

Revenge of the 4D: Can 4-dimensional isogenies become practical?

Pierrick Dartois

2025, December 9



- 1 Isogenies and the Deuring correspondence
- 2 From 1D to 4D to 2D: a brief history of SQIsign
- 3 The 4D revival: (qt-)Pegasis and MIKE
- 4 Computing higher dimensional isogenies

Overview of my contributions involved in this presentation

On SQIsign:

- *SQIsignHD: New Dimensions in Cryptography*, with Antonin Leroux, Damien Robert and Benjamin Wesolowski. EUROCRYPT 2024.
- *SQIsign2D-West: The Fast, the Small and the Safer*, with Andrea Basso, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert and Benjamin Wesolowski. ASIACRYPT 2024.

Overview of my contributions involved in this presentation

On new 4D applications:

- *PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies*, with Jonathan Komada Eriksen, Tako Boris Fouotsa, Arthur Herlédan Le Merdy, Riccardo Invernizzi, Damien Robert, Ryan Rueger, Frederik Vercauteren and Benjamin Wesolowski. CRYPTO 2025.
- *qt-Pegasis: Simpler and Faster Effective Class Group Actions*, with Jonathan Komada Eriksen, Riccardo Invernizzi and Frederik Vercauteren. Preprint, 2025.
- Implementation of MIKE *in preparation*, with Jonathan Komada Eriksen, Krijn Reijnders, Damien Robert and Ryan Rueger.

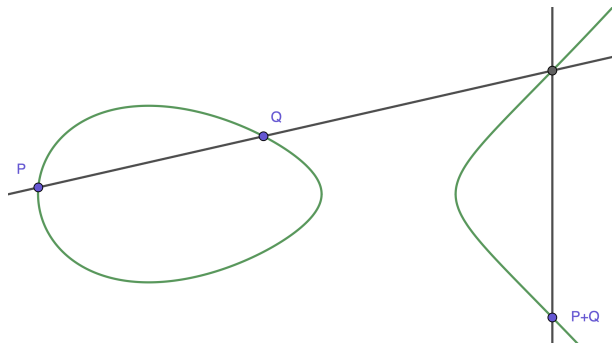
Overview of my contributions involved in this presentation

On 4D computations:

- *Fast computation of 2-isogenies in dimension 4 and cryptographic applications*, single author, Journal of Algebra, 2025.
- Improving 4-dimensional isogeny formulae *in preparation*, with Max Duparc.

Isogenies and the Deuring correspondence

Elliptic curves



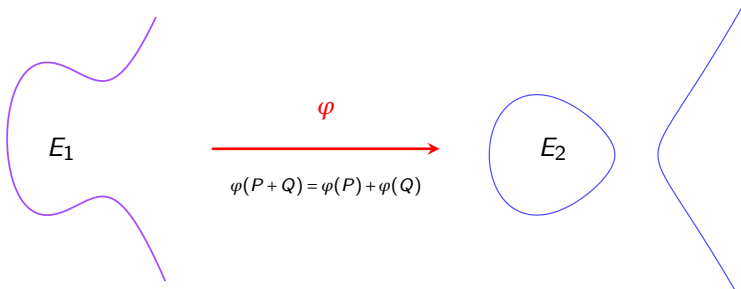
- An elliptic curve E/\mathbb{F}_q is defined by:

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

with an infinite element 0_E .

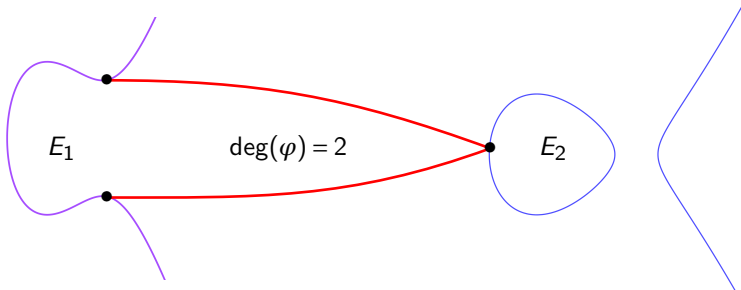
- E is equipped with a commutative group law.

Isogenies



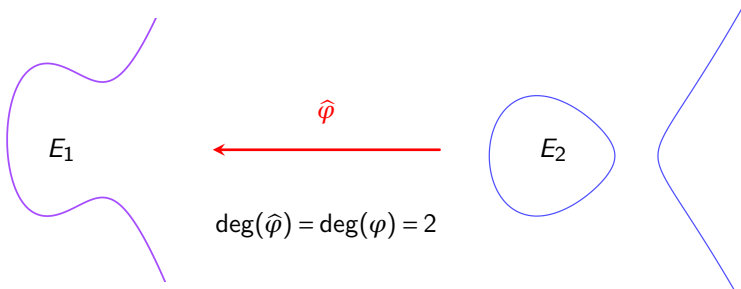
$$\varphi(x, y) = \left(\frac{p(x)}{q(x)}, y \frac{r(x)}{s(x)} \right)$$

Isogenies - degree



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

Isogenies - the dual isogeny



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

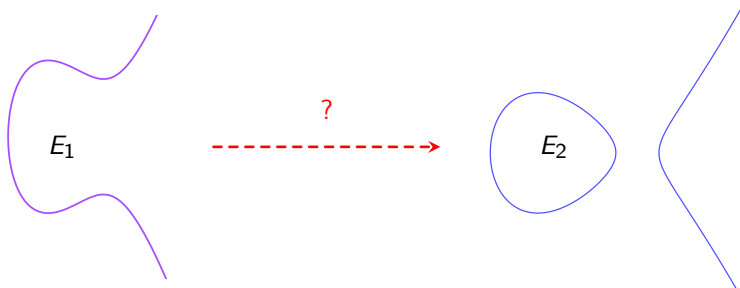
Isogeny chains



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

Why are isogenies interesting in cryptography?

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



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

What does it mean to "compute" an isogeny?

Definition (Efficient representation)

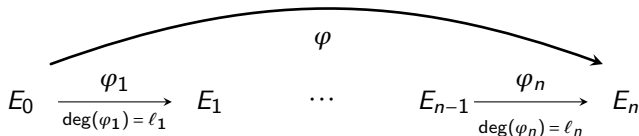
Let $\varphi : E \rightarrow E'$ be a d -isogeny over \mathbb{F}_q . An efficient representation of φ with respect to an algorithm \mathcal{A} is some data $D_\varphi \in \{0,1\}^*$ such that:

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

What does it mean to "compute" an isogeny?

Examples of efficient representations:

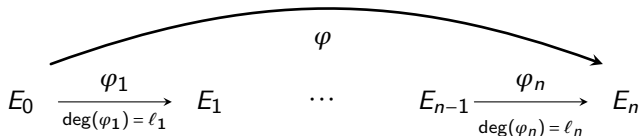
- If $\deg(\varphi) = \prod_{i=1}^r \ell_i$, a chain of isogenies:



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:

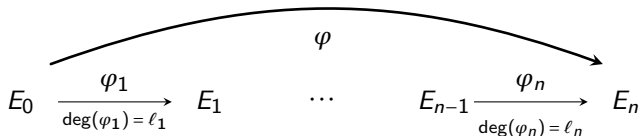


- If $\deg(\varphi)$ is smooth, a generator $P \in E(\mathbb{F}_q)$ s.t. $\ker(\varphi) = \langle P \rangle$ (Vélu).

What does it mean to "compute" an isogeny?

Examples of efficient representations:

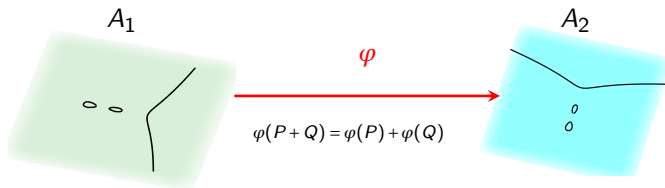
- If $\deg(\varphi) = \prod_{i=1}^r \ell_i$, a chain of isogenies:



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

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* $\tilde{\varphi} : B \longrightarrow A$ with $\deg(\varphi) = \deg(\tilde{\varphi})$.
- φ is an n -isogeny if $\tilde{\varphi} \circ \varphi = [n]$.

n -isogenies in higher dimension and their degree

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

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

Defines a ring for the addition and composition of isogenies.

