An introduction to SQIsign

Pierrick Dartois

2025, December 5

Contributions covered in this talk

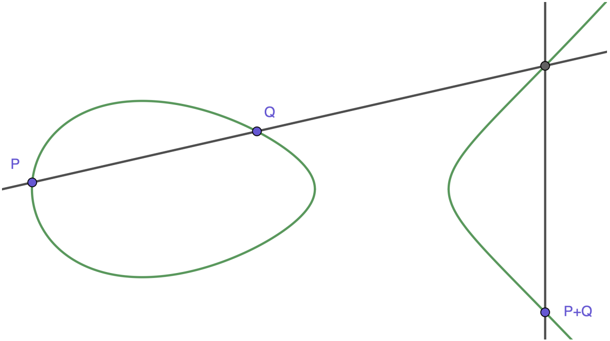
- [DLRW24] *SQIsignHD: New Dimensions in Cryptography*, Pierrick Dartois, Antonin Leroux, Damien Robert and Benjamin Wesolowski. EUROCRYPT 2024.

- [BFD+24] *SQIsign2D-West: The Fast, the Small and the Safer*, Andrea Basso, Pierrick Dartois, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert and Benjamin Wesolowski. ASIACRYPT 2024.

- [BSE+25] *Qlapoti: Simple and Efficient Translation of Quaternion Ideals to Isogenies*, Giacomo Borin, Maria Corte-Real Santos, Jonathan Komada Eriksen, Riccardo Invernizzi, Marzio Mula, Sina Scheffler, Frederik Vercauteren. Preprint, 2025.

A brief introduction to isogenies

Elliptic curves

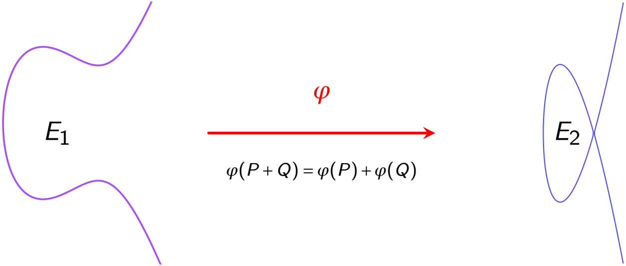


- An elliptic curve $E/\mathbb{F}_q$ is defined by:

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

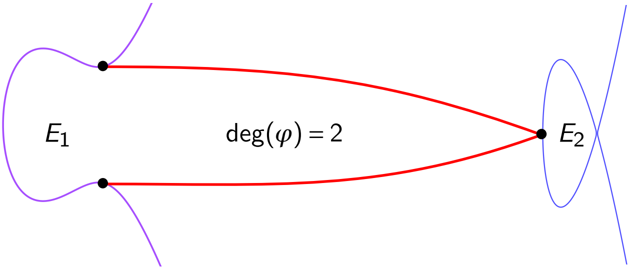
  with an infinite element 0_E.
- E is equipped with a commutative group law.

Isogenies between elliptic curves

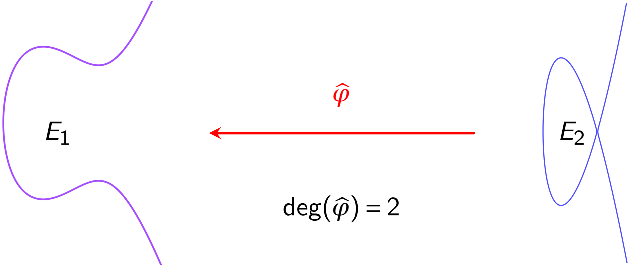


$$\varphi(x,y)=\left(\frac{p(x)}{q(x)},y\frac{r(x)}{s(x)}\right)$$

Isogenies - degree



Isogenies - the dual isogeny

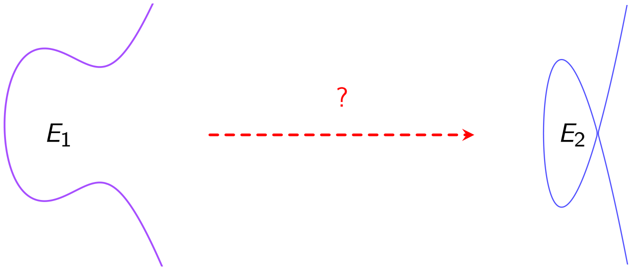


Isogeny chains

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

Why are isogenies interesting in cryptography?

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



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

Path in the supesingular isogeny graph

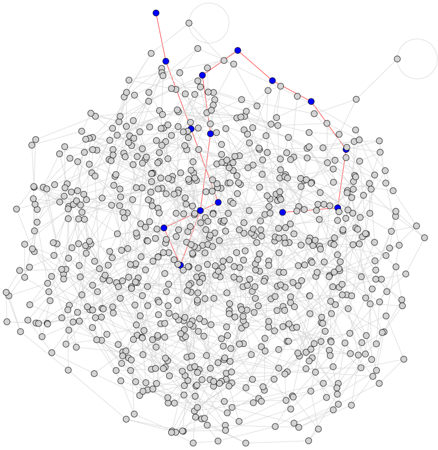


Figure: A 2^{14}-isogeny in the supersingular 2-isogeny graph over $\mathbb{F}_{10007^2}$.

Path in the supesingular isogeny graph

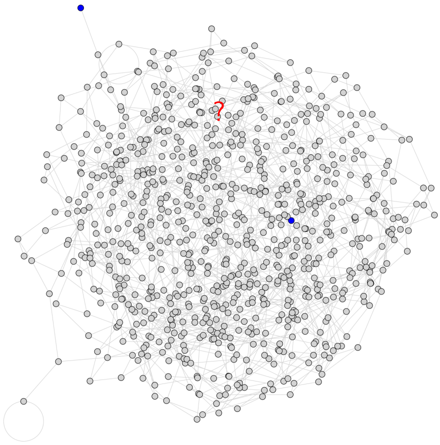


Figure: An instance of the supersingular 2-isogeny path problem over $\mathbb{F}_{10007^2}$.

