The Deuring Correspondence in isogeny-based cryptography: SQISign and new isogeny problems.

Antonin Leroux

International Workshop on Post-Quantum Cryptography, 11/12/2021

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

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 ⇒ long sig, slow.
- [GPS17] GPS signature: Based on quaternions ⇒ weaker assumption,
  Multiple rounds ⇒ long sig, no implem.
- [DG19] SeaSign: Based on CSIDH,
  Multiple rounds ⇒ 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:[1] one round, high soundness from Deuring Correspondence.

[1] "SQISign: Compact Post-Quantum Signatures from Isogenies and Quaternions", L. De Feo, D. Kohel, **A. Leroux**, C. Petit and B. Wesolowski, ASIACRYPT 2020

SQISign: Short Quaternion Isogeny Signature

Signature:[1] one round, high soundness from Deuring Correspondence.

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

[1] "SQISign: Compact Post-Quantum Signatures from Isogenies and Quaternions", L. De Feo, D. Kohel, **A. Leroux**, C. Petit and B. Wesolowski, ASIACRYPT 2020

SQISign: Short Quaternion Isogeny Signature

Signature:[1] one round, high soundness from Deuring Correspondence.

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

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

[1] "SQISign: Compact Post-Quantum Signatures from Isogenies and Quaternions", L. De Feo, D. Kohel, **A. Leroux**, C. Petit and B. Wesolowski, ASIACRYPT 2020

SQISign: Short Quaternion Isogeny Signature

Signature:[1] one round, high soundness from Deuring Correspondence.

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*.

[1] "SQISign: Compact Post-Quantum Signatures from Isogenies and Quaternions", L. De Feo, D. Kohel, **A. Leroux**, C. Petit and B. Wesolowski, ASIACRYPT 2020

SQISign: Short Quaternion Isogeny Signature

Signature:[1] one round, high soundness from Deuring Correspondence.

Most compact PQ signature scheme: PK + Signature combined 5× **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

[1] "SQISign: Compact Post-Quantum Signatures from Isogenies and Quaternions", L. De Feo, D. Kohel, **A. Leroux**, C. Petit and B. Wesolowski, ASIACRYPT 2020

SQISign: Short Quaternion Isogeny Signature

Signature:[1] one round, high soundness from Deuring Correspondence.
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.

[1] "SQISign: Compact Post-Quantum Signatures from Isogenies and Quaternions", L. De Feo, D. Kohel, **A. Leroux**, C. Petit and B. Wesolowski, ASIACRYPT 2020

The Deuring Correspondence

Quaternion Algebra, Orders and Ideals

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

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

[2] 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** $n(I) = \{\gcd(n(\alpha)), \alpha \in I\}$

[2] 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.

[2]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**[2] $\mathcal{O}_L(I)$ of an *ideal* is

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

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

The Deuring Correspondence

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 and right $\mathcal{O}_1$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

The Deuring Correspondence

Supersingular elliptic curves over $\mathbb{F}_{p^2}$ E	Maximal Orders in $\mathcal{A}_p$ $\mathcal{O} \cong \text{End}(E)$
Isogeny with $\varphi : E \to E_1$	Ideal I_φ left $\mathcal{O}$-ideal and right $\mathcal{O}_1$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

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

The Deuring Correspondence

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 and right $\mathcal{O}_1$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

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

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

$$\mathrm{End}(E_0) = \langle 1, \iota, \frac{\iota + \pi}{2}, \frac{1 + \iota\pi}{2} \rangle \cong \langle 1, i, \frac{i + j}{2}, \frac{1 + k}{2} \rangle$$

The Deuring Correspondence

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 and right $\mathcal{O}_1$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

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

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

$$\mathrm{End}(E_0) = \langle 1, \iota, \frac{\iota + \pi}{2}, \frac{1 + \iota\pi}{2} \rangle \cong \langle 1, i, \frac{i + j}{2}, \frac{1 + k}{2} \rangle$$

$\pi : (x, y) \mapsto (x^p, y^p)$ is the Frobenius

The Deuring Correspondence

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 and right $\mathcal{O}_1$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

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

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

$$\mathrm{End}(E_0) = \langle 1, \iota, \frac{\iota + \pi}{2}, \frac{1 + \iota\pi}{2} \rangle \cong \langle 1, i, \frac{i + j}{2}, \frac{1 + k}{2} \rangle$$

$\pi : (x, y) \mapsto (x^p, y^p)$ is the Frobenius

$\iota : (x, y) \mapsto (-x, \sqrt{-1}y)$ is the twisting automorphism of E_0.

