Improvements of SQIsign: faster and safer isogeny signatures

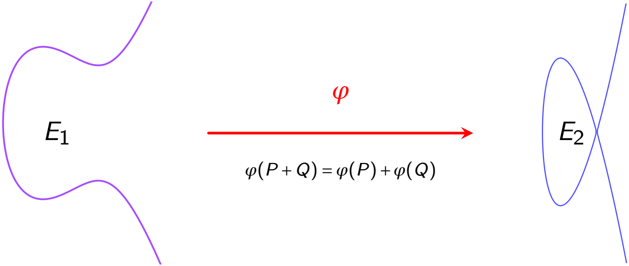
Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert and Benjamin Wesolowski

2025, February 13

What you need to know about isogenies

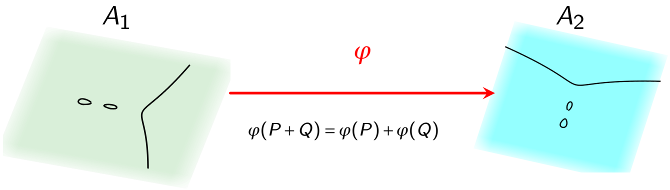
Isogenies between elliptic curves

Between elliptic curves, isogenies are non-zero morphisms of algebraic groups.



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

The degree

- An isogeny $\varphi : E_1 \longrightarrow E_2$ can be described by rational fractions:

$$\varphi(x,y) = \left(\frac{f(x)}{g(x)}, y\frac{p(x)}{q(x)}\right).$$

The degree

- An isogeny $\varphi : E_1 \longrightarrow E_2$ can be described by rational fractions:

$$\varphi(x,y) = \left(\frac{f(x)}{g(x)}, y\frac{p(x)}{q(x)}\right).$$

- The degree measures the "size" of an isogeny:

$$\deg(\varphi) = \max(\deg(f(x)), \deg(g(x))).$$

- If $\deg(\varphi) = n$, we say that φ is an n-isogeny.

The degree

- An isogeny $\varphi : E_1 \longrightarrow E_2$ can be described by rational fractions:

$$\varphi(x,y) = \left(\frac{f(x)}{g(x)}, y\frac{p(x)}{q(x)}\right).$$

- The degree measures the "size" of an isogeny:

$$\deg(\varphi) = \max(\deg(f(x)), \deg(g(x))).$$

- If $\deg(\varphi) = n$, we say that φ is an n-isogeny.
- The degree is multiplicative: $\deg(\varphi \circ \psi) = \deg(\varphi)\deg(\psi)$.

The degree

- An isogeny $\varphi : E_1 \longrightarrow E_2$ can be described by rational fractions:

$$\varphi(x,y) = \left(\frac{f(x)}{g(x)}, y\frac{p(x)}{q(x)}\right).$$

- The degree measures the "size" of an isogeny:

$$\deg(\varphi) = \max(\deg(f(x)), \deg(g(x))).$$

- If $\deg(\varphi) = n$, we say that φ is an n-isogeny.
- The degree is multiplicative: $\deg(\varphi \circ \psi) = \deg(\varphi)\deg(\psi)$.
- Most isogenies are separable: they satisfy $\deg(\varphi) = \#\ker(\varphi)$.

The degree

- An isogeny $\varphi : E_1 \longrightarrow E_2$ can be described by rational fractions:

$$\varphi(x,y) = \left(\frac{f(x)}{g(x)}, y\frac{p(x)}{q(x)}\right).$$

- The degree measures the "size" of an isogeny:

$$\deg(\varphi) = \max(\deg(f(x)), \deg(g(x))).$$

- If $\deg(\varphi) = n$, we say that φ is an n-isogeny.
- The degree is multiplicative: $\deg(\varphi \circ \psi) = \deg(\varphi)\deg(\psi)$.
- Most isogenies are separable: they satisfy $\deg(\varphi) = \#\ker(\varphi)$.
- The dual isogeny $\widehat{\varphi} : E_2 \longrightarrow E_1$ satisfies $\widehat{\varphi} \circ \varphi = [\deg(\varphi)]_{E_1}$ and $\deg(\varphi) = \deg(\widehat{\varphi})$.

Examples

- The scalar multiplication $[n] : E \longrightarrow E$ is an isogeny of **degree** n^2.
- The Frobenius:

$$\begin{array}{rcl} \pi_q : E & \longrightarrow & E \\ (x,y) & \longmapsto & (x^q, y^q) \end{array}$$

with $E/\mathbb{F}_q$ is an **inseparable isogeny of degree** q.

Examples

- The scalar multiplication $[n] : E \longrightarrow E$ is an isogeny of **degree** n^2.
- The Frobenius:

$$\begin{array}{rcl} \pi_q : E & \longrightarrow & E \\ (x,y) & \longmapsto & (x^q, y^q) \end{array}$$

  with $E/\mathbb{F}_q$ is an **inseparable isogeny of degree** q.
- Consider

$$E_1 : y^2 = x^3 + x + 4 \quad \text{and} \quad E_2 : y^2 = x^3 - x + 4$$

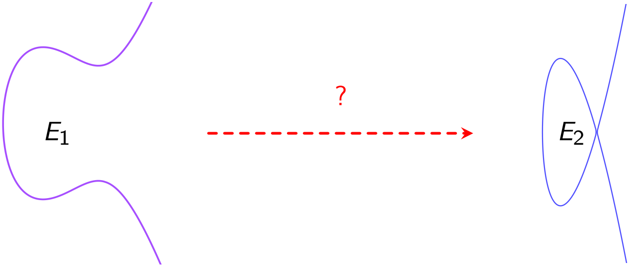
  over $\mathbb{F}_7$. Then

$$\begin{array}{rcl} \varphi : E_1 & \longrightarrow & E_2 \\ (x,y) & \longmapsto & \left(\dfrac{x^2 - 2x - 1}{x - 2}, y \dfrac{x^2 + 3x - 2}{(x-2)^2} \right) \end{array}$$

  is a **separable** 2-**isogeny**.

Why are isogenies interesting in cryptography?

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



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

What does it mean to "compute" an isogeny?