Path in the supesingular isogeny graph

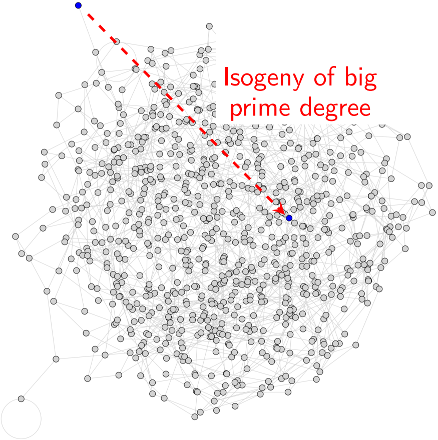


Figure: An instance of the supersingular isogeny problem over $\mathbb{F}_{10007^2}$.

What does it mean to "compute" an isogeny?

Definition (Efficient representation)

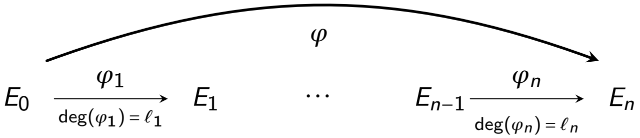
Let $\varphi : E \longrightarrow E'$ be a d-isogeny over $\mathbb{F}_q$. An efficient representation of φ with respect to an algorithm $\mathscr{A}$ is some data $D_\varphi \in \{0,1\}^*$ such that:

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:

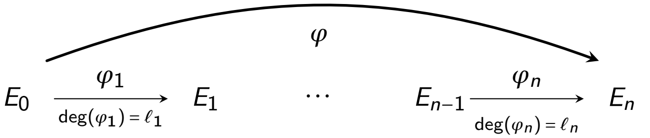


- If $\deg(\varphi)$ is smooth, a generator $P \in E(\mathbb{F}_q)$ s.t. $\ker(\varphi) = \langle P \rangle$ (Vélu).

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:

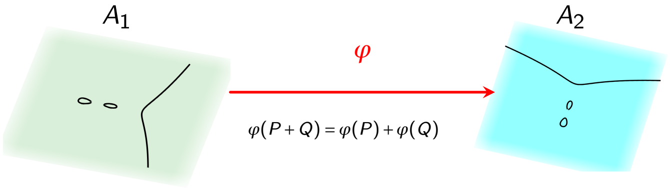


- If $\deg(\varphi)$ is smooth, a generator $P \in E(\mathbb{F}_q)$ s.t. $\ker(\varphi) = \langle P \rangle$ (Vélu).

- **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

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

n-isogenies in higher dimension

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

n-isogenies in higher dimension

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

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 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 $\mathbb{Q}$:

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

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:**

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

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

The Deuring correspondence

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

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
$\varphi, \psi : E \longrightarrow E'$	$I_\varphi \sim I_\psi \ (I_\psi = I_\varphi \alpha,\ \alpha \in \mathcal{B}_{p,\infty})$
$\widehat{\varphi}$	$\overline{I_\varphi}$

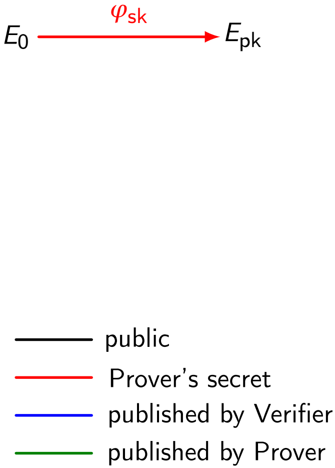
The Deuring correspondence

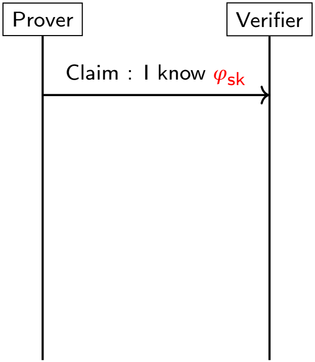
Supersingular elliptic curves	Quaternions
$j(E)$ or $j(E)^p$ supersingular	$\mathcal{O} \cong \mathrm{End}(E)$ maximal order in $\mathcal{B}_{p,\infty}$
$\varphi : E \longrightarrow E'$	left $\mathcal{O}$-ideal and right $\mathcal{O}'$-ideal I_φ
$\varphi, \psi : E \longrightarrow E'$	$I_\varphi \sim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

The Deuring correspondence

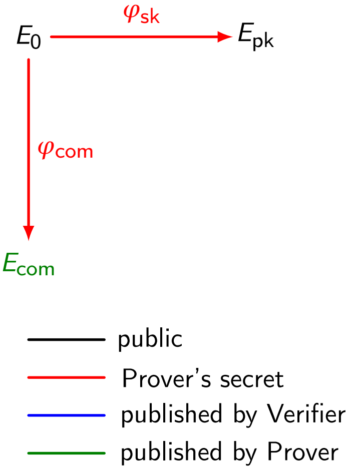
Supersingular elliptic curves	Quaternions
$j(E)$ or $j(E)^p$ supersingular	$\mathcal{O} \cong \mathrm{End}(E)$ maximal order in $\mathcal{B}_{p,\infty}$
$\varphi : E \longrightarrow E'$	left $\mathcal{O}$-ideal and right $\mathcal{O}'$-ideal I_φ
$\varphi, \psi : E \longrightarrow E'$	$I_\varphi \sim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

