Fast computation of higher dimensional isogenies for cryptographic applications

Pierrick Dartois

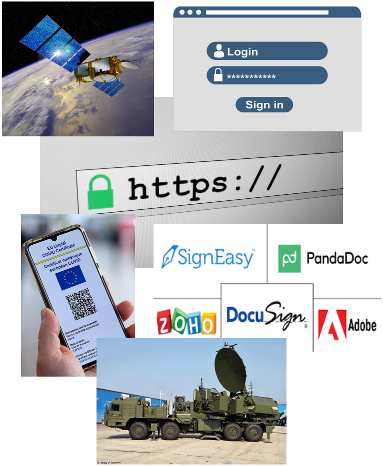
PhD Defense
Under the supervision of Damien Robert, Benjamin Wesolowski and Luca De Feo

2025, July 9

Cryptography in daily life

What people think crypto is:

What crypto really is:



Hard problems for public key cryptography

Widely used underlying problems...

Hard problems for public key cryptography

Widely used underlying problems...

- The factorisation problem (RSA):

$$N = p \times q.$$

Hard problems for public key cryptography

Widely used underlying problems...

- The factorisation problem (RSA):

$$N = p \times q.$$

- The discrete logarithm problem in a group $(G, +)$ generated by P (ECC):

$$Q = [n]P.$$

Hard problems for public key cryptography

Widely used underlying problems...

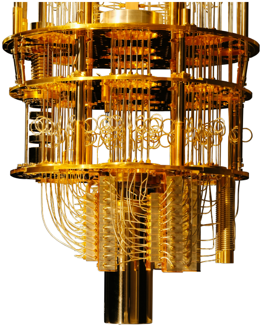
- The factorisation problem (RSA):

$$N = p \times q.$$

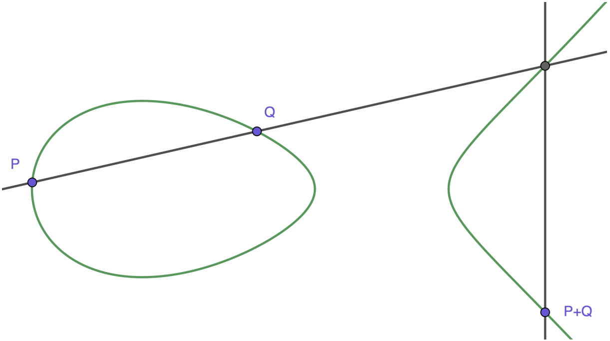
- The discrete logarithm problem in a group $(G, +)$ generated by P (ECC):

$$Q = [n]P.$$

...All broken by quantum computers



Elliptic curves

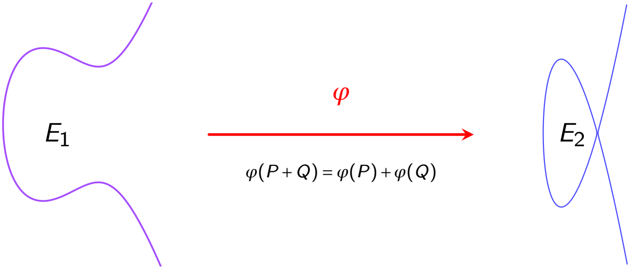


- An elliptic curve $E/\mathbb{F}_q$ is defined by:

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

  with an infinite element 0_E.
- E is equipped with a commutative group law.

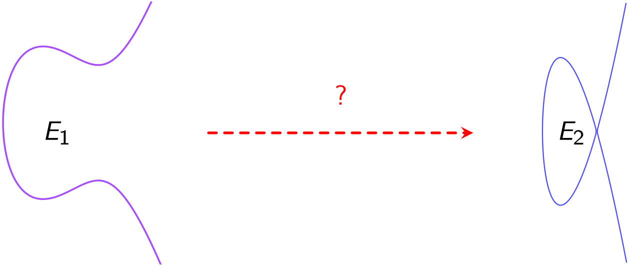
Isogenies



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

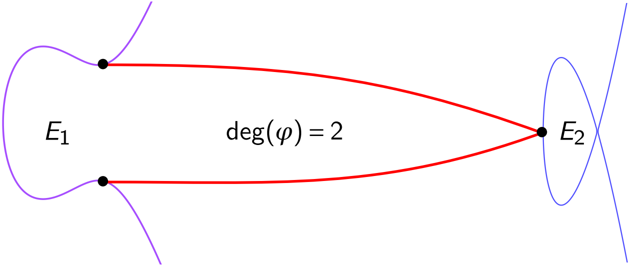
Why are isogenies interesting in cryptography?

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



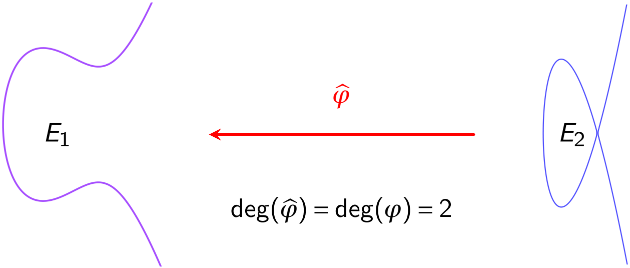
This problem is assumed to be hard for both classical and quantum computers.

