A(T_m)^{\odot 2})_{i+e_m}},$$

  whenever $H(\theta^A(T_m)^{\odot 2})_{i+e_m} \neq 0$.

- Consider a subgraph of the hypercube of dimension g.
- Vertices: $i \in (\mathbb{Z}/2\mathbb{Z})^g$ labelled by $\widetilde{\theta}_i^B(0_B)^{-1}$.
- Edges: $(i, i+e_m)$ such that $H(\theta^A(T_m)^{\odot 2})_{i+e_m} \neq 0$ labelled by ratios.

Theorem (D., Duparc, 2026)

We can compute $\widetilde{\theta}^B(0_B)^{\odot -1}$ iff the graph is connected.

Generic 2-isogeny - codomain computation

A graph theoretic problem:

- In practice, we find a covering subtree.
- Use **Hamiltonian paths** to reduce the cost.
- Example for $g = 3$:

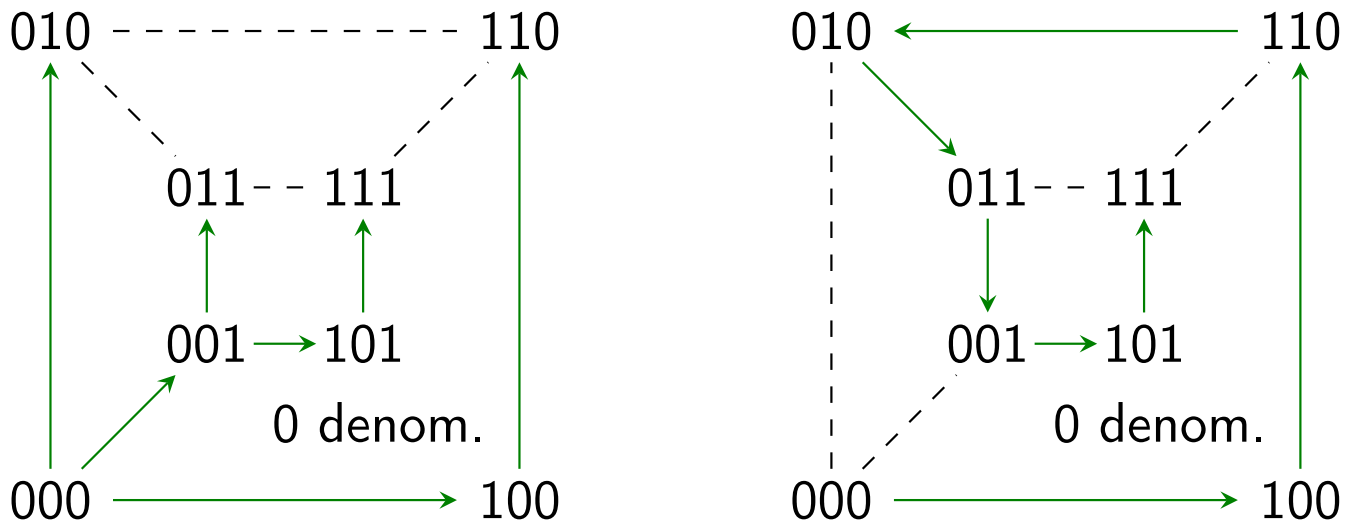


Figure: Non-hamiltonian covering tree (left) and Hamiltonian path (right).

Generic 2-isogeny - codomain computation

- We compute $\widetilde{\theta}^B(0_B)^{\odot -1}$ projectively. No inversion needed.
- The Hamiltonian path method reduces the cost compared to the former one (any covering subtree):

	dim. g	dim. 4
Old method [Dar25]	$(6\cdot 2^g - 9)\mathrm{M} + g2^g\mathrm{S} + g^2 2^g\mathrm{a}$	$87\mathrm{M} + 64\mathrm{S} + 256\mathrm{a}$
New method [DD26]	$3(2^g - 2)\mathrm{M} + g2^g\mathrm{S} + g^2 2^g\mathrm{a}$	$42\mathrm{M} + 64\mathrm{S} + 256\mathrm{a}$

Table: Computational cost of codomain theta null-point computation with the old and new methods in dimensions g and 4. M, S and a are respectively the cost of one multiplication, squaring and addition/subtraction over the base field.