The Endomorphism ring

Definition (Endomorphism ring)

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

Defines a ring for the addition and composition of isogenies.

Theorem (Deuring)

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

- An order in a quadratic imaginary field. We say that E is ordinary.
- A maximal order in the quaternion algebra ramifying at p and ∞ . We say that E is supersingular.

Quaternions - Definitions

- **Quaternion algebra ramifying at p and ∞ :** A 4-dimensional non commutative division algebra over \mathbb{Q} :

$$\mathcal{B}_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k,$$

with

$$i^2 = -1 \text{ (if } p \equiv 3 \pmod{4}), \quad j^2 = -p \quad \text{and} \quad k = ij = -ji.$$

Quaternions - Definitions

- **Quaternion algebra ramifying at p and ∞ :** A 4-dimensional non commutative division algebra over \mathbb{Q} :

$$\mathcal{B}_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k,$$

with

$$i^2 = -1 \text{ (if } p \equiv 3 \pmod{4}), \quad j^2 = -p \quad \text{and} \quad k = ij = -ji.$$

- **Order:** A full rank lattice $\mathcal{O} \subset \mathcal{B}_{p,\infty}$ with a ring structure.
- **Maximal Order:** An order $\mathcal{O} \subset \mathcal{B}_{p,\infty}$ such that for any other order $\mathcal{O}' \supseteq \mathcal{O}$, we have $\mathcal{O}' = \mathcal{O}$.

Quaternions - Definitions

- **Quaternion algebra ramifying at p and ∞ :** A 4-dimensional non commutative division algebra over \mathbb{Q} :

$$\mathcal{B}_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k,$$

with

$$i^2 = -1 \text{ (if } p \equiv 3 \pmod{4}), \quad j^2 = -p \quad \text{and} \quad k = ij = -ji.$$

- **Order:** A full rank lattice $\mathcal{O} \subset \mathcal{B}_{p,\infty}$ with a ring structure.
- **Maximal Order:** An order $\mathcal{O} \subset \mathcal{B}_{p,\infty}$ such that for any other order $\mathcal{O}' \supseteq \mathcal{O}$, we have $\mathcal{O}' = \mathcal{O}$.
- **Left Ideal:** A left \mathcal{O} -ideal I is a full rank lattice $I \subset \mathcal{B}_{p,\infty}$ such that $\mathcal{O} \cdot I = I$.
- **Right Ideal:** A right \mathcal{O} -ideal I is a full rank lattice $I \subset \mathcal{B}_{p,\infty}$ such that $I \cdot \mathcal{O} = I$.

Quaternions - Definitions

- **Conjugation:**

$$\alpha = x + yi + zj + tk \longmapsto \bar{\alpha} = x - yi - zj - tk$$

- **Norm:** $\text{nrd}(\alpha) := \alpha\bar{\alpha} = x^2 + y^2 + p(z^2 + t^2).$

Quaternions - Definitions

- **Conjugation:**

$$\alpha = x + yi + zj + tk \longmapsto \bar{\alpha} = x - yi - zj - tk$$

- **Norm:** $\text{nrd}(\alpha) := \alpha \bar{\alpha} = x^2 + y^2 + p(z^2 + t^2)$.
- **Ideal norm:** $\text{nrd}(I) := \gcd\{\text{nrd}(\alpha) \mid \alpha \in I\}$.
- **Ideal conjugate:** $\bar{I} := \{\bar{\alpha} \mid \alpha \in I\}$.

Quaternions - Definitions

- **Conjugation:**

$$\alpha = x + yi + zj + tk \longmapsto \bar{\alpha} = x - yi - zj - tk$$

- **Norm:** $\text{nrd}(\alpha) := \alpha \bar{\alpha} = x^2 + y^2 + p(z^2 + t^2)$.
- **Ideal norm:** $\text{nrd}(I) := \gcd\{\text{nrd}(\alpha) \mid \alpha \in I\}$.
- **Ideal conjugate:** $\bar{I} := \{\bar{\alpha} \mid \alpha \in I\}$.
- **Equivalent left \mathcal{O} -ideals:** $I \sim J \iff \exists \alpha \in \mathcal{B}_{p,\infty}^*, \quad J = I\alpha$.

The Deuring correspondence

Supersingular elliptic curves

Quaternions

 $j(E)$ or $j(E)^p$ supersingular

 $\mathcal{O} \cong \text{End}(E)$ maximal order in $\mathcal{B}_{p,\infty}$

The Deuring correspondence

Supersingular elliptic curves	Quaternions
$j(E)$ or $j(E)^p$ supersingular	$\mathcal{O} \cong \text{End}(E)$ maximal order in $\mathcal{B}_{p,\infty}$
$\varphi : E \rightarrow E'$	left \mathcal{O} -ideal and right \mathcal{O}' -ideal I_φ

The Deuring correspondence

Supersingular elliptic curves	Quaternions
$j(E)$ or $j(E)^p$ supersingular	$\mathcal{O} \cong \text{End}(E)$ maximal order in $\mathcal{B}_{p,\infty}$
$\varphi : E \longrightarrow E'$	left \mathcal{O} -ideal and right \mathcal{O}' -ideal l_φ
$\varphi, \psi : E \longrightarrow E'$	$l_\varphi \sim l_\psi$ ($l_\psi = l_\varphi \alpha$, $\alpha \in \mathcal{B}_{p,\infty}$)

The Deuring correspondence

Supersingular elliptic curves	Quaternions
$j(E)$ or $j(E)^p$ supersingular	$\mathcal{O} \cong \text{End}(E)$ maximal order in $\mathcal{B}_{p,\infty}$
$\varphi : E \longrightarrow E'$	left \mathcal{O} -ideal and right \mathcal{O}' -ideal l_φ
$\varphi, \psi : E \longrightarrow E'$	$l_\varphi \sim l_\psi$ ($l_\psi = l_\varphi \alpha$, $\alpha \in \mathcal{B}_{p,\infty}$)
$\hat{\varphi}$	$\overline{l_\varphi}$

The Deuring correspondence

Supersingular elliptic curves	Quaternions
$j(E)$ or $j(E)^p$ supersingular	$\mathcal{O} \cong \text{End}(E)$ maximal order in $\mathcal{B}_{p,\infty}$
$\varphi : E \longrightarrow E'$	left \mathcal{O} -ideal and right \mathcal{O}' -ideal l_φ
$\varphi, \psi : E \longrightarrow E'$	$l_\varphi \sim l_\psi$ ($l_\psi = l_\varphi \alpha$, $\alpha \in \mathcal{B}_{p,\infty}$)
$\hat{\varphi}$	$\overline{l_\varphi}$
$\varphi \circ \psi$	$l_\psi \cdot l_\varphi$

The Deuring correspondence

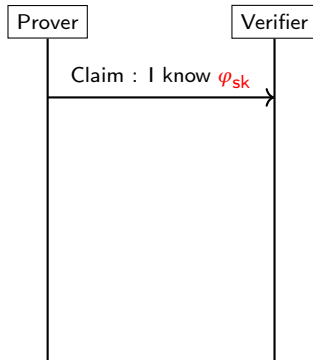
Supersingular elliptic curves	Quaternions
$j(E)$ or $j(E)^p$ supersingular	$\mathcal{O} \cong \text{End}(E)$ maximal order in $\mathcal{B}_{p,\infty}$
$\varphi : E \longrightarrow E'$	left \mathcal{O} -ideal and right \mathcal{O}' -ideal l_φ
$\varphi, \psi : E \longrightarrow E'$	$l_\varphi \sim l_\psi$ ($l_\psi = l_\varphi \alpha$, $\alpha \in \mathcal{B}_{p,\infty}$)
$\hat{\varphi}$	$\overline{l_\varphi}$
$\varphi \circ \psi$	$l_\psi \cdot l_\varphi$
$\deg(\varphi)$	$\text{nrd}(l_\varphi)$