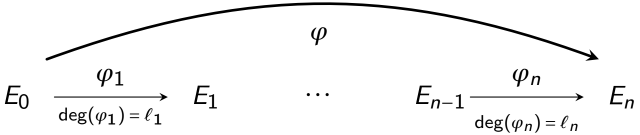
Definition (Efficient representation)

Let $\varphi : E \longrightarrow E'$ be a d-isogeny over $\mathbb{F}_q$. An efficient representation of φ with respect to an algorithm $\mathscr{A}$ is some data $D_\varphi \in \{0,1\}^*$ of size $\text{poly}(\log(d), \log(q))$ s.t. on input $P \in E(\mathbb{F}_{q^k})$ and D_φ, $\mathscr{A}$ returns $\varphi(P)$ in time $\text{poly}(\log(d), k\log(q))$.

What does it mean to "compute" an isogeny?

Examples of efficient representations:

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



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

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.*

The advantages of supersingular elliptic curves

- A strong security reduction.

Theorem (Wesolowski, 2022)

The problem of computing the endomorphism ring of any supersingular elliptic curve is equivalent to the isogeny problem between supersingular elliptic curves.

The advantages of supersingular elliptic curves

- A strong security reduction.

Theorem (Wesolowski, 2022)

The problem of computing the endomorphism ring of any supersingular elliptic curve is equivalent to the isogeny problem between supersingular elliptic curves.

- If E is supersingular, then it can be defined over $\mathbb{F}_{p^2}$.
- For isogeny computations, we control the the accessible torsion subgroups $E[T] \subseteq E(\mathbb{F}_{p^2})$ by controlling p.

The Deuring correspondence

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:** $I \sim J \Longleftrightarrow \exists \alpha \in \mathscr{B}_{p,\infty}^*, \quad J = I\alpha$.

The Deuring correspondence

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

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	$\mathscr{O} \cong \mathrm{End}(E)$ maximal order in $\mathscr{B}_{p,\infty}$
$\varphi : E \longrightarrow E'$	left $\mathscr{O}$-ideal and right $\mathscr{O}'$-ideal I_φ
$\varphi, \psi : E \longrightarrow E'$	$I_\varphi \sim I_\psi$ $(I_\psi = I_\varphi \alpha,\ \alpha \in \mathscr{B}_{p,\infty})$
$\widehat{\varphi}$	$\overline{I_\varphi}$

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 $\mathscr{B}_{p,\infty}$
$\varphi : E \longrightarrow E'$	left $\mathcal{O}$-ideal and right $\mathcal{O}'$-ideal I_φ
$\varphi, \psi : E \longrightarrow E'$	$I_\varphi \sim I_\psi \ (I_\psi = I_\varphi \alpha,\ \alpha \in \mathscr{B}_{p,\infty})$
$\widehat{\varphi}$	$\overline{I_\varphi}$
$\varphi \circ \psi$	$I_\psi \cdot I_\varphi$
$\deg(\varphi)$	$\mathrm{nrd}(I_\varphi)$

Computing isogenies via the Deuring correspondence

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

Computing isogenies via the Deuring correspondence

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

General method:

- 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).
- Translate I into an isogeny $\varphi_I : E_1 \longrightarrow E_2$.

Computing isogenies via the Deuring correspondence

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

General method:

- 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).
- Translate I into an isogeny $\varphi_I : E_1 \longrightarrow E_2$.

✓ Takes polynomial time.

Computing isogenies via the Deuring correspondence

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

General method:

- 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).
- Translate I into an isogeny $\varphi_I : E_1 \longrightarrow E_2$.

✓ Takes polynomial time.

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

Computing isogenies via the Deuring correspondence

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

General method:

- 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).
- Translate I into an isogeny $\varphi_I : E_1 \longrightarrow E_2$.

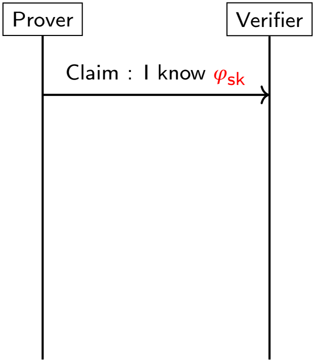
✓ Takes polynomial time.

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

Problem: How to make the last step efficient?

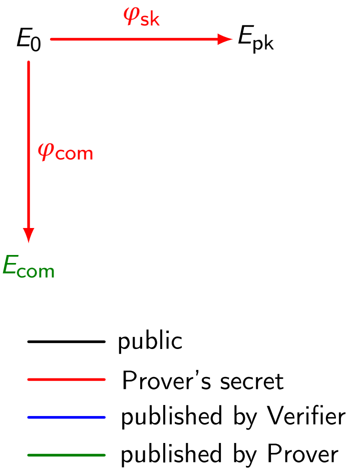
Overview of SQIsign

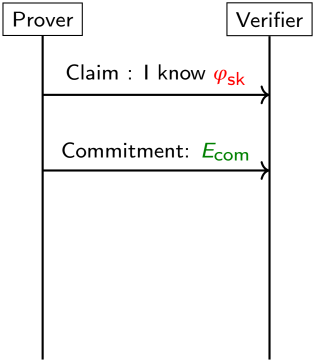
The SQIsign identification scheme



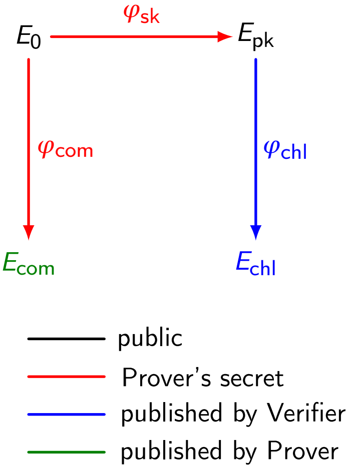
- public
- Prover's secret
- published by Verifier
- published by Prover

