SQISign: Compact Post-Quantum Signatures from Quaternions and Isogenies

Antonin Leroux, joint work with L. De Feo, D. Kohel, C. Petit and B. Wesolowski

DGA, Ecole Polytechnique, Institut Polytechnique de Paris, Inria Saclay

The State of Post-Quantum Cryptography

Six families still in Round 3 NIST post-quantum competition (Finalists + Alternate Candidates):

Lattices	4 encryption	2 signature
Codes	3 encryption	
Multivariate		2 signature
Isogenies	1 encryption	
Hash-based		1 signature
MPC		1 signature

The State of Post-Quantum Cryptography

Six families still in Round 3 NIST post-quantum competition (Finalists + Alternate Candidates):

Lattices	4 encryption	2 signature	
Codes	3 encryption		
Multivariate		2 signature	
Isogenies	1 encryption		compact keys
Hash-based		1 signature	
MPC		1 signature	

The State of Post-Quantum Cryptography

Six families still in Round 3 NIST post-quantum competition (Finalists + Alternate Candidates):

Lattices	4 encryption	2 signature	
Codes	3 encryption		
Multivariate		2 signature	
Isogenies	1 encryption		compact keys poor efficiency
Hash-based		1 signature	
MPC		1 signature	

The State of Post-Quantum Cryptography

Six families still in Round 3 NIST post-quantum competition (Finalists + Alternate Candidates):

Lattices	4 encryption	2 signature	
Codes	3 encryption		
Multivariate		2 signature	
Isogenies	1 encryption		compact keys poor efficiency
Hash-based		1 signature	
MPC		1 signature	

Many more isogeny-based protocols since then....

The State of Post-Quantum Cryptography

Six families still in Round 3 NIST post-quantum competition (Finalists + Alternate Candidates):

Lattices	4 encryption	2 signature	
Codes	3 encryption		
Multivariate		2 signature	
Isogenies	1 encryption		compact keys poor efficiency
Hash-based		1 signature	
MPC		1 signature	

Many more isogeny-based protocols since then....

Signatures maybe?

Isogeny-based Signatures

Generic Isogeny feature: compact keys (unless specific tradeoffs).

Isogeny-based Signatures

Generic Isogeny feature: compact keys (unless specific tradeoffs).

- [Yoo+17] Digital Signature: Based on SIDH,
  Multiple rounds $\Rightarrow$ long sig, slow.

Yoo et al. "A post-quantum digital signature scheme based on supersingular isogenies"

Isogeny-based Signatures

Generic Isogeny feature: compact keys (unless specific tradeoffs).

- [Yoo+17] Digital Signature: Based on SIDH,
  Multiple rounds $\Rightarrow$ long sig, slow.
- [GPS17] GPS signature: Based on quaternions $\Rightarrow$ weaker assumption,
  Multiple rounds $\Rightarrow$ long sig, no implem.

Galbraith, Petit, and Silva "Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems"

Isogeny-based Signatures

Generic Isogeny feature: compact keys (unless specific tradeoffs).

- [Yoo+17] Digital Signature: Based on SIDH,
  Multiple rounds $\Rightarrow$ long sig, slow.
- [GPS17] GPS signature: Based on quaternions $\Rightarrow$ weaker assumption,
  Multiple rounds $\Rightarrow$ long sig, no implem.
- [DG19] SeaSign: Based on CSIDH,
  Multiple rounds $\Rightarrow$ slow, size tradeoffs.

De Feo and Galbraith "SeaSign: Compact isogeny signatures from class group actions"

Isogeny-based Signatures

Generic Isogeny feature: compact keys (unless specific tradeoffs).

- [Yoo+17] Digital Signature: Based on SIDH,
  Multiple rounds $\Rightarrow$ long sig, slow.
- [GPS17] GPS signature: Based on quaternions $\Rightarrow$ weaker assumption,
  Multiple rounds $\Rightarrow$ long sig, no implem.
- [DG19] SeaSign: Based on CSIDH,
  Multiple rounds $\Rightarrow$ slow, size tradeoffs.
- [BKV19] CSI-FiSh: Based on CSIDH + precomp. $\Rightarrow$ bad scaling,
  similar to SeaSign with improved efficiency and sizes.

Beullens, Kleinjung, and Vercauteren "CSI-FiSh: Efficient isogeny based signatures through class group computations"

SQISign: Short Quaternion Isogeny Signature

Signature from one round, high soundness identification protocol based on proof of knowledge of endomorphism ring.

SQISign: Short Quaternion Isogeny Signature

Signature from one round, high soundness identification protocol based on proof of knowledge of endomorphism ring.

Most compact PQ signature scheme: PK + Signature combined $5\times$ **smaller** than Falcon (most compact NIST Round 3 candidate).

SQISign: Short Quaternion Isogeny Signature

Signature from one round, high soundness identification protocol based on proof of knowledge of endomorphism ring.

Most compact PQ signature scheme: PK + Signature combined $5\times$ **smaller** than Falcon (most compact NIST Round 3 candidate).

Secret Key (bytes)	Public Key (bytes)	Signature (bytes)	Security
16	64	204	NIST-1

SQISign: Short Quaternion Isogeny Signature

Signature from one round, high soundness identification protocol based on proof of knowledge of endomorphism ring.

Most compact PQ signature scheme: PK + Signature combined 5$\times$ **smaller** than Falcon (most compact NIST Round 3 candidate).