From 1D to 4D to 2D: a brief history of SQIsign

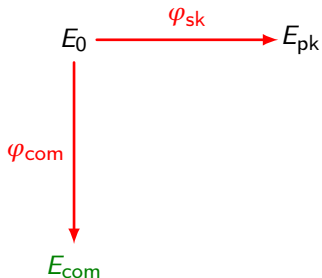
The SQIsign identification scheme

$$E_0 \xrightarrow{\varphi_{sk}} E_{pk}$$

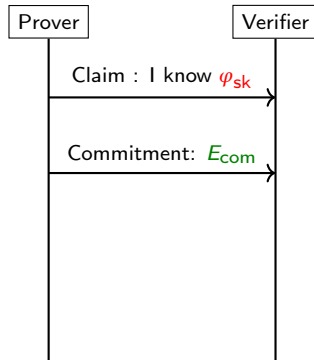
- public
- Prover's secret
- published by Verifier
- published by Prover



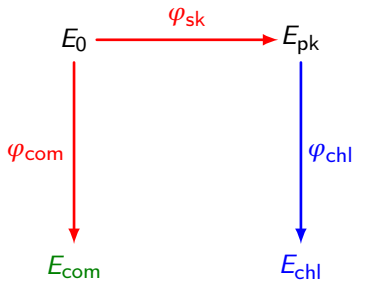
The SQIsign identification scheme



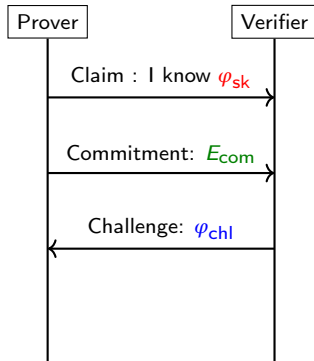
- public
- Prover's secret
- published by Verifier
- published by Prover



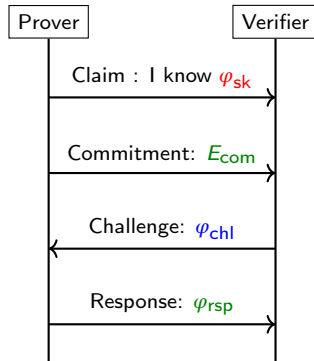
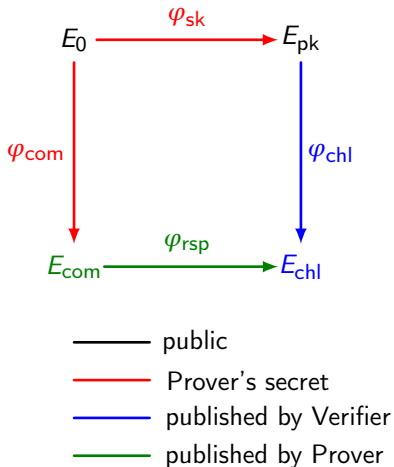
The SQIsign identification scheme



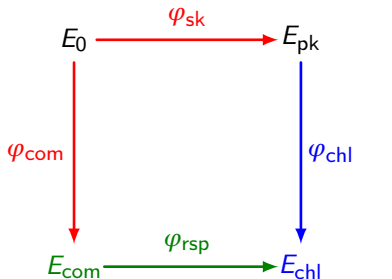
- public
- Prover's secret
- published by Verifier
- published by Prover



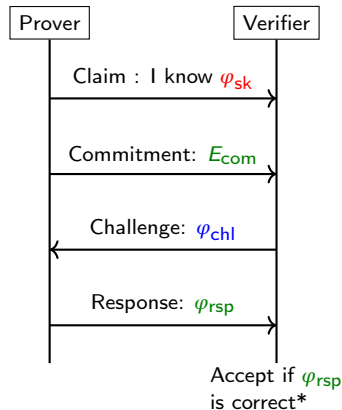
The SQIsign identification scheme



The SQIsign identification scheme

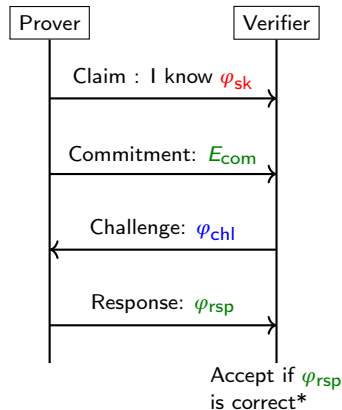
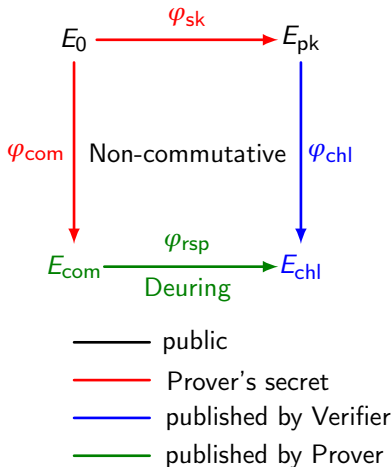


- public
- Prover's secret
- published by Verifier
- published by Prover



* φ_{rsp} should not factor through φ_{chl} .

The SQIsign identification scheme



* φ_{rsp} should not factor through φ_{chl} .

Computing isogenies via the Deuring correspondence

Goal: In SQIsign, we know $\text{End}(E_{\text{com}})$ and $\text{End}(E_{\text{chl}})$ and we want an isogeny $\varphi_{\text{rsp}} : E_{\text{com}} \rightarrow E_{\text{chl}}$.

Computing isogenies via the Deuring correspondence

Goal: In SQIsign, we know $\text{End}(E_{\text{com}})$ and $\text{End}(E_{\text{chl}})$ and we want an isogeny $\varphi_{\text{rsp}} : E_{\text{com}} \longrightarrow E_{\text{chl}}$.

Problem: How to compute isogenies between elliptic curves of known endomorphism rings?

- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \text{End}(E_1)$ and $\mathcal{O}_2 \cong \text{End}(E_2)$.
- Compute a connecting ideal I between \mathcal{O}_1 and \mathcal{O}_2 (left \mathcal{O}_1 -ideal and right \mathcal{O}_2 -ideal).
- Compute $J \sim I$ random of smooth norm via [KLPT14].
- Translate J into an isogeny $\varphi_J : E_1 \longrightarrow E_2$.

Computing isogenies via the Deuring correspondence

Goal: In SQIsign, we know $\text{End}(E_{\text{com}})$ and $\text{End}(E_{\text{chl}})$ and we want an isogeny $\varphi_{\text{rsp}} : E_{\text{com}} \rightarrow E_{\text{chl}}$.

Problem: How to compute isogenies between elliptic curves of known endomorphism rings?

- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \text{End}(E_1)$ and $\mathcal{O}_2 \cong \text{End}(E_2)$.
- Compute a connecting ideal I between \mathcal{O}_1 and \mathcal{O}_2 (left \mathcal{O}_1 -ideal and right \mathcal{O}_2 -ideal).
- Compute $J \sim I$ random of smooth norm via [KLPT14].
- Translate J into an isogeny $\varphi_J : E_1 \rightarrow E_2$.

✓ Takes polynomial time.

Computing isogenies via the Deuring correspondence

Goal: In SQuSign, we know $\text{End}(E_{\text{com}})$ and $\text{End}(E_{\text{chl}})$ and we want an isogeny $\varphi_{\text{rsp}} : E_{\text{com}} \rightarrow E_{\text{chl}}$.

Problem: How to compute isogenies between elliptic curves of known endomorphism rings?

- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \text{End}(E_1)$ and $\mathcal{O}_2 \cong \text{End}(E_2)$.
 - Compute a connecting ideal I between \mathcal{O}_1 and \mathcal{O}_2 (left \mathcal{O}_1 -ideal and right \mathcal{O}_2 -ideal).
 - Compute $J \sim I$ random of smooth norm via [KLPT14].
 - Translate J into an isogeny $\varphi_J : E_1 \rightarrow E_2$.
- ✓ Takes polynomial time.
- ✓ Becomes hard when $\text{End}(E_1)$ or $\text{End}(E_2)$ is unknown.