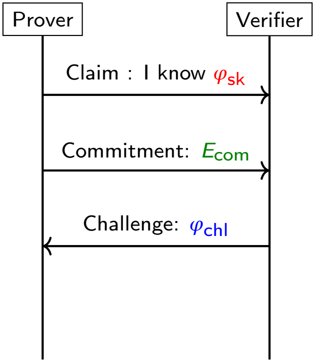
The SQIsign identification scheme



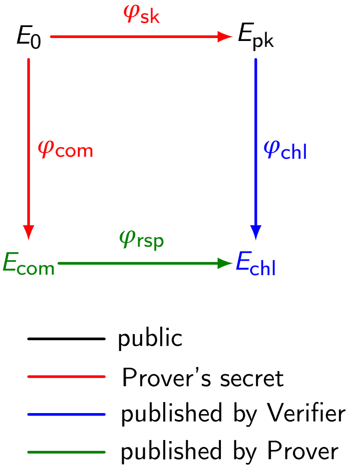


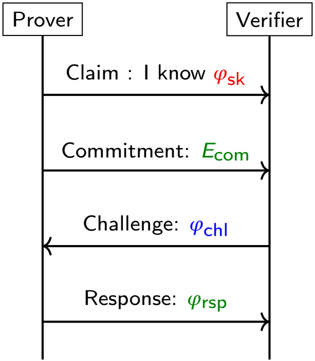
The SQIsign identification scheme



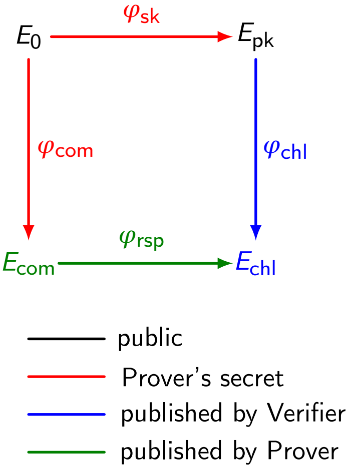


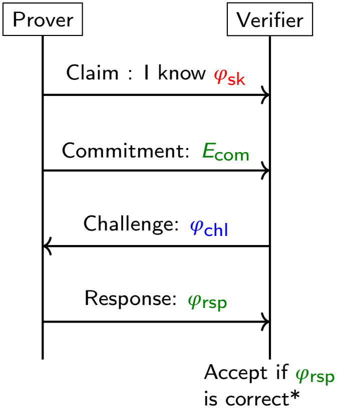
The SQIsign identification scheme





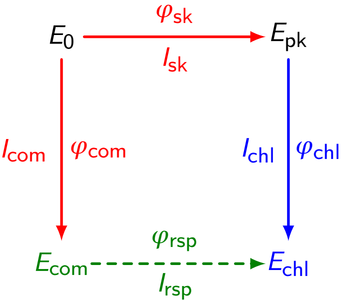
The SQIsign identification scheme





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

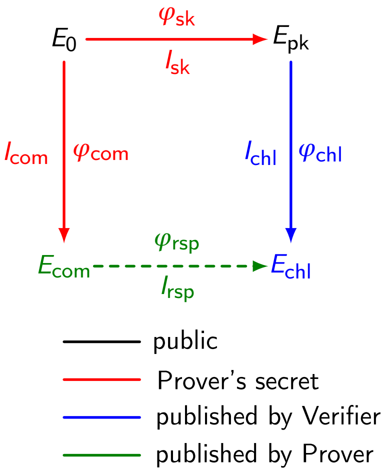
Computing the response/signature



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

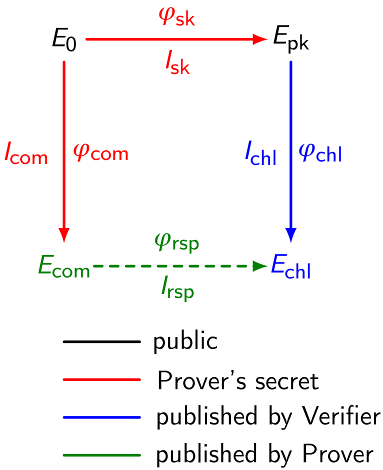
- $\varphi_{rsp} = \varphi_{chl} \circ \varphi_{sk} \circ \widehat{\varphi}_{com}$ would neither be valid nor secure.
- Instead, use the Deuring correspondence.

Computing the response/signature



- $\varphi_{rsp} = \varphi_{chl} \circ \varphi_{sk} \circ \widehat{\varphi}_{com}$ would neither be valid nor secure.
- Instead, use the Deuring correspondence.
- Find $I_{rsp} \sim \overline{I}_{com} \cdot I_{sk} \cdot I_{chl}$ random and of smooth norm via [KLPT14].
- Translate I_{rsp} into φ_{rsp}.

Computing the response/signature



- $\varphi_{rsp} = \varphi_{chl} \circ \varphi_{sk} \circ \widehat{\varphi}_{com}$ would neither be valid nor secure.
- Instead, use the Deuring correspondence.
- Find $I_{rsp} \sim \overline{I}_{com} \cdot I_{sk} \cdot I_{chl}$ random and of smooth norm via [KLPT14].
- Translate I_{rsp} into φ_{rsp}.

✗ Slow in practice because of the orange steps.

The direct method [GPS20]

Input: $E/\mathbb{F}_{p^2}$ supersingular, $\mathcal{O} \cong \mathrm{End}(E)$ and J a left $\mathcal{O}$-ideal of smooth norm.

Output: $\varphi_J : E \longrightarrow E_J$.

The direct method [GPS20]

Input: $E/\mathbb{F}_{p^2}$ supersingular, $\mathcal{O} \cong \mathrm{End}(E)$ and J a left $\mathcal{O}$-ideal of smooth norm.

Output: $\varphi_J : E \longrightarrow E_J$.

- Compute

$$\ker(\varphi_J) := \{P \in E \mid \forall \alpha \in J, \quad \alpha(P) = 0\}.$$

The direct method [GPS20]

Input: $E/\mathbb{F}_{p^2}$ supersingular, $\mathcal{O} \cong \mathrm{End}(E)$ and J a left $\mathcal{O}$-ideal of smooth norm.

Output: $\varphi_J : E \longrightarrow E_J$.

- Compute
$$\ker(\varphi_J) := \{P \in E \mid \forall \alpha \in J, \quad \alpha(P) = 0\}.$$
- Then φ_J can be computed in $O(\mathrm{polylog}\,\mathrm{nrd}(J))$ operations over the field of definition $\mathbb{F}_{p^k}$ of $\ker(\varphi_J)$.

The direct method [GPS20]

Input: $E/\mathbb{F}_{p^2}$ supersingular, $\mathcal{O} \cong \mathrm{End}(E)$ and J a left $\mathcal{O}$-ideal of smooth norm.

Output: $\varphi_J : E \longrightarrow E_J$.

- Compute
$$\ker(\varphi_J) := \{P \in E \mid \forall \alpha \in J, \quad \alpha(P) = 0\}.$$
- Then φ_J can be computed in $O(\mathrm{polylog}\,\mathrm{nrd}(J))$ operations over the field of definition $\mathbb{F}_{p^k}$ of $\ker(\varphi_J)$.

⚠ **Issue:** If J is a KLPT output, then $\mathrm{nrd}(J) \simeq p^{15/4} \gg p$ so the extension degree k is exponentially big. Not practical for SQISign !