Secret Key (bytes)	Public Key (bytes)	Signature (bytes)	Security
16	64	204	NIST-1

Efficient *verification* and reasonably efficient *signature*.

SQISign: Short Quaternion Isogeny Signature

Signature from one round, high soundness identification protocol based on proof of knowledge of endomorphism ring.

Most compact PQ signature scheme: PK + Signature combined $5\times$ **smaller** than Falcon (most compact NIST Round 3 candidate).

Secret Key (bytes)	Public Key (bytes)	Signature (bytes)	Security
16	64	204	NIST-1

Efficient *verification* and reasonably efficient *signature*.

	Keygen	Sign	Verify
ms	575	2,279	42

SQISign: Short Quaternion Isogeny Signature

Signature from one round, high soundness identification protocol based on proof of knowledge of endomorphism ring.

Most compact PQ signature scheme: PK + Signature combined 5$\times$ **smaller** than Falcon (most compact NIST Round 3 candidate).

Secret Key (bytes)	Public Key (bytes)	Signature (bytes)	Security
16	64	204	NIST-1

Efficient *verification* and reasonably efficient *signature*.

	Keygen	Sign	Verify
ms	575	2,279	42

New security assumption.

Isogeny-based Cryptography

Elliptic curve and Isogeny notations

Elliptic Curve over $\mathbb{F}_q$:

$$y^2 = x^3 + ax + b$$

Elliptic curve and Isogeny notations

Elliptic Curve over $\mathbb{F}_q$:

$$y^2 = x^3 + ax + b$$

$E(\mathbb{F}_q)$ is an *additive* group.

Elliptic curve and Isogeny notations

Elliptic Curve over $\mathbb{F}_q$:

$$y^2 = x^3 + ax + b$$

$E(\mathbb{F}_q)$ is an *additive* group. *Scalar multiplication* $[n]$ is the analog of exponentiation in this group.

Elliptic curve and Isogeny notations

Elliptic Curve over $\mathbb{F}_q$:

$$y^2 = x^3 + ax + b$$

$E(\mathbb{F}_q)$ is an *additive* group. *Scalar multiplication* $[n]$ is the analog of exponentiation in this group.

Separable isogeny:

$$\varphi : E \to F$$

Elliptic curve and Isogeny notations

Elliptic Curve over $\mathbb{F}_q$:

$$y^2 = x^3 + ax + b$$

$E(\mathbb{F}_q)$ is an *additive* group. *Scalar multiplication* $[n]$ is the analog of exponentiation in this group.

Separable isogeny:

$$\varphi : E \to F$$

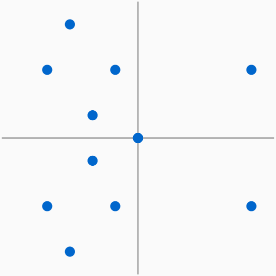
The **degree** is $\deg(\varphi) = \# \ker(\varphi)$.

The **dual** isogeny $\hat{\varphi} : F \to E$

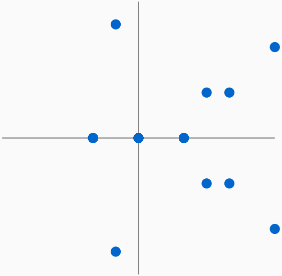
$$\hat{\varphi} \circ \varphi = [\deg(\varphi)]_E$$

Isogenies: an example over $\mathbb{F}_{11}$

$E : y^2 = x^3 + x$

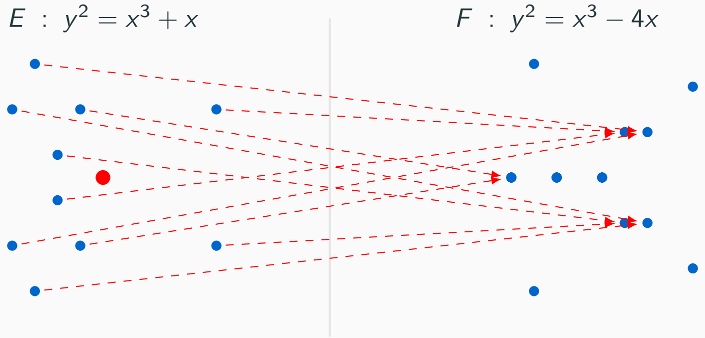


$F : y^2 = x^3 - 4x$



$$\varphi(x, y) = \left(\frac{x^2+1}{x}, \quad y\frac{x^2-1}{x^2}\right)$$

Isogenies: an example over $\mathbb{F}_{11}$



$$\varphi(x, y) = \left(\frac{x^2+1}{x},\quad y\frac{x^2-1}{x^2}\right)$$

- Kernel generator in red.
- This is a degree 2 map.
- Analogous to $x \mapsto x^2$ in $\mathbb{F}_q^*$.

Endomorphism ring

An *isogeny* $\varphi : E \to E$ is an **endomorphism**. $\mathrm{End}(E)$ is a ring with *addition* and *composition*.

Endomorphism ring

An *isogeny* $\varphi : E \to E$ is an **endomorphism**. $\mathrm{End}(E)$ is a ring with *addition* and *composition*.

Examples: $[n]$ for $n \in \mathbb{Z}$,

Endomorphism ring

An *isogeny* $\varphi : E \to E$ is an **endomorphism**. $\mathrm{End}(E)$ is a ring with *addition* and *composition*.