Computing isogenies via the Deuring correspondence

Goal: In SQuSign, we know $\text{End}(E_{\text{com}})$ and $\text{End}(E_{\text{chl}})$ and we want an isogeny $\varphi_{\text{rsp}} : E_{\text{com}} \rightarrow E_{\text{chl}}$.

Problem: How to compute isogenies between elliptic curves of known endomorphism rings?

- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \text{End}(E_1)$ and $\mathcal{O}_2 \cong \text{End}(E_2)$.
- Compute a connecting ideal I between \mathcal{O}_1 and \mathcal{O}_2 (left \mathcal{O}_1 -ideal and right \mathcal{O}_2 -ideal).
- Compute $J \sim I$ random of smooth norm via [KLPT14].
- **Translate** J into an isogeny $\varphi_J : E_1 \rightarrow E_2$.

✓ Takes polynomial time.

✓ Becomes hard when $\text{End}(E_1)$ or $\text{End}(E_2)$ is unknown.

✗ Slow in practice because of the **red** steps.

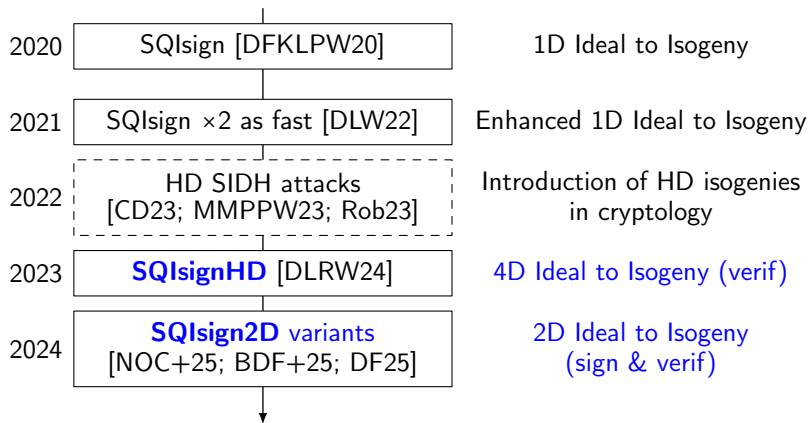
HD techniques for the Deuring correspondence

Problem: How to compute isogenies between elliptic curves of known endomorphism rings?

- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \text{End}(E_1)$ and $\mathcal{O}_2 \cong \text{End}(E_2)$.
- Compute a connecting ideal I between \mathcal{O}_1 and \mathcal{O}_2 (left \mathcal{O}_1 -ideal and right \mathcal{O}_2 -ideal).
- Compute $J \sim I$ random of ~~smooth norm via [KLPT14]~~ of (small) norm.
- Translate J into an isogeny $\varphi_J : E_1 \rightarrow E_2$ using dimension 2 or 4 interpolation techniques.

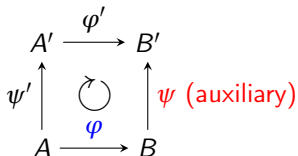
- ✓ Takes polynomial time.
- ✓ Becomes hard when $\text{End}(E_1)$ or $\text{End}(E_2)$ is unknown.
- ✓ Faster than the previous method.

A brief history of SQIsign



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:

$$\begin{array}{ccc}
 A' & \xrightarrow{\varphi'} & B' \\
 \psi' \uparrow & \circlearrowleft & \uparrow \psi \text{ (auxiliary)} \\
 A & \xrightarrow{\varphi} & B
 \end{array}$$

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

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

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

Kani's lemma [Kan97]

- Consider the commutative diagram:

$$\begin{array}{ccc}
 A' & \xrightarrow{\varphi'} & B' \\
 \psi' \uparrow & \circlearrowright & \uparrow \psi \text{ (auxiliary)} \\
 A & \xrightarrow{\varphi} & B
 \end{array}$$

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

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

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

- 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:

$$\begin{array}{ccc}
 A' & \xrightarrow{\varphi'} & B' \\
 \psi' \uparrow & \circlearrowleft & \uparrow \psi \text{ (auxiliary)} \\
 A & \xrightarrow{\varphi} & B
 \end{array}$$

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

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

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

- 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 :

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

From SQIsignHD to SQIsign2D

Goal: How to efficiently represent $\varphi = \varphi_{\text{rsp}} : E_{\text{com}} \rightarrow E_{\text{chl}}?$

From SQIsignHD to SQIsign2D

Goal: How to efficiently represent $\varphi = \varphi_{\text{rsp}} : E_{\text{com}} \rightarrow E_{\text{chl}}$?

SQIsignHD:

- The auxiliary isogeny is:

$$\psi := \begin{pmatrix} a_1 & -a_2 \\ a_2 & a_1 \end{pmatrix} : E_{\text{chl}}^2 \rightarrow E_{\text{chl}}^2,$$

with $r = 2^e - q = a_1^2 + a_2^2$.

- $F : E_{\text{com}}^2 \times E_{\text{chl}}^2 \rightarrow E_{\text{com}}^2 \times E_{\text{chl}}^2$ is 4-dimensional and embeds $\text{Diag}(\varphi, \varphi)$.

From SQIsignHD to SQIsign2D

Goal: How to efficiently represent $\varphi = \varphi_{\text{rsp}} : E_{\text{com}} \rightarrow E_{\text{chl}}$?

SQIsignHD:

- The auxiliary isogeny is:

$$\psi := \begin{pmatrix} a_1 & -a_2 \\ a_2 & a_1 \end{pmatrix} : E_{\text{chl}}^2 \rightarrow E_{\text{chl}}^2,$$

with $r = 2^e - q = a_1^2 + a_2^2$.

- $F : E_{\text{com}}^2 \times E_{\text{chl}}^2 \rightarrow E_{\text{com}}^2 \times E_{\text{chl}}^2$ is 4-dimensional and embeds $\text{Diag}(\varphi, \varphi)$.
- ✓ **Signature:** $\varphi(E_{\text{com}}[2^e])$ and q easy to compute.
- ✗ Costly 4-dimensional verification.

From SQIsignHD to SQIsign2D

Goal: How to efficiently represent $\varphi = \varphi_{\text{rsp}} : E_{\text{com}} \rightarrow E_{\text{chl}}?$

SQIsignHD:

- The auxiliary isogeny is:

$$\psi := \begin{pmatrix} a_1 & -a_2 \\ a_2 & a_1 \end{pmatrix} : E_{\text{chl}}^2 \rightarrow E_{\text{chl}}^2,$$

with $r = 2^e - q = a_1^2 + a_2^2$.

- $F : E_{\text{com}}^2 \times E_{\text{chl}}^2 \rightarrow E_{\text{com}}^2 \times E_{\text{chl}}^2$ is 4-dimensional and embeds $\text{Diag}(\varphi, \varphi)$.
- ✓ **Signature:** $\varphi(E_{\text{com}}[2^e])$ and q easy to compute.
- ✗ Costly 4-dimensional verification.

SQIsign2D*:

- The auxiliary isogeny is $\psi : E_{\text{chl}} \rightarrow E_{\text{aux}}$ of degree $r = 2^e - q$.
- $F : E_{\text{com}} \times E_{\text{aux}} \rightarrow E_{\text{chl}} \times E'$ is 2-dimensional.

From SQIsignHD to SQIsign2D

Goal: How to efficiently represent $\varphi = \varphi_{\text{rsp}} : E_{\text{com}} \rightarrow E_{\text{chl}}?$

SQIsignHD:

- The auxiliary isogeny is:

$$\psi := \begin{pmatrix} a_1 & -a_2 \\ a_2 & a_1 \end{pmatrix} : E_{\text{chl}}^2 \rightarrow E_{\text{chl}}^2,$$

with $r = 2^e - q = a_1^2 + a_2^2$.