Isogenies - degree



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

Isogenies - the dual isogeny



$\deg(\widehat{\varphi}) = \deg(\varphi) = 2$

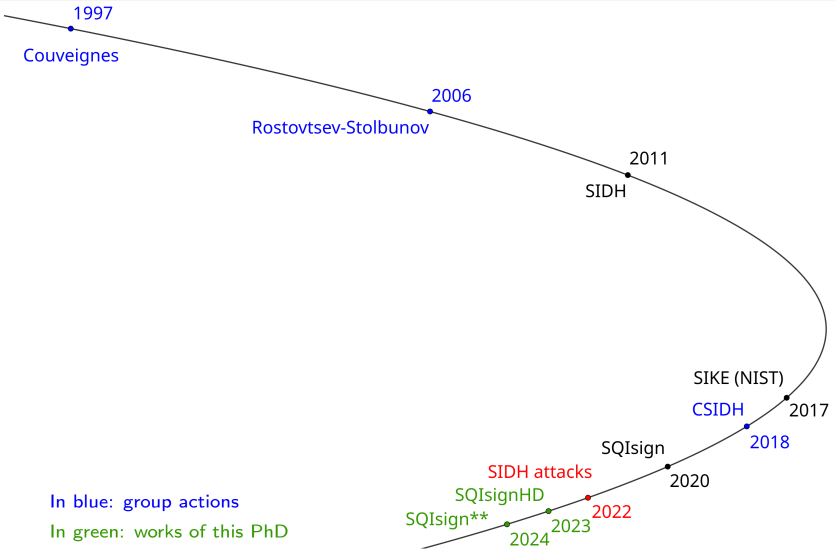
An n-isogeny φ satisfies $\widehat{\varphi} \circ \varphi = [n]$.

Isogeny chains

$$E_0 \xrightarrow{\varphi_1} E_1 \qquad \cdots \qquad E_{n-1} \xrightarrow{\varphi_n} E_n$$

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

A brief (biased) history of isogeny based cryptography



In blue: group actions

In green: works of this PhD

SQIsign and the Deuring correspondence

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 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 $\mathbb{Q}$:

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

with

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

Quaternions - Definitions

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

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

with

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

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

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

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

- **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:**

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

Quaternions - Definitions

- **Conjugation:**

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

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

Quaternions - Definitions

- **Conjugation:**

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

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

Quaternions - Definitions

- **Conjugation:**

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

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

The Deuring correspondence

Supersingular elliptic curves	**Quaternions**
$j(E)$ or $j(E)^p$ supersingular	$\mathscr{O} \cong \mathrm{End}(E)$ maximal order in $\mathscr{B}_{p,\infty}$

The Deuring correspondence

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

The Deuring correspondence

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

The Deuring correspondence

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

The Deuring correspondence

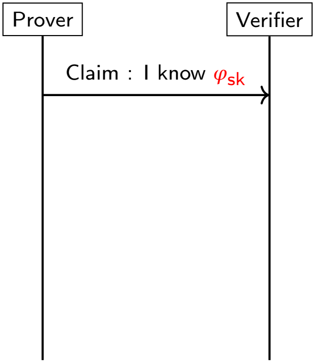
Supersingular elliptic curves	**Quaternions**
$j(E)$ or $j(E)^p$ supersingular	$\mathcal{O} \cong \mathrm{End}(E)$ maximal order in $\mathscr{B}_{p,\infty}$
$\varphi : E \longrightarrow E'$	left $\mathcal{O}$-ideal and right $\mathcal{O}'$-ideal I_φ
$\varphi, \psi : E \longrightarrow E'$	$I_\varphi \sim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

The Deuring correspondence

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

The SQIsign identification scheme

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



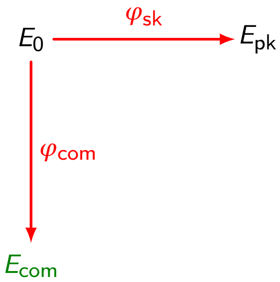
public

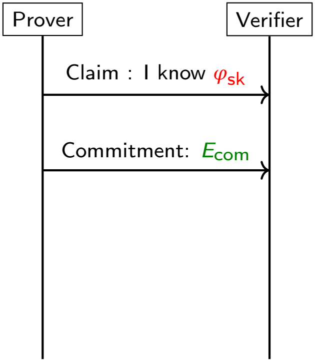
Prover's secret

published by Verifier

published by Prover

The SQIsign identification scheme





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

The SQIsign identification scheme

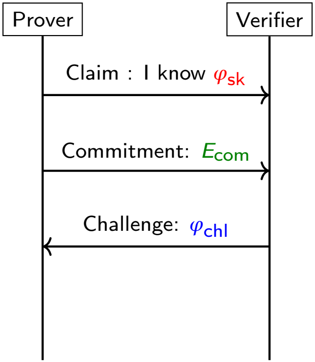
$$\begin{tikzcd} E_0 \arrow[r, "\varphi_{\mathrm{sk}}"] \arrow[d, "\varphi_{\mathrm{com}}"] & E_{\mathrm{pk}} \arrow[d, "\varphi_{\mathrm{chl}}"] \\ E_{\mathrm{com}} & E_{\mathrm{chl}} \end{tikzcd}$$