The SQIsign method [FLLW23]

Main idea: Cut the computation into smaller pieces. Write

$$J = J_0 \cdot J_1 \cdots J_{n-1} \quad \text{and} \quad \varphi_J = \varphi_{n-1} \circ \cdots \circ \varphi_1 \circ \varphi_0$$

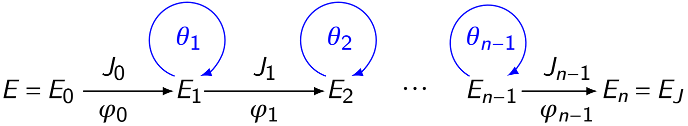
with $\mathrm{nrd}(J_0) = \cdots = \mathrm{nrd}(J_{n-1}) = 2^f$.

The SQIsign method [FLLW23]

Main idea: Cut the computation into smaller pieces. Write

$$J = J_0 \cdot J_1 \cdots J_{n-1} \quad \text{and} \quad \varphi_J = \varphi_{n-1} \circ \cdots \circ \varphi_1 \circ \varphi_0$$

with $\mathrm{nrd}(J_0) = \cdots = \mathrm{nrd}(J_{n-1}) = 2^f$.

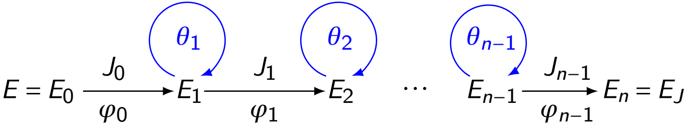


The SQIsign method [FLLW23]

Main idea: Cut the computation into smaller pieces. Write

$$J = J_0 \cdot J_1 \cdots J_{n-1} \quad \text{and} \quad \varphi_J = \varphi_{n-1} \circ \cdots \circ \varphi_1 \circ \varphi_0$$

with $\mathrm{nrd}(J_0) = \cdots = \mathrm{nrd}(J_{n-1}) = 2^f$.



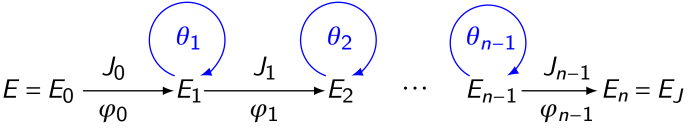
✗ This is slow in practice!

The SQIsign method [FLLW23]

Main idea: Cut the computation into smaller pieces. Write

$$J = J_0 \cdot J_1 \cdots J_{n-1} \quad \text{and} \quad \varphi_J = \varphi_{n-1} \circ \cdots \circ \varphi_1 \circ \varphi_0$$

with $\mathrm{nrd}(J_0) = \cdots = \mathrm{nrd}(J_{n-1}) = 2^f$.



✗ This is slow in practice!

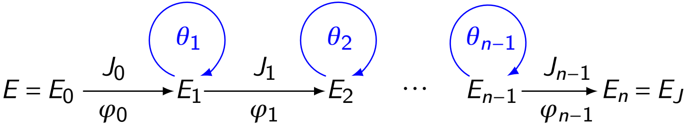
✗ Torsion requirements: $\deg(\theta_i) = T^2$ coprime with 2, so we need $E[2^f T] \subseteq E(\mathbb{F}_{p^4})$. This constrains the choice of p.

The SQIsign method [FLLW23]

Main idea: Cut the computation into smaller pieces. Write

$$J = J_0 \cdot J_1 \cdots J_{n-1} \quad \text{and} \quad \varphi_J = \varphi_{n-1} \circ \cdots \circ \varphi_1 \circ \varphi_0$$

with $\mathrm{nrd}(J_0) = \cdots = \mathrm{nrd}(J_{n-1}) = 2^f$.

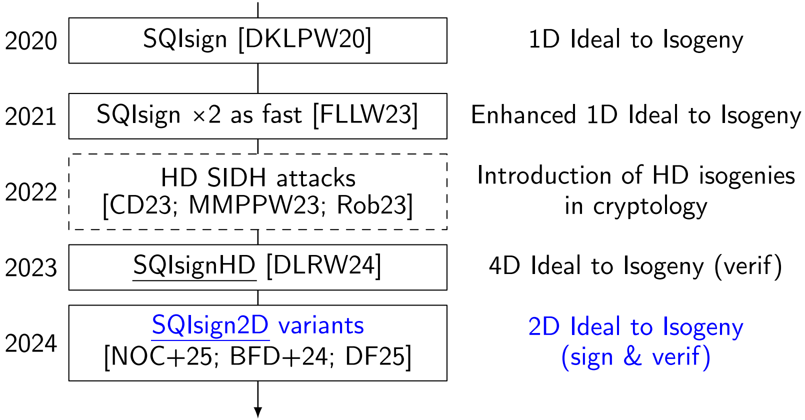


✗ This is slow in practice!

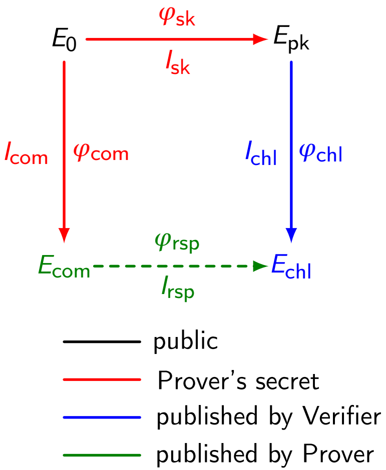
✗ Torsion requirements: $\deg(\theta_i) = T^2$ coprime with 2, so we need $E[2^f T] \subseteq E(\mathbb{F}_{p^4})$. This constrains the choice of p.

✓ Torsion requirements can be relaxed with intermediate steps θ_i in dimension 2 [ON24] but this is still not efficient enough.

A brief history of SQIsign



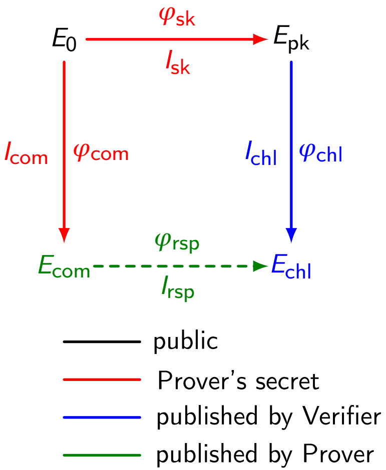
Response/signature in SQIsign



- $\varphi_{rsp} = \varphi_{chl} \circ \varphi_{sk} \circ \widehat{\varphi}_{com}$ would neither be valid nor secure.
- Instead, use the Deuring correspondence.
- Find $I_{rsp} \sim \overline{I}_{com} \cdot I_{sk} \cdot I_{chl}$ random and of smooth norm via [KLPT14].
- Translate I_{rsp} into φ_{rsp}.