Examples: $[n]$ for $n \in \mathbb{Z}$, Frobenius over $\mathbb{F}_p$ i.e $\pi : (x, y) \to (x^p, y^p)$

Endomorphism ring

An *isogeny* $\varphi : E \to E$ is an **endomorphism**. $\mathrm{End}(E)$ is a ring with *addition* and *composition*.

Examples: $[n]$ for $n \in \mathbb{Z}$, Frobenius over $\mathbb{F}_p$ i.e $\pi : (x, y) \to (x^p, y^p)$

$E(\mathbb{F}_q)$:

- **Ordinary** when $\mathrm{End}(E)$ is an *order* of a quadratic imaginary field.

Endomorphism ring

An *isogeny* $\varphi : E \to E$ is an **endomorphism**. End(E) is a ring with *addition* and *composition*.

Examples: $[n]$ for $n \in \mathbb{Z}$, Frobenius over $\mathbb{F}_p$ i.e $\pi : (x, y) \to (x^p, y^p)$

$E(\mathbb{F}_q)$:

- **Ordinary** when End(E) is an *order* of a quadratic imaginary field.
- **Supersingular** when End(E) is a maximal *order* of a quaternion algebra.

Endomorphism ring

An *isogeny* $\varphi : E \to E$ is an **endomorphism**. $\mathrm{End}(E)$ is a ring with *addition* and *composition*.

Examples: $[n]$ for $n \in \mathbb{Z}$, Frobenius over $\mathbb{F}_p$ i.e $\pi : (x, y) \to (x^p, y^p)$

$E(\mathbb{F}_q)$:

- **Ordinary** when $\mathrm{End}(E)$ is an *order* of a quadratic imaginary field.
- **Supersingular** when $\mathrm{End}(E)$ is a maximal *order* of a quaternion algebra.

This talk $\to$ supersingular curves.

Key exchange betw. Alice and Bob.

Jao and De Feo "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies"

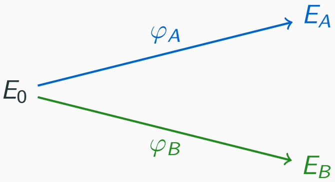
Supersingular Isogeny Diffie Hellman

Key exchange betw. Alice and Bob. Deg. N_A, N_B with $N_A \wedge N_B = 1$.

Jao and De Feo "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies"

Supersingular Isogeny Diffie Hellman

Key exchange betw. Alice and Bob. Deg. N_A, N_B with $N_A \wedge N_B = 1$.



Jao and De Feo "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies"

Key exchange betw. Alice and Bob. Deg. N_A, N_B with $N_A \wedge N_B = 1$.

$$
\begin{tikzcd}
 & E_A \arrow[r, "{[\varphi_A]_*\varphi_B}"] & {} \\
E_0 \arrow[ur, "\varphi_A"] \arrow[dr, "\varphi_B"'] & & \\
 & E_B \arrow[r, "{[\varphi_B]_*\varphi_A}"'] & {}
\end{tikzcd}
$$

Push-forward kernel $\ker([\varphi]_*\psi) = \varphi(\ker\psi)$.

Jao and De Feo "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies"

Supersingular Isogeny Diffie Hellman

Key exchange betw. Alice and Bob. Deg. N_A, N_B with $N_A \wedge N_B = 1$.

$$\begin{tikzcd}
 & E_A \arrow[r, "{[\varphi_A]_*\varphi_B}"] & E_{AB} \arrow[d, phantom, "\simeq"] \\
E_0 \arrow[ur, "\varphi_A"] \arrow[dr, "\varphi_B"'] & & E_{BA} \\
 & E_B \arrow[ur, "{[\varphi_B]_*\varphi_A}"'] &
\end{tikzcd}$$

Push-forward kernel $\ker([\varphi]_*\psi) = \varphi(\ker\psi)$.

Jao and De Feo "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies"

Supersingular Isogeny Diffie Hellman

Key exchange betw. Alice and Bob. Deg. N_A, N_B with $N_A \wedge N_B = 1$.

$$
\begin{tikzcd}
 & E_A \arrow[r, "{[\varphi_A]_*\varphi_B}"] & E_{AB} \arrow[d, phantom, "\simeq"] \\
E_0 \arrow[ur, "\varphi_A"] \arrow[dr, "\varphi_B"'] & & E_{BA} \\
 & E_B \arrow[ur, "{[\varphi_B]_*\varphi_A}"'] &
\end{tikzcd}
$$

Push-forward kernel $\ker([\varphi]_*\psi) = \varphi(\ker\psi)$.

Efficient when N_A, N_B are *smooth*.

Jao and De Feo "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies"

Supersingular Isogeny Problem

The underlying *security problem*:

Supersingular ℓ-Isogeny Problem: Given a prime p and two supersingular curves E_1 and E_2 over $\mathbb{F}_{p^2}$, compute an ℓ^e-isogeny $\varphi : E_1 \rightarrow E_2$.

Supersingular Isogeny Problem

The underlying *security problem*:

Supersingular ℓ-Isogeny Problem: Given a prime p and two supersingular curves E_1 and E_2 over $\mathbb{F}_{p^2}$, compute an ℓ^e-isogeny $\varphi : E_1 \to E_2$.