—— public

—— Prover's secret

—— published by Verifier

—— published by Prover



The SQIsign identification scheme

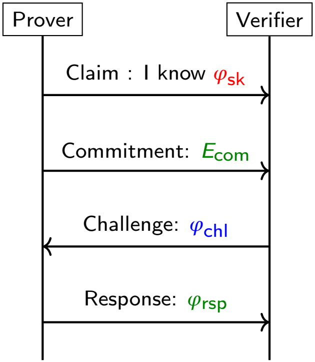
$$\begin{tikzcd} E_0 \arrow[r, "\varphi_{\mathrm{sk}}"] \arrow[d, "\varphi_{\mathrm{com}}"] & E_{\mathrm{pk}} \arrow[d, "\varphi_{\mathrm{chl}}"] \\ E_{\mathrm{com}} \arrow[r, "\varphi_{\mathrm{rsp}}"] & E_{\mathrm{chl}} \end{tikzcd}$$

public

Prover's secret

published by Verifier

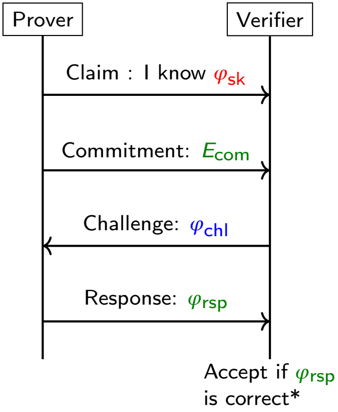
published by Prover



The SQIsign identification scheme

$$\begin{tikzcd} E_0 \arrow[r, "\varphi_{\mathrm{sk}}"] \arrow[d, "\varphi_{\mathrm{com}}"] & E_{\mathrm{pk}} \arrow[d, "\varphi_{\mathrm{chl}}"] \\ E_{\mathrm{com}} \arrow[r, "\varphi_{\mathrm{rsp}}"] & E_{\mathrm{chl}} \end{tikzcd}$$

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



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

The SQIsign identification scheme

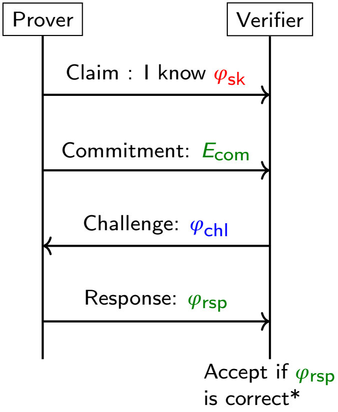
$$\begin{tikzcd}
E_0 \arrow[r, "\varphi_{\mathrm{sk}}"] \arrow[d, "\varphi_{\mathrm{com}}"'] & E_{\mathrm{pk}} \arrow[d, "\varphi_{\mathrm{chl}}"] \\
E_{\mathrm{com}} \arrow[r, "\varphi_{\mathrm{rsp}}", "\text{Deuring}"'] & E_{\mathrm{chl}}
\end{tikzcd}$$

public

Prover's secret

published by Verifier

published by Prover



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

Computing isogenies via the Deuring correspondence

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

Computing isogenies via the Deuring correspondence

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

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

- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$.
- 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 $\mathrm{End}(E_{\mathsf{com}})$ and $\mathrm{End}(E_{\mathsf{chl}})$ and we want an isogeny $\varphi_{\mathsf{rsp}} : E_{\mathsf{com}} \longrightarrow E_{\mathsf{chl}}$.

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

- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$.
- 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 $\varphi_J : E_1 \longrightarrow E_2$.

✓ Takes polynomial time.

Computing isogenies via the Deuring correspondence

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

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

- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$.
- 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 $\varphi_J : E_1 \longrightarrow E_2$.

✓ Takes polynomial time.

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

Computing isogenies via the Deuring correspondence

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

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

- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$.
- 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 $\varphi_J : E_1 \longrightarrow E_2$.

✓ Takes polynomial time.

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

✗ Slow in practice because of the red steps.

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

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:

$$\begin{tikzcd} E_0 \arrow[r, "\varphi_1", "\deg(\varphi_1)=\ell_1"'] \arrow[rrr, bend left, "\varphi"] & E_1 & \cdots & E_{n-1} \arrow[r, "\varphi_n", "\deg(\varphi_n)=\ell_n"'] & E_n \end{tikzcd}$$

- 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:

$$\begin{tikzcd} E_0 \arrow[r, "\varphi_1", "\deg(\varphi_1)=\ell_1"'] \arrow[rrr, bend left, "\varphi"] & E_1 & \cdots & E_{n-1} \arrow[r, "\varphi_n", "\deg(\varphi_n)=\ell_n"'] & E_n \end{tikzcd}$$

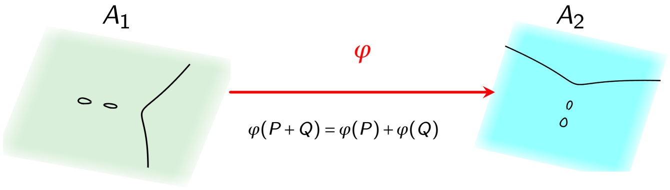
- If $\deg(\varphi)$ is smooth, a generator $P \in E(\mathbb{F}_q)$ s.t. $\ker(\varphi) = \langle P \rangle$ (Vélu).

- **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).

