SQIsign2D-West: the Fast, the Small, the Safer

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

2024, June 24

The Deuring correspondence

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
$\varphi, \psi : E \longrightarrow E'$	$I_\varphi \sim I_\psi$ ($I_\psi = I_\varphi \alpha$, $\alpha \in \mathcal{B}_{p,\infty}$)
$\widehat{\varphi}$	$\overline{I_\varphi}$
$\varphi \circ \psi$	$I_\psi \cdot I_\varphi$
$\deg(\varphi)$	$\mathrm{nrd}(I_\varphi) = \sqrt{[\mathcal{O} : I_\varphi]}$

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?

Old 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).
- Compute $J \sim I$ of smooth norm via [KLPT14].
- Translate J into an isogeny $\varphi_J : E_1 \longrightarrow E_2$.

Computing isogenies via the Deuring correspondence

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

Old method:

- Let E_1 and E_2 of known endomorphism rings $\mathcal{O}_1 \cong \text{End}(E_1)$ and $\mathcal{O}_2 \cong \text{End}(E_2)$.
- Compute a connecting ideal I between $\mathcal{O}_1$ and $\mathcal{O}_2$ (left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal).
- Compute $J \sim I$ 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

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

Old 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).
- Compute $J \sim I$ 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

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

Old 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).
- Compute $J \sim I$ 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.

Computing isogenies via the Deuring correspondence

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

New 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).
- Compute $J \sim I$ ~~of smooth norm via [KLPT14].~~
- Translate J into an isogeny $\varphi_J : E_1 \longrightarrow E_2$ with higher dimension.

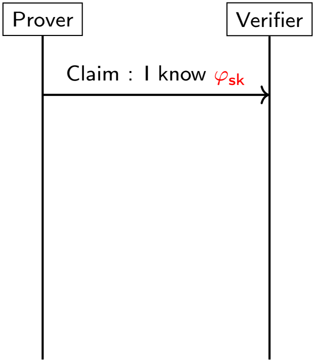
✓ Takes polynomial time.

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

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

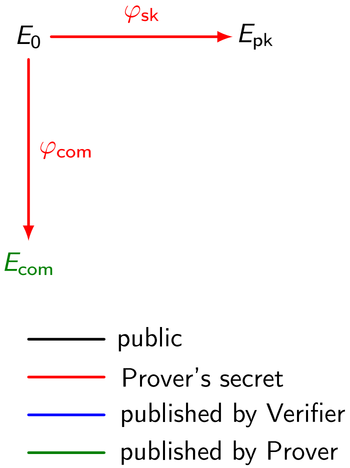
Overview of SQIsign2D

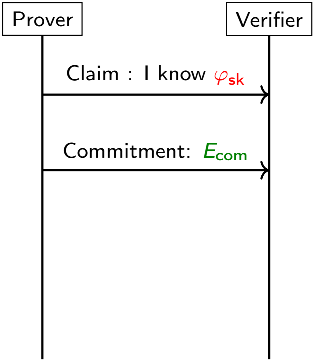
The SQIsign identification scheme



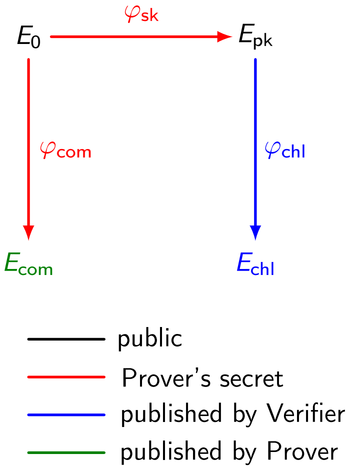
- public
- Prover's secret
- published by Verifier
- published by Prover

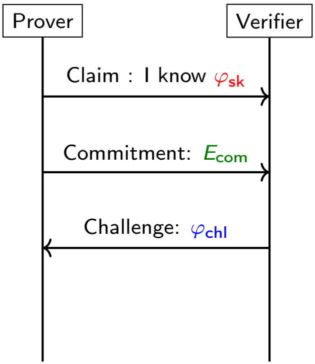
The SQIsign identification scheme



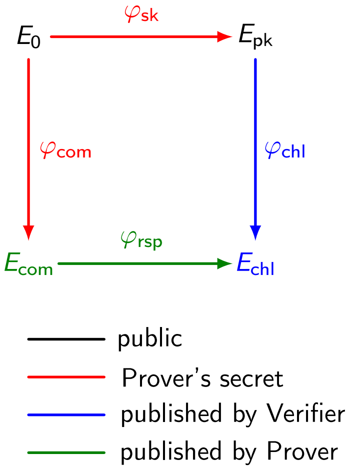


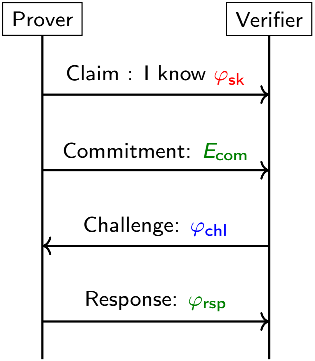
The SQIsign identification scheme



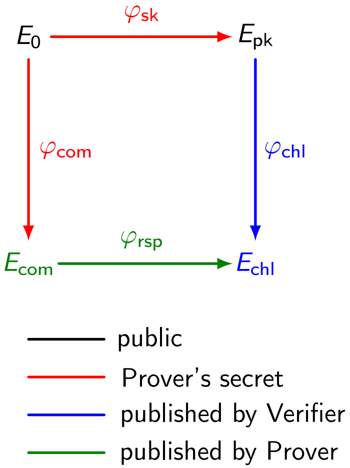


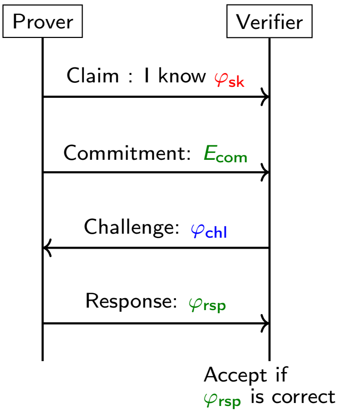
The SQIsign identification scheme





The SQIsign identification scheme





New tools

SQIsignHD used dimension 4 isogenies to represent the response and came short of doing it in dimension 2. We now have the tools to do it.

New tools we use:

- **RandIsogImages in QFESTA [NO23]:** Starting from E_0 s.t. $j(E_0) = 1728$, we can compute an isogeny $\varphi : E_0 \longrightarrow *$ of given non-smooth degree.
- **AnyIdealToIsogeny:** Starting from E_0 translate <u>any</u> ideal $I \subset \mathcal{O}_0 \cong \text{End}(E_0)$ into an isogeny $\varphi_I : E_0 \longrightarrow *$ (inspired from Clapoti/QFESTA [PR23; NO23]).
- Sampling a random uniform ideal of fixed norm in any maximal quaternion order.

Efficient representation

Definition

Let $\mathscr{A}$ be an algorithm and $\varphi : E \longrightarrow E'$ be an isogeny defined over $\mathbb{F}_q$. An efficient representation of φ (with respect to $\mathscr{A}$) is data $D \in \{0,1\}^*$ of polynomial size in $\log(\deg(\varphi))$ and $\log(q)$ such that, given D and $P \in E(\mathbb{F}_{q^k})$, $\mathscr{A}$ computes $\varphi(P)$ in polynomial time in $k\log(q)$ and $\log(\deg(\varphi))$.

Efficient representation

Definition

Let $\mathscr{A}$ be an algorithm and $\varphi : E \longrightarrow E'$ be an isogeny defined over $\mathbb{F}_q$. An efficient representation of φ (with respect to $\mathscr{A}$) is data $D \in \{0,1\}^*$ of polynomial size in $\log(\deg(\varphi))$ and $\log(q)$ such that, given D and $P \in E(\mathbb{F}_{q^k})$, $\mathscr{A}$ computes $\varphi(P)$ in polynomial time in $k\log(q)$ and $\log(\deg(\varphi))$.

Examples: When $\deg(\varphi)$ is smooth:

- $\ker(\varphi)$.
- An isogeny chain of small degrees $\varphi_1, \cdots, \varphi_e$ such that

$$\varphi = \varphi_e \circ \cdots \cdots \varphi_1.$$

Efficient representation

Definition

Let $\mathscr{A}$ be an algorithm and $\varphi : E \longrightarrow E'$ be an isogeny defined over $\mathbb{F}_q$. An efficient representation of φ (with respect to $\mathscr{A}$) is data $D \in \{0,1\}^*$ of polynomial size in $\log(\deg(\varphi))$ and $\log(q)$ such that, given D and $P \in E(\mathbb{F}_{q^k})$, $\mathscr{A}$ computes $\varphi(P)$ in polynomial time in $k\log(q)$ and $\log(\deg(\varphi))$.

Examples: When $\deg(\varphi)$ is smooth:

- $\ker(\varphi)$.
- An isogeny chain of small degrees $\varphi_1, \cdots, \varphi_e$ such that

$$\varphi = \varphi_e \circ \cdots\cdots \varphi_1.$$

And when $\deg(\varphi)$ is not smooth?

Kani's lemma (dimension 2)

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)

Consider the following commutative diagram:

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

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)

- 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)

- 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)

- 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.

Kani's lemma (dimension 2)

- 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.
- Knowing Φ, we can evaluate φ everywhere:

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

Kani's lemma (dimension 2)

- 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.
- Knowing Φ, we can evaluate φ everywhere:

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

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

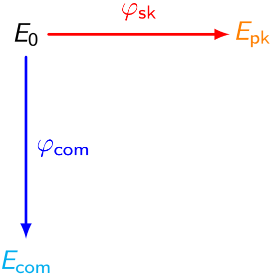
Key Generation

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.
- $\mathrm{pk} = E_{\mathrm{pk}}$.
- $\mathrm{sk} = (I_{\mathrm{sk}}, \varphi_{\mathrm{sk}}(P_0), \varphi_{\mathrm{sk}}(Q_0))$.

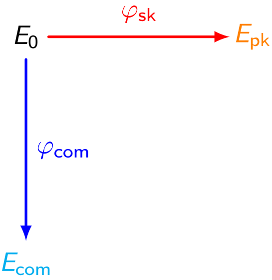
Commitment



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



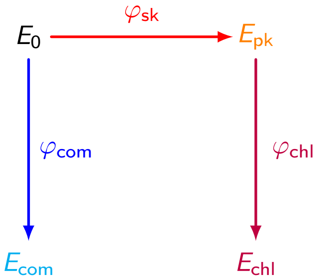
Commitment:

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

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.

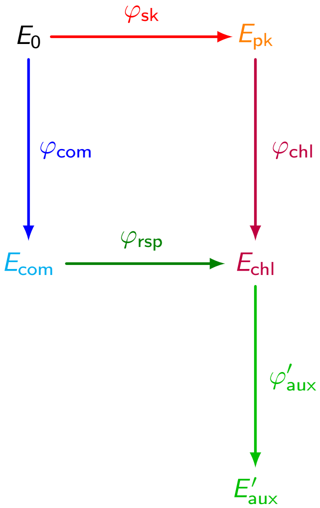
Challenge



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.

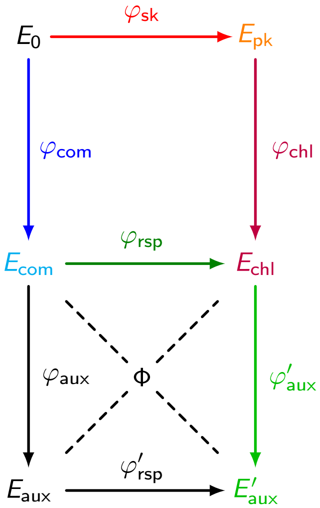
Response



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:

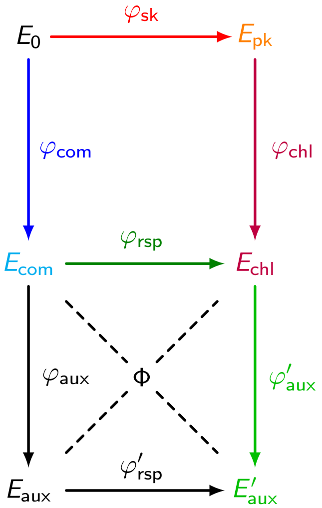
$$\Phi : E_{\text{com}} \times E'_{\text{aux}} \longrightarrow E_{\text{chl}} \times E_{\text{aux}}$$

of kernel:

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

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

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 $E_{com} \times \_$.

Translating ideals of non-smooth norm into isogenies

RandIsogImages [NO23]

Input: An odd number $u < 2^e$ and a basis (P_0, Q_0) of $E_0[2^e]$.

Output: The codomain E and the image $\varphi(P_0, Q_0)$ of an isogeny $\varphi : E_0 \longrightarrow E$ of degree u.

RandIsogImages [NO23]

Input: An odd number $u < 2^e$ and a basis (P_0, Q_0) of $E_0[2^e]$.

Output: The codomain E and the image $\varphi(P_0, Q_0)$ of an isogeny $\varphi : E_0 \longrightarrow E$ of degree u.

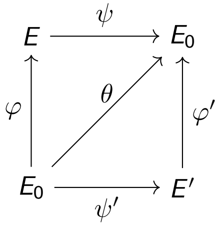
- Compute $\theta \in \mathcal{O}_0$ of norm $u(2^e - u)$.

RandIsogImages [NO23]

Input: An odd number $u < 2^e$ and a basis (P_0, Q_0) of $E_0[2^e]$.

Output: The codomain E and the image $\varphi(P_0, Q_0)$ of an isogeny $\varphi : E_0 \longrightarrow E$ of degree u.

- Compute $\theta \in \mathcal{O}_0$ of norm $u(2^e - u)$.
- Consider the commutative diagram:



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

RandIsogImages [NO23]

- Compute $\theta(P_0, Q_0)$ to obtain the kernel:

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

of

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

- Compute the $(2^e, 2^e)$-isogeny Φ with the Theta model.

RandIsogImages [NO23]

- Compute $\theta(P_0, Q_0)$ to obtain the kernel:

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

of

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

- Compute the $(2^e, 2^e)$-isogeny Φ with the Theta model.
- Compute $\Phi(P_0, 0) = (\varphi(P_0), *)$ and $\Phi(Q_0, 0) = (\varphi(Q_0), *)$.
- Return E and $\varphi(P_0, Q_0)$.

AnyIdealToIsogeny

Input: An ideal $I \subset \mathcal{O}_0$ and a basis (P_0, Q_0) of $E_0[2^e]$.

Output: The codomain E_I and the image $\varphi_I(P_0, Q_0)$ of $\varphi_I : E_0 \longrightarrow E_I$.

AnyIdealToIsogeny

Input: An ideal $I \subset \mathcal{O}_0$ and a basis (P_0, Q_0) of $E_0[2^e]$.

Output: The codomain E_I and the image $\varphi_I(P_0, Q_0)$ of $\varphi_I : E_0 \longrightarrow E_I$.

- Find ideals $I_1, I_2 \sim I$ of odd norms and $u, v \in \mathbb{N}$ odd s.t. $\gcd(u\,\mathrm{nrd}(I_1), v\,\mathrm{nrd}(I_2)) = 1$ and $u\,\mathrm{nrd}(I_1) + v\,\mathrm{nrd}(I_2) = 2^e$.

AnyIdealToIsogeny

Input: An ideal $I \subset \mathcal{O}_0$ and a basis (P_0, Q_0) of $E_0[2^e]$.

Output: The codomain E_I and the image $\varphi_I(P_0, Q_0)$ of $\varphi_I : E_0 \longrightarrow E_I$.

- Find ideals $I_1, I_2 \sim I$ of odd norms and $u, v \in \mathbb{N}$ odd s.t. $\gcd(u \operatorname{nrd}(I_1), v \operatorname{nrd}(I_2)) = 1$ and $u \operatorname{nrd}(I_1) + v \operatorname{nrd}(I_2) = 2^e$.
- Use RandIsogImages of QFESTA to obtain the images of (P_0, Q_0) via isogenies $\varphi_u : E_0 \longrightarrow E_u$ and $\varphi_v : E_0 \longrightarrow E_v$ of degrees u and v.

AnyIdealToIsogeny

Input: An ideal $I \subset \mathcal{O}_0$ and a basis (P_0, Q_0) of $E_0[2^e]$.

Output: The codomain E_I and the image $\varphi_I(P_0, Q_0)$ of $\varphi_I : E_0 \longrightarrow E_I$.

- Find ideals $I_1, I_2 \sim I$ of odd norms and $u, v \in \mathbb{N}$ odd s.t. $\gcd(u\,\mathrm{nrd}(I_1), v\,\mathrm{nrd}(I_2)) = 1$ and $u\,\mathrm{nrd}(I_1) + v\,\mathrm{nrd}(I_2) = 2^e$.
- Use RandIsogImages of QFESTA to obtain the images of (P_0, Q_0) via isogenies $\varphi_u : E_0 \longrightarrow E_u$ and $\varphi_v : E_0 \longrightarrow E_v$ of degrees u and v.
- Let $\beta_1, \beta_2 \in I$ s.t. $I_1 = I\overline{\beta_1}/\,\mathrm{nrd}(I)$ and $I_2 = I\overline{\beta_2}/\,\mathrm{nrd}(I)$.
- Then $\theta := \widehat{\varphi}_{I_2} \circ \varphi_{I_1} = \beta_2\overline{\beta_1}/\,\mathrm{nrd}(I)$.
- Compute $\theta(P_0, Q_0)$.

AnyIdealToIsogeny

- Now, consider the Kani isogeny diamond:

$$\begin{array}{ccc} E' & \xrightarrow{\widehat{\varphi'}_v} & E_v \\ \uparrow{\scriptstyle \varphi'_u} & & \uparrow{\scriptstyle \varphi_v \circ \widehat{\varphi}_{I_2}} \\ E_u & \xrightarrow{\widehat{\varphi}_u \circ \varphi_{I_1}} & E_I \end{array}$$

- And the $(2^e, 2^e)$-isogeny:

$$\Phi := \begin{pmatrix} \varphi_{I_1} \circ \widehat{\varphi}_u & \varphi_{I_2} \circ \widehat{\varphi}_v \\ -\varphi'_u & \varphi'_v \end{pmatrix} : E_u \times E_v \longrightarrow E_I \times E'$$

AnyIdealToIsogeny

- Now, consider the Kani isogeny diamond:

$$\begin{array}{ccc} E' & \xrightarrow{\widehat{\varphi'}_v} & E_v \\ {\scriptstyle \varphi'_u}\uparrow & & \uparrow{\scriptstyle \varphi_v \circ \widehat{\varphi}_{I_2}} \\ E_u & \xrightarrow{\widehat{\varphi}_u \circ \varphi_{I_1}} & E_I \end{array}$$

- And the $(2^e, 2^e)$-isogeny:

$$\Phi := \begin{pmatrix} \varphi_{I_1} \circ \widehat{\varphi}_u & \varphi_{I_2} \circ \widehat{\varphi}_v \\ -\varphi'_u & \varphi'_v \end{pmatrix} : E_u \times E_v \longrightarrow E_I \times E'$$

- It has kernel:

$$\ker(\Phi) = \{([\mathrm{nrd}(I_1)]\varphi_u(P), \varphi_v \circ \theta(P)) \mid P \in E_0[2^e]\}$$

- Using the images of $\theta, \varphi_u, \varphi_v$ of P_0, Q_0 and some DLPs, we obtain $\ker(\Phi)$.
- We then compute Φ in the Theta model.

AnyIdealToIsogeny

- The $(2^e, 2^e)$-isogeny:

$$\Phi := \begin{pmatrix} \varphi_{I_1} \circ \widehat{\varphi}_u & \varphi_{I_2} \circ \widehat{\varphi}_v \\ -\varphi'_u & \varphi'_v \end{pmatrix} : E_u \times E_v \longrightarrow E_I \times E'$$

  represents $\varphi_{I_1} \circ \widehat{\varphi}_u$ and we know $\varphi_u(P_0, Q_0)$.
- Hence, we can get $\varphi_{I_1}(P_0, Q_0)$.
- Besides, $[\mathrm{nrd}(I_1)]\varphi_I = \varphi_{I_1} \circ \beta_1$ so we can get $\varphi_I(P_0, Q_0)$.

Performance

Compactness, scalability, choice of prime

Table: Chosen parameters for SQIsign2D and SQIsignHD. Public key and signature sizes in bytes.

		NIST I	NIST III	NIST V
SQIsign2D	Prime	$5 \cdot 2^{248} - 1$	$65 \cdot 2^{376} - 1$	$27 \cdot 2^{500} - 1$
	Pub. key	66	98	130
	Signature	148	222	294
SQIsignHD	Prime	$13 \cdot 2^{126} \cdot 3^{78} - 1$	—	—
	Pub. key	66	—	—
	Signature	109	—	—

Timings - rigorous version (in C)

Table: Performance of SQIsign2D on Intel Xeon Gold 6338 (Ice Lake, 2GHz), using generic finite field arithmetic (Fiat-Crypto), GMP 6.2.1. Turbo-boost disabled. Timings in 10^6 cycles.

	Level	SQIsign	SQIsignHD	SQIsign2D
Keygen	I	2,800	190	120
	III	21,300	—	440
	V	91,600	—	1,070
Sign	I	4,600	115	290
	III	39,300	—	1,040
	V	165,000	—	2,490
Verify	I	93	—	25
	III	641	—	98
	V	2,080	—	247

Timings - heuristic version (in C, optimized arithmetic)

Table: Performance of SQIsign2D on Intel Xeon Gold 6338 (Ice Lake, 2GHz), with finite field arithmetic optimised using intrinsics for the Ice Lake architecture, GMP 6.2.1. Turbo-boost disabled. Timings in 10^6 cycles.

	Level	SQIsign (NIST)	SQIsign (EC 2023)	SQIsign2D	SQIsign2D-H
Keygen	I	1,700	400	60	58
	III	—	—	170	170
	V	—	—	360	350
Sign	I	2,400	1880	160	100
	III	—	—	460	280
	V	—	—	940	570
Verify	I	39	29	9	9
	III	—	—	29	29
	V	—	—	62	60

Security analysis

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.

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 $\mathcal{S}$ 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 $\mathcal{S}$ 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 $\mathcal{S}$ 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 $\mathcal{S}$ 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.

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

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 $\mathcal{S}$ 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.

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

Conclusion

Welcoming a new member to the SQIsign family

	SQIsign	SQIsignHD	SQIsign2D
Security proof	✗	✗✓	✓
Scalability	✗	✓	✓
Signing time	✗	✓✓	✓
Signature size	✓	✓	✓
Verification	✓	✗	✓✓