Computing a 2^e-isogeny: example of qt-Pegasis

$$A = E^4 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \quad \cdots \quad A_{e-2} \xrightarrow{f_{e-1}} A_{e-1} \xrightarrow{f_e} B = E_a \times E_{\overline{a}} \times S$$

Gluing — Generic isogenies — Splitting

Steps:

1. **Gluing:** Compute the gluing $f_1 : A \to A_1$.
   Using 8-torsion points $[2^{e-1}]T_1, \cdots, [2^{e-1}]T_g$.
2. **Generic:** Compute generic isogenies $f_i : A_{i-1} \to A_i$ $(2 \le i \le e)$.
   Using 8-torsion points $[2^{e-i}]f_{i-1} \circ \cdots \circ f_1(T_1, \cdots, T_g)$.
   $O(g \cdot e \log(e))$ point duplications and 2-isogeny evaluations needed.
3. **Splitting:** Split the codomain B (into $E_a \times E_{\overline{a}} \times S$).

Gluing isogeny (qt-Pegasis) - domain theta structure

Problem: how to obtain a level 2 theta structure on $A = E^4$ compatible with a gluing $f : A = E^4 \to B$ (similar to qt-Pegasis)?

- Let X, Z be Montgomery coordinates of E.
- Level 2 theta structure Θ_E on E: $\theta^E := (a(X - Z) : b(X + Z))$, with a, b depending on a basis of $E[4]$.

Gluing isogeny (qt-Pegasis) - domain theta structure

Problem: how to obtain a level 2 theta structure on $A = E^4$ compatible with a gluing $f : A = E^4 \to B$ (similar to qt-Pegasis)?

- Let X, Z be Montgomery coordinates of E.
- Level 2 theta structure Θ_E on E: $\theta^E := (a(X-Z) : b(X+Z))$, with a, b depending on a basis of $E[4]$.
- Product level 2 theta structure $\Theta_A = \Theta_E \times \Theta_E \times \Theta_E \times \Theta_E$ on $A = E^4$:

$$\theta^A = \theta^E \otimes \theta^E \otimes \theta^E \otimes \theta^E.$$

Gluing isogeny (qt-Pegasis) - domain theta structure

Problem: how to obtain a level 2 theta structure on $A = E^4$ compatible with a gluing $f : A = E^4 \to B$ (similar to qt-Pegasis)?

- Let X, Z be Montgomery coordinates of E.
- Level 2 theta structure Θ_E on E: $\theta^E := (a(X-Z) : b(X+Z))$, with a, b depending on a basis of $E[4]$.
- Product level 2 theta structure $\Theta_A = \Theta_E \times \Theta_E \times \Theta_E \times \Theta_E$ on $A = E^4$:

$$\theta^A = \theta^E \otimes \theta^E \otimes \theta^E \otimes \theta^E.$$

- **Issue:** Θ_A is not compatible with f, $\overline{\Theta_A}(\{0\} \times \widehat{(\mathbb{Z}/2\mathbb{Z})^g}) \neq \ker(f)$.
- **Solution:** Compute a change of theta structure $\Theta_A \to \Theta'_A$ such that $\overline{\Theta'_A}(\{0\} \times \widehat{(\mathbb{Z}/2\mathbb{Z})^g}) = \ker(f)$.

Gluing isogeny (qt-Pegasis) - evaluation

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

Gluing isogeny (qt-Pegasis) - evaluation

- The evaluation algorithm no longer works because the $\widetilde{\theta}_i^B(0_B)$ may vanish.
- Why? Because level 2 theta coordinates embeds product of Kummers:

$$\theta^A : E/\pm \times E/\pm \times E/\pm \times E/\pm \hookrightarrow \mathbb{P}^{2^4-1}$$

- So we are computing:

$$(\pm P_1, \pm P_2, \pm P_3, \pm P_4) \longmapsto \pm f(P_1, P_2, P_3, P_4)$$

- We need additional information to lift the sign indeterminations.