New dimensions in cryptography

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

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

n-isogenies in higher dimension

- Let $\varphi : A \longrightarrow B$ be an isogeny between principally polarised abelian varieties (PPAVs).
- Then there exists a *contravariant 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

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

Kani's lemma (dimension 2) [Kan97]

Consider the following commutative diagram:

$$\begin{tikzcd} E_4 \arrow[r, "\varphi'"] & E_3 \\ E_1 \arrow[u, "\psi'"] \arrow[r, "\varphi"'] \arrow[ur, phantom, "\circlearrowright"] & E_2 \arrow[u, "\psi"'] \end{tikzcd}$$

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

Kani's lemma (dimension 2) [Kan97]

Consider the following commutative diagram:

$$\begin{tikzcd} E_4 \arrow[r, "\varphi'"] & E_3 \\ E_1 \arrow[u, "\psi'"] \arrow[r, "\varphi"] \arrow[ur, phantom, "\circlearrowright"] & E_2 \arrow[u, "\psi"'] \end{tikzcd}$$

s.t. $\deg(\varphi) = \deg(\varphi') = q$ and $\deg(\psi) = \deg(\psi') = r$ are coprime. 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 $(q+r)$-isogeny, i.e. $\widetilde{\Phi} \circ \Phi = [q+r]$, and its kernel is:

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

Kani's lemma (dimension 2) [Kan97]

- Let $\varphi : E_1 \longrightarrow E_2$ be an isogeny of odd degree $q < 2^e$ to be computed.
- Let $\psi : E_2 \longrightarrow E_3$ be an auxiliary isogeny of degree $r := 2^e - q$.

Kani's lemma (dimension 2) [Kan97]

- Let $\varphi : E_1 \longrightarrow E_2$ be an isogeny of odd degree $q < 2^e$ to be computed.
- Let $\psi : E_2 \longrightarrow E_3$ be an auxiliary isogeny of degree $r := 2^e - q$.
- Suppose we know $\psi \circ \varphi(E_1[2^e])$.
- Then we can compute:

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

Kani's lemma (dimension 2) [Kan97]

- Let $\varphi : E_1 \longrightarrow E_2$ be an isogeny of odd degree $q < 2^e$ to be computed.
- Let $\psi : E_2 \longrightarrow E_3$ be an auxiliary isogeny of degree $r := 2^e - q$.
- 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 e 2-isogenies [DMPR25]:

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

Kani's lemma [Kan97] and efficient representations

- Knowing Φ, we can evaluate φ everywhere:

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

- So $(\psi \circ \varphi(E_1[2^e]), q, e)$ is an *efficient representation* of φ (and ψ').

Kani's lemma [Kan97] and efficient representations

- Knowing Φ, we can evaluate φ everywhere:

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

- So $(\psi \circ \varphi(E_1[2^e]), q, e)$ is an *efficient representation* of φ (and ψ').

The Power of Kani's lemma:

- A way to interpolate isogenies given their images on torsion points (led to SIDH attacks).
- Provides efficient representations on non-smooth degree isogenies.

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 $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ and $\mathcal{O}_2 \cong \mathrm{End}(E_2)$.
- 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 $\varphi_J : E_1 \longrightarrow E_2$ using dimension 2 or 4 interpolation techniques.

✓ Takes polynomial time.

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

✓ Faster than the previous method.

The Clapoti method [PR23]

Goal: Given $E_0/\mathbb{F}_{p^2}$ of equation $y^2 = x^3 + x$ and known endomorphism ring $\mathscr{O}_0$, and a left $\mathscr{O}_0$-ideal I, compute $\varphi_I : E_0 \longrightarrow E_I$.

$$
\begin{tikzcd}
E' \arrow[r] & E_0 \\
E_0 \arrow[u] \arrow[r, "\varphi_{I_1}"] & E_I \arrow[u, "\widehat{\varphi}_{I_2}"']
\end{tikzcd}
$$

$$\Phi : E_0^2 \longrightarrow E_I \times E'$$

The Clapoti method [PR23]

Goal: Given $E_0/\mathbb{F}_{p^2}$ of equation $y^2 = x^3 + x$ and known endomorphism ring $\mathscr{O}_0$, and a left $\mathscr{O}_0$-ideal I, compute $\varphi_I : E_0 \longrightarrow E_I$.

$$\begin{tikzcd} E' \arrow[r] & E_0 \\ E_0 \arrow[u] \arrow[r, "\varphi_{I_1}"] & E_I \arrow[u, "\widehat{\varphi}_{I_2}"'] \end{tikzcd}$$

$$\Phi : E_0^2 \longrightarrow E_I \times E'$$

- Find $I_1, I_2 \sim I$ such that:

$$\mathrm{nrd}(I_1) + \mathrm{nrd}(I_2) = 2^e.$$

The Clapoti method [PR23]

Goal: Given $E_0/\mathbb{F}_{p^2}$ of equation $y^2 = x^3 + x$ and known endomorphism ring $\mathscr{O}_0$, and a left $\mathscr{O}_0$-ideal I, compute $\varphi_I : E_0 \longrightarrow E_I$.

$$\begin{tikzcd}
E' \arrow[r] & E_0 \\
E_0 \arrow[u] \arrow[r, "\varphi_{I_1}"] & E_I \arrow[u, "\widehat{\varphi}_{I_2}"']
\end{tikzcd}$$

$$\Phi : E_0^2 \longrightarrow E_I \times E'$$

- Find $I_1, I_2 \sim I$ such that:

$$\mathrm{nrd}(I_1) + \mathrm{nrd}(I_2) = 2^e.$$

- By Kani's lemma, there exists a 2^e-isogeny $\Phi : E_0^2 \longrightarrow E_I \times E'$ that embeds φ_{I_1} and φ_{I_2}.
- $\ker(\Phi)$ can be computed from $\theta := \widehat{\varphi}_{I_2} \circ \varphi_{I_1}$ that generates $I_1 \cdot \overline{I}_2$.