✗ Slow in practice because of the orange steps.

Response/signature in SQIsignHD/2D



- $\varphi_{rsp} = \varphi_{chl} \circ \varphi_{sk} \circ \widehat{\varphi}_{com}$ would neither be valid nor secure.
- Instead, use the Deuring correspondence.
- Find $I_{rsp} \sim \overline{I}_{com} \cdot I_{sk} \cdot I_{chl}$ random and of ~~smooth norm via [KLPT14]~~ small norm $\simeq \sqrt{p}$.
- Translate I_{rsp} into φ_{rsp}.

✓ Faster in practice with dimension 2 (or 4) isogenies.

New techniques for ideal to isogeny translations

Kani's lemma (dimension 2) [Kan97]

Consider the following commutative diagram:

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

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:

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

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.

Exploiting an easy instance of the endomorphism ring problem [NO23]

Let $E_0 : y^2 = x^3 + x$ defined over $\mathbb{F}_p$ (with $2^e | p+1$ so that $E[2^e] \subseteq E(\mathbb{F}_{p^2})$).

Goal: Given $u < 2^e$ odd, compute $\varphi : E_0 \longrightarrow E$ of degree u.

Exploiting an easy instance of the endomorphism ring problem [NO23]

Let $E_0 : y^2 = x^3 + x$ defined over $\mathbb{F}_p$ (with $2^e | p+1$ so that $E[2^e] \subseteq E(\mathbb{F}_{p^2})$).

Goal: Given $u < 2^e$ odd, compute $\varphi : E_0 \longrightarrow E$ of degree u.

Idea: Exploit our knowledge of $\mathrm{End}(E_0)$:

$$\mathrm{End}(E_0) = \mathbb{Z} \oplus \mathbb{Z}\iota \oplus \mathbb{Z}\frac{\iota + \pi_p}{2} \oplus \mathbb{Z}\frac{1 + \iota \circ \pi_p}{2},$$

where:

- $\iota : (x, y) \longmapsto (-x, \sqrt{-1}y)$ (corresponds to $i \in \mathscr{B}_{p,\infty}$, $i^2 = -1$);
- $\pi_p : (x, y) \longmapsto (x^p, y^p)$ is the p-th Frobenius endomorphism (corresponds to $j \in \mathscr{B}_{p,\infty}$, $j^2 = -p$).

Applying Kani's lemma [NO23]

Goal: Given $u < 2^e$ odd, compute $\varphi : E_0 \longrightarrow E$ of degree u.

- Compute a solution (x, y, z, t) to:

$$x^2 + y^2 + p(z^2 + t^2) = u(2^e - u).$$

Applying Kani's lemma [NO23]

Goal: Given $u < 2^e$ odd, compute $\varphi : E_0 \longrightarrow E$ of degree u.

- Compute a solution (x, y, z, t) to:

$$x^2 + y^2 + p(z^2 + t^2) = u(2^e - u).$$

- Consider the endomorphism of degree $u(2^e - u)$:

$$\theta := x + y\iota + z\pi_p + t\iota \circ \pi_p \in \mathrm{End}(E_0).$$

Applying Kani's lemma [NO23]

Goal: Given $u < 2^e$ odd, compute $\varphi : E_0 \longrightarrow E$ of degree u.

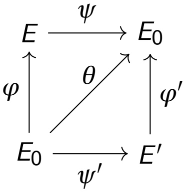
- Compute a solution (x, y, z, t) to:

$$x^2 + y^2 + p(z^2 + t^2) = u(2^e - u).$$

- Consider the endomorphism of degree $u(2^e - u)$:

$$\theta := x + y\iota + z\pi_p + t\iota \circ \pi_p \in \mathrm{End}(E_0).$$

- Consider the commutative diagram:



with $\theta = \psi \circ \varphi$, $\deg(\varphi) = u$ and $\deg(\psi) = 2^e - u$.

The solution [NO23]

Goal: Given $u < 2^e$ odd, compute $\varphi : E_0 \longrightarrow E$ of degree u.

- By Kani's lemma, we have a $(2^e, 2^e)$-isogeny

$$\Phi = \begin{pmatrix} \varphi & \widehat{\psi} \\ -\psi' & \widehat{\varphi}' \end{pmatrix} : E_0 \times E_0 \to E \times E'.$$

with kernel

$$\ker(\Phi) = \{([u]P, \theta(P)) \mid P \in E_0[2^e]\}.$$

The solution [NO23]

Goal: Given $u < 2^e$ odd, compute $\varphi : E_0 \longrightarrow E$ of degree u.

- By Kani's lemma, we have a $(2^e, 2^e)$-isogeny

$$\Phi = \begin{pmatrix} \varphi & \widehat{\psi} \\ -\psi' & \widehat{\varphi}' \end{pmatrix} : E_0 \times E_0 \to E \times E'.$$

with kernel

$$\ker(\Phi) = \{([u]P, \theta(P)) \mid P \in E_0[2^e]\}.$$

- Knowing θ, we can compute $\ker(\Phi)$ and Φ [DMPR25].

The solution [NO23]

Goal: Given $u < 2^e$ odd, compute $\varphi : E_0 \longrightarrow E$ of degree u.

- By Kani's lemma, we have a $(2^e, 2^e)$-isogeny

$$\Phi = \begin{pmatrix} \varphi & \widehat{\psi} \\ -\psi' & \widehat{\varphi}' \end{pmatrix} : E_0 \times E_0 \to E \times E'.$$

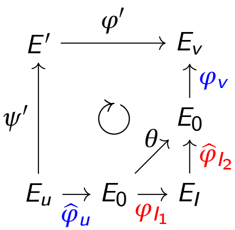
  with kernel

$$\ker(\Phi) = \{([u]P, \theta(P)) \mid P \in E_0[2^e]\}.$$

- Knowing θ, we can compute $\ker(\Phi)$ and Φ [DMPR25].
- Φ efficiently represents $\varphi : E_0 \longrightarrow E$ of degree u.

The Clapoti method (inspired from [PR23])

Goal: Translate any ideal $I \subseteq \mathrm{End}(E_0)$ into an isogeny $\varphi_I : E_0 \longrightarrow E_I$.