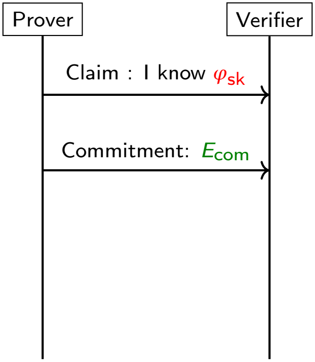
The SQIsign identification scheme



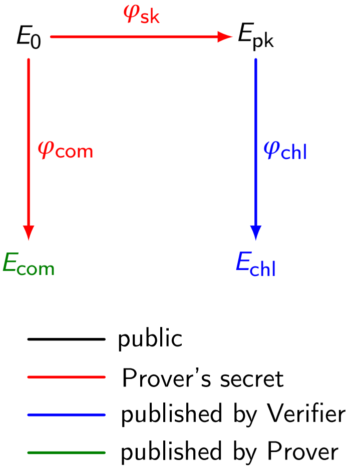


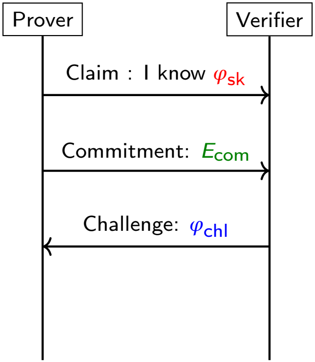
The SQIsign identification scheme



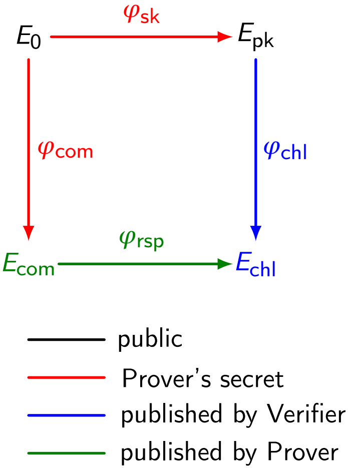


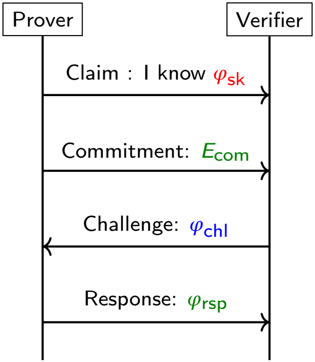
The SQIsign identification scheme



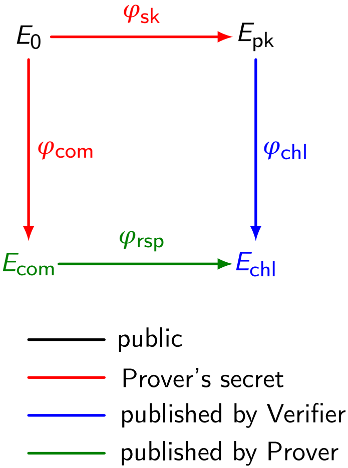


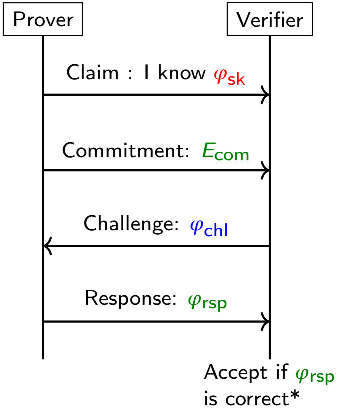
The SQIsign identification scheme





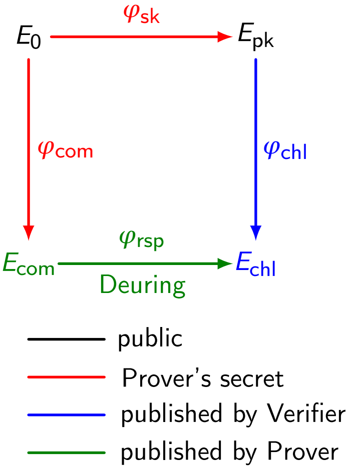
The SQIsign identification scheme

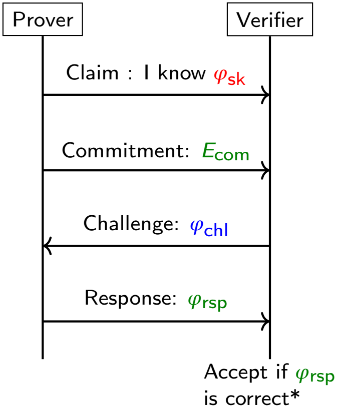




*φ_{rsp} should not factor through φ_{chl}.

The SQIsign identification scheme





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

Computing isogenies via the Deuring correspondence

Goal: In SQIsign, we know $\mathrm{End}(E_{\mathrm{com}})$ 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 $\mathrm{End}(E_{\mathrm{com}})$ 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.

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 $\mathrm{End}(E_{\mathrm{com}})$ 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.

✗ 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 $\mathcal{O}_1 \cong \mathrm{End}(E_1)$ 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.

A brief history of SQIsign

2020	SQIsign [DKLPW20]	1D Ideal to Isogeny
2021	SQIsign ×2 as fast [FLLW23]	Enhanced 1D Ideal to Isogeny
2022	HD SIDH attacks [CD23; MMPPW23; Rob23]	Introduction of HD isogenies in cryptology
2023	**SQIsignHD** [DLRW24]	4D Ideal to Isogeny (verif)
2024	**SQIsign2D** variants [NOC+25; BFD+24; DF25]	2D Ideal to Isogeny (sign & verif)
2025	**Qlapoti** [BSE+25]	Faster 2D Ideal to Isogeny

New algorithms for ideal-to-isogeny translations

Kani's lemma (dimension 2) [Kan97]

Consider the following commutative diagram:

$$\begin{array}{ccc} E_4 & \xrightarrow{\varphi'} & E_3 \\ \uparrow{\scriptstyle \psi'} & \circlearrowright & \uparrow{\scriptstyle \color{red}{\psi}} \\ E_1 & \xrightarrow{\color{blue}{\varphi}} & E_2 \end{array}$$

s.t. $\deg(\color{blue}{\varphi}) = \deg(\varphi') = q$ and $\deg(\color{red}{\psi}) = \deg(\psi') = r$ are coprime.