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 $\varphi : E_1 \to E_2$ for $e \in \mathbb{N}^\star$.

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 $\varphi : E_1 \to E_2$ for $e \in \mathbb{N}^\star$.

$$\Updownarrow$$

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 for $e \in \mathbb{N}^\star$ with $\mathcal{O}_L(J) \cong \mathcal{O}_1$, $\mathcal{O}_R(J) \cong \mathcal{O}_2$.

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 $\varphi : E_1 \to E_2$ for $e \in \mathbb{N}^\star$.

$$\Updownarrow$$

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 for $e \in \mathbb{N}^\star$ with $\mathcal{O}_L(J) \cong \mathcal{O}_1$, $\mathcal{O}_R(J) \cong \mathcal{O}_2$.

[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.

Algorithmic summary of effective Deuring Correspondence

Problems with ✗ are hard, ✓ are easy. All ✓ are obtained using `KLPT`.

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

Algorithmic summary of effective Deuring Correspondence

Problems with ✗ are hard, ✓ are easy. All ✓ are obtained using `KLPT`.

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

[Eis+18; Wes22]: use `KLPT` to prove *polynomial* time reduction from supersingular ℓ-isogeny problem to :

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" and Wesolowski "The supersingular isogeny path and endomorphism ring problems are equivalent"

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*.

$$\begin{tikzcd} E_0 \arrow[d, dashed, "\tau"'] \\ E_A \end{tikzcd}$$

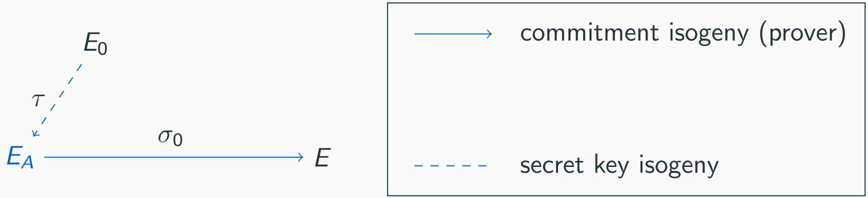
- - - - - secret key isogeny

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*.

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

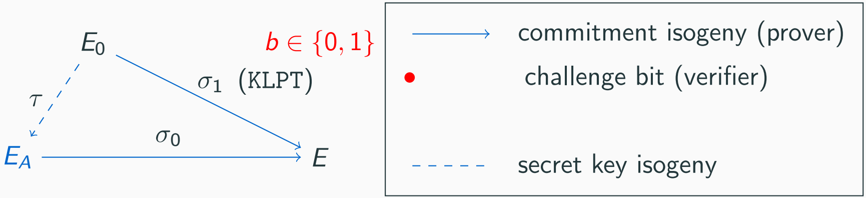
$\longrightarrow$	commitment isogeny (prover)
$\dashrightarrow$	secret key isogeny

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*.

$$\begin{tikzcd}
E_0 \arrow[d, dashed, "\tau"'] \arrow[dr, "\sigma_b"] & \\
E_A \arrow[r, "\sigma_{1-b}"'] & E
\end{tikzcd}$$

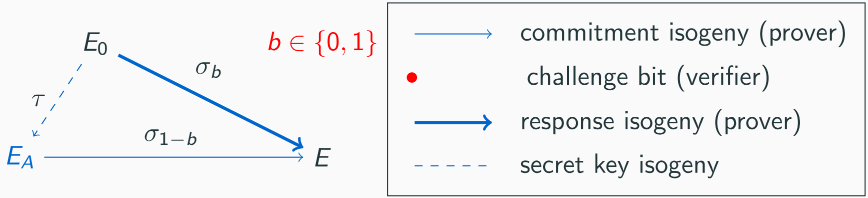
$b \in \{0, 1\}$

- commitment isogeny (prover)
- challenge bit (verifier)
- response 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*.