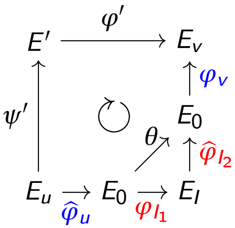


1. Find $I_1, I_2 \sim I$ and $u, v > 0$ s.t. $\gcd(u\,\mathrm{nrd}(I_1), v\,\mathrm{nrd}(I_2)) = 1$ and

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

The Clapoti method (inspired from [PR23])

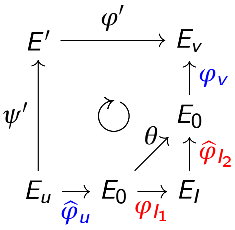
Goal: Translate any ideal $I \subseteq \mathrm{End}(E_0)$ into an isogeny $\varphi_I : E_0 \longrightarrow E_I$.



1. Find $I_1, I_2 \sim I$ and $u, v > 0$ s.t. $\gcd(u\,\mathrm{nrd}(I_1), v\,\mathrm{nrd}(I_2)) = 1$ and
$$u\,\mathrm{nrd}(I_1) + v\,\mathrm{nrd}(I_2) = 2^e.$$
2. Compute a generator $\theta \in \mathrm{End}(E_0)$ of $I_1 \overline{I_2} = \theta \cdot \mathrm{End}(E_0)$.

The Clapoti method (inspired from [PR23])

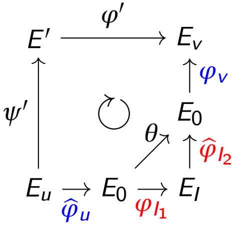
Goal: Translate any ideal $I \subseteq \mathrm{End}(E_0)$ into an isogeny $\varphi_I : E_0 \longrightarrow E_I$.



1. Find $I_1, I_2 \sim I$ and $u, v > 0$ s.t. $\gcd(u\,\mathrm{nrd}(I_1), v\,\mathrm{nrd}(I_2)) = 1$ and
$$u\,\mathrm{nrd}(I_1) + v\,\mathrm{nrd}(I_2) = 2^e.$$
2. Compute a generator $\theta \in \mathrm{End}(E_0)$ of $I_1 \overline{I_2} = \theta \cdot \mathrm{End}(E_0)$.
3. Compute isogenies $\varphi_u : E_0 \longrightarrow E_u$ and $\varphi_v : E_0 \longrightarrow E_v$ of degrees u, v.

The Clapoti method (inspired from [PR23])

Goal: Translate any ideal $I \subseteq \mathrm{End}(E_0)$ into an isogeny $\varphi_I : E_0 \longrightarrow E_I$.



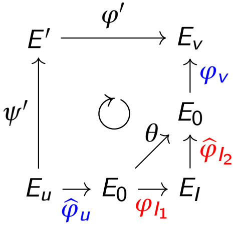
Consider the $(2^e, 2^e)$-isogeny

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

embedding $\varphi_{I_1} \circ \widehat{\varphi}_u$ and $\varphi_v \circ \widehat{\varphi}_{I_2}$.

The Clapoti method (inspired from [PR23])

Goal: Translate any ideal $I \subseteq \mathrm{End}(E_0)$ into an isogeny $\varphi_I : E_0 \longrightarrow E_I$.



Consider the $(2^e, 2^e)$-isogeny

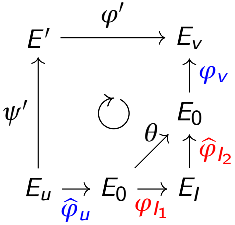
$$\Phi : E_u \times E_v \longrightarrow E_I \times E'$$

embedding $\varphi_{I_1} \circ \widehat{\varphi}_u$ and $\varphi_v \circ \widehat{\varphi}_{I_2}$.

4. Use $\theta, \varphi_u, \varphi_v$ to compute $\ker(\Phi)$ and then compute Φ.

The Clapoti method (inspired from [PR23])

Goal: Translate any ideal $I \subseteq \mathrm{End}(E_0)$ into an isogeny $\varphi_I : E_0 \longrightarrow E_I$.



Consider the $(2^e, 2^e)$-isogeny

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

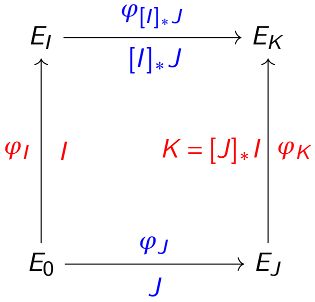
embedding $\varphi_{I_1} \circ \widehat{\varphi}_u$ and $\varphi_v \circ \widehat{\varphi}_{I_2}$.

4. Use $\theta, \varphi_u, \varphi_v$ to compute $\ker(\Phi)$ and then compute Φ.
5. Evaluating Φ we can evaluate φ_{I_1} then φ_I (by the equivalence $I \sim I_1$).

✓ Φ efficiently represents φ_I.

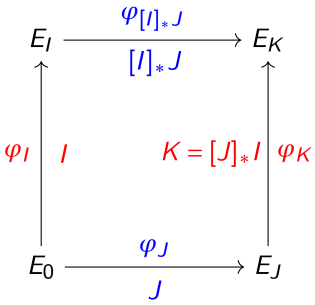
How to translate an ideal outside of $\mathrm{End}(E_0)$?

Goal: Given $\varphi_J : E_0 \longrightarrow E_J$ and $K = [J]_* I \subseteq \mathrm{End}(E_J)$, compute $\varphi_K : E_J \longrightarrow E_K$.



How to translate an ideal outside of $\mathrm{End}(E_0)$?

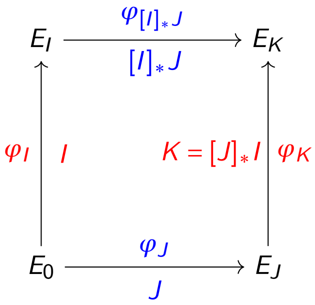
Goal: Given $\varphi_J : E_0 \longrightarrow E_J$ and $K = [J]_* I \subseteq \mathrm{End}(E_J)$, compute $\varphi_K : E_J \longrightarrow E_K$.



- Compute $L := J \cdot K \subseteq \mathrm{End}(E_0)$.
- Compute $\varphi_L = \varphi_K \circ \varphi_J : E_0 \longrightarrow E_K$.
- Given φ_L and φ_J, we obtain φ_K.