The Clapoti method [PR23]

Goal: Given $E_0/\mathbb{F}_{p^2}$ of equation $y^2 = x^3 + x$ and known endomorphism ring $\mathcal{O}_0$, and a left $\mathcal{O}_0$-ideal I, compute $\varphi_I : E_0 \longrightarrow E_I$.

$$\begin{tikzcd}
E' \arrow[r] & E_0 \\
E_0 \arrow[u] \arrow[r, "\varphi_{I_1}"] & E_I \arrow[u, "\widehat{\varphi}_{I_2}"']
\end{tikzcd}$$

$$\Phi : E_0^2 \longrightarrow E_I \times E'$$

- Find $I_1, I_2 \sim I$ such that:

$$\mathrm{nrd}(I_1) + \mathrm{nrd}(I_2) = 2^e.$$

- By Kani's lemma, there exists a 2^e-isogeny $\Phi : E_0^2 \longrightarrow E_I \times E'$ that embeds φ_{I_1} and φ_{I_2}.
- $\ker(\Phi)$ can be computed from $\theta := \widehat{\varphi}_{I_2} \circ \varphi_{I_1}$ that generates $I_1 \cdot \overline{I}_2$.
- From Φ, one can evaluate φ_{I_1} and then φ_I.

The Clapoti method [PR23]

Goal: Given $E_0/\mathbb{F}_{p^2}$ of equation $y^2 = x^3 + x$ and known endomorphism ring $\mathscr{O}_0$, and a left $\mathscr{O}_0$-ideal I, compute $\varphi_I : E_0 \longrightarrow E_I$.

$$\begin{tikzcd}
E' \arrow[r] & E_0 \\
E_0 \arrow[u] \arrow[r, "\varphi_{I_1}"] & E_I \arrow[u, "\widehat{\varphi}_{I_2}"']
\end{tikzcd}$$

$$\Phi : E_0^2 \longrightarrow E_I \times E'$$

- Find $I_1, I_2 \sim I$ such that:

$$\cancel{\mathrm{nrd}(I_1) + \mathrm{nrd}(I_2) = 2^e}.$$

Previously too hard to solve.

- By Kani's lemma, there exists a 2^e-isogeny $\Phi : E_0^2 \longrightarrow E_I \times E'$ that embeds φ_{I_1} and φ_{I_2}.
- $\ker(\Phi)$ can be computed from $\theta := \widehat{\varphi}_{I_2} \circ \varphi_{I_1}$ that generates $I_1 \cdot \overline{I}_2$.
- From Φ, one can evaluate φ_{I_1} and then φ_I.

The Clapoti method in SQIsign2D-West [BDF+25]

Goal: Given $E_0/\mathbb{F}_{p^2}$ of equation $y^2 = x^3 + x$ and known endomorphism ring $\mathscr{O}_0$, and a left $\mathscr{O}_0$-ideal I, compute $\varphi_I : E_0 \longrightarrow E_I$.

$$\begin{tikzcd}
E'^2 \arrow[rr] & & E_v \\
 & & E_0 \arrow[u, "\varphi_v"'] \\
E_u \arrow[uu] \arrow[r, "\widehat{\varphi}_u"] & E_0 \arrow[r, "\varphi_{I_1}"] & E_I \arrow[u, "\widehat{\varphi}_{I_2}"']
\end{tikzcd}$$

- Find $u, v > 0$ and $I_1, I_2 \sim I$ such that:

$$u\,\mathrm{nrd}(I_1) + v\,\mathrm{nrd}(I_2) = 2^e.$$

$$\Phi : E_u \times E_v \longrightarrow E_I \times E'$$

The Clapoti method in SQIsign2D-West [BDF+25]

Goal: Given $E_0/\mathbb{F}_{p^2}$ of equation $y^2 = x^3 + x$ and known endomorphism ring $\mathscr{O}_0$, and a left $\mathscr{O}_0$-ideal I, compute $\varphi_I : E_0 \longrightarrow E_I$.

$$\begin{tikzcd}
E'^2 \arrow[rr] & & E_v \\
& & E_0 \arrow[u, "\varphi_v"] \\
E_u \arrow[uu] \arrow[r, "\widehat{\varphi}_u"] & E_0 \arrow[r, "\varphi_{I_1}"] & E_I \arrow[u, "\widehat{\varphi}_{I_2}"]
\end{tikzcd}$$

$$\Phi : E_u \times E_v \longrightarrow E_I \times E'$$

- Find $u, v > 0$ and $I_1, I_2 \sim I$ such that:
$$u\,\mathrm{nrd}(I_1) + v\,\mathrm{nrd}(I_2) = 2^e.$$
- Use Kani's lemma to compute isogenies φ_u and φ_v of degrees u and v [NO24].

The Clapoti method in SQIsign2D-West [BDF+25]

Goal: Given $E_0/\mathbb{F}_{p^2}$ of equation $y^2 = x^3 + x$ and known endomorphism ring $\mathscr{O}_0$, and a left $\mathscr{O}_0$-ideal I, compute $\varphi_I : E_0 \longrightarrow E_I$.

$$\begin{tikzcd}
E'^2 \arrow[rr] & & E_v \\
& & E_0 \arrow[u, "\varphi_v"'] \\
E_u \arrow[uu] \arrow[r, "\widehat{\varphi}_u"] & E_0 \arrow[r, "\varphi_{I_1}"] & E_I \arrow[u, "\widehat{\varphi}_{I_2}"']
\end{tikzcd}$$

$$\Phi : E_u \times E_v \longrightarrow E_I \times E'$$

- Find $u, v > 0$ and $I_1, I_2 \sim I$ such that:

$$u \,\mathrm{nrd}(I_1) + v \,\mathrm{nrd}(I_2) = 2^e.$$

- Use Kani's lemma to compute isogenies φ_u and φ_v of degrees u and v [NO24].
- By Kani's lemma, there exists a 2^e-isogeny $\Phi : E_u \times E_v \longrightarrow E_I \times E'$ that embeds $\varphi_{I_1} \circ \widehat{\varphi}_u$ and $\varphi_{I_2} \circ \widehat{\varphi}_v$.
- $\ker(\Phi)$ can be computed from φ_u, φ_v and $\theta := \widehat{\varphi}_{I_2} \circ \varphi_{I_1}$ that generates $I_1 \cdot \overline{I}_2$.