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

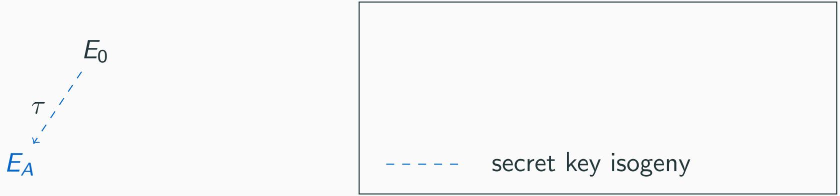
SQISign Identification Scheme

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*.

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

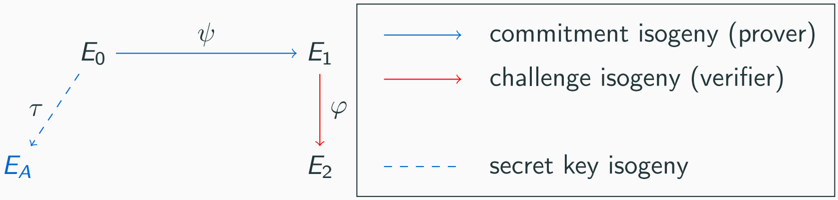
$\longrightarrow$ commitment isogeny (prover)

$- - - - -$ secret key isogeny

SQISign Identification Scheme

SQISign: A 2$^\lambda$-sound *identification* protocol.

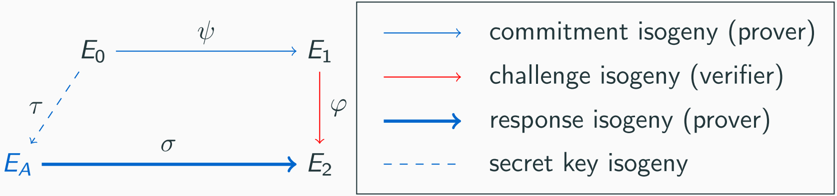
Prover wants to *demonstrate knowledge* of $\mathrm{End}(E_A)$ for *public key* E_A.
E_0 is a **public** *special curve*.



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*.

$$\begin{tikzcd}
E_0 \arrow[r, "\psi"] \arrow[d, dashed, "\tau"'] & E_1 \arrow[d, "\varphi"] \\
E_A \arrow[r, "\sigma"] & E_2
\end{tikzcd}$$

commitment isogeny (prover)

challenge isogeny (verifier)

response isogeny (prover)

secret key isogeny

Probability to cheat without knowledge of $\mathrm{End}(E_A)$: $O(\frac{1}{\deg \varphi})$.

Proving the Soundness

Soundness: Given *two* valid transcripts for *two* different challenges for the *same* commitment, some knowledge is revealed on the secret key.

Proving the Soundness

Soundness: Given *two* valid transcripts for *two* different challenges for the *same* commitment, some knowledge is revealed on the secret key.

$$\begin{tikzcd}
 & E_0 \arrow[rr, "\psi"] \arrow[dl, dashed, "\tau"'] & & E_1 \arrow[d, "\varphi"] \\
E_A \arrow[rrr, "\sigma"] & & & E_2
\end{tikzcd}$$

$\longrightarrow$ commitment isogeny (prover)

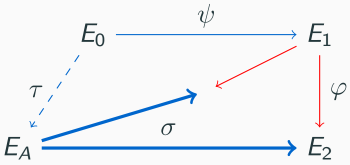
$\longrightarrow$ challenge isogeny (verifier)

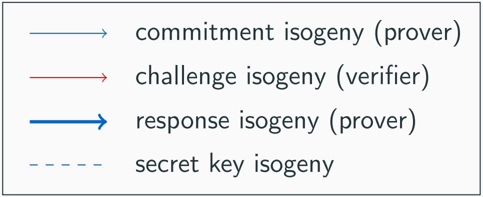
$\longrightarrow$ response isogeny (prover)