- $F : E_{\text{com}}^2 \times E_{\text{chl}}^2 \rightarrow E_{\text{com}}^2 \times E_{\text{chl}}^2$ is 4-dimensional and embeds $\text{Diag}(\varphi, \varphi)$.
- ✓ **Signature:** $\varphi(E_{\text{com}}[2^e])$ and q easy to compute.
- ✗ Costly 4-dimensional verification.

SQIsign2D*:

- The auxiliary isogeny is $\psi : E_{\text{chl}} \rightarrow E_{\text{aux}}$ of degree $r = 2^e - q$.
- $F : E_{\text{com}} \times E_{\text{aux}} \rightarrow E_{\text{chl}} \times E'$ is 2-dimensional.
- ✗ **Signature:** $\psi \circ \varphi(E_{\text{com}}[2^e])$ and q more tricky to compute (2D computation).
- ✓ Fast 2-dimensional verification.

Timings

Table: Comparison of time performance in ms of SQIsign-v1 (NIST round 1), SQIsignHD and SQIsign2D-West on an Intel Core i5-1335U 4600MHz CPU. These variants have been implemented in C, except SQIsignHD verification (starred) that has been implemented in Python/Sagemath.

		NIST I	NIST III	NIST V
SQIsign 1.0	Key Gen.	355.72	5 625.72	22 445.3
	Signature	554.78	10 553.18	41 322.21
	Verification	7.77	195.86	571.77
SQIsignHD	Key Gen.	14	46	109
	Signature	8	24	52
	Verification	710.63*	1 308.14*	2 037.14*
SQIsign2D-West	Key Gen.	16.53	52.24	113.18
	Signature	58.17	220.26	413.46
	Verification	2.53	9.77	23.57

The 4D revival: (qt-)Pegasis and MIKE

Ideal class group action [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 $\iota: \mathfrak{O} \hookrightarrow \text{End}(E)$.

Ideal class group action [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 $\iota: \mathfrak{O} \hookrightarrow \text{End}(E)$.

Theorem (Belding, Colò, Kohel)

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

Ideal class group action [CK20]

\mathfrak{O} -ideals	\mathfrak{O} -oriented curves and isogenies
Ideal $\mathfrak{a} \subseteq \mathfrak{O}$	$\varphi_{\mathfrak{a}} : E \longrightarrow E_{\mathfrak{a}} := \mathfrak{a} \cdot E$
$\mathfrak{b} \sim \mathfrak{a}$	$\mathfrak{a} \cdot E \simeq \mathfrak{b} \cdot E$
$\alpha \mathfrak{O}$	$\iota(\alpha) : E \longrightarrow E$
$\bar{\mathfrak{a}}$	$\hat{\varphi}_{\mathfrak{a}}$
$\mathfrak{a}\mathfrak{b}$	$\varphi_{\mathfrak{b}} \circ \varphi_{\mathfrak{a}}$
$N(\mathfrak{a})$	$\deg(\varphi_{\mathfrak{a}})$

Effective group action

Definition

An *effective group action* (EGA) $G \curvearrowright X$ is:

- 1 Commutative, free and transitive.
- 2 *Easy to compute*: $g \cdot x$ can be evaluated in polynomial time for all $g \in G$ and $x \in X$.
- 3 *One way*: given x and $g \cdot x$, $g \in G$ is hard to find.

Effective group action

Definition


An *effective group action* (EGA) $G \curvearrowright X$ is:

- ❶ Commutative, free and transitive.
 - ❷ *Easy to compute*: $g \cdot x$ can be evaluated in polynomial time for all $g \in G$ and $x \in X$.
 - ❸ *One way*: given x and $g \cdot x$, $g \in G$ is hard to find.
- With effective group actions, we can derive many schemes (including key exchange, signatures and more).

Effective group action

Definition

An *effective group action* (EGA) $G \curvearrowright X$ is:

- 1 Commutative, free and transitive.
 - 2 *Easy to compute*: $g \cdot x$ can be evaluated in polynomial time for all $g \in G$ and $x \in X$.
 - 3 *One way*: given x and $g \cdot x$, $g \in G$ is hard to find.
- With effective group actions, we can derive many schemes (including key exchange, signatures and more).
 - Actually, group actions based on orientations are *restricted* effective group actions. We can act by ideals of small norms $\mathfrak{l}_1, \dots, \mathfrak{l}_t$ that generate $\text{Cl}(\mathfrak{D})$.
 -  **Issue:** This makes schemes less efficient and less scalable to bigger parameters.

The Clapoti method [PR23]

Clapoti: CLass group Action in POlynomial TIme. Generic method that also applies to SQIsign2D.

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

The Clapoti method [PR23]

Clapoti: CLass group Action in POlynomial TIme. Generic method that also applies to SQIsign2D.

Goal: Given an \mathfrak{D} -oriented curve E and **any** ideal $\mathfrak{a} \subseteq \mathfrak{D}$, 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 $b_1, c_1, b_2, c_2 \sim a$ such that

$$N(b_1) + N(c_1) + N(b_2) + N(c_2) = 2^e$$

with $N(b_i)$ odd and $N(c_i)$ even.

- **Step 2:** Compute $F : E^4 \rightarrow E_a \times E_{\bar{a}} \times A$ given by ([Kan97] $\times 2$):

In 2D

$$\begin{array}{ccc} E_{\bar{a}} & \xrightarrow{\varphi'_{b_i}} & E \\ \widehat{\varphi}'_{c_i} \uparrow & & \uparrow \widehat{\varphi}_{c_i} \\ E & \xrightarrow{\varphi_{b_i}} & E_a \end{array}$$

In 4D

$$\begin{array}{ccc} A & \xrightarrow{\Psi_1} & E^2 \\ \Psi_2 \uparrow & & \uparrow \tilde{\Phi}_2 \\ E^2 & \xrightarrow{\Phi_1} & E_a \times E_{\bar{a}} \end{array}$$

$$\Phi_i := \begin{pmatrix} \varphi_{b_i} & \varphi_{c_i} \\ -\widehat{\varphi}'_{c_i} & \widehat{\varphi}'_{b_i} \end{pmatrix} : E^2 \rightarrow E_a \times E_{\bar{a}}$$

$$F := \begin{pmatrix} \Phi_1 & \Phi_2 \\ -\Psi_2 & \tilde{\Psi}_1 \end{pmatrix} : E^4 \rightarrow E_a \times E_{\bar{a}} \times A$$

Comparison with state of the art

Paper	$\log_2(\Delta_D)$		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 (This work)	Sage		0.85s	2.48s	5.54s	9.69s	47.6s

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.

The module action on abelian varieties [Rob24]

- An abelian variety A is \mathfrak{O} -oriented if there is a maximal embedding $\iota: \mathfrak{O} \hookrightarrow \text{End}(A)$.
- If M is a finitely presented projective \mathfrak{O} -module, $M \cdot A$ defines an \mathfrak{O} -oriented abelian variety of dimension:

$$\dim(M \cdot A) = \text{rank}(M) \cdot \dim(A).$$

The module action on abelian varieties [Rob24]

- An abelian variety A is \mathfrak{O} -oriented if there is a maximal embedding $\iota: \mathfrak{O} \hookrightarrow \text{End}(A)$.
- If M is a finitely presented projective \mathfrak{O} -module, $M \cdot A$ defines an \mathfrak{O} -oriented abelian variety of dimension:

$$\dim(M \cdot A) = \text{rank}(M) \cdot \dim(A).$$

- An injective homomorphism $M_2 \rightarrow M_1$ with finite cokernel induces an isogeny $M_1 \cdot A \rightarrow M_2 \cdot A$.
- Hence, if $M \subseteq \mathfrak{O}^n$ is a submodule of rank n , $M \cdot A$ can be computed via an isogeny $\mathfrak{O}^n \cdot A = A^n \rightarrow M \cdot A$.