Kani's lemma (dimension 2) [Kan97]

Consider the following commutative diagram:

$$\begin{array}{ccc} E_4 & \xrightarrow{\varphi'} & E_3 \\ \psi' \uparrow & \circlearrowright & \uparrow \psi \\ E_1 & \xrightarrow{\varphi} & E_2 \end{array}$$

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 $(q+r, q+r)$-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 $(2,2)$-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.

A solvable problem with 2-dimensional techniques

Set-up:

- $p = c \cdot 2^e - 1$.
- $E_0 : y^2 = x^3 + x$ defined over $\mathbb{F}_p$.
- $\mathscr{O}_0 \simeq \mathrm{End}(E_0)$ is known and of special form.

A solvable problem with 2-dimensional techniques

Set-up:

- $p = c \cdot 2^e - 1$.
- $E_0 : y^2 = x^3 + x$ defined over $\mathbb{F}_p$.
- $\mathcal{O}_0 \simeq \mathrm{End}(E_0)$ is known and of special form.

Input: A left $\mathcal{O}_0$-ideal I.

Output: An efficient representation of $\varphi_I : E_0 \longrightarrow E_I$.

In practice: $(\varphi_I(P_0), \varphi_I(Q_0))$, where (P_0, Q_0) is a basis of $E_0[2^e]$.

A solvable problem with 2-dimensional techniques

Set-up:

- $p = c \cdot 2^e - 1$.
- $E_0 : y^2 = x^3 + x$ defined over $\mathbb{F}_p$.
- $\mathcal{O}_0 \simeq \mathrm{End}(E_0)$ is known and of special form.

Input: A left $\mathcal{O}_0$-ideal I.

Output: An efficient representation of $\varphi_I : E_0 \longrightarrow E_I$.

In practice: $(\varphi_I(P_0), \varphi_I(Q_0))$, where (P_0, Q_0) is a basis of $E_0[2^e]$.

Starting from E_0 is necessary to stay in dimension 2.

A solvable problem with 2-dimensional techniques

Set-up:

- $p = c \cdot 2^e - 1$.
- $E_0 : y^2 = x^3 + x$ defined over $\mathbb{F}_p$.
- $\mathcal{O}_0 \simeq \mathrm{End}(E_0)$ is known and of special form.

Input: A left $\mathcal{O}_0$-ideal I.

Output: An efficient representation of $\varphi_I : E_0 \longrightarrow E_I$.

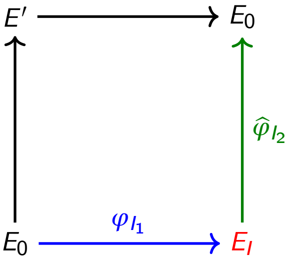
In practice: $(\varphi_I(P_0), \varphi_I(Q_0))$, where (P_0, Q_0) is a basis of $E_0[2^e]$.

Starting from E_0 is necessary to stay in dimension 2.

We can manage this constraint in SQIsign2D (teasing).

The Qlapoti method [PR23; BSE+25]

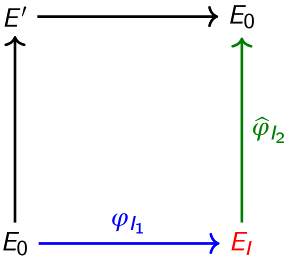
Goal: Given $E_0/\mathbb{F}_{p^2}$ of equation $y^2 = x^3 + x$ and known endomorphism ring $\mathcal{O}_0$, and a left $\mathcal{O}_0$-ideal I, compute $\varphi_I : E_0 \longrightarrow E_I$.



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

The Qlapoti method [PR23; BSE+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 $\varphi_I : E_0 \longrightarrow E_I$.



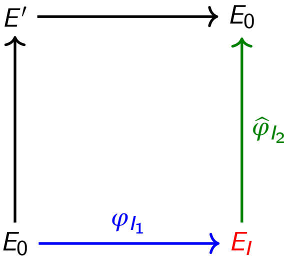
$$\Phi : E_0^2 \longrightarrow E_I \times E'$$

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

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

The Qlapoti method [PR23; BSE+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 $\varphi_I : E_0 \longrightarrow E_I$.



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

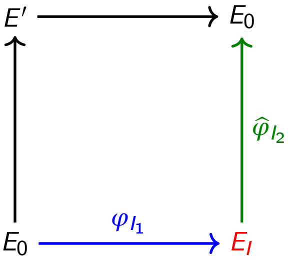
- Find $I_1, I_2 \sim I$ such that:

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

- 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 Qlapoti method [PR23; BSE+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 $\varphi_I : E_0 \longrightarrow E_I$.



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

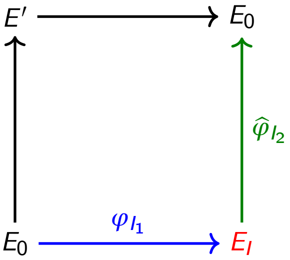
- Find $I_1, I_2 \sim I$ such that:

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

- 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 Qlapoti method [PR23; BSE+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 $\varphi_I : E_0 \longrightarrow E_I$.