The Clapoti method in SQIsign2D-West [BDF+25]

Goal: Given $E_0/\mathbb{F}_{p^2}$ of equation $y^2 = x^3 + x$ and known endomorphism ring $\mathcal{O}_0$, and a left $\mathcal{O}_0$-ideal I, compute $\varphi_I : E_0 \longrightarrow E_I$.

$$\begin{tikzcd}
E'^2 \arrow[rr] & & E_v \\
& & E_0 \arrow[u, "\varphi_v"'] \\
E_u \arrow[uu] \arrow[r, "\widehat{\varphi}_u"] & E_0 \arrow[r, "\varphi_{I_1}"] & E_I \arrow[u, "\widehat{\varphi}_{I_2}"']
\end{tikzcd}$$

$$\Phi : E_u \times E_v \longrightarrow E_I \times E'$$

- Find $u, v > 0$ and $I_1, I_2 \sim I$ such that:

$$u \,\mathrm{nrd}(I_1) + v \,\mathrm{nrd}(I_2) = 2^e.$$

- Use Kani's lemma to compute isogenies φ_u and φ_v of degrees u and v [NO24].
- By Kani's lemma, there exists a 2^e-isogeny $\Phi : E_u \times E_v \longrightarrow E_I \times E'$ that embeds $\varphi_{I_1} \circ \widehat{\varphi}_u$ and $\varphi_{I_2} \circ \widehat{\varphi}_v$.
- $\ker(\Phi)$ can be computed from φ_u, φ_v and $\theta := \widehat{\varphi}_{I_2} \circ \varphi_{I_1}$ that generates $I_1 \cdot \overline{I}_2$.
- From Φ, one can evaluate $\varphi_{I_1} \circ \varphi_u$ and then φ_I.

Ideal class group action

- Let $\mathfrak{O}$ be a quadratic imaginary order.

Ideal class group action

- Let $\mathfrak{O}$ be a quadratic imaginary order.
- A (primitively) $\mathfrak{O}$-*oriented* curve is a supersingular elliptic curve E with a maximal embedding $\iota : \mathfrak{O} \hookrightarrow \mathrm{End}(E)$.

Ideal class group action

- Let $\mathfrak{O}$ be a quadratic imaginary order.
- A (primitively) $\mathfrak{O}$-*oriented* curve is a supersingular elliptic curve E with a maximal embedding $\iota : \mathfrak{O} \hookrightarrow \mathrm{End}(E)$.
- $\mathrm{Cl}(\mathfrak{O})$ acts freely and (almost) transitively on $\mathfrak{O}$-oriented curves.

Ideal class group action

- Let $\mathfrak{O}$ be a quadratic imaginary order.
- A (primitively) $\mathfrak{O}$-*oriented* curve is a supersingular elliptic curve E with a maximal embedding $\iota : \mathfrak{O} \hookrightarrow \mathrm{End}(E)$.
- $\mathrm{Cl}(\mathfrak{O})$ acts freely and (almost) transitively on $\mathfrak{O}$-oriented curves.

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

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:

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).

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 $\mathfrak{l}_1, \cdots, \mathfrak{l}_t$ that generate $\mathrm{Cl}(\mathfrak{O})$.
- ⚠ **Issue:** This makes schemes less efficient and less scalable to bigger parameters.

The Clapoti method in PEGASIS [DEF+25]

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

$$\begin{tikzcd}
E'^2 \arrow[rr] & & A_v \\
& & E^2 \arrow[u, "\Phi_v"'] \\
A_u \arrow[uu] \arrow[r, "\widetilde{\Phi}_u"] & E^2 \arrow[r, "\Phi_{\mathfrak{b}}"] & E^2_{\mathfrak{a}} \arrow[u, "\widetilde{\Phi}_{\mathfrak{c}}"']
\end{tikzcd}$$

$$F : A_u \times A_v \longrightarrow E^2_{\mathfrak{a}} \times E'^2$$

- Find $u, v > 0$ and $\mathfrak{b}, \mathfrak{c} \sim \mathfrak{a}$ such that:

$$u\,\mathrm{nrd}(\mathfrak{b}) + v\,\mathrm{nrd}(\mathfrak{c}) = 2^e.$$

- Compute u and v-isogenies Φ_u and Φ_v in dimension 2.
- By Kani's lemma, there exists a 2^e-isogeny $F : A_u \times A_v \longrightarrow E^2_{\mathfrak{a}} \times E'^2$ that embeds $\Phi_{\mathfrak{b}} \circ \widetilde{\Phi}_u$ and $\Phi_{\mathfrak{c}} \circ \widetilde{\Phi}_v$.
- $\ker(F)$ can be computed from Φ_u, Φ_v and $\theta := \widehat{\varphi}_{\mathfrak{c}} \circ \varphi_{\mathfrak{c}}$ that generates $\mathfrak{b} \cdot \overline{\mathfrak{c}}$.
- From F, we extract $E_{\mathfrak{a}}$.