E_1 $\qquad\qquad$ E_2

Supersingular Isogeny Problem

The underlying *security problem*:

Supersingular ℓ-Isogeny Problem: Given a prime p and two supersingular curves E_1 and E_2 over $\mathbb{F}_{p^2}$, compute an ℓ^e-isogeny $\varphi : E_1 \to E_2$.

$$E_1 \xrightarrow{\quad\quad\varphi\quad\quad} E_2$$

The Deuring Correspondence

Quaternion Algebra, Orders and Ideals

The **Quaternion algebra** $H(a, b)$ is

$$H(a, b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q} \text{ with } i^2 = a, j^2 = b$$

[1]similary for the **right order** $\mathcal{O}_R(I)$

Quaternion Algebra, Orders and Ideals

The **Quaternion algebra** $H(a, b)$ is

$$H(a, b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q} \text{ with } i^2 = a, j^2 = b$$

Fractional ideals are $\mathbb{Z}$-lattices of rank 4 inside $H(a, b)$

$$I = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$$

The **Reduced norm** $n(I) = \{\gcd(n(\alpha)), \alpha \in I\}$

[1]similary for the **right order** $\mathcal{O}_R(I)$

Quaternion Algebra, Orders and Ideals

The **Quaternion algebra** $H(a, b)$ is

$$H(a, b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q} \text{ with } i^2 = a, j^2 = b$$

Fractional ideals are $\mathbb{Z}$-lattices of rank 4 inside $H(a, b)$

$$I = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$$

The **Reduced norm** $n(I) = \{\mathrm{gcd}(n(\alpha)), \alpha \in I\}$

An **order** $\mathcal{O}$ is an *ideal* which is also a ring, it is **maximal** when not contained in another order.

[1] similary for the **right order** $\mathcal{O}_R(I)$

Quaternion Algebra, Orders and Ideals

The **Quaternion algebra** $H(a, b)$ is

$$H(a, b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q} \text{ with } i^2 = a, j^2 = b$$

Fractional ideals are $\mathbb{Z}$-lattices of rank 4 inside $H(a, b)$

$$I = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$$

The **Reduced norm** $n(I) = \{\gcd(n(\alpha)), \alpha \in I\}$

An **order** $\mathcal{O}$ is an *ideal* which is also a ring, it is **maximal** when not contained in another order.

The (maximal) **left order**[1] $\mathcal{O}_L(I)$ of an *ideal* is

$$\mathcal{O}_L(I) = \{\alpha \in H(a, b), \alpha I \subset I\}$$

[1] similary for the **right order** $\mathcal{O}_R(I)$

The Deuring Correspondence

$\mathcal{A}_p$: quaternion algebra depending only on p.

Supersingular elliptic curves over $\mathbb{F}_{p^2}$ E	Maximal Orders in $\mathcal{A}_p$ $\mathcal{O} \cong \mathrm{End}(E)$
Isogeny with $\varphi : E \to E_1$	Ideal I_φ left $\mathcal{O}$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

The Deuring Correspondence

$\mathcal{A}_p$: quaternion algebra depending only on p.

Supersingular elliptic curves over $\mathbb{F}_{p^2}$ E	Maximal Orders in $\mathcal{A}_p$ $\mathcal{O} \cong \mathrm{End}(E)$
Isogeny with $\varphi : E \to E_1$	Ideal I_φ left $\mathcal{O}$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

Example : $p \equiv 3 \mod 4$, $\mathcal{A}_p = \mathbb{Q}(\sqrt{-1}, \sqrt{-p})$.

The Deuring Correspondence

$\mathcal{A}_p$: quaternion algebra depending only on p.

Supersingular elliptic curves over $\mathbb{F}_{p^2}$ E	Maximal Orders in $\mathcal{A}_p$ $\mathcal{O} \cong \mathrm{End}(E)$
Isogeny with $\varphi : E \to E_1$	Ideal I_φ left $\mathcal{O}$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

Example : $p \equiv 3 \mod 4$, $\mathcal{A}_p = \mathbb{Q}(\sqrt{-1}, \sqrt{-p})$.

$$E_0 : y^2 = x^3 + x$$

$$\mathrm{End}(E_0) = \langle 1, \iota, \frac{\iota + \pi}{2}, \frac{1 + \iota\pi}{2} \rangle \cong \langle 1, \sqrt{-1}, \frac{\sqrt{-1} + \sqrt{-p}}{2}, \frac{1 + \sqrt{-1}\sqrt{-p}}{2} \rangle$$

$\mathcal{A}_p$: quaternion algebra depending only on p.

Supersingular elliptic curves over $\mathbb{F}_{p^2}$ E	Maximal Orders in $\mathcal{A}_p$ $\mathcal{O} \cong \mathrm{End}(E)$
Isogeny with $\varphi : E \to E_1$	Ideal I_φ left $\mathcal{O}$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

Example : $p \equiv 3 \mod 4$, $\mathcal{A}_p = \mathbb{Q}(\sqrt{-1}, \sqrt{-p})$.

$$E_0 : y^2 = x^3 + x$$

$$\mathrm{End}(E_0) = \langle 1, \iota, \frac{\iota + \pi}{2}, \frac{1 + \iota\pi}{2} \rangle \cong \langle 1, \sqrt{-1}, \frac{\sqrt{-1} + \sqrt{-p}}{2}, \frac{1 + \sqrt{-1}\sqrt{-p}}{2} \rangle$$

$\pi : (x, y) \mapsto (x^p, y^p)$ is the Frobenius morphism with $\pi \circ \pi = [-p]$.

The Deuring Correspondence

$\mathcal{A}_p$: quaternion algebra depending only on p.