Gluing isogeny (qt-Pegasis) - evaluation

- The evaluation algorithm no longer works because the $\widetilde{\theta}_i^B(0_B)$ may vanish.
- Why? Because level 2 theta coordinates embeds product of Kummers:

$$\theta^A : E/\pm \times E/\pm \times E/\pm \times E/\pm \hookrightarrow \mathbb{P}^{2^4-1}$$

- So we are computing:

$$(\pm P_1, \pm P_2, \pm P_3, \pm P_4) \longmapsto \pm f(P_1, P_2, P_3, P_4)$$

- We need additional information to lift the sign indeterminations.

Solution: Using P and translates $P+T$, we can evaluate $f(P)$ [Dar25].

New: Exploit the symmetries in the evaluation formula [DD26].

Gluing isogeny (qt-Pegasis) - evaluation

New gluing evaluation method:

- Evaluation formula:

$$\widetilde{\theta}^B(f(T)) \odot \widetilde{\theta}^B(f(P)) = H(\theta^A(P+T) \odot \theta^A(P-T))$$

- We use $T \in A[16]$ such that $[8]T \in \ker(f)$.

Gluing isogeny (qt-Pegasis) - evaluation

New gluing evaluation method:

- Evaluation formula:

$$\widetilde{\theta}^B(f(T)) \odot \widetilde{\theta}^B(f(P)) = H(\theta^A(P+T) \odot \theta^A(P-T))$$

- We use $T \in A[16]$ such that $[8]T \in \ker(f)$.
- $\theta^A(P+T)$ and $\theta^A(P-T)$ can be computed simultaneously and efficiently using *barycentric coordinates* [Dup25].

Gluing isogeny (qt-Pegasis) - evaluation

New gluing evaluation method:

- Evaluation formula:

$$\widetilde{\theta}^B(f(T)) \odot \widetilde{\theta}^B(f(P)) = H(\theta^A(P+T) \odot \theta^A(P-T))$$

- We use $T \in A[16]$ such that $[8]T \in \ker(f)$.
- $\theta^A(P+T)$ and $\theta^A(P-T)$ can be computed simultaneously and efficiently using *barycentric coordinates* [Dup25].
- $\widetilde{\theta}^B(f(T))^{\odot -1}$ has to be precomputed instead of $\widetilde{\theta}^B(0_B)^{\odot -1}$.

Gluing isogeny (qt-Pegasis) - codomain computation

Problem: how to compute $\widetilde{\theta}^B(f(T))^{\odot -1}$?

- We use the evaluation formula for $1 \leq m \leq 4$:

$$\widetilde{\theta}^B(f(T)) \odot \widetilde{\theta}^B(f(T_m)) = H(\theta^A(T_m + T) \odot \theta^A(T_m - T))$$

Gluing isogeny (qt-Pegasis) - codomain computation

Problem: how to compute $\widetilde{\theta}^B(f(T))^{\odot -1}$?

- We use the evaluation formula for $1 \leq m \leq 4$:

$$\widetilde{\theta}^B(f(T)) \odot \widetilde{\theta}^B(f(T_m)) = H(\theta^A(T_m + T) \odot \theta^A(T_m - T))$$

- Using $\widetilde{\theta}^B_i(f(T_m)) = \widetilde{\theta}^B_{i+e_m}(f(T_m))$, we obtain:

$$\widetilde{\theta}^B_i(f(T)) \cdot \pi_{e_m, i+e_m} = \widetilde{\theta}^B_{i+e_m}(f(T)) \cdot \pi_{e_m, i}.$$

with $\pi_{e_m,i} = H(\theta^A(T_m + T) \odot \theta^A(T_m - T))_i$.

Gluing isogeny (qt-Pegasis) - codomain computation

Problem: how to compute $\widetilde{\theta}^B(f(T))^{\odot -1}$?