Fast computation of higher 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: 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:

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

- Such a symplectic isomorphism is determined by a (ζ-)*symplectic basis* $(S_1, \cdots, S_g, T_1, \cdots, T_g)$ of $A[n]$ *i.e.* a basis such that:

$$\forall 1 \leq i, j \leq g, \quad e_n(S_i, S_j) = e_n(T_i, T_j) = 1 \quad \text{and} \quad e_n(S_i, T_j) = \zeta^{\delta_{i,j}},$$

where ζ is a primitive n-th root of unity.

Definition: theta structure

Definition (Max Duparc)

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

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

along with a symplectic isomorphism:

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

satisfying the *theta group action relation*:

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

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

Properties of theta structures

Theta structures are induced by symplectic isomorphisms

Theorem (Mumford, 1966)

A level n theta structure $(\Theta(n), \overline{\Theta}(n))$ on a PPAV A is fully determined by a symplectic isomorphism $\overline{\Theta}(2n) : (\mathbb{Z}/2n\mathbb{Z})^g \times \widehat{(\mathbb{Z}/2n\mathbb{Z})^g} \xrightarrow{\sim} A[2n]$ inducing $\overline{\Theta}(n)$ i.e. by a symplectic basis of $A[2n]$ inducing $\overline{\Theta}(n)$.

Properties of theta structures

Theta structures are induced by symplectic isomorphisms

Theorem (Mumford, 1966)

A level n theta structure $(\Theta(n), \overline{\Theta}(n))$ on a PPAV A is fully determined by a symplectic isomorphism $\overline{\Theta}(2n) : (\mathbb{Z}/2n\mathbb{Z})^g \times \widehat{(\mathbb{Z}/2n\mathbb{Z})^g} \xrightarrow{\sim} A[2n]$ inducing $\overline{\Theta}(n)$ i.e. by a symplectic basis of $A[2n]$ inducing $\overline{\Theta}(n)$.

Theta structures and theta null points:

- When $4|n$, the *marked AV* (PPAV and theta structure) $(A, \Theta(n), \overline{\Theta}(n))$ is determined by the *theta null point* $(\theta_i(0_A))_i$.

Properties of theta structures

Theta structures are induced by symplectic isomorphisms

Theorem (Mumford, 1966)

A level n theta structure $(\Theta(n), \overline{\Theta}(n))$ on a PPAV A is fully determined by a symplectic isomorphism $\overline{\Theta}(2n) : (\mathbb{Z}/2n\mathbb{Z})^g \times \widehat{(\mathbb{Z}/2n\mathbb{Z})^g} \xrightarrow{\sim} A[2n]$ inducing $\overline{\Theta}(n)$ i.e. by a symplectic basis of $A[2n]$ inducing $\overline{\Theta}(n)$.

Theta structures and theta null points:

- When $4|n$, the *marked AV* (PPAV and theta structure) $(A, \Theta(n), \overline{\Theta}(n))$ is determined by the *theta null point* $(\theta_i(0_A))_i$.
- In other cases, we still use the theta null point as a representative of a marked AV.
- This is enough for arithmetic operations.

Theta structures of level 2

Theorem

Let $(A, \Theta(n), \overline{\Theta}(n))$ be a marked AV of level n and dimension g. Then:

1. *[Mum74] If $n \geq 3$, then $\Theta(n) : A \hookrightarrow \mathbb{P}^{n^g-1}$ is an embedding.*
2. *[BL04] If $n = 2$ and A is not a product, then $\Theta(2)$ defines an embedding $A/\pm \hookrightarrow \mathbb{P}^{2^g-1}$.*
3. *[BL04] If $n = 2$ and $A \simeq A_1 \times \cdots \times A_m$, then $\Theta(2)$ defines an embedding*
$$A_1/\pm \times \cdots \times A_m/\pm \hookrightarrow \mathbb{P}^{2^g-1}.$$

Our goal

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:

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

Our goal

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:

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

Our goal

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:

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

Method:

- Decompose f as a chain of 2-isogenies:

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

- Compute every 2-isogeny iteratively, using:

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

Our goal

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:

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

Method:

- Decompose f as a chain of 2-isogenies:

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

- Compute every 2-isogeny iteratively, using:

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

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.

$$\begin{tikzcd}
(A, \Theta^A(4), \overline{\Theta}^A(4)) \arrow[dr, "f", "\text{isogeny theorem}"'] & \\
(A, \Theta^A(2), \overline{\Theta}^A(2)) \arrow[u, "\text{change of level}"] & (B, \Theta^B(2), \overline{\Theta}^B(2))
\end{tikzcd}$$

Computing a 2-isogeny: change of level

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

$$\begin{tikzcd}
(A, \Theta^A(4), \overline{\Theta}^A(4)) \arrow[dr, "f", "\text{isogeny theorem}"'] & \\
(A, \Theta^A(2), \overline{\Theta}^A(2)) \arrow[u, "\text{change of level}"] & (B, \Theta^B(2), \overline{\Theta}^B(2))
\end{tikzcd}$$

- The level 4 theta structure $(A, \Theta^A(4), \overline{\Theta}^A(4))$ is induced by a symplectic basis of $A[8]$.
- For that reason, we need 8-torsion points $T_1, \cdots, T_g$ such that $\ker(f) = \langle [4]T_1, \cdots, [4]T_g \rangle$ to compute f.