The module action on abelian varieties [Rob24]

- An abelian variety A is \mathfrak{O} -oriented if there is a maximal embedding $\iota: \mathfrak{O} \hookrightarrow \text{End}(A)$.
- If M is a finitely presented projective \mathfrak{O} -module, $M \cdot A$ defines an \mathfrak{O} -oriented abelian variety of dimension:

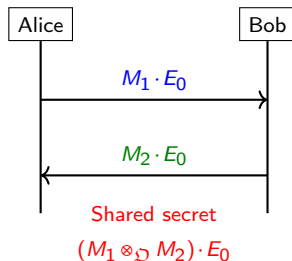
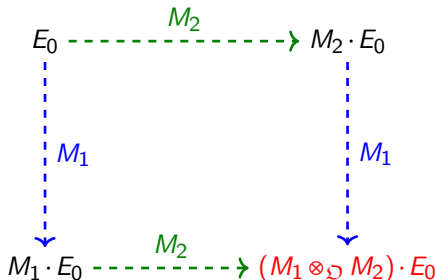
$$\dim(M \cdot A) = \text{rank}(M) \cdot \dim(A).$$

- An injective homomorphism $M_2 \rightarrow M_1$ with finite cokernel induces an isogeny $M_1 \cdot A \rightarrow M_2 \cdot A$.
- Hence, if $M \subseteq \mathfrak{O}^n$ is a submodule of rank n , $M \cdot A$ can be computed via an isogeny $\mathfrak{O}^n \cdot A = A^n \rightarrow M \cdot A$.

Theorem (Page, Robert, 2023)

This defines an anti-equivalence of categories between finitely presented projective \mathfrak{O} -modules and \mathfrak{O} -oriented abelian varieties \mathfrak{O} -isogenous to a product of supersingular elliptic curves.

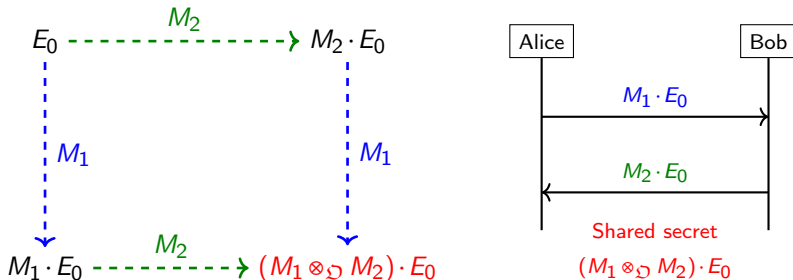
Module isogeny key exchange (MIKE) [Rob24]



- Exploits the commutativity of the module action:

$$M_2 \cdot (M_1 \cdot E_0) = (M_1 \otimes_{\mathcal{O}} M_2) \cdot E_0 = M_1 \cdot (M_2 \cdot E_0)$$

Module isogeny key exchange (MIKE) [Rob24]

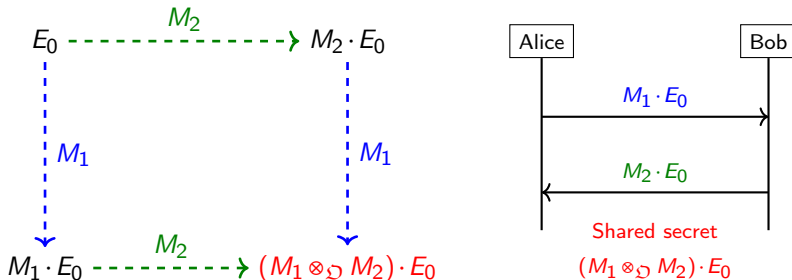


- Exploits the commutativity of the module action:

$$M_2 \cdot (M_1 \cdot E_0) = (M_1 \otimes_{\mathfrak{D}} M_2) \cdot E_0 = M_1 \cdot (M_2 \cdot E_0)$$

- Similar to (C)SIDH but without the torsion points vulnerability or Kuperberg's subexponential attack.

Module isogeny key exchange (MIKE) (Ongoing)



- Assume $\text{rank}(M_1) = \text{rank}(M_2) = 2$.
- Alice computes a 2-dimensional isogeny $E_0^2 \rightarrow M_1 \cdot E_0$.
- Then she computes a 4-dimensional isogeny

$$(M_2 \cdot E_0)^2 \rightarrow M_1 \cdot (M_2 \cdot E_0) = (M_1 \otimes_{\mathfrak{O}} M_2) \cdot E_0.$$

Computing higher dimensional isogenies

Definition: theta structure

Definition (Mumford, Duparc)

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

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

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

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

satisfying the *theta group action relation*:

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

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

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.

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.
- If A is not a (polarised) product, a level 2 theta structure induces an embedding of the Kummer variety:

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

- Points are represented up to sign: $\Theta(2)(P)$ represents $\pm P \in A/\pm$.

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.
- If A is not a (polarised) product, a level 2 theta structure induces an embedding of the Kummer variety:

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

- Points are represented up to sign: $\Theta(2)(P)$ represents $\pm P \in A/\pm$.
- Analogue of working with $(x : z)$ -coordinates over elliptic curves, e.g. we have differential addition formulas

$$(\pm P, \pm Q, \pm(P - Q)) \mapsto \pm(P + Q).$$

Computing a 2^e -isogeny in dimension g

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

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

Computing a 2^e -isogeny in dimension g

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

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

Method:

- Decompose f as a chain of 2-isogenies:

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

- Compute every 2-isogeny iteratively, using:

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

- The number of duplications and evaluations is $O(e \log(e))$.

Computing a 2^e -isogeny in dimension g

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

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

Method:

- Decompose f as a chain of 2-isogenies:

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

- Compute every 2-isogeny iteratively, using:

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

- The number of duplications and evaluations is $O(e \log(e))$.

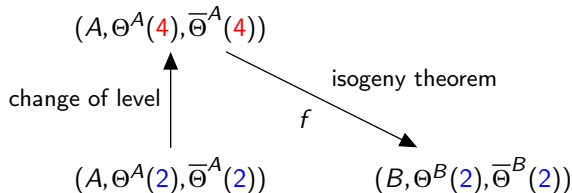
Technicality: We need more torsion $K \subset A[2^{e+2}]$ above the kernel.

Computing a 2-isogeny: change of level

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

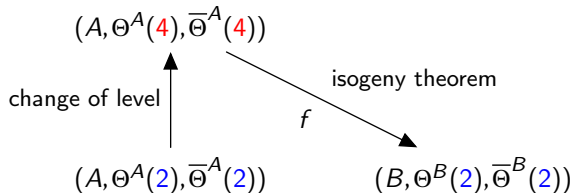
Computing a 2-isogeny: change of level

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



Computing a 2-isogeny: change of level

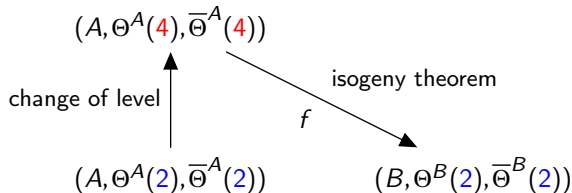
- Let $f : A \rightarrow B$ be a 2-isogeny.



- The level 4 theta structure $(A, \Theta^A(\textcolor{red}{4}), \overline{\Theta}^A(\textcolor{red}{4}))$ is induced by a symplectic isomorphism $(\mathbb{Z}/8\mathbb{Z})^g \times \widehat{(\mathbb{Z}/8\mathbb{Z})^g} \xrightarrow{\sim} A[8]$.
- For that reason, we need 8-torsion points T_1, \dots, T_g such that $\ker(f) = \langle [4]T_1, \dots, [4]T_g \rangle$ to compute f .

Computing a 2-isogeny: change of level

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



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

2-isogeny evaluation algorithm

A very simple isogeny evaluation algorithm:

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

where:

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

Computational cost [DMPR25; Dar25]

	dim. 2 [DMPR25]	dim. 4	
		Old [Dar25]	New (in progress)
Codomain	$6M + 8S + 16a$	$87M + 64S + 64a$	$62M + 64S + 64a$
Evaluation	$4S + 4M + 16a$	$16M + 16S + 128a$	

Table: Computational cost of codomain theta null-point computation and isogeny evaluation in dimensions 2 and 4. M, S and a are respectively the cost of one multiplication, squaring and addition/subtraction over the base field.