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

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

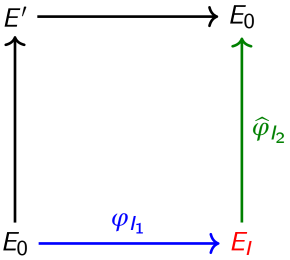
$$\mathrm{nrd}(I_1) + \mathrm{nrd}(I_2) = 2^e.$$

Exploits the structure of $\mathscr{O}_0$

- 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.

Before Qlapoti

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 $\varphi_I : E_0 \longrightarrow E_I$.



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

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

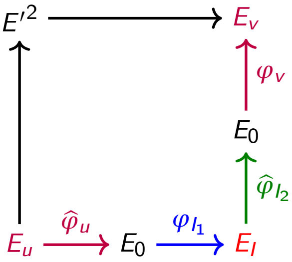
  ~~$\mathrm{nrd}(I_1) + \mathrm{nrd}(I_2) = 2^e.$~~

  How to solve that ?

- 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 SQIsign2D-West solution [BFD+24]

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 $\varphi_I : E_0 \longrightarrow E_I$.



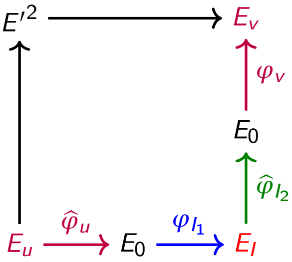
$$\Phi : E_u \times E_v \longrightarrow E_I \times E'$$

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

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

The SQIsign2D-West solution [BFD+24]

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 $\varphi_I : E_0 \longrightarrow E_I$.



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

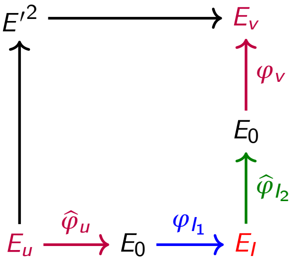
- Find $u, v > 0$ and $I_1, I_2 \sim I$ such that:

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

- Use Kani's lemma to compute isogenies φ_u and φ_v of degrees u and v [NO23].

The SQIsign2D-West solution [BFD+24]

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 $\varphi_I : E_0 \longrightarrow E_I$.



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

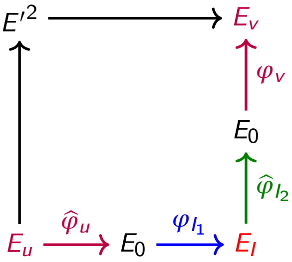
- Find $u, v > 0$ and $I_1, I_2 \sim I$ such that:

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

- Use Kani's lemma to compute isogenies φ_u and φ_v of degrees u and v [NO23].
- 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.

The SQIsign2D-West solution [BFD+24]

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 $\varphi_I : E_0 \longrightarrow E_I$.



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

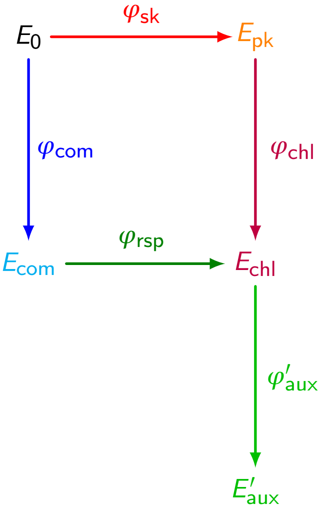
Costs 3 2D isogenies.

- 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 [NO23].
- 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.

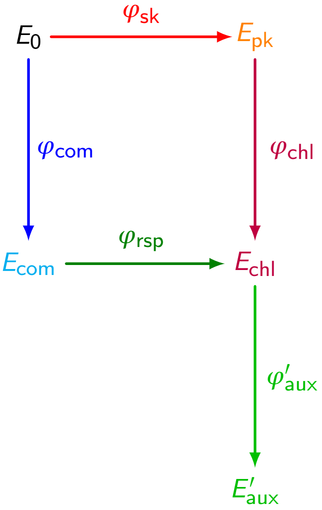
Response/signature



Response:

- Compute $I_{\mathrm{chl}} \subset \mathrm{End}(E_{\mathrm{pk}})$ associated to φ_{chl}.
- $J \longleftarrow \overline{I}_{\mathrm{com}} \cdot I_{\mathrm{sk}} \cdot I_{\mathrm{chl}}$.
- Compute $I_{\mathrm{rsp}} \sim J$ random of norm $q < 2^r \simeq \sqrt{p}$.
- Sample $I'_{\mathrm{aux}} \subset \mathrm{End}(E_{\mathrm{chl}})$ at random of norm $2^r - q$.
- Translate $I_{\mathrm{com}} \cdot I_{\mathrm{rsp}} \cdot I'_{\mathrm{aux}}$ into $\varphi'_{\mathrm{aux}} \circ \varphi_{\mathrm{rsp}} \circ \varphi_{\mathrm{com}}$.

Response/signature

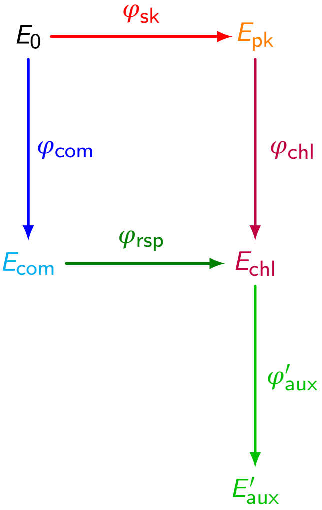


Response:

- Compute $I_{\mathrm{chl}} \subset \mathrm{End}(E_{\mathrm{pk}})$ associated to φ_{chl}.
- $J \longleftarrow \overline{I}_{\mathrm{com}} \cdot I_{\mathrm{sk}} \cdot I_{\mathrm{chl}}$.
- Compute $I_{\mathrm{rsp}} \sim J$ random of norm $q < 2^r \simeq \sqrt{p}$.
- Sample $I'_{\mathrm{aux}} \subset \mathrm{End}(E_{\mathrm{chl}})$ at random of norm $2^r - q$.
- Translate $I_{\mathrm{com}} \cdot I_{\mathrm{rsp}} \cdot I'_{\mathrm{aux}}$ into $\varphi'_{\mathrm{aux}} \circ \varphi_{\mathrm{rsp}} \circ \varphi_{\mathrm{com}}$.