Supersingular elliptic curves over $\mathbb{F}_{p^2}$ E	Maximal Orders in $\mathcal{A}_p$ $\mathcal{O} \cong \mathrm{End}(E)$
Isogeny with $\varphi : E \to E_1$	Ideal I_φ left $\mathcal{O}$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

Example : $p \equiv 3 \mod 4$, $\mathcal{A}_p = \mathbb{Q}(\sqrt{-1}, \sqrt{-p})$.

$$E_0 : y^2 = x^3 + x$$

$$\mathrm{End}(E_0) = \langle 1, \iota, \frac{\iota + \pi}{2}, \frac{1 + \iota\pi}{2} \rangle \cong \langle 1, \sqrt{-1}, \frac{\sqrt{-1} + \sqrt{-p}}{2}, \frac{1 + \sqrt{-1}\sqrt{-p}}{2} \rangle$$

$\pi : (x, y) \mapsto (x^p, y^p)$ is the Frobenius morphism with $\pi \circ \pi = [-p]$.

$\iota : (x, y) \mapsto (-x, \sqrt{-1}y)$ is a twisting automorphism with $\iota \circ \iota = [-1]$.

A new security problem?

Supersingular ℓ-Isogeny Problem: Given a prime p and two supersingular curves E_1 and E_2 over $\mathbb{F}_{p^2}$, compute an ℓ^e-isogeny $\varphi : E_1 \to E_2$.

A new security problem?

Supersingular ℓ-Isogeny Problem: Given a prime p and two supersingular curves E_1 and E_2 over $\mathbb{F}_{p^2}$, compute an ℓ^e-isogeny $\varphi : E_1 \to E_2$.

$$\Updownarrow$$

Quaternion ℓ-Isogeny Path Problem: Given a prime number p, two maximal orders $\mathcal{O}_1, \mathcal{O}_2$ of $\mathcal{A}_p$, find an ideal J of norm ℓ^e with left order $\mathcal{O}_1$ and right order $\mathcal{O}_2$.

A new security problem?

Supersingular ℓ-Isogeny Problem: Given a prime p and two supersingular curves E_1 and E_2 over $\mathbb{F}_{p^2}$, compute an ℓ^e-isogeny $\varphi : E_1 \to E_2$.

$$\Updownarrow$$

Quaternion ℓ-Isogeny Path Problem: Given a prime number p, two maximal orders $\mathcal{O}_1, \mathcal{O}_2$ of $\mathcal{A}_p$, find an ideal J of norm ℓ^e with left order $\mathcal{O}_1$ and right order $\mathcal{O}_2$.

[Koh+14]: *heuristic polynomial* time algorithm `KLPT` for quaternion path problem.

Kohel et al. "On the quaternion ℓ-isogeny path problem"

Algorithmic summary of effective Deuring Correspondence

Problems with ✗ are hard, ✓ are easy. All ✓ are obtained using KLPT in [Eis+18].

Eisenträger et al. "Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions"

Algorithmic summary of effective Deuring Correspondence

Problems with ✗ are hard, ✓ are easy. All ✓ are obtained using KLPT in [Eis+18].

$$E_1, E_2 \to \varphi \qquad \qquad \mathcal{O}_1, \mathcal{O}_2 \to I$$

Eisenträger et al. "Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions"

Algorithmic summary of effective Deuring Correspondence

Problems with ✗ are hard, ✓ are easy. All ✓ are obtained using KLPT in [Eis+18].

$E_1, E_2 \to \varphi$ ✗ $\qquad$ $\mathcal{O}_1, \mathcal{O}_2 \to I$ ✓

Eisenträger et al. "Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions"

Algorithmic summary of effective Deuring Correspondence

Problems with ✗ are hard, ✓ are easy. All ✓ are obtained using KLPT in [Eis+18].

$$E \to \mathcal{O} \qquad\qquad \mathcal{O} \to E$$

$$E_1, E_2 \to \varphi \quad ✗ \qquad\qquad \mathcal{O}_1, \mathcal{O}_2 \to I \quad ✓$$

Endomorphism Ring Problem: Given a *supersingular elliptic curve* E over $\mathbb{F}_{p^2}$, compute its endomorphism ring.

Eisenträger et al. "Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions"

Algorithmic summary of effective Deuring Correspondence

Problems with ✗ are hard, ✓ are easy. All ✓ are obtained using KLPT in [Eis+18].

$$E \to \mathcal{O} \qquad\qquad \mathcal{O} \to E$$

$$\varphi \to I_\varphi \qquad\qquad I_\varphi \to \varphi$$

$$E_1, E_2 \to \varphi \quad ✗ \qquad\qquad \mathcal{O}_1, \mathcal{O}_2 \to I \quad ✓$$

Endomorphism Ring Problem: Given a *supersingular elliptic curve* E over $\mathbb{F}_{p^2}$, compute its endomorphism ring.

Eisenträger et al. "Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions"

Algorithmic summary of effective Deuring Correspondence

Problems with ✗ are hard, ✓ are easy. All ✓ are obtained using KLPT in [Eis+18].

$E \to \mathcal{O}$ ✗	$\mathcal{O} \to E$ ✓
$\varphi \to I_\varphi$ ✗	$I_\varphi \to \varphi$ ✓
$E_1, E_2 \to \varphi$ ✗	$\mathcal{O}_1, \mathcal{O}_2 \to I$ ✓

Endomorphism Ring Problem: Given a *supersingular elliptic curve* E over $\mathbb{F}_{p^2}$, compute its endomorphism ring.

Eisenträger et al. "Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions"

Proof of Knowledge of Endomorphism Ring

Quaternions for Proofs?