Non-generic 2-isogenies in the beginning of the chain

When $A = B_1 \times B_2$ is a product, non-generic isogenies appear in the beginning of the chain:

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

Non-generic
Generic isogenies

Non-generic 2-isogenies in the beginning of the chain

When $A = B_1 \times B_2$ is a product, non-generic isogenies appear in the beginning of the chain:

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

Non-generic
Generic isogenies

Common non-generic isogenies:

Non-gluing isogenies (computed in lower dimension):

- Diagonal isogenies $f : (x, y) \in B_1 \times B_2 \mapsto (\varphi(x), \psi(y)) \in C_1 \times C_2$.
- Special endomorphisms, e.g. $f : (x, y) \in B^2 \mapsto (x + y, x - y) \in B^2$.

Gluing isogenies $f : B_1 \times B_2 \rightarrow C$ where C is not a product.

Evaluating a gluing 2-isogeny

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

Evaluating a gluing 2-isogeny

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

$$\Theta(2) : A_1/\pm \times A_2/\pm \hookrightarrow \mathbb{P}^{2^g-1}$$

- So we are computing:

$$(\pm x, \pm y) \longmapsto \pm f(x, y)$$

- We need additional information to lift the sign indetermination.

Evaluating a gluing 2-isogeny

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

$$\Theta(2) : A_1 / \pm \times A_2 / \pm \hookrightarrow \mathbb{P}^{2^g-1}$$

- So we are computing:

$$(\pm x, \pm y) \longmapsto \pm f(x, y)$$

- We need additional information to lift the sign indetermination.

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

Evaluating a gluing 2-isogeny

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

$$\Theta(2): A_1/\pm \times A_2/\pm \hookrightarrow \mathbb{P}^{2^g-1}$$

- So we are computing:

$$(\pm x, \pm y) \longmapsto \pm f(x, y)$$

- We need additional information to lift the sign indetermination.

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

Ongoing work: new formulas in dimension 4 using $x + T$ and $x - T$, extending a previous work in dimension 2 [Dup25].

Thank you for listening

- 4-dimensional isogenies have been introduced to attack SIDH and accelerate SQIsign signature.
- Despite the existence of 2-dimensional competitors (e.g. for SQIsign), they are still relevant (Pegasis, MIKE).

Future works:

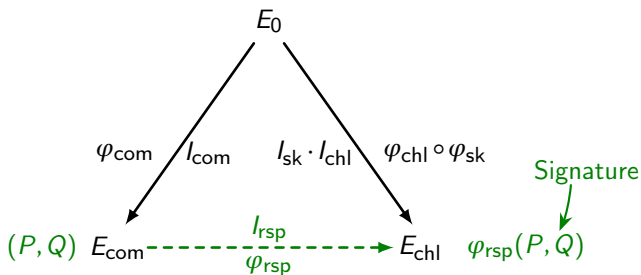
- Research to lower the dimension (e.g. 2-dimensional Pegasis) .
- Keep improving the formulae, e.g. with uniform formulae for generic and non-generic isogenies (for simplicity, constant time).

My works can be found on
my webpage:

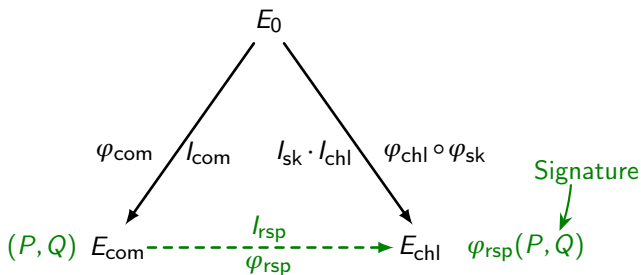


Appendix: more on SQLsgnHD and SQLsgn2D*

Signature in SQLsignHD: evaluate torsion points



Signature in SQLsignHD: evaluate torsion points



Via the Deuring correspondence: If $P \in E_{\text{com}}[2^e]$, then

$$\varphi_{\text{rsp}}(P) = [\mu] \varphi_{\text{chl}} \circ \varphi_{\text{sk}} \circ \hat{\alpha} \circ \hat{\varphi}_{\text{com}}(P),$$

with $\mu \equiv (\deg(\varphi_{\text{sk}}) \deg(\varphi_{\text{com}}) \deg(\varphi_{\text{chl}}))^{-1} \pmod{2^e}$ and $\alpha \in \mathcal{O}_0$ such that $l_{\text{sk}} \cdot l_{\text{chl}} \cdot \bar{l}_{\text{rsp}} \cdot \bar{l}_{\text{com}} = \mathcal{O}_0 \cdot \alpha$.

Verification in SQIsignHD: 4-dimensional interpolation

- Find $a_1, a_2 \in \mathbb{Z}$ such that $\text{nrd}(l_{\text{rsp}}) + a_1^2 + a_2^2 = 2^e$.

Verification in SQIsignHD: 4-dimensional interpolation

- Find $a_1, a_2 \in \mathbb{Z}$ such that $\text{nrd}(l_{\text{rsp}}) + a_1^2 + a_2^2 = 2^e$.
- Consider the 4-dimensional isogeny:

$$F := \begin{pmatrix} a_1 & a_2 & \hat{\varphi}_{\text{rsp}} & 0 \\ -a_2 & a_1 & 0 & \hat{\varphi}_{\text{rsp}} \\ -\varphi_{\text{rsp}} & 0 & a_1 & -a_2 \\ 0 & -\varphi_{\text{rsp}} & a_2 & a_1 \end{pmatrix} \in \text{End}(E_{\text{com}}^2 \times E_{\text{chl}}^2).$$

It is a 2^e -isogeny *i.e.* $\tilde{F} \circ F = [2^e]$ (4D Kani's lemma [Kan97]).

Verification in SQIsignHD: 4-dimensional interpolation

- Find $a_1, a_2 \in \mathbb{Z}$ such that $\text{nrd}(l_{\text{rsp}}) + a_1^2 + a_2^2 = 2^e$.
- Consider the 4-dimensional isogeny:

$$F := \begin{pmatrix} a_1 & a_2 & \hat{\varphi}_{\text{rsp}} & 0 \\ -a_2 & a_1 & 0 & \hat{\varphi}_{\text{rsp}} \\ -\varphi_{\text{rsp}} & 0 & a_1 & -a_2 \\ 0 & -\varphi_{\text{rsp}} & a_2 & a_1 \end{pmatrix} \in \text{End}(E_{\text{com}}^2 \times E_{\text{chl}}^2).$$

It is a 2^e -isogeny *i.e.* $\tilde{F} \circ F = [2^e]$ (4D Kani's lemma [Kan97]).

- Its kernel is given by:

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

Verification in SQIsignHD: 4-dimensional interpolation

- Find $a_1, a_2 \in \mathbb{Z}$ such that $\text{nrd}(l_{\text{rsp}}) + a_1^2 + a_2^2 = 2^e$.
- Consider the 4-dimensional isogeny:

$$F := \begin{pmatrix} a_1 & a_2 & \hat{\varphi}_{\text{rsp}} & 0 \\ -a_2 & a_1 & 0 & \hat{\varphi}_{\text{rsp}} \\ -\varphi_{\text{rsp}} & 0 & a_1 & -a_2 \\ 0 & -\varphi_{\text{rsp}} & a_2 & a_1 \end{pmatrix} \in \text{End}(E_{\text{com}}^2 \times E_{\text{chl}}^2).$$

It is a 2^e -isogeny *i.e.* $\tilde{F} \circ F = [2^e]$ (4D Kani's lemma [Kan97]).

- Its kernel is given by:

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

- From $a_1, a_2, P, Q, \varphi_{\text{rsp}}(P), \varphi_{\text{rsp}}(Q)$, one can compute F .