How to translate an ideal outside of $\mathrm{End}(E_0)$?

Goal: Given $\varphi_J : E_0 \longrightarrow E_J$ and $K = [J]_* I \subseteq \mathrm{End}(E_J)$, compute $\varphi_K : E_J \longrightarrow E_K$.



- Compute $L := J \cdot K \subseteq \mathrm{End}(E_0)$.
- Compute $\varphi_L = \varphi_K \circ \varphi_J : E_0 \longrightarrow E_K$.
- Given φ_L and φ_J, we obtain φ_K.

✓ Efficient representations of φ_L and φ_J yield an efficient representation of φ_K.

SQIsign2D-West: the fast, the small and the safer

A dramatic improvement of time performance

Table: Comparison of time performance in 10^6 CPU cycles of SQIsign (NIST round 1) on an Intel Xeon Gold 6338 CPU (Ice Lake) and SQIsign2D (NIST round 2) on an Intel Core i7-13700K CPU.

		NIST I	NIST III	NIST V
SQIsign	Key Gen.	2 834	21 359	84 944
	Signature	4 781	38 884	160 458
	Verification	103	687	2 051
SQIsign2D	Key Gen.	71.8	188.2	325.4
	Signature	163.1	427.0	751.8
	Verification	11.3	30.4	61.9

Compactness slightly improved

Table: Comparison of key and signature sizes in bytes of SQIsign (NIST round 1) and SQIsign2D (NIST round 2).

		NIST I	NIST III	NIST V
SQIsign	Pub. key	64	96	128
	Priv. key	782	1138	1509
	Signature	177	263	335
SQIsign2D	Pub. key	65	97	129
	Priv. key	353	529	701
	Signature	148	224	292

Fiat-Shamir transform

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.

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.

Conclusion

A bief history of SQIsign improvements

	SQIsign	SQIsignHD	SQIsign2D
Security proof	✗	✗✓	✓
Scalability	✗	✓	✓
Signing time	✗	✓✓	✓
Compactness	✓	✓	✓
Verification	✓	✗	✓✓

Thanks for listening!

You can find my paper here:

A. Basso, P. Dartois, L. De Feo, A. Leroux, L. Maino, G. Pope, D. Robert and B. Wesolowski. SQIsign2D-West: The Fast, the Small, and the Safer. Asiacrypt 2024.
https://eprint.iacr.org/2024/760

Appendix: some details

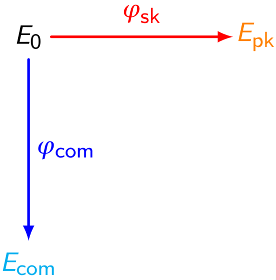
Key Generation

Public parameters: $p = c \cdot 2^e - 1$ with c small, E_0 of j-invariant 1728 and (P_0, Q_0) s.t. $E_0[2^e] = \langle P_0, Q_0 \rangle$.

Key Generation:

- Sample a left-ideal I_{sk} of $\mathcal{O}_0 \cong \mathrm{End}(E_0)$ of big fixed norm N.
- Translate I_{sk} into φ_{sk} via AnyIdealToIsogeny.
- $\mathrm{pk} = E_{pk}$.
- $\mathrm{sk} = (I_{sk}, \varphi_{sk}(P_0), \varphi_{sk}(Q_0))$.

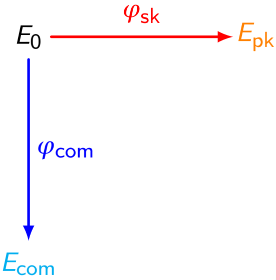
Commitment



Commitment:

- Sample a left-ideal I_{com} of $\mathcal{O}_0 \cong \mathrm{End}(E_0)$ of norm N.
- Translate I_{com} into φ_{com} via AnyIdealToIsogeny.
- $\mathrm{com} = E_{com}$.
- $\mathrm{sc} = (I_{com}, \varphi_{com}(P_0), \varphi_{com}(Q_0))$.

Commitment



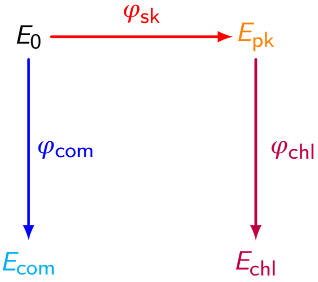
Commitment:

- Sample a left-ideal I_{com} of $\mathscr{O}_0 \cong \mathrm{End}(E_0)$ of norm N.
- Translate I_{com} into φ_{com} via AnyIdealToIsogeny.
- $\mathrm{com} = E_{com}$.
- $\mathrm{sc} = (I_{com}, \varphi_{com}(P_0), \varphi_{com}(Q_0))$.

Differences with SQIsign(HD):

- $\deg(\varphi_{sk})$ and $\deg(\varphi_{com})$ are not smooth.
- The distribution of E_{com} (and E_{pk}) is provably uniform.

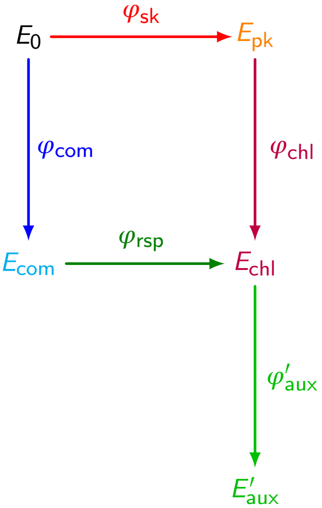
Challenge



Challenge:

- Sample $\varphi_{chl} : E_{pk} \longrightarrow E_{chl}$ of degree $2^e \simeq p$.
- In SQIsignHD, $\deg(\varphi_{chl}) \simeq \sqrt{p}$ was sufficient for the challenge space but we need $\deg(\varphi_{chl}) \simeq p$ here for security reasons.