The knowledge of the endomorphism ring of a curve E lets us perform *powerful operations* otherwise impossible.

Quaternions for Proofs?

The knowledge of the endomorphism ring of a curve E lets us perform *powerful operations* otherwise impossible.

Use `KLPT` to prove knowledge of endomorphism ring?

Quaternions for Proofs?

The knowledge of the endomorphism ring of a curve E lets us perform *powerful operations* otherwise impossible.

Use `KLPT` to prove knowledge of endomorphism ring?

First attempt: GPS Signature in 2017, derived from 2-special sound *identification protocol*.

Quaternions for Proofs?

The knowledge of the endomorphism ring of a curve E lets us perform *powerful operations* otherwise impossible.

Use `KLPT` to prove knowledge of endomorphism ring?

First attempt: GPS Signature in 2017, derived from 2-special sound *identification protocol*.

SQISign contributions:

- A new generic `KLPT` algorithm to reach high soundness.
- New algorithmic tools to make the scheme **practical**.

Galbraith, Petit, and Silva "Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems"

GPS Identification Scheme

[GPS17]: A 2-special sound *identification* protocol.

GPS Identification Scheme

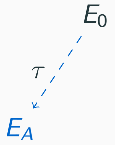
[GPS17]: A 2-special sound *identification* protocol.

Prover wants to *demonstrate knowledge* of $\mathrm{End}(E_A)$ for *public key* E_A.
E_0 is a **public** *special curve*.

GPS Identification Scheme

[GPS17]: A 2-special sound *identification* protocol.

Prover wants to *demonstrate knowledge* of $\mathrm{End}(E_A)$ for *public key* E_A.
E_0 is a **public** *special curve*.



- - - - - secret key isogeny

GPS Identification Scheme

[GPS17]: A 2-special sound *identification* protocol.

Prover wants to *demonstrate knowledge* of $\mathrm{End}(E_A)$ for *public key* E_A.
E_0 is a **public** *special curve*.

$$\begin{tikzcd}
 & E_0 \arrow[dl, dashed, "\tau"'] & \\
E_A \arrow[rr, "\sigma_0"] & & E
\end{tikzcd}$$

$\longrightarrow$ commitment isogeny (prover)

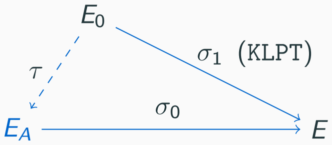
$- - - - -$ secret key isogeny

GPS Identification Scheme

[GPS17]: A 2-special sound *identification* protocol.

Prover wants to *demonstrate knowledge* of $\mathrm{End}(E_A)$ for *public key* E_A.

E_0 is a **public** *special curve*.



commitment isogeny (prover)

secret key isogeny

GPS Identification Scheme

[GPS17]: A 2-special sound *identification* protocol.

Prover wants to *demonstrate knowledge* of $\mathrm{End}(E_A)$ for *public key* E_A.

E_0 is a **public** *special curve*.

$$\begin{tikzcd} & E_0 \arrow[dl, dashed, "\tau"'] \arrow[dr, "\sigma_1\ (\texttt{KLPT})"] & \\ E_A \arrow[rr, "\sigma_0"] & & E \end{tikzcd}$$

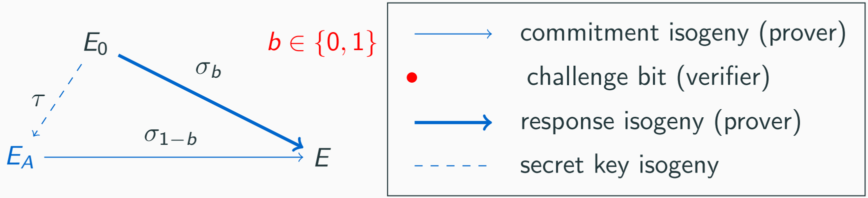
$b \in \{0, 1\}$

$\longrightarrow$	commitment isogeny (prover)
•	challenge bit (verifier)
- - - - -	secret key isogeny

GPS Identification Scheme

[GPS17]: A 2-special sound *identification* protocol.

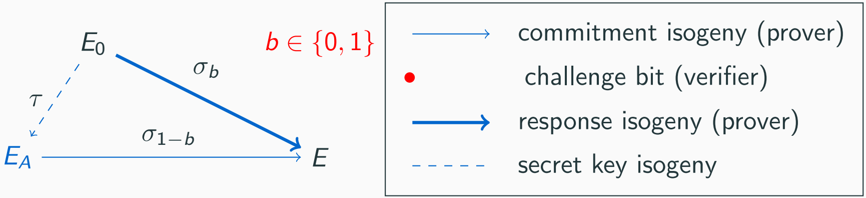
Prover wants to *demonstrate knowledge* of $\mathrm{End}(E_A)$ for *public key* E_A.
E_0 is a **public** *special curve*.



GPS Identification Scheme

[GPS17]: A 2-special sound *identification* protocol.

Prover wants to *demonstrate knowledge* of $\mathrm{End}(E_A)$ for *public key* E_A.
E_0 is a **public** *special curve*.



Repeat this λ times to reach 2^{λ}-bits of soundness.

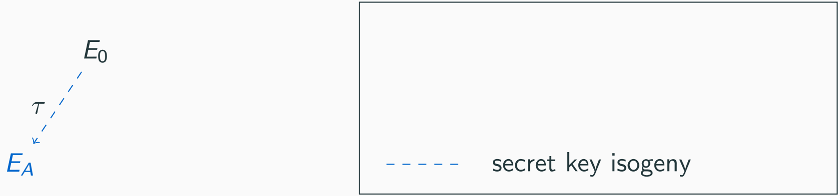
SQISign Identification Scheme

SQISign: A 2^λ-sound *identification* protocol.