✓ Starting from E_0.

Response/signature



Response:

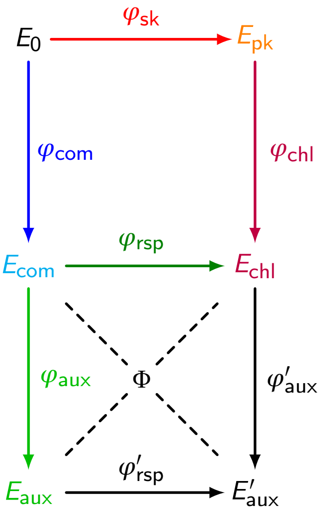
- Compute $I_{chl} \subset \mathrm{End}(E_{pk})$ associated to φ_{chl}.
- $J \longleftarrow \overline{I}_{com} \cdot I_{sk} \cdot I_{chl}$.
- Compute $I_{rsp} \sim J$ random of norm $q < 2^r \simeq \sqrt{p}$.
- Sample $I'_{aux} \subset \mathrm{End}(E_{chl})$ at random of norm $2^r - q$.
- Translate $I_{com} \cdot I_{rsp} \cdot I'_{aux}$ into $\varphi'_{aux} \circ \varphi_{rsp} \circ \varphi_{com}$.

✓ Starting from E_0.

Signature: Could be

$$(E_{com}, E'_{aux}, \varphi'_{aux} \circ \varphi_{rsp}(E_{com}[2^r])).$$

Response/signature - commitment recoverability



Response/signature:

- Compute the $(2^r, 2^r)$-isogeny:

$$\Phi : E_{com} \times E'_{aux} \longrightarrow E_{chl} \times E_{aux}$$

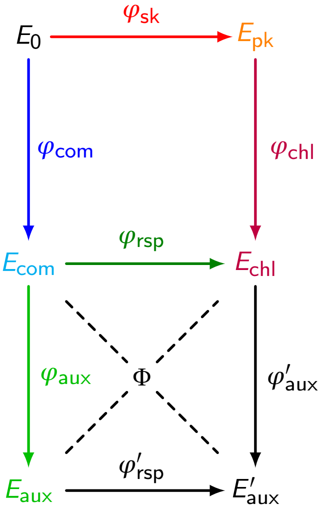
  from $\varphi'_{aux} \circ \varphi_{rsp}(E_{com}[2^r])$.

- Evaluate Φ to compute $\varphi_{aux} \circ \widehat{\varphi}_{rsp}(E_{chl}[2^r])$.

Signature:

$$(E_{aux}, \varphi_{aux} \circ \widehat{\varphi}_{rsp}(E_{chl}[2^r])).$$

Verification



Verification:

- Compute the $(2^r, 2^r)$-isogeny:

$$\widehat{\Phi} : E_{chl} \times E_{aux} \longrightarrow E_{com} \times E'_{aux}$$

  from $\varphi_{aux} \circ \widehat{\varphi}_{rsp}(E_{chl}[2^r])$.
- Check its codomain is $E_{com} \times \_$.

Improvements in performance and security

Dramatic improvement of time performance

Table: Comparison of time performance in 10^6 CPU cycles of SQIsign-v1 (NIST round 1), SQIsign-v2 (NIST round 2) and the Qlapoti version of SQIsign on an AMD Ryzen 7040 Series.

		NIST I	NIST III	NIST V
SQIsign-v1	Key Gen.	2 805	18 068	72 183
	Signature	4 090	32 514	129 899
	Verification	100.9	542.7	1 698
SQIsign-v2	Key Gen.	121.5	303.9	530.2
	Signature	266.7	602.5	1355.7
	Verification	19.9	26.7	53.7
SQIsign Qlapoti	Key Gen.	77.0	266.3	389.0
	Signature	179.6	510.6	630.97
	Verification	19.9	26.7	53.7

Compactness slightly improved

Table: Comparison of key and signature sizes in bytes of SQIsign-v1 (NIST round 1) and SQIsign-v2 (NIST round 2).

		NIST I	NIST III	NIST V
SQIsign-v1	Pub. key	64	96	128
	Priv. key	782	1138	1509
	Signature	177	263	335
SQIsign-v2	Pub. key	65	97	129
	Priv. key	353	529	701
	Signature	148	224	292

Security of a Fiat-Shamir signature

Theorem (Fiat-Shamir, 1986)

Let ID be an identification protocol that is:

- ***Complete:*** *a honest execution is always accepted by the verifier.*
- ***Sound:*** *an attacker cannot "guess" a response.*
- ***Zero-knowledge:*** *the response does not leak any information on the secret key.*

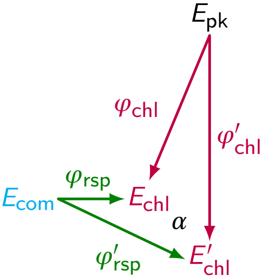
Then the Fiat-Shamir transform of ID is a universally unforgeable signature under chosen message attacks in the random oracle model.

Special soundness

Theorem (Special soundness)

From two transcripts $(E_{com}, \varphi_{chl}, \varphi_{rsp})$ $(E_{com}, \varphi'_{chl}, \varphi'_{rsp})$ with the same commitment E_{com} but different challenges $\varphi_{rsp} \neq \varphi'_{rsp}$ one can extract $\alpha \in \mathrm{End}(E_{\mathrm{pk}}) \setminus \mathbb{Z}$ in polynomial time.