Verification in SQIsignHD: 4-dimensional interpolation

- Find $a_1, a_2 \in \mathbb{Z}$ such that $\text{nrd}(l_{\text{rsp}}) + a_1^2 + a_2^2 = 2^e$.
- Consider the 4-dimensional isogeny:

$$F := \begin{pmatrix} a_1 & a_2 & \hat{\varphi}_{\text{rsp}} & 0 \\ -a_2 & a_1 & 0 & \hat{\varphi}_{\text{rsp}} \\ -\varphi_{\text{rsp}} & 0 & a_1 & -a_2 \\ 0 & -\varphi_{\text{rsp}} & a_2 & a_1 \end{pmatrix} \in \text{End}(E_{\text{com}}^2 \times E_{\text{chl}}^2).$$

It is a 2^e -isogeny *i.e.* $\tilde{F} \circ F = [2^e]$ (4D Kani's lemma [Kan97]).

- Its kernel is given by:

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

- From $a_1, a_2, P, Q, \varphi_{\text{rsp}}(P), \varphi_{\text{rsp}}(Q)$, one can compute F .
- Then F **efficiently represents** φ_{rsp} : for all $P \in E_{\text{com}}$,

$$F(P, 0, 0, 0) = ([a_1]P, -[a_2]P, -\varphi_{\text{rsp}}(P), 0).$$

Verification in SQIsignHD: 4-dimensional interpolation

Checking the validity of a signature:

- From $(\text{nrd}(I_{\text{rsp}}), \varphi_{\text{rsp}}(P, Q))$, compute $F : E_{\text{com}}^2 \times E_{\text{chl}}^2 \rightarrow C$.
- F can be computed as a chain of 2-isogenies of length e in theta coordinates:

$$E_{\text{com}}^2 \times E_{\text{chl}}^2 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \cdots A_{e-1} \xrightarrow{f_e} C.$$

Verification in SQIsignHD: 4-dimensional interpolation

Checking the validity of a signature:

- From $(\text{nrd}(I_{\text{rsp}}), \varphi_{\text{rsp}}(P, Q))$, compute $F : E_{\text{com}}^2 \times E_{\text{chl}}^2 \rightarrow C$.
- F can be computed as a chain of 2-isogenies of length e in theta coordinates:

$$E_{\text{com}}^2 \times E_{\text{chl}}^2 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \cdots A_{e-1} \xrightarrow{f_e} C.$$

- Check that $C \stackrel{?}{=} E_{\text{com}}^2 \times E_{\text{chl}}^2$.

Verification in SQIsignHD: 4-dimensional interpolation

Checking the validity of a signature:

- From $(\text{nrd}(I_{\text{rsp}}), \varphi_{\text{rsp}}(P, Q))$, compute $F : E_{\text{com}}^2 \times E_{\text{chl}}^2 \rightarrow C$.
- F can be computed as a chain of 2-isogenies of length e in theta coordinates:

$$E_{\text{com}}^2 \times E_{\text{chl}}^2 \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2 \cdots A_{e-1} \xrightarrow{f_e} C.$$

- Check that $C \stackrel{?}{=} E_{\text{com}}^2 \times E_{\text{chl}}^2$.
- For a point $P \in E_{\text{com}}$ of big order, check that:

$$F(P, 0, 0, 0) \stackrel{?}{=} ([a_1]P, -[a_2]P, *, 0).$$

Kani's lemma: efficient representation in 2D [Kan97]

Consider the following commutative diagram:

$$\begin{array}{ccc}
 E_4 & \xrightarrow{\varphi'} & E_3 \\
 \psi' \uparrow & \circlearrowright & \uparrow \psi \text{ (auxiliary isogeny)} \\
 E_1 & \xrightarrow{\varphi} & E_2
 \end{array}$$

s.t. $\deg(\varphi) = \deg(\varphi') = q$ and $\deg(\psi) = \deg(\psi') = r$ are coprime and $q + r = 2^e$.

Kani's lemma: efficient representation in 2D [Kan97]

Consider the following commutative diagram:

$$\begin{array}{ccc}
 E_4 & \xrightarrow{\varphi'} & E_3 \\
 \psi' \uparrow & \circlearrowleft & \uparrow \psi \text{ (auxiliary isogeny)} \\
 E_1 & \xrightarrow{\varphi} & E_2
 \end{array}$$

s.t. $\deg(\varphi) = \deg(\varphi') = q$ and $\deg(\psi) = \deg(\psi') = r$ are coprime and $q + r = 2^e$. Then the isogeny:

$$\Phi := \begin{pmatrix} \varphi & \widehat{\psi} \\ -\psi' & \widehat{\varphi'} \end{pmatrix} : E_1 \times E_3 \longrightarrow E_2 \times E_4$$

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

$$\ker(\Phi) = \{([q]P, \psi \circ \varphi(P)) \mid P \in E_1[2^e]\}.$$

Kani's lemma: efficient representation in 2D [Kan97]

- Suppose we know $\psi \circ \phi(E_1[2^e])$.
- Then we can compute:

$$\ker(\Phi) = \{([q]P, \psi \circ \phi(P)) \mid P \in E_1[2^e]\}.$$

Kani's lemma: efficient representation in 2D [Kan97]

- Suppose we know $\psi \circ \varphi(E_1[2^e])$.
- Then we can compute:

$$\ker(\Phi) = \{([q]P, \psi \circ \varphi(P)) \mid P \in E_1[2^e]\}.$$

- So we can compute

$$\Phi := \begin{pmatrix} \varphi & \widehat{\psi} \\ -\psi' & \widehat{\varphi'} \end{pmatrix} : E_1 \times E_3 \longrightarrow E_2 \times E_4$$

as a chain of 2-isogenies of length e :

$$E_1 \times E_3 \xrightarrow{\Phi_1} A_1 \xrightarrow{\Phi_2} A_2 \cdots A_{e-1} \xrightarrow{\Phi_e} E_2 \times E_4.$$

Kani's lemma: efficient representation in 2D [Kan97]

- Suppose we know $\psi \circ \varphi(E_1[2^e])$.
- Then we can compute:

$$\ker(\Phi) = \{([q]P, \psi \circ \varphi(P)) \mid P \in E_1[2^e]\}.$$

- So we can compute

$$\Phi := \begin{pmatrix} \varphi & \widehat{\psi} \\ -\psi' & \widehat{\varphi'} \end{pmatrix} : E_1 \times E_3 \longrightarrow E_2 \times E_4$$

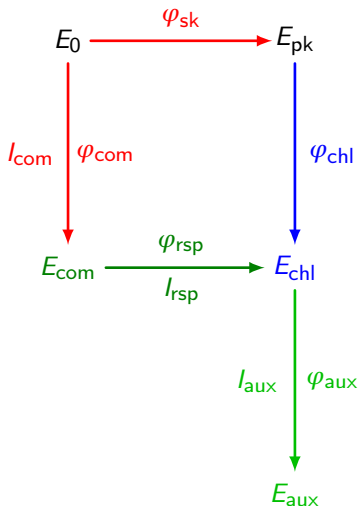
as a chain of 2-isogenies of length e :

$$E_1 \times E_3 \xrightarrow{\Phi_1} A_1 \xrightarrow{\Phi_2} A_2 \cdots A_{e-1} \xrightarrow{\Phi_e} E_2 \times E_4.$$

- Φ efficiently represents φ : for all $P \in E_1$,

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

SQLsign2D-West: signing in dimension 2 [BDF+25]



Starting from E_0 , we can translate ideals into isogenies **in 2D**.

- Generate $I_{aux} \subset \text{End}(E_{chl})$ of norm $2^e - \text{nr}d(I_{rsp})$.
- Translate $I_{com} \cdot I_{rsp} \cdot I_{aux}$ into $\varphi_{aux} \circ \varphi_{rsp} \circ \varphi_{com}$ (in 2D).
- **Response:** $\varphi_{aux} \circ \varphi_{rsp}(P, Q)$ with $\langle P, Q \rangle = E_{com}[2^e]$.
- φ_{rsp} can be verified from $\varphi_{aux} \circ \varphi_{rsp}(P, Q)$ (in 2D).