SQISign Identification Scheme

SQISign: A 2^{λ}-sound *identification* protocol.

Prover wants to *demonstrate knowledge* of $\mathrm{End}(E_A)$ for *public key* E_A.
E_0 is a **public** *special curve*.



SQISign Identification Scheme

SQISign: A 2^λ-sound *identification* protocol.

Prover wants to *demonstrate knowledge* of $\mathrm{End}(E_A)$ for *public key* E_A.
E_0 is a **public** *special curve*.

$$\begin{tikzcd} & E_0 \arrow[rr, "\psi"] \arrow[dl, dashed, "\tau"'] & & E_1 \\ E_A & & & \end{tikzcd}$$

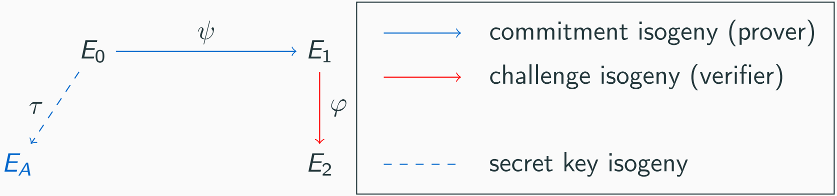
$\longrightarrow$ commitment isogeny (prover)

$- - - - -$ secret key isogeny

SQISign Identification Scheme

SQISign: A 2^{λ}-sound *identification* protocol.

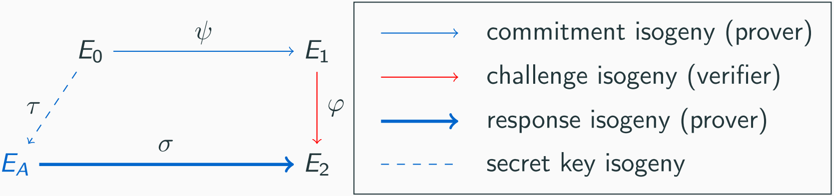
Prover wants to *demonstrate knowledge* of $\mathrm{End}(E_A)$ for *public key* E_A.
E_0 is a **public** *special curve*.



SQISign Identification Scheme

SQISign: A 2^λ-sound *identification* protocol.

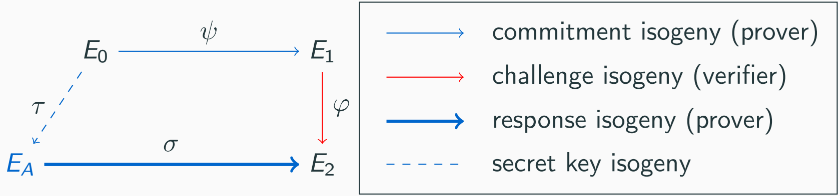
Prover wants to *demonstrate knowledge* of $\mathrm{End}(E_A)$ for *public key* E_A.
E_0 is a **public** *special curve*.



SQISign Identification Scheme

SQISign: A 2^λ-sound *identification* protocol.

Prover wants to *demonstrate knowledge* of $\mathrm{End}(E_A)$ for *public key* E_A.
E_0 is a **public** *special curve*.

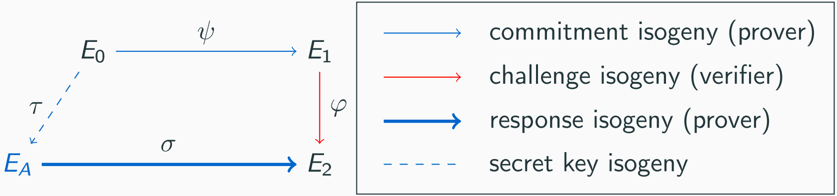


Soundness: Probability of cheating without $\mathrm{End}(E_A)$: $O(\frac{1}{\deg \varphi})$.

SQISign Identification Scheme

SQISign: A 2^λ-sound *identification* protocol.

Prover wants to *demonstrate knowledge* of $\mathrm{End}(E_A)$ for *public key* E_A.
E_0 is a **public** *special curve*.



Soundness: Probability of cheating without $\mathrm{End}(E_A)$: $O(\frac{1}{\deg\varphi})$.
Zero-Knowledge: prove that σ is a random isogeny $\Rightarrow$ depends on the algorithm computing σ.

SQISign in Practice

Effective Deuring Correspondence: from Ideals to Isogenies

`SigningKLPT` computes an ideal. Translate into the isogeny σ.

Effective Deuring Correspondence: from Ideals to Isogenies

`SigningKLPT` computes an ideal. Translate into the isogeny σ.

[GPS17]: `IdealToIsogeny` $: J \mapsto \sigma$ polynomial alg. for degree D, domain E with $E[D]$ and action of $\mathrm{End}(E)$ on this set. No implementation!

Effective Deuring Correspondence: from Ideals to Isogenies

`SigningKLPT` computes an ideal. Translate into the isogeny σ.

[GPS17]: `IdealToIsogeny` $: J \mapsto \sigma$ polynomial alg. for degree D, domain E with $E[D]$ and action of $\mathrm{End}(E)$ on this set. No implementation!

We have $D \gg p^2$ and the kernel cannot be represented in $\mathbb{F}_{p^2}$.