- We use the evaluation formula for $1 \leq m \leq 4$:

$$\widetilde{\theta}^B(f(T)) \odot \widetilde{\theta}^B(f(T_m)) = H(\theta^A(T_m + T) \odot \theta^A(T_m - T))$$

- Using $\widetilde{\theta}^B_i(f(T_m)) = \widetilde{\theta}^B_{i+e_m}(f(T_m))$, we obtain:

$$\widetilde{\theta}^B_i(f(T)) \cdot \pi_{e_m, i+e_m} = \widetilde{\theta}^B_{i+e_m}(f(T)) \cdot \pi_{e_m, i}.$$

  with $\pi_{e_m,i} = H(\theta^A(T_m + T) \odot \theta^A(T_m - T))_i$.

- We can obtain $\widetilde{\theta}^B_{i+e_m}(f(T))^{-1}$ from $\widetilde{\theta}^B_i(f(T))^{-1}$ as previously.

Gluing isogeny (qt-Pegasis) - codomain computation

Another graph theoretic problem:

- Vertices: $i \in (\mathbb{Z}/2\mathbb{Z})^g$ labelled by $\widetilde{\theta}_i^B(f(T))^{-1}$.
- Edges: $(i, i+e_m)$ such that $\pi_{e_m,i} \neq 0$ labelled by $\pi_{e_m,i}/\pi_{e_m,i+e_m}$.

Gluing isogeny (qt-Pegasis) - codomain computation

Another graph theoretic problem:

- Vertices: $i \in (\mathbb{Z}/2\mathbb{Z})^g$ labelled by $\widetilde{\theta}_i^B(f(T))^{-1}$.
- Edges: $(i, i+e_m)$ such that $\pi_{e_m,i} \neq 0$ labelled by $\pi_{e_m,i}/\pi_{e_m,i+e_m}$.
- **Issue:** The graph is not connected!

Gluing isogeny (qt-Pegasis) - codomain computation

Another graph theoretic problem:

- Vertices: $i \in (\mathbb{Z}/2\mathbb{Z})^g$ labelled by $\widetilde{\theta}_i^B(f(T))^{-1}$.
- Edges: $(i, i+e_m)$ such that $\pi_{e_m,i} \neq 0$ labelled by $\pi_{e_m,i}/\pi_{e_m,i+e_m}$.
- **Issue:** The graph is not connected!
- We need to add a 5-th point $T_n + T_q$ and use:

$$\widetilde{\theta}_i^B(f(T)) \cdot \pi_{e_n+e_q,i+e_n+e_q} = \widetilde{\theta}_{i+e_n+e_q}^B(f(T)) \cdot \pi_{e_n+e_q,i},$$

  with $\pi_{e_n+e_q,i} = H(\theta^A(T_n + T_q + T) \odot \theta^A(T_n + T_q - T))_i$.
- Additional edges: $(i, i+e_n+e_q)$ such that $\pi_{e_n+e_q,i} \neq 0$ **yield a connected graph.**

Gluing isogeny (qt-Pegasis) - codomain computation

We found the rabbit!

- Can we find a Hamiltonian path in the graph to reduce the computational cost?

Gluing isogeny (qt-Pegasis) - codomain computation

We found the rabbit!

- Can we find a Hamiltonian path in the graph to reduce the computational cost?
- No!
- Why? Because the graph has a rabbit structure.