Sketch of proof: Consider $\alpha := \widehat{\varphi}'_{\mathrm{chl}} \circ \varphi'_{\mathrm{rsp}} \circ \widehat{\varphi}_{\mathrm{rsp}} \circ \varphi_{\mathrm{chl}}$.



Special soundness: finding an endomorphism is hard

Problem (One Endomorphism Problem)

Given a supersingular elliptic curve E, compute $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$.

Problem (Endomorphism Ring Problem)

Given a supersingular elliptic curve E, compute $\mathrm{End}(E)$.

Special soundness: finding an endomorphism is hard

Problem (One Endomorphism Problem)

Given a supersingular elliptic curve E, compute $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$.

Problem (Endomorphism Ring Problem)

Given a supersingular elliptic curve E, compute $\mathrm{End}(E)$.

Theorem (Wesolowski, 2022)

The Endomorphism Ring Problem and the Supersingular Isogeny Problem are equivalent.

The zero knowledge property

Definition (Honest Verifier Zero Knowledge - HVZK)

There exists a polynomial time simulator $\mathscr{S}$ that produces random transcripts $(\mathrm{com}', \mathrm{chl}', \mathrm{rsp}')$ which are statistically indistinguishable from honest transcripts $(\mathrm{com}, \mathrm{chl}, \mathrm{rsp})$.

Sketch of proof:

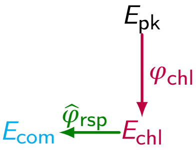
- Challenge $\varphi_{\mathrm{chl}} : E_{\mathrm{pk}} \to E_{\mathrm{chl}}$ generated as in SQIsign.

The zero knowledge property

Definition (Honest Verifier Zero Knowledge - HVZK)

There exists a polynomial time simulator $\mathscr{S}$ that produces random transcripts $(\mathrm{com}', \mathrm{chl}', \mathrm{rsp}')$ which are statistically indistinguishable from honest transcripts $(\mathrm{com}, \mathrm{chl}, \mathrm{rsp})$.

Sketch of proof:



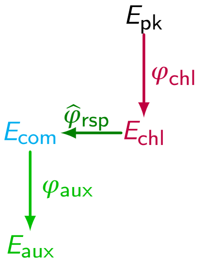
- Challenge $\varphi_{\mathrm{chl}} : E_{\mathrm{pk}} \to E_{\mathrm{chl}}$ generated as in SQIsign.
- ⚠ Needs an oracle that returns $\widehat{\varphi}_{\mathrm{rsp}} : E_{\mathrm{chl}} \to E_{\mathrm{com}}$ of degree $< 2^r$.

The zero knowledge property

Definition (Honest Verifier Zero Knowledge - HVZK)

There exists a polynomial time simulator $\mathscr{S}$ that produces random transcripts $(\mathrm{com}', \mathrm{chl}', \mathrm{rsp}')$ which are statistically indistinguishable from honest transcripts $(\mathrm{com}, \mathrm{chl}, \mathrm{rsp})$.

Sketch of proof:



- Challenge $\varphi_{chl} : E_{pk} \to E_{chl}$ generated as in SQIsign.
- ⚠ Needs an oracle that returns $\widehat{\varphi}_{rsp} : E_{chl} \to E_{com}$ of degree $< 2^r$.
- ⚠ Needs an oracle that returns $\widehat{\varphi}_{aux} : E_{com} \to E_{aux}$ of degree $2^r - \deg(\widehat{\varphi}_{rsp})$.

Special soundness is still hard with hints

Problem (One Endomorphism Problem with Hints)

Given a supersingular elliptic curve E, compute $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$ with access to "hints" .

Problem (Endomorphism Ring Problem with Hints)

Given a supersingular elliptic curve E, compute $\mathrm{End}(E)$ with access to "hints".

Special soundness is still hard with hints

Problem (One Endomorphism Problem with Hints)

Given a supersingular elliptic curve E, compute $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$ with access to "hints" .

Problem (Endomorphism Ring Problem with Hints)

Given a supersingular elliptic curve E, compute $\mathrm{End}(E)$ with access to "hints".

Theorem ([ABDFPW25])

The Endomorphism Ring Problem with Hints and the Supersingular Isogeny Problem with Hints are equivalent.

Improvements of SQIsign security assumptions

	SQIsign	SQIsignHD	SQIsign2D
Soundness	The Endomorphism Ring Problem (strong)		
Zero knowledge	• Heuristic on the distribution of φ_{rsp}.	• An oracle returning "random" isogenies. • Heuristic on the distribution of E_{com} (uniform).	• 2 oracles returning "random" isogenies.

Cutting failure rates in the signature

- In SQIsign2D-West, the ideal to isogeny translation in the response phase could fail with a significant probability.
- This was due to the tightness of the norm equation:

$$u\,\mathrm{nrd}(I_1) + v\,\mathrm{nrd}(I_2) = 2^e \quad (u, v > 0,\ I_1, I_2 \sim I).$$

Cutting failure rates in the signature

- In SQIsign2D-West, the ideal to isogeny translation in the response phase could fail with a significant probability.
- This was due to the tightness of the norm equation:

$$u\,\mathrm{nrd}(I_1) + v\,\mathrm{nrd}(I_2) = 2^e \quad (u, v > 0,\ I_1, I_2 \sim I).$$

- The failure rate is cryptographically negligible when we solve the following equation instead:

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

Cutting failure rates in the signature

- In SQIsign2D-West, the ideal to isogeny translation in the response phase could fail with a significant probability.
- This was due to the tightness of the norm equation:

$$u\,\mathrm{nrd}(I_1) + v\,\mathrm{nrd}(I_2) = 2^e \quad (u, v > 0,\ I_1, I_2 \sim I).$$

- The failure rate is cryptographically negligible when we solve the following equation instead:

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

Table: Comparison of failure rates in ideal-to-isogeny translation.