Effective Deuring Correspondence: from Ideals to Isogenies

`SigningKLPT` computes an ideal. Translate into the isogeny σ.

[GPS17]: `IdealToIsogeny` : $J \mapsto \sigma$ polynomial alg. for degree D, domain E with $E[D]$ and action of $\mathrm{End}(E)$ on this set. No implementation!

We have $D \gg p^2$ and the kernel cannot be represented in $\mathbb{F}_{p^2}$. Two solutions:

- Take D powersmooth $\rightarrow$ $E[D]$ in $\sim$ small extension ([GPS17]).

Effective Deuring Correspondence: from Ideals to Isogenies

`SigningKLPT` computes an ideal. Translate into the isogeny σ.

[GPS17]: `IdealToIsogeny` : $J \mapsto \sigma$ polynomial alg. for degree D, domain E with $E[D]$ and action of $\mathrm{End}(E)$ on this set. No implementation!

We have $D \gg p^2$ and the kernel cannot be represented in $\mathbb{F}_{p^2}$. Two solutions:

- Take D powersmooth $\to E[D]$ in $\sim$ small extension ([GPS17]).
- Take $D = \ell^f$ and split σ in smaller isogenies of degree ℓ^e and apply `IdealToIsogeny` for each (**SQISign**).

New Pb: for generic E of known $\mathrm{End}(E)$, hard to evaluate $\mathrm{End}(E)$...

Choice of Parameters

For fast verification we take σ of degree 2^f, $f = O(\log_2(p))$.

Choice of Parameters

For fast verification we take σ of degree 2^f, $f = O(\log_2(p))$.

For efficient signature: need a prime p such that $p^2 - 1$ is divided by $2^e T$ with odd smooth T satisfying $T^2 \sim p^3$.

Choice of Parameters

For fast verification we take σ of degree 2^f, $f = O(\log_2(p))$.

For efficient signature: need a prime p such that $p^2 - 1$ is divided by $2^e T$ with odd smooth T satisfying $T^2 \sim p^3$.

We found a 256 bits prime p with $e = 33, f = 1000$ and 2^{13}-smooth integer of 395 bits:

$$
\begin{aligned}
T = \; & 5^{21} \cdot 7^2 \cdot 11 \cdot 31 \cdot 83 \cdot 107 \cdot 137 \cdot 751 \cdot 827 \cdot 3691 \cdot 4019 \cdot 6983 \\
& 3^{53} \cdot 43 \cdot 103 \cdot 109 \cdot 199 \cdot 227 \cdot 419 \cdot 491 \cdot 569 \cdot 631 \cdot 677 \cdot 857 \cdot 859 \\
& 883 \cdot 1019 \cdot 2713 \cdot 4283
\end{aligned}
$$

Choice of Parameters

For fast verification we take σ of degree 2^f, $f = O(\log_2(p))$.

For efficient signature: need a prime p such that $p^2 - 1$ is divided by $2^e T$ with odd smooth T satisfying $T^2 \sim p^3$.

We found a 256 bits prime p with $e = 33, f = 1000$ and 2^{13}-smooth integer of 395 bits:

$$\begin{aligned} T = \; & 5^{21} \cdot 7^2 \cdot 11 \cdot 31 \cdot 83 \cdot 107 \cdot 137 \cdot 751 \cdot 827 \cdot 3691 \cdot 4019 \cdot 6983 \\ & 3^{53} \cdot 43 \cdot 103 \cdot 109 \cdot 199 \cdot 227 \cdot 419 \cdot 491 \cdot 569 \cdot 631 \cdot 677 \cdot 857 \cdot 859 \\ & 883 \cdot 1019 \cdot 2713 \cdot 4283 \end{aligned}$$

Bottleneck of the signature: $\Theta(f/e)$ T-isogeny computations .

What now?

Conclusion and Important Problems

We introduced the most compact post-quantum signatures but efficiency is still order of magnitudes below the competitors. The underlying sigma protocol has zero-knowledge property relying on a new assumption.

Main future theoretical directions:

Conclusion and Important Problems

We introduced the most compact post-quantum signatures but efficiency is still order of magnitudes below the competitors. The underlying sigma protocol has zero-knowledge property relying on a new assumption.

Main future theoretical directions:

- Upgrade the implementation: lots of room for improvement.

Conclusion and Important Problems

We introduced the most compact post-quantum signatures but efficiency is still order of magnitudes below the competitors. The underlying sigma protocol has zero-knowledge property relying on a new assumption.

Main future theoretical directions:

- Upgrade the implementation: lots of room for improvement.
- Advance on the `KLPT` algorithm: either for efficiency or security.

Conclusion and Important Problems

We introduced the most compact post-quantum signatures but efficiency is still order of magnitudes below the competitors. The underlying sigma protocol has zero-knowledge property relying on a new assumption.

Main future theoretical directions:

- Upgrade the implementation: lots of room for improvement.
- Advance on the `KLPT` algorithm: either for efficiency or security.
- Better understanding of the current ZK assumption.

Conclusion and Important Problems

We introduced the most compact post-quantum signatures but efficiency is still order of magnitudes below the competitors. The underlying sigma protocol has zero-knowledge property relying on a new assumption.

Main future theoretical directions:

- Upgrade the implementation: lots of room for improvement.
- Advance on the `KLPT` algorithm: either for efficiency or security.
- Better understanding of the current ZK assumption.
- Find new algorithms for effective Deuring Correspondence.

Questions?

https://eprint.iacr.org/2020/1240