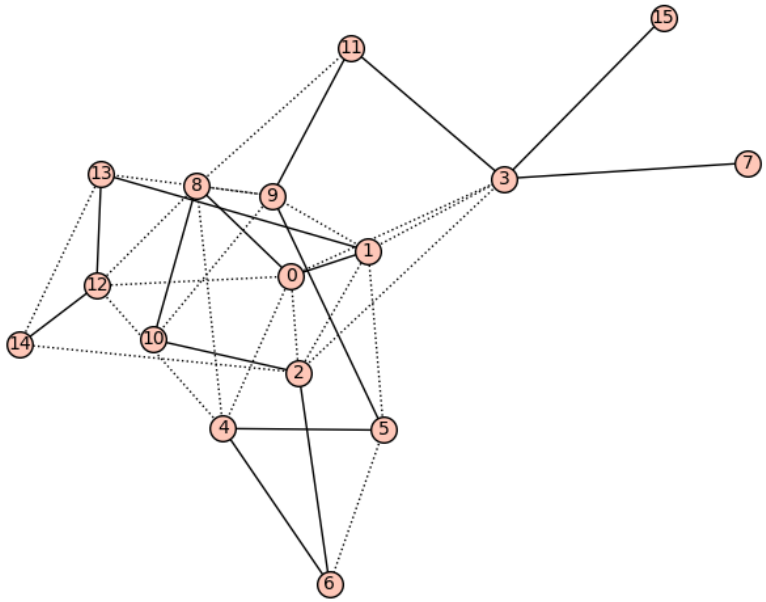


Figure: Example of rabbit shaped graph to compute the gluing in qt-Pegasis. Vectors $i \in (\mathbb{Z}/2\mathbb{Z})^4$ are represented as integers decomposed in base 2 as $i_1 + 2i_2 + 4i_3 + 8i_4$.

Computing a 2^e-isogeny: example of qt-Pegasis

$$A = E^4 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \quad \cdots \quad A_{e-2} \xrightarrow{f_{e-1}} A_{e-1} \xrightarrow{f_e} B = E_{\mathfrak{a}} \times E_{\overline{\mathfrak{a}}} \times S$$

Gluing — Generic isogenies — Splitting

Steps:

1. **Gluing:** Compute the gluing $f_1 : A \to A_1$.
   Using 8-torsion points $[2^{e-1}]T_1, \cdots, [2^{e-1}]T_g$.
2. **Generic:** Compute generic isogenies $f_i : A_{i-1} \to A_i$ $(2 \le i \le e)$.
   Using 8-torsion points $[2^{e-i}]f_{i-1} \circ \cdots \circ f_1(T_1, \cdots, T_g)$.
   $O(g \cdot e \log(e))$ point duplications and 2-isogeny evaluations needed.
3. **Splitting:** Split the codomain B (into $E_{\mathfrak{a}} \times E_{\overline{\mathfrak{a}}} \times S$).

Splitting

- From the last isogeny (splitting) $f_e : A_{e-1} \to A_e = B$, we obtain a level 2 theta structure Θ_B.
- In general, Θ_B is not a product whereas $B = E_\mathfrak{a} \times E_{\overline{\mathfrak{a}}} \times S$.
- Applying a change of theta structure $\Theta_B \to \Theta'_B$, we obtain a product theta structure $\Theta'_B = \Theta_{E_\mathfrak{a}} \times \Theta_{E_{\overline{\mathfrak{a}}}} \times \Theta_S$.
- From Θ'_B, we extract $\Theta_{E_\mathfrak{a}}$.
- From $\Theta_{E_\mathfrak{a}}$, we find the equation of $E_\mathfrak{a}$.

Experimental results (qt-Pegasis)

With our new formulae [DD26], we gain:

- A constant time 2-isogeny chain.
- Faster kernel computation and gluing by working fully over $\mathbb{F}_p$.
- Faster generic codomain computations using Hamiltonian paths.

Table: Comparison between new and old formulae in the SageMath implementation of qt-Pegasis. Results are the average of 100 runs on an AMD Ryzen 77840 U 8 cores CPU with 3.3 GHz clock speed, running Ubuntu 24.04.02 LTS, using SageMath 10.6 and Python 3.12.11.

$\lceil \log_2(p) \rceil$	Old formulae	New formulae	Gain
505	0.757	0.613	19.0 %
1008	2.155	1.889	12.3 %
1525	4.516	4.013	12.3 %
2017	8.152	7.431	11.1 %
4030	41.426	39.073	5.7 %

Thank you for listening

- 4-dimensional isogenies can be efficient.
- qt-Pegasis allows for advanced cryptographic applications (NIST PQarrots future candidate).

Future works:

- Progress needed to solve the norm equation in constant time.
- Research to lower the dimension (*e.g.* 2-dimensional Pegasis) .

My works can be found on my webpage: