SQIsign

Lorenz Panny

Technische Universität München

ECC 2024, Taipei, 30 October 2024

SQIsign: What?

https://sqisign.org

SQIsign: What?

https://sqisign.org

- A new and very hot post-quantum signature scheme.
- In **round 2** of the NISTPQC signature on-ramp!

SQIsign: Why?

+ It's extremely small compared to the competition.

SQIsign: Why?

+ It's extremely small compared to the competition.
– It's relatively slow compared to the competition.

SQIsign: Why?

- \+ It's extremely small compared to the competition.
- – It's relatively slow compared to the competition.
- \+ ...but SQIsign is getting better by the $\approx$ week!

(See e.g. Benjamin's talk just afterwards.)

SQIsign: Why?

- \+ It's extremely <u>small</u> compared to the competition.
- – It's relatively <u>slow</u> compared to the competition.
- \+ ...but SQIsign is getting better by the $\approx$ week!

(See e.g. Benjamin's talk just afterwards.)

Big picture

SQIsign: How?

$\rightsquigarrow$ Fiat–Shamir: signature scheme from identification scheme by replacing the verifier by a hash function.

SQIsign: How?

⇝ Fiat–Shamir: signature scheme from identification scheme by replacing the verifier by a hash function.

- Identification scheme based on isogenies:

$$E_0 \xrightarrow{\textit{secret}} E_A$$

SQIsign: How?

⇝ <u>Fiat–Shamir</u>: signature scheme from identification scheme by replacing the verifier by a hash function.

- Identification scheme based on isogenies:

$$\begin{tikzcd}
E_0 \arrow[r, dashed, "\textit{secret}"] \arrow[d, dashed, "\textit{commitment}"'] & E_A \\
E_1 &
\end{tikzcd}$$

SQIsign: How?

- ⇝ <u>Fiat–Shamir</u>: signature scheme from identification scheme by replacing the verifier by a hash function.
- ► Identification scheme based on isogenies:

$$\begin{tikzcd}
E_0 \arrow[r, dashed, "secret"] \arrow[d, dashed, "commitment"'] & E_A \\
E_1 \arrow[r, "challenge"'] & E_2
\end{tikzcd}$$

SQIsign: How?

⇝ Fiat–Shamir: signature scheme from identification scheme by replacing the verifier by a hash function.

- Identification scheme based on isogenies:

$$\begin{tikzcd}
E_0 \arrow[r, dashed, "\textit{secret}"] \arrow[d, dashed, "\textit{commitment}"'] & E_A \arrow[d, "\textit{response}"] \\
E_1 \arrow[r, "\textit{challenge}"'] & E_2
\end{tikzcd}$$

SQIsign: How?

⇝ <u>Fiat–Shamir</u>: signature scheme from identification scheme by replacing the verifier by a hash function.

- Identification scheme based on isogenies:

$$\begin{tikzcd}
E_0 \arrow[r, dashed, "secret"] \arrow[d, dashed, "commitment"'] & E_A \arrow[d, very thick, "response"] \\
E_1 \arrow[r, "challenge"'] & E_2
\end{tikzcd}$$

- Easy response: $E_A \to E_0 \to E_1 \to E_2$. *Obviously broken.*

SQIsign: How?

$\rightsquigarrow$ Fiat–Shamir: signature scheme from identification scheme by replacing the verifier by a hash function.

- Identification scheme based on isogenies:

$$\begin{tikzcd}
E_0 \arrow[rrr, dashed, "\textit{secret}"] \arrow[d, dashed, "\textit{commitment}"'] & & & E_A \arrow[d, Rightarrow, "\textit{response}"] \\
E_1 \arrow[rrr, "\textit{challenge}"'] & & & E_2
\end{tikzcd}$$

- Easy response: $E_A \to E_0 \to E_1 \to E_2$. *Obviously broken.*
- **SQIsign**'s solution: Construct new path $E_A \to E_2$ (using *secret*).

SQIsign: How, really?

The Deuring correspondence:

SQIsign: How, really?

The Deuring correspondence:

SQIsign: How, really?

The Deuring correspondence:

Almost exact equivalence between two very different worlds:

- Supersingular elliptic curves defined over $\mathbb{F}_{p^2}$.

SQIsign: How, really?

The Deuring correspondence:

Almost exact equivalence between two very different worlds:

- Supersingular elliptic curves defined over $\mathbb{F}_{p^2}$.
- Quaternion maximal orders in a certain algebra $B_{p,\infty}$.

SQIsign: How, really?

The Deuring correspondence:

Almost exact equivalence between two very different worlds:

- Supersingular elliptic curves defined over $\mathbb{F}_{p^2}$.
- Quaternion maximal orders in a certain algebra $B_{p,\infty}$.

Isogenies become connecting ideals in quaternion land.

SQIsign: How, really?

The Deuring correspondence:

Almost exact equivalence between two very different worlds:

- Supersingular elliptic curves defined over $\mathbb{F}_{p^2}$.
- Quaternion maximal orders in a certain algebra $B_{p,\infty}$.

Isogenies become connecting ideals in quaternion land.

The correspondence is through the endomorphism ring.

SQIsign: How, really?

The Deuring correspondence:

Almost exact equivalence between two very different worlds:

- Supersingular elliptic curves defined over $\mathbb{F}_{p^2}$.
- Quaternion maximal orders in a certain algebra $B_{p,\infty}$.

Isogenies become connecting ideals in quaternion land.

The correspondence is through the endomorphism ring.

☺ The "$\Leftarrow$" direction is easy, the "$\Rightarrow$" direction seems hard!

SQIsign: How, really?

The Deuring correspondence:

Almost exact equivalence between two very different worlds:

- Supersingular elliptic curves defined over $\mathbb{F}_{p^2}$.
- Quaternion maximal orders in a certain algebra $B_{p,\infty}$.

Isogenies become connecting ideals in quaternion land.

The correspondence is through the endomorphism ring.

☺ The "$\Leftarrow$" direction is easy, the "$\Rightarrow$" direction seems hard!

$\rightsquigarrow$ *Cryptography!*

Endomorphisms $\longleftrightarrow$ isogenies

We now know that **the Deuring correspondence lies at the heart of contemporary isogeny-based cryptography.**

Endomorphisms $\longleftrightarrow$ isogenies

We now know that **the Deuring correspondence lies at the heart of contemporary isogeny-based cryptography.**

- $\approx$All isogeny security reduces to the "$\Rightarrow$" direction.

Endomorphisms $\longleftrightarrow$ isogenies

We now know that **the Deuring correspondence lies at the heart of contemporary isogeny-based cryptography.**

- $\approx$All isogeny security reduces to the "$\Rightarrow$" direction.
- **SQIsign** builds on the "$\Leftarrow$" direction constructively.

Endomorphisms $\longleftrightarrow$ isogenies

We now know that **the Deuring correspondence lies at the heart of contemporary isogeny-based cryptography.**

- $\approx$All isogeny security reduces to the "$\Rightarrow$" direction.
- **SQIsign** builds on the "$\Leftarrow$" direction constructively.
- Essential tool for both constructions and attacks.

Endomorphisms $\longleftrightarrow$ isogenies

We now know that **the Deuring correspondence lies at the heart of contemporary isogeny-based cryptography.**

- $\approx$All isogeny security reduces to the "$\Rightarrow$" direction.
- **SQIsign** builds on the "$\Leftarrow$" direction constructively.
- Essential tool for both constructions and attacks.

Constructively, *partially* known endomorphism rings are useful.
$\rightsquigarrow$ **Oriented curves** and **the isogeny class-group action**. 🏝️

(See my autumn-school lecture yesterday.)

The Deuring correspondence

Deuring correspondence: Example #1

Assume $p \equiv 3 \pmod 4$.

Then $E\colon y^2 = x^3 + x$ is supersingular,

Deuring correspondence: Example #1

Assume $p \equiv 3 \pmod 4$.

Then $E\colon y^2 = x^3 + x$ is supersingular, and it has endomorphisms

$$\begin{aligned} \iota\colon \ (x,y) &\longmapsto (-x, \sqrt{-1}\cdot y)\,, \\ \pi\colon \ (x,y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

Deuring correspondence: Example #1

Assume $p \equiv 3 \pmod 4$.

Then $E\colon y^2 = x^3 + x$ is supersingular, and it has endomorphisms

$$\begin{aligned} \iota\colon\ (x,y) &\longmapsto (-x, \sqrt{-1}\cdot y)\,, \\ \pi\colon\ (x,y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

In decreasing order of obviousness, one can show that

$$\iota^2 = [-1], \qquad \pi\iota = -\iota\pi, \qquad \pi^2 = [-p].$$

Deuring correspondence: Example #1

Assume $p \equiv 3 \pmod 4$.

Then $E\colon y^2 = x^3 + x$ is supersingular, and it has endomorphisms

$$\begin{aligned} \iota\colon\ (x,y) &\longmapsto (-x, \sqrt{-1}\cdot y)\,, \\ \pi\colon\ (x,y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

In decreasing order of obviousness, one can show that

$$\iota^2 = [-1], \qquad \pi\iota = -\iota\pi, \qquad \pi^2 = [-p].$$

In fact, the image in $B_{p,\infty}$ of a $\mathbb{Z}$-basis of $\mathrm{End}(E)$ is given by

$$\{1, \quad \iota, \quad (\iota+\pi)/2, \quad (1+\iota\pi)/2\}\,.$$

Deuring correspondence: Example #2

Assume $p \equiv 2 \pmod 3$.

Then $E'\colon y^2 = x^3 + 1$ is supersingular,

Deuring correspondence: Example #2

Assume $p \equiv 2 \pmod{3}$.

Then $E'\colon y^2 = x^3 + 1$ is supersingular, and it has endomorphisms

$$\begin{aligned} \omega : \ (x, y) &\longmapsto (\zeta_3 \cdot x, y)\,, \\ \pi : \ (x, y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

Deuring correspondence: Example #2

Assume $p \equiv 2 \pmod 3$.

Then E': $y^2 = x^3 + 1$ is supersingular, and it has endomorphisms

$$\begin{aligned} \omega: \ (x, y) &\longmapsto (\zeta_3 \cdot x, y)\,, \\ \pi: \ (x, y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

In decreasing order of obviousness, one can show that

$$\omega^3 = [1], \qquad \omega\pi + \pi\omega = -\pi, \qquad \pi^2 = [-p].$$

Deuring correspondence: Example #2

Assume $p \equiv 2 \pmod 3$.

Then $E'\colon y^2 = x^3 + 1$ is supersingular, and it has endomorphisms

$$\begin{aligned} \omega &: \ (x, y) \longmapsto (\zeta_3 \cdot x, y)\,, \\ \pi &: \ (x, y) \longmapsto (x^p, y^p)\,. \end{aligned}$$

In decreasing order of obviousness, one can show that

$$\omega^3 = [1], \qquad \omega\pi + \pi\omega = -\pi, \qquad \pi^2 = [-p].$$

In fact, a $\mathbb{Z}$-basis of $\mathrm{End}(E')$ is given by

$$\left\{1, \quad \omega, \quad \omega\pi, \quad (1+2\omega)(1+\pi)/3\right\}.$$

Deuring correspondence: Example #3

For the sake of an example, let $p = 7799999 \equiv 11 \pmod{12}$.

Then $E\colon y^2 = x^3 + x$ and $E'\colon y^2 = x^3 + 1$ are both supersingular with endomorphism rings as shown before.

Deuring correspondence: Example #3

For the sake of an example, let $p = 7799999 \equiv 11 \pmod{12}$.

Then $E\colon y^2 = x^3 + x$ and $E'\colon y^2 = x^3 + 1$ are both supersingular with endomorphism rings as shown before.

Moreover, the lattice

$$\mathbb{Z}\,4947 \oplus \mathbb{Z}\,4947\iota \oplus \mathbb{Z}\,\frac{598 + 4947\iota + \pi}{2} \oplus \mathbb{Z}\,\frac{4947 + 598\iota + \iota\pi}{2}$$

inside $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ corresponds to an isogeny $E \to E'$.

(I haven't yet said *how*.)

From curves to quaternions

As far as we know, these are *hard* problems (even quantumly):

From curves to quaternions

As far as we know, these are *hard* problems (even quantumly):

The supersingular endomorphism-ring problem.
Given a supersingular elliptic curve,
find its endomorphism ring.

From curves to quaternions

As far as we know, these are *hard* problems (even quantumly):

The supersingular endomorphism-ring problem.
Given a supersingular elliptic curve,
find its endomorphism ring.

Equivalently (Wesolowski 2021, assuming GRH):

The isogeny problem.
Given two supersingular elliptic curves,
find any isogeny between them.

From curves to quaternions

As far as we know, these are *hard* problems (even quantumly):

The supersingular endomorphism-ring problem.
Given a supersingular elliptic curve,
find its endomorphism ring.

Equivalently (Wesolowski 2021, assuming GRH):

The isogeny problem.
Given two supersingular elliptic curves,
find any isogeny between them.

Core of the connection: The Deuring correspondence!

From curves to quaternions

As far as we know, these are *hard* problems (even quantumly):

The supersingular endomorphism-ring problem.
Given a supersingular elliptic curve,
find its endomorphism ring.

Equivalently (Wesolowski 2021, assuming GRH):

The isogeny problem.
Given two supersingular elliptic curves,
find any isogeny between them.

<u>Core of the connection:</u> The Deuring correspondence!

$\Leftarrow$: Isogenies "transport" knowledge of endomorphism rings.

From curves to quaternions

As far as we know, these are *hard* problems (even quantumly):

> **The supersingular endomorphism-ring problem.**
> Given a supersingular elliptic curve,
> find its endomorphism ring.

Equivalently (Wesolowski 2021, assuming GRH):

> **The isogeny problem.**
> Given two supersingular elliptic curves,
> find any isogeny between them.

<u>Core of the connection:</u> The Deuring correspondence!

$\Leftarrow$: Isogenies "transport" knowledge of endomorphism rings.

$\Rightarrow$: Finding powersmooth "connecting ideals" is easy (🪄);
converting them to isogenies is easy.

⚠️ About **4** math-heavy slides ahead.
It will become less technical afterwards! :)

"Abstract" quaternions

It is convenient to fix one curve E_0 and embed all other $\mathrm{End}(E)$ into $\mathrm{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$.

“Abstract” quaternions

It is convenient to fix one curve E_0 and embed all other $\mathrm{End}(E)$ into $\mathrm{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$. $\rightsquigarrow$ Assume $p \equiv 3 \pmod 4$ and let

$$B_{p,\infty} := \mathrm{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$$

where $E_0\colon y^2 = x^3 + x$ as before.

“Abstract” quaternions

It is convenient to fix one curve E_0 and embed all other $\mathrm{End}(E)$ into $\mathrm{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$. $\rightsquigarrow$ Assume $p \equiv 3 \pmod 4$ and let

$$B_{p,\infty} := \mathrm{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$$

where $E_0 \colon y^2 = x^3 + x$ as before.

For clarity, when dealing with “abstract” elements on the quaternion side, it is customary to write $\mathbf{i}$ for ι and $\mathbf{j}$ for π.

“Abstract” quaternions

It is convenient to fix one curve E_0 and embed all other $\operatorname{End}(E)$ into $\operatorname{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$. $\rightsquigarrow$ Assume $p \equiv 3 \pmod 4$ and let

$$B_{p,\infty} := \operatorname{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$$

where $E_0 \colon y^2 = x^3 + x$ as before.

For clarity, when dealing with “abstract” elements on the quaternion side, it is customary to write $\mathbf{i}$ for ι and $\mathbf{j}$ for π.

Indeed, this means

$$B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}\mathbf{i} \oplus \mathbb{Q}\mathbf{j} \oplus \mathbb{Q}\mathbf{ij}$$

with multiplication defined by $\mathbf{i}^2 = -1$, $\mathbf{j}^2 = -p$, $\mathbf{ji} = -\mathbf{ij}$.
(This $B_{p,\infty}$ is the “quaternion algebra over $\mathbb{Q}$ ramified at p and ∞”.)

The main theorem

- Fix a supersingular elliptic curve $E_0/\mathbb{F}_{p^2}$. Let $\mathcal{O}_0 := \mathrm{End}(E_0)$.

The main theorem

- Fix a supersingular elliptic curve $E_0/\mathbb{F}_{p^2}$. Let $\mathcal{O}_0 := \mathrm{End}(E_0)$.

Theorem. The (contravariant) functor

$$E \longmapsto \mathrm{Hom}(E, E_0)$$

defines an equivalence of categories between

- supersingular elliptic curves with isogenies; and
- invertible left $\mathcal{O}_0$-modules

with nonzero left $\mathcal{O}_0$-module homomorphisms.

(up to their respective notions of isomorphism, etc. etc.)

The main theorem

- Fix a supersingular elliptic curve $E_0/\mathbb{F}_{p^2}$. Let $\mathcal{O}_0 := \mathrm{End}(E_0)$.

Theorem. The (contravariant) functor

$$E \longmapsto \mathrm{Hom}(E, E_0)$$

defines an equivalence of categories between

- supersingular elliptic curves with isogenies; and
- invertible left $\mathcal{O}_0$-modules

with nonzero left $\mathcal{O}_0$-module homomorphisms.

(up to their respective notions of isomorphism, etc. etc.)

Corollary (Deuring). Isomorphism classes of supersingular elliptic curves are in bijection with the (left) class set of $\mathcal{O}_0$.

The main theorem

- Fix a supersingular elliptic curve $E_0/\mathbb{F}_{p^2}$. Let $\mathcal{O}_0 := \operatorname{End}(E_0)$.

Theorem. The (contravariant) functor

$$E \longmapsto \operatorname{Hom}(E, E_0)$$

defines an equivalence of categories between

- supersingular elliptic curves with isogenies; and
- invertible left $\mathcal{O}_0$-modules

with nonzero left $\mathcal{O}_0$-module homomorphisms.

(up to their respective notions of isomorphism, etc. etc.)

Corollary (Deuring). Isomorphism classes of supersingular elliptic curves are in bijection with the (left) class set of $\mathcal{O}_0$.

⚠ There is no equivalence between elliptic curves/$\sim$ and endomorphism rings/$\sim$. (The map $\{E\}/\sim \to \{\mathcal{O}\}/\sim$ is not injective.)

Ideals & isogenies

One particular consequence of this equivalence is that

isogenies from E_0 correspond to left ideals of $\mathcal{O}_0$,

Ideals & isogenies

One particular consequence of this equivalence is that

isogenies from E_0 correspond to left ideals of $\mathcal{O}_0$,

and

isogeny *codomains* from E_0 correspond to left ideal *classes* of $\mathcal{O}_0$.

Ideals & isogenies

One particular consequence of this equivalence is that

isogenies from E_0 correspond to left ideals of $\mathcal{O}_0$,

and

isogeny *codomains* from E_0 correspond to left ideal *classes* of $\mathcal{O}_0$.

- Given $\psi\colon E_0 \to E$, the associated $\mathcal{O}_0$-ideal is $\mathrm{Hom}(E, E_0)\psi$.

Ideals & isogenies

One particular consequence of this equivalence is that

$\boxed{\text{isogenies from } E_0 \text{ correspond to left ideals of } \mathcal{O}_0,}$

and

$\boxed{\text{isogeny \textit{codomains} from } E_0 \text{ correspond to left ideal \textit{classes} of } \mathcal{O}_0.}$

- Given $\psi\colon E_0 \to E$, the associated $\mathcal{O}_0$-ideal is $\mathrm{Hom}(E, E_0)\psi$.

Important consequence: The isogeny $\varphi_I\colon E_0 \to E$ defined by a left $\mathcal{O}_0$-ideal I has kernel $\bigcap_{\alpha\in I} \ker\alpha \le E_0$.

Ideals & isogenies

One particular consequence of this equivalence is that

isogenies from E_0 correspond to left ideals of $\mathcal{O}_0$,

and

isogeny *codomains* from E_0 correspond to left ideal *classes* of $\mathcal{O}_0$.

- Given $\psi\colon E_0 \to E$, the associated $\mathcal{O}_0$-ideal is $\mathrm{Hom}(E, E_0)\psi$.

<u>Important consequence:</u> The isogeny $\varphi_I\colon E_0 \to E$ defined by a left $\mathcal{O}_0$-ideal I has kernel $\bigcap_{\alpha\in I} \ker\alpha \le E_0$.

$\rightsquigarrow$ Explicit **ideal-to-isogeny** conversion, provided all the points of $\mathrm{norm}(I)$-torsion are accessible (defined over small field extensions):

1. Write $I = \mathcal{O}_0 N + \mathcal{O}_0\alpha$ where $N = \mathrm{norm}(I) \in \mathbb{Z}$ and $\alpha \in \mathcal{O}_0$.
2. Compute the isogeny with kernel $E[I] = \ker(\alpha|_{E_0[N]})$.

All the $\mathrm{End}(E) \hookrightarrow B_{p,\infty}$

From any isogeny $\varphi\colon E_0 \to E$, we obtain (abstractly) an embedding of the endomorphism ring

$$\begin{aligned} \mathrm{End}(E) &\longhookrightarrow B_{p,\infty} = \mathrm{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}\,, \\ \alpha &\longmapsto \widehat{\varphi}\alpha\varphi/\deg(\varphi)\,. \end{aligned}$$

All the $\mathrm{End}(E) \hookrightarrow B_{p,\infty}$

From any isogeny $\varphi\colon E_0 \to E$, we obtain (abstractly) an embedding of the endomorphism ring

$$\begin{aligned} \mathrm{End}(E) &\longrightarrow B_{p,\infty} = \mathrm{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}\,, \\ \alpha &\longmapsto \widehat{\varphi}\alpha\varphi/\deg(\varphi)\,. \end{aligned}$$

<u>"Transporting" endomorphism knowledge:</u>

Knowing $\mathrm{End}(E_0)$ and an isogeny $\varphi\colon E_0 \to E$ reveals $\mathrm{End}(E)$.

All the $\mathrm{End}(E) \hookrightarrow B_{p,\infty}$

From any isogeny $\varphi\colon E_0 \to E$, we obtain (abstractly) an embedding of the endomorphism ring

$$\begin{aligned} \mathrm{End}(E) &\longrightarrow B_{p,\infty} = \mathrm{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}\,, \\ \alpha &\longmapsto \widehat{\varphi}\alpha\varphi/\deg(\varphi)\,. \end{aligned}$$

<u>"Transporting" endomorphism knowledge:</u>

Knowing $\mathrm{End}(E_0)$ and an isogeny $\varphi\colon E_0 \to E$ reveals $\mathrm{End}(E)$.

Concretely: Under the embedding above, we have

$$\mathrm{End}(E) = \mathcal{O}_R(I_\varphi) = \{\alpha \in B_{p,\infty} : I_\varphi\alpha \subseteq I_\varphi\}\,,$$

where

$$I_\varphi := \mathrm{Hom}(E, E_0)\varphi$$

is the ideal of $\mathrm{End}(E_0)$ associated to φ.

All the $\mathrm{End}(E) \hookrightarrow B_{p,\infty}$

From any isogeny $\varphi\colon E_0 \to E$, we obtain (abstractly) an embedding of the endomorphism ring

$$\begin{aligned} \mathrm{End}(E) &\longrightarrow B_{p,\infty} = \mathrm{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}\,, \\ \alpha &\longmapsto \widehat{\varphi}\alpha\varphi/\deg(\varphi)\,. \end{aligned}$$

<u>"Transporting" endomorphism knowledge:</u>

Knowing $\mathrm{End}(E_0)$ and an isogeny $\varphi\colon E_0 \to E$ reveals $\mathrm{End}(E)$.

Concretely: Under the embedding above, we have

$$\mathrm{End}(E) = \mathcal{O}_R(I_\varphi) = \{\alpha \in B_{p,\infty} : I_\varphi \alpha \subseteq I_\varphi\}\,,$$

where

$$I_\varphi := \mathrm{Hom}(E, E_0)\varphi$$

is the ideal of $\mathrm{End}(E_0)$ associated to φ.

($\rightsquigarrow$ Open problem: Constructing supersingular E with unknown $\mathrm{End}(E)$.)

Endomorphisms as a trapdoor

<u>Recall:</u> In SQIsign, creating a signature means finding an isogeny $E_A \to E_2$ where $\mathrm{End}(E_2)$ is known.

Endomorphisms as a trapdoor

Recall: In SQIsign, creating a signature means finding an isogeny $E_A \to E_2$ where $\mathrm{End}(E_2)$ is known.

- The legitimate signer also knows $\mathrm{End}(E_A)$.

(They transported this knowledge from E_0.)

Endomorphisms as a trapdoor

Recall: In SQIsign, creating a signature means finding an isogeny $E_A \to E_2$ where $\mathrm{End}(E_2)$ is known.

- The legitimate signer also knows $\mathrm{End}(E_A)$.

  (They transported this knowledge from E_0.)

- Supposedly noone else is able to know $\mathrm{End}(E_A)$.

Endomorphisms as a trapdoor

Recall: In SQIsign, creating a signature means finding an isogeny $E_A \to E_2$ where $\mathrm{End}(E_2)$ is known.

- The legitimate signer also knows $\mathrm{End}(E_A)$.

  (They transported this knowledge from E_0.)

- Supposedly noone else is able to know $\mathrm{End}(E_A)$.

$\rightsquigarrow$ Knowledge of $\mathrm{End}(E_A)$ is a *trapdoor* for finding $E_A \to E_2$.

SQIsign: main algorithms

SQIsign: How?

Recall:

- Identification scheme based on isogenies:

$$\begin{tikzcd} E_0 \arrow[r, dashed, "\textit{secret}"] \arrow[d, dashed, "\textit{commitment}"'] & E_A \arrow[d, "\textit{response}"] \\ E_1 \arrow[r, "\textit{challenge}"'] & E_2 \end{tikzcd}$$

- Easy response: $E_A \to E_0 \to E_1 \to E_2$. *Obviously broken.*
- **SQIsign**'s solution: Construct new path $E_A \to E_2$ (using *secret*).

SQIsign: How?

Main idea:

- "Lift" the *commitment* and *challenge* to quaternion land.

SQIsign: How?

<u>Main idea:</u>

- "Lift" the *commitment* and *challenge* to quaternion land.
- Construct the *response* in quaternion land using *secret*; project it "down" to the curve world (ideal-to-isogeny).

SQIsign: How?

Main idea:

- "Lift" the *commitment* and *challenge* to quaternion land.
- Construct the *response* in quaternion land using *secret*; project it "down" to the curve world (ideal-to-isogeny).
- The verifier can check on curves that it's all correct.

SQIsign: How?

Main idea:

- "Lift" the *commitment* and *challenge* to quaternion land.
- Construct the *response* in quaternion land using *secret*; project it "down" to the curve world (ideal-to-isogeny).
- The verifier can check on curves that it's all correct.

Main technical tool: The KLPT algorithm.

- From $\mathrm{End}(E), \mathrm{End}(E')$, can randomize within $\mathrm{Hom}(E, E')$.

  ...with very good control over the degree of the resulting isogeny!

SQIsign: How?

Main idea:

- "Lift" the *commitment* and *challenge* to quaternion land.
- Construct the *response* in quaternion land using *secret*; project it "down" to the curve world (ideal-to-isogeny).
- The verifier can check on curves that it's all correct.

Main technical tool: The KLPT algorithm.

- From $\mathrm{End}(E), \mathrm{End}(E')$, can randomize within $\mathrm{Hom}(E, E')$.

  ...with very good control over the degree of the resulting isogeny!

$\rightsquigarrow$ SQIsign takes the "broken" signature $E_A \to E_0 \to E_1 \to E_2$ and rewrites it into a random isogeny $E_A \to E_2$.

SQIsign: How?

Main idea:

- "Lift" the *commitment* and *challenge* to quaternion land.
- Construct the *response* in quaternion land using *secret*; project it "down" to the curve world (ideal-to-isogeny).
- The verifier can check on curves that it's all correct.

Main technical tool: The KLPT algorithm.

- From $\mathrm{End}(E), \mathrm{End}(E')$, can randomize within $\mathrm{Hom}(E, E')$.

  ...with very good control over the degree of the resulting isogeny!

$\rightsquigarrow$ SQIsign takes the "broken" signature $E_A \to E_0 \to E_1 \to E_2$ and rewrites it into a random isogeny $E_A \to E_2$.

> *"If you have KLPT implemented very nicely as a black box, then anyone can implement SQIsign."*
>
> — Yan Bo Ti

SQIsigning

Parameters:

SQIsigning

<u>Parameters:</u>

- Large prime p such that $p^2 - 1$ has a large *smooth* part.
  (Finding such primes is tricky $\rightsquigarrow$ research on "SQIsign-friendly primes".)

SQIsigning

Parameters:

- Large prime p such that $p^2 - 1$ has a large *smooth* part.
  (Finding such primes is tricky $\rightsquigarrow$ research on "SQIsign-friendly primes".)
- "Special" starting curve $E_0/\mathbb{F}_{p^2}$ (usually $E_0\colon y^2 = x^3 + x$) with explicitly known endomorphism ring $\mathrm{End}(E_0)$.

SQIsigning

Parameters:

- Large prime p such that $p^2 - 1$ has a large *smooth* part.
  (Finding such primes is tricky $\rightsquigarrow$ research on "SQIsign-friendly primes".)
- "Special" starting curve $E_0/\mathbb{F}_{p^2}$ (usually $E_0\colon y^2 = x^3 + x$) with explicitly known endomorphism ring $\mathrm{End}(E_0)$.
- Degrees for all (to be) involved isogenies, tons of precomputed constants, etc.

SQIsigning

Key generation:

SQIsigning

Key generation:

- Sample a random *secret* isogeny $\varphi\colon E_0 \to E_A$ together with its associated $\mathrm{End}(E_0)$-ideal I_φ.

  (Constructing φ and I_φ *jointly* is much faster than picking one and converting.)

SQIsigning

Key generation:

- Sample a random *secret* isogeny $\varphi\colon E_0 \to E_A$ together with its associated $\mathrm{End}(E_0)$-ideal I_φ.

  (Constructing φ and I_φ *jointly* is much faster than picking one and converting.)
- The public key is just the codomain E_A.

SQIsigning

<u>Signing:</u>

SQIsigning

<u>Signing:</u>

- Sample a random *commitment* isogeny $\psi\colon E_0 \to E_1$ together with its associated $\mathrm{End}(E_0)$-ideal I_ψ.

SQIsigning

<u>Signing:</u>

- Sample a random *commitment* isogeny $\psi\colon E_0 \to E_1$ together with its associated $\mathrm{End}(E_0)$-ideal I_ψ.
- Hash the tuple $(E_A, E_1, \textit{message})$ to obtain a *challenge* isogeny $\chi\colon E_1 \to E_2$.

SQIsigning

Signing:

- Sample a random *commitment* isogeny $\psi\colon E_0 \to E_1$ together with its associated $\mathrm{End}(E_0)$-ideal I_ψ.
- Hash the tuple $(E_A, E_1, \mathit{message})$ to obtain a *challenge* isogeny $\chi\colon E_1 \to E_2$.
- Using the (secret) commitment isogeny ψ, convert χ into an $\mathrm{End}(E_1)$-ideal I_χ.

SQIsigning

Signing:

- Sample a random *commitment* isogeny $\psi\colon E_0 \to E_1$ together with its associated $\mathrm{End}(E_0)$-ideal I_ψ.
- Hash the tuple $(E_A, E_1, \mathit{message})$ to obtain a *challenge* isogeny $\chi\colon E_1 \to E_2$.
- Using the (secret) commitment isogeny ψ, convert χ into an $\mathrm{End}(E_1)$-ideal I_χ.
- Compute the $\mathrm{End}(E_A)$-ideal $I'_\sigma := \bar{I}_\varphi \cdot I_\psi \cdot I_\chi$ which corresponds to the isogeny $\chi \circ \psi \circ \widehat{\varphi}\colon E_A \to E_0 \to E_1 \to E_2$.

SQIsigning

Signing:

- Sample a random *commitment* isogeny $\psi\colon E_0 \to E_1$ together with its associated $\mathrm{End}(E_0)$-ideal I_ψ.
- Hash the tuple $(E_A, E_1, \mathit{message})$ to obtain a *challenge* isogeny $\chi\colon E_1 \to E_2$.
- Using the (secret) commitment isogeny ψ, convert χ into an $\mathrm{End}(E_1)$-ideal I_χ.
- Compute the $\mathrm{End}(E_A)$-ideal $I'_\sigma := \bar{I}_\varphi \cdot I_\psi \cdot I_\chi$ which corresponds to the isogeny $\chi \circ \psi \circ \widehat{\varphi}\colon E_A \to E_0 \to E_1 \to E_2$.
- Convert I'_σ into a random equivalent ideal I_σ. (KLPT!)

SQIsigning

Signing:

- Sample a random *commitment* isogeny $\psi\colon E_0 \to E_1$ together with its associated $\mathrm{End}(E_0)$-ideal I_ψ.
- Hash the tuple $(E_A, E_1, \mathit{message})$ to obtain a *challenge* isogeny $\chi\colon E_1 \to E_2$.
- Using the (secret) commitment isogeny ψ, convert χ into an $\mathrm{End}(E_1)$-ideal I_χ.
- Compute the $\mathrm{End}(E_A)$-ideal $I'_\sigma := \bar{I}_\varphi \cdot I_\psi \cdot I_\chi$ which corresponds to the isogeny $\chi \circ \psi \circ \widehat{\varphi}\colon E_A \to E_0 \to E_1 \to E_2$.
- Convert I'_σ into a random equivalent ideal I_σ. (KLPT!)
- Compute the isogeny $\sigma\colon E_A \to E_2$ corresponding to I_σ.

SQIsigning

Signing:

- Sample a random *commitment* isogeny $\psi\colon E_0 \to E_1$ together with its associated $\mathrm{End}(E_0)$-ideal I_ψ.
- Hash the tuple $(E_A, E_1, \mathit{message})$ to obtain a *challenge* isogeny $\chi\colon E_1 \to E_2$.
- Using the (secret) commitment isogeny ψ, convert χ into an $\mathrm{End}(E_1)$-ideal I_χ.
- Compute the $\mathrm{End}(E_A)$-ideal $I'_\sigma := \bar{I}_\varphi \cdot I_\psi \cdot I_\chi$ which corresponds to the isogeny $\chi \circ \psi \circ \widehat{\varphi}\colon E_A \to E_0 \to E_1 \to E_2$.
- Convert I'_σ into a random equivalent ideal I_σ. (KLPT!)
- Compute the isogeny $\sigma\colon E_A \to E_2$ corresponding to I_σ.
- Return the signature (E_1, σ).

SQIsigning

Verification:

SQIsigning

<u>Verification:</u>

- Given public key E_A, signature (E_1, σ), and the *message*.

SQIsigning

Verification:

- Given public key E_A, signature (E_1, σ), and the *message*.
- Hash the tuple $(E_A, E_1, \textit{message})$ to recompute the challenge $\chi\colon E_1 \to E_2$. (There are better ways of doing it; this is the simplest.)

SQIsigning

<u>Verification:</u>

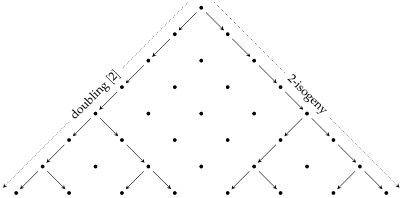
- Given public key E_A, signature (E_1, σ), and the *message*.
- Hash the tuple $(E_A, E_1, \mathit{message})$ to recompute the challenge $\chi\colon E_1 \to E_2$. (There are better ways of doing it; this is the simplest.)
- Check that σ is indeed an isogeny from E_A to E_2, and that $\widehat{\chi} \circ \sigma$ is cyclic.

SQIsigning

Verification:

- Given public key E_A, signature (E_1, σ), and the *message*.
- Hash the tuple $(E_A, E_1, \textit{message})$ to recompute the challenge $\chi \colon E_1 \to E_2$. (There are better ways of doing it; this is the simplest.)
- Check that σ is indeed an isogeny from E_A to E_2, and that $\widehat{\chi} \circ \sigma$ is cyclic.

In SQIsign, the degrees are chosen so that $\deg(\sigma) = 2^n$.
$\rightsquigarrow$ very efficient isogeny chains in time $O(n \log n)$ using "optimal strategies".



Security

Required properties

For SQIsign to be secure, we need two main properties:

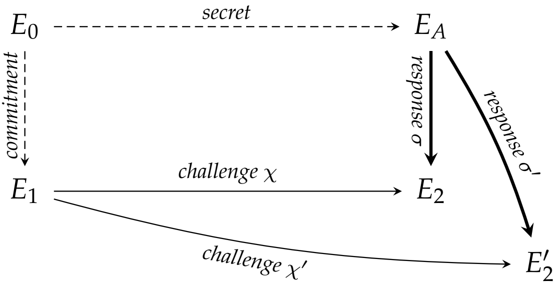
- Soundness: Ability to sign proves knowledge of a secret.
- Zero-knowledge: Signatures do not leak anything secret.

Soundness

We want extractability: Given two valid *signatures* for the same *commitment* but different *challenges*, can we compute the *secret*?

Soundness

We want <u>extractability:</u> Given two valid *signatures* for the same *commitment* but different *challenges*, can we compute the *secret*?



Soundness

We want <u>extractability:</u> Given two valid *signatures* for the same *commitment* but different *challenges*, can we compute the *secret*?

$$
\begin{tikzcd}
E_0 \arrow[rr, dashed, "secret"] \arrow[d, dashed, "commitment"'] & & E_A \arrow[d, "\text{response } \sigma"'] \arrow[dr, bend left, "\text{response } \sigma'"] & \\
E_1 \arrow[rr, "\text{challenge } \chi"] \arrow[rrr, bend right, "\text{challenge } \chi'"'] & & E_2 & E_2'
\end{tikzcd}
$$

☹ We cannot directly extract the secret $\varphi\colon E_0 \to E_A$, but we *can* extract an endomorphism in $\mathrm{End}(E_A)\backslash\mathbb{Z}$:

$$E_A \xrightarrow{\sigma'} E_2' \xrightarrow{\widehat{\chi}'} E_1 \xrightarrow{\chi} E_2 \xrightarrow{\widehat{\sigma}} E_A\,.$$

One endomorphism to rule them all?

New question: Is computing *some* nonscalar endomorphism just as hard as finding $\varphi \colon E_0 \to E_A$?

One endomorphism to rule them all?

New question: Is computing *some* nonscalar endomorphism just as hard as finding $\varphi\colon E_0 \to E_A$?

Answer: Essentially **yes!**

(See Benjamin's autumn-school lecture past Monday.)

One endomorphism to rule them all?

New <u>question</u>: Is computing *some* nonscalar endomorphism just as hard as finding $\varphi\colon E_0 \to E_A$?

<u>Answer:</u> Essentially **yes!**

(See Benjamin's autumn-school lecture past Monday.)

$\Longrightarrow$ Modulo minor details, soundness of SQIsign is equivalent to the hardness of the isogeny problem.

Zero-knowledge

...is, in this variant of SQIsign, basically a heuristic assumption.

Zero-knowledge

...is, in this variant of SQIsign, basically a heuristic assumption.

Key question:

- (How) is the distribution of responses related to the secret?

Zero-knowledge

...is, in this variant of SQIsign, basically a heuristic assumption.

Key question:

- (How) is the distribution of responses related to the secret?

Standard proof technique: Give a *simulator* that outputs *transcripts* (E_1, χ, σ) with the same distribution as the signing algorithm, but without the secret.

Zero-knowledge

...is, in this variant of SQIsign, basically a heuristic assumption.

Key question:

- (How) is the distribution of responses related to the secret?

Standard proof technique: Give a *simulator* that outputs *transcripts* (E_1, χ, σ) with the same distribution as the signing algorithm, but without the secret.

☹ Here, intimately related to gory internals of KLPT.

Zero-knowledge

...is, in this variant of SQIsign, basically a heuristic assumption.

Key <u>question:</u>

- (How) is the distribution of responses related to the secret?

Standard proof technique: Give a *simulator* that outputs *transcripts* (E_1, χ, σ) with the same distribution as the signing algorithm, but without the secret.

☹ Here, intimately related to gory internals of KLPT.
☹ It seems difficult to *prove* anything about this.

Zero-knowledge

...is, in this variant of SQIsign, basically a heuristic assumption.

Key <u>question:</u>

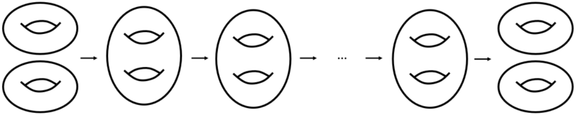
- (How) is the distribution of responses related to the secret?

Standard proof technique: Give a *simulator* that outputs *transcripts* (E_1, χ, σ) with the same distribution as the signing algorithm, but without the secret.

☹ Here, intimately related to gory internals of KLPT.
☹ It seems difficult to *prove* anything about this.

☺ Some newer SQIsign variants are much better in this regard!

⇝ See next talk.



Performance

SQIsign: Numbers

⚠️ These are from the round-1 submission to NISTPQC.
They will change very significantly in the coming months. 🚀

SQIsign: Numbers

⚠️ These are from the round-1 submission to NISTPQC.
They will change very significantly in the coming months. 🚀

sizes

parameter set	public keys	signatures
NIST-**I**	**64** bytes	**177** bytes
NIST-**III**	**96** bytes	**263** bytes
NIST-**V**	**128** bytes	**335** bytes

SQIsign: Numbers

⚠️ These are from the round-1 submission to NISTPQC.
They will change very significantly in the coming months. 🚀

sizes

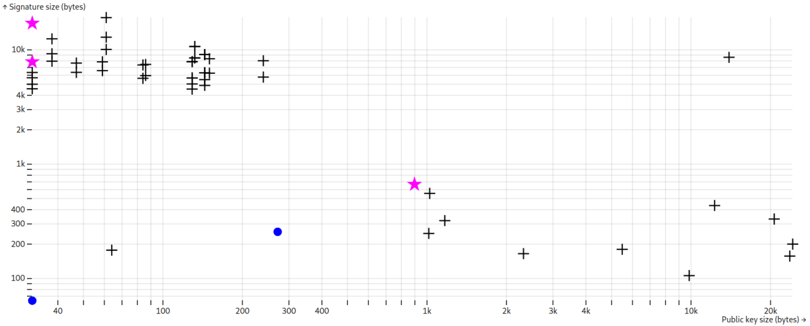
parameter set	public keys	signatures
NIST-**I**	**64** bytes	**177** bytes
NIST-**III**	**96** bytes	**263** bytes
NIST-**V**	**128** bytes	**335** bytes

performance

Cycle counts for a *generic C implementation* running on an Intel *Ice Lake* CPU.
Optimizations are certainly possible and work in progress.

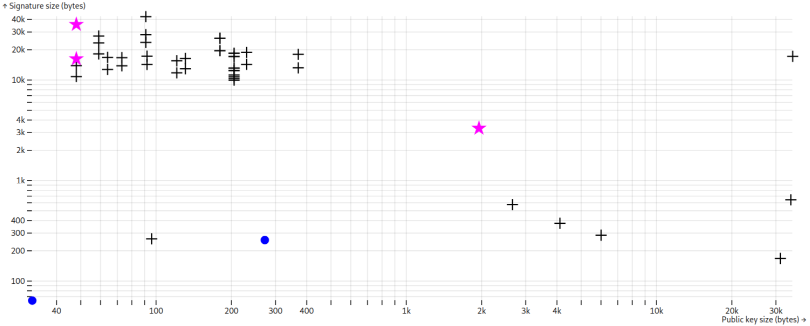
parameter set	keygen	signing	verifying
NIST-**I**	**3728** megacycles	**5779** megacycles	**108** megacycles
NIST-**III**	**23734** megacycles	**43760** megacycles	**654** megacycles
NIST-**V**	**91049** megacycles	**158544** megacycles	**2177** megacycles

SQIsign: Comparison (NIST level 1)



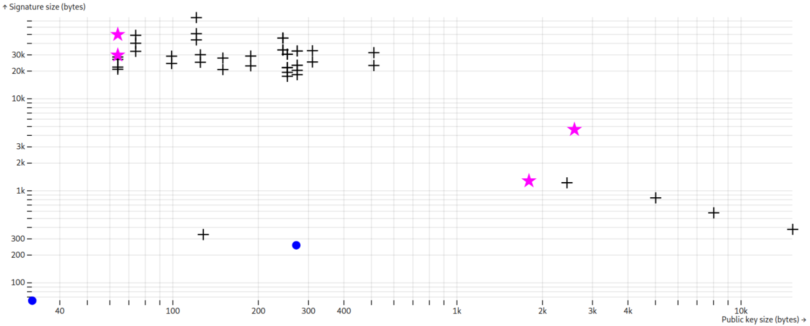
Source: `https://pqshield.github.io/nist-sigs-zoo`

SQIsign: Comparison (NIST level 3)



Source: `https://pqshield.github.io/nist-sigs-zoo`

SQIsign: Comparison (NIST level 5)



Source: `https://pqshield.github.io/nist-sigs-zoo`

Questions?

(Also feel free to email me: `lorenz@yx7.cc`)