	NIST I	NIST III	NIST V
SQIsign-v2	2^{-65}	2^{-61}	2^{-60}
SQIsign Qlapoti	2^{-197}	2^{-312}	2^{-438}

Open implementation problems

What makes Qlapoti non constant time

Solving the equation:

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

is highly non-constant time.

What makes Qlapoti non constant time

Solving the equation:

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

is highly non-constant time.

Some algorithmic features hard to implement in constant time:

What makes Qlapoti non constant time

Solving the equation:

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

is highly non-constant time.

Some algorithmic features hard to implement in constant time:

- Unknown number of iterations.

What makes Qlapoti non constant time

Solving the equation:

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

is highly non-constant time.

Some algorithmic features hard to implement in constant time:

- Unknown number of iterations.
- Finding a short vector in dimension 4.

What makes Qlapoti non constant time

Solving the equation:

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

is highly non-constant time.

Some algorithmic features hard to implement in constant time:

- Unknown number of iterations.
- Finding a short vector in dimension 4.
- Solving a closest vector problem (CVP) in dimension 2.

What makes Qlapoti non constant time

Solving the equation:

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

is highly non-constant time.

Some algorithmic features hard to implement in constant time:

- Unknown number of iterations.
- Finding a short vector in dimension 4.
- Solving a closest vector problem (CVP) in dimension 2.
- Cornacchia's algorithm to solve $x^2 + y^2 = n$ for $n \in \mathbb{N}$ fixed and $x, y \in \mathbb{Z}$ unknown.

Qlapoti: the lucky case

- **Recall:** To translate a left $\mathcal{O}_0$-ideal I into an isogeny $\varphi_I : E_0 \to E_I$, we compute a 2-dimensional 2^e-isogeny:

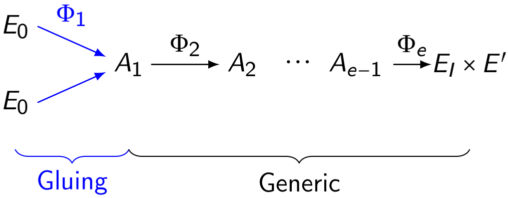
$$\Phi : E_0^2 \longrightarrow E_I \times E'.$$

Qlapoti: the lucky case

- **Recall:** To translate a left $\mathcal{O}_0$-ideal I into an isogeny $\varphi_I : E_0 \to E_I$, we compute a 2-dimensional 2^e-isogeny:

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

- **Lucky case:** the first isogeny is a *gluing* and the others are generic.



Qlapoti: the unlucky case

- **Recall:** To translate a left $\mathcal{O}_0$-ideal I into an isogeny $\varphi_I : E_0 \to E_I$, we compute a 2-dimensional 2^e-isogeny:

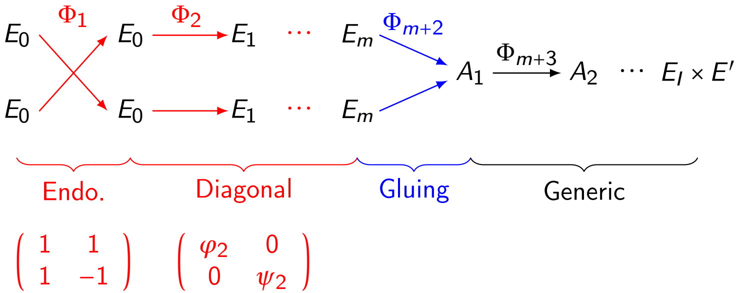
$$\Phi : E_0^2 \longrightarrow E_I \times E'.$$

Qlapoti: the unlucky case

- **Recall:** To translate a left $\mathcal{O}_0$-ideal I into an isogeny $\varphi_I : E_0 \to E_I$, we compute a 2-dimensional 2^e-isogeny:

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

- **Unlucky case:** the gluing follows a an endomorphism and m diagonal isogenies (where m can vary). Not constant time !



Qlapoti: solutions?

A list of imperfect non-exclusive solutions:

Qlapoti: solutions?

A list of imperfect non-exclusive solutions:

- Reject solutions to the norm equation that produce unlucky cases.
  ✗ Makes the norm equation slower to solve.

Qlapoti: solutions?

A list of imperfect non-exclusive solutions:

- Reject solutions to the norm equation that produce unlucky cases.
  ✗ Makes the norm equation slower to solve.
- Change E_0 to reduce the probability of unlucky cases.
  ✗ Makes the norm equation slower to solve.

Qlapoti: solutions?

A list of imperfect non-exclusive solutions:

- Reject solutions to the norm equation that produce unlucky cases.
  ✗ Makes the norm equation slower to solve.
- Change E_0 to reduce the probability of unlucky cases.
  ✗ Makes the norm equation slower to solve.
- Change the input ideal distribution.
  ✗ Non trivial to do.

Qlapoti: solutions?

A list of imperfect non-exclusive solutions:

- Reject solutions to the norm equation that produce unlucky cases.
  ✗ Makes the norm equation slower to solve.
- Change E_0 to reduce the probability of unlucky cases.
  ✗ Makes the norm equation slower to solve.
- Change the input ideal distribution.
  ✗ Non trivial to do.
- Uniformize the generic and non-generic isogeny formulae.
  ✗ Non trivial to do.

Thanks for listening!

- The use of higher dimensional isogenies greatly improved SQIsign.
- Optimising integer arithmetic is becoming more and more important.
- It is still an algorithmically non-trivial research challenge to implement SQIsign in constant time.

My works can be found on my webpage:

https://www.pierrickdartois.fr/homepage/