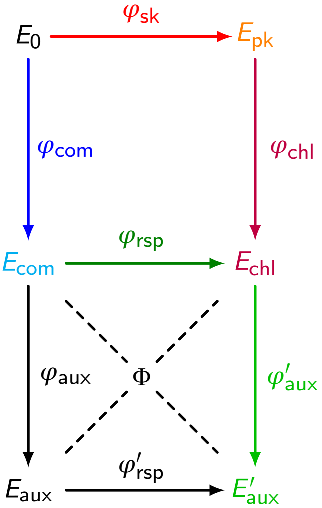
Response



Response:

- Compute $I_{chl} \subset \mathrm{End}(E_{pk})$ associated to φ_{chl} (SQIsignHD).
- $J \longleftarrow \overline{I}_{com} \cdot I_{sk} \cdot I_{chl}$.
- Compute $I_{rsp} \sim J$ random of norm $q < 2^r \simeq \sqrt{p}$.
- q can be even (suppose it is odd for clarity).
- Sample $I''_{aux} \subseteq \mathcal{O}_0$ at random of norm $2^r - q$.
- $I'_{aux} \longleftarrow [I_{com} \cdot I_{rsp}]_* I''_{aux}$.
- Apply AnyIdealToIsogeny to $I_{com} \cdot I_{rsp} \cdot I'_{aux}$ to compute E_{aux} and $\varphi'_{aux} \circ \varphi_{rsp} \circ \varphi_{com}(P_0, Q_0)$.

Response



Response:

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

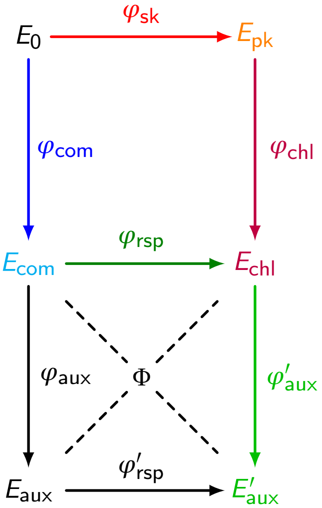
$$\Phi : E_{com} \times E'_{aux} \longrightarrow E_{chl} \times E_{aux}$$

  of kernel:

$$\langle ([q]P_0, \varphi'_{aux} \circ \varphi_{rsp} \circ \varphi_{com}(P_0)), \\ ([q]Q_0, \varphi'_{aux} \circ \varphi_{rsp} \circ \varphi_{com}(Q_0)) \rangle.$$

- Compute a deterministic basis (P_{chl}, Q_{chl}) of $E_{chl}[2^r]$.
- Evaluate Φ to obtain $(P_{aux}, Q_{aux}) = [1/(2^r - q)]\varphi_{aux} \circ \widehat{\varphi}_{rsp}(P_{chl}, Q_{chl})$.
- Return $(E_{aux}, P_{aux}, Q_{aux})$.

Verification



Verification:

- Compute a deterministic basis (P_{chl}, Q_{chl}) of $E_{chl}[2^r]$.
- Compute the $(2^r, 2^r)$-isogeny:

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

of kernel:

$$\langle (P_{chl}, P_{aux}), (Q_{chl}, Q_{aux}) \rangle.$$

- Check its codomain is $E_{com} \times \_$.

Zero Knowledge Property

Definition (Uniform Target Oracle)

A uniform target oracle (UTO) is an oracle taking as input a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ and an integer $N = \Omega(\sqrt{p})$, and outputs a random isogeny $\varphi : E \to E'$ such that:

1. The distribution of E' is uniform among all the supersingular elliptic curves.
2. The conditional distribution of φ given E' is uniform among isogenies $E \to E'$ of degree smaller or equal to N.

Definition (Fixed Degree Isogeny Oracle)

A fixed degree isogeny oracle (FIDIO) is an oracle taking as input a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ and an integer N, and outputs a uniformly random isogeny $\varphi : E \to E'$ with domain E and degree N.

Zero Knowledge Property

Theorem

The identification protocol is statistically honest-verifier zero-knowledge in the UTO and FIDIO model. In other words, there exists a polynomial time simulator $\mathscr{S}$ with access to a UTO and a FIDIO that produces random transcripts which are statistically indistinguishable from honest transcripts.

Zero Knowledge Property

Theorem

The identification protocol is statistically honest-verifier zero-knowledge in the UTO and FIDIO model. In other words, there exists a polynomial time simulator $\mathscr{S}$ with access to a UTO and a FIDIO that produces random transcripts which are statistically indistinguishable from honest transcripts.

Sketch of proof: Case when $q := \deg(\varphi_{\mathsf{rsp}})$ is odd.

Zero Knowledge Property

Theorem

The identification protocol is statistically honest-verifier zero-knowledge in the UTO and FIDIO model. In other words, there exists a polynomial time simulator $\mathscr{S}$ with access to a UTO and a FIDIO that produces random transcripts which are statistically indistinguishable from honest transcripts.

Sketch of proof: Case when $q := \deg(\varphi_{\mathrm{rsp}})$ is odd.

- Generate an isogeny $\varphi_{\mathrm{chl}} : E_{\mathrm{pk}} \to E_{\mathrm{chl}}$ according to the honest challenge distribution.

Zero Knowledge Property

Theorem

The identification protocol is statistically honest-verifier zero-knowledge in the UTO and FIDIO model. In other words, there exists a polynomial time simulator $\mathscr{S}$ with access to a UTO and a FIDIO that produces random transcripts which are statistically indistinguishable from honest transcripts.

Sketch of proof: Case when $q := \deg(\varphi_{\mathrm{rsp}})$ is odd.

- Generate an isogeny $\varphi_{\mathrm{chl}} : E_{\mathrm{pk}} \to E_{\mathrm{chl}}$ according to the honest challenge distribution.
- Call the UTO on input $(E_{\mathrm{chl}}, 2^e)$, resulting in the isogeny $\widehat{\varphi}_{\mathrm{rsp}} : E_{\mathrm{chl}} \to E_{\mathrm{com}}$.

Zero Knowledge Property

Theorem

The identification protocol is statistically honest-verifier zero-knowledge in the UTO and FIDIO model. In other words, there exists a polynomial time simulator $\mathscr{S}$ with access to a UTO and a FIDIO that produces random transcripts which are statistically indistinguishable from honest transcripts.

Sketch of proof: Case when $q := \deg(\varphi_{\mathrm{rsp}})$ is odd.

- Generate an isogeny $\varphi_{\mathrm{chl}} : E_{\mathrm{pk}} \to E_{\mathrm{chl}}$ according to the honest challenge distribution.
- Call the UTO on input $(E_{\mathrm{chl}}, 2^e)$, resulting in the isogeny $\widehat{\varphi}_{\mathrm{rsp}} : E_{\mathrm{chl}} \to E_{\mathrm{com}}$.
- Call the FIDIO on input $(E_{\mathrm{com}}, 2^e - q)$, resulting in the isogeny $\varphi_{\mathrm{aux}} : E_{\mathrm{com}} \to E_{\mathrm{aux}}$.