Computing a 2-isogeny: change of level

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

$$\begin{tikzcd}
(A,\Theta^A(4),\overline{\Theta}^A(4)) \arrow[dr, "f"', "\text{isogeny theorem}"] & \\
(A,\Theta^A(2),\overline{\Theta}^A(2)) \arrow[u, "\text{change of level}"] & (B,\Theta^B(2),\overline{\Theta}^B(2))
\end{tikzcd}$$

- The level 4 theta structure $(A,\Theta^A(4),\overline{\Theta}^A(4))$ is induced by a symplectic basis of $A[8]$.
- For that reason, we need 8-torsion points $T_1,\cdots,T_g$ such that $\ker(f)=\langle[4]T_1,\cdots,[4]T_g\rangle$ 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:

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

where:

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

Issues with the first 2-isogeny in the chain

Usually, the first isogeny of the chain is a *gluing* $f : A_1 \times A_2 \longrightarrow B$.

Issues with the first 2-isogeny in the chain

Usually, the first isogeny of the chain is a *gluing* $f : A_1 \times A_2 \longrightarrow B$.

Issue 1:

- The starting domain theta structure $\Theta^{A_1 \times A_2}$ is the product $\Theta^{A_1} \times \Theta^{A_2}$:

$$\theta_{i,j}^{A_1 \times A_2}(x, y) = \theta_i^{A_1}(x) \cdot \theta_j^{A_2}(y).$$

- The isogeny formulas only work when

$$\overline{\Theta}^{A_1 \times A_2}(\{0\} \times \widehat{(\mathbb{Z}/2\mathbb{Z})^g}) = \ker(f).$$

- This is usually not the case when $\Theta^{A_1 \times A_2} = \Theta^{A_1} \times \Theta^{A_2}$.

Issues with the first 2-isogeny in the chain

Usually, the first isogeny of the chain is a *gluing* $f : A_1 \times A_2 \longrightarrow B$.

Issue 1:

- The starting domain theta structure $\Theta^{A_1 \times A_2}$ is the product $\Theta^{A_1} \times \Theta^{A_2}$:

$$\theta_{i,j}^{A_1 \times A_2}(x, y) = \theta_i^{A_1}(x) \cdot \theta_j^{A_2}(y).$$

- The isogeny formulas only work when

$$\overline{\Theta}^{A_1 \times A_2}(\{0\} \times \widehat{(\mathbb{Z}/2\mathbb{Z})^g}) = \ker(f).$$

- This is usually not the case when $\Theta^{A_1 \times A_2} = \Theta^{A_1} \times \Theta^{A_2}$.

Solution 1: Compute a new theta structure $\Theta'^{A_1 \times A_2}$ such that

$$\overline{\Theta'}^{A_1 \times A_2}(\{0\} \times \widehat{(\mathbb{Z}/2\mathbb{Z})^g}) = \ker(f).$$

Change of coordinate formulas

$$\begin{tikzcd}
\text{ζ-symplectic basis } \mathscr{B} \text{ of } A[4] \arrow[r, "\text{Change of basis}", "\text{matrix } M \in \mathrm{Sp}_{2g}(\mathbb{Z}/4\mathbb{Z})"'] \arrow[d] & \text{ζ-symplectic basis } \mathscr{B}' \text{ of } A[4] \arrow[d] \\
\text{Theta structure } (\Theta^A, \overline{\Theta}^A) \arrow[d] & \text{Theta structure } (\Theta'^A, \overline{\Theta'}^A) \arrow[d] \\
\text{Initial theta coordinates } (\theta_i^A)_i \arrow[r, "\text{Change of coordinates}", "\text{matrix } N(\zeta, M)"'] & \text{New theta coordinates } (\theta'^A_i)_i
\end{tikzcd}$$

*ζ is a primitive 4-th root of unity given by the Weil-pairings of symplectic basis.

The right choice of theta structure propagates

When there is only one gluing isogeny, only 2 change of theta structures are needed

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

Change of theta coordinates

Change of theta coordinates

Evaluating a gluing 2-isogeny

Issue 2:

- The evaluation algorithm:

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

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

Evaluating a gluing 2-isogeny

Issue 2:

- The evaluation algorithm:

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

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

- Why? Because level 2 theta coordinates encode points up to a sign, 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

Issue 2:

- The evaluation algorithm:

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

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

- Why? Because level 2 theta coordinates encode points up to a sign, we are computing:

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

- We need additional information to lift the sign indetermination.

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

A dramatic improvement of SQIsign with dimension 2

Table: Comparison of time performance in ms of SQIsign (NIST round 1) and SQIsign (NIST round 2) on an Intel Core i5-1335U 4600MHz CPU.

		NIST I	NIST III	NIST V
SQIsign v 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
SQIsign v 2.0	Key Gen.	10.63	32.05	51.37
	Signature	24.53	74.20	126.72
	Verification	1.13	4.10	8.49

PEGASIS: the proof dimension 4 can be efficient

Paper	Impl.	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 (This work)	Sage	1.53s	4.21s	10.5s	21.3s	2m2s

Table: Comparison between 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.

Thank you for listening

- SIDH attacks and HD isogenies are a breakthrough in isogeny based cryptography.
- There have been many grounbreaking constructive applications (*e.g.* SQIsign) and new applications are still unfolding.
- Research is still needed to accelerate HD algorithms (*e.g.* for odd degree).