$- - - -$ secret key isogeny

Proving the Soundness

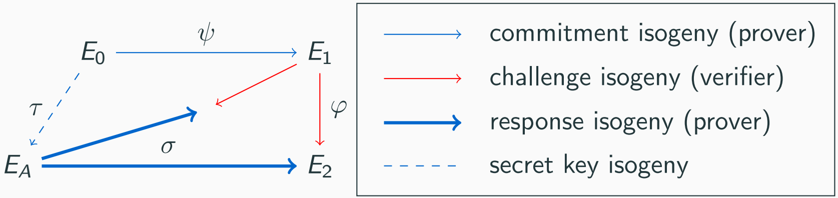
Soundness: Given *two* valid transcripts for *two* different challenges for the *same* commitment, some knowledge is revealed on the secret key.





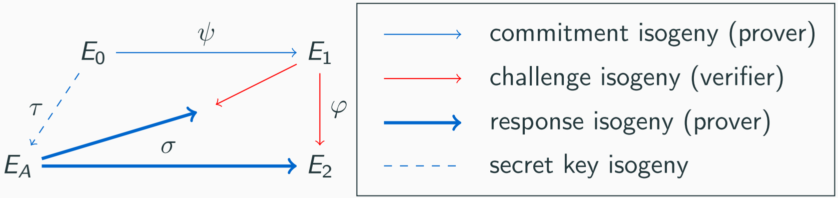
Proving the Soundness

Soundness: Given *two* valid transcripts for *two* different challenges for the *same* commitment, some knowledge is revealed on the secret key.



Smooth Endomorphism Problem: Given a *supersingular elliptic curve* E over $\mathbb{F}_{p^2}$, compute a non-trivial endomorphism $\theta \in End(E)$ of *smooth* norm.

Soundness: Given *two* valid transcripts for *two* different challenges for the *same* commitment, some knowledge is revealed on the secret key.



Smooth Endomorphism Problem: Given a *supersingular elliptic curve* E over $\mathbb{F}_{p^2}$, compute a non-trivial endomorphism $\theta \in End(E)$ of *smooth* norm.

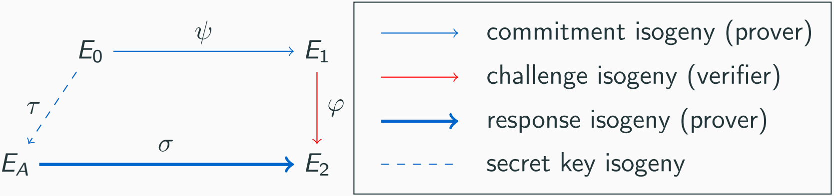
[Eis+18]: prove *heuristic polynomial* reduction to the **Endomorphism Ring Problem**.

The KLPT algorithm and the Zero-knowledge

Zero-Knowledge: It is possible to generate a transcript indistinguishable from a valid one with the *sole knowledge* of the public key.

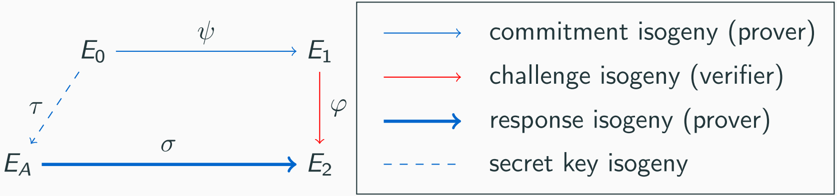
The KLPT algorithm and the Zero-knowledge

Zero-Knowledge: It is possible to generate a transcript indistinguishable from a valid one with the *sole knowledge* of the public key.



The KLPT algorithm and the Zero-knowledge

Zero-Knowledge: It is possible to generate a transcript indistinguishable from a valid one with the *sole knowledge* of the public key.



Show that σ is a random isogeny $\Rightarrow$ depends on the alg. to compute σ.

The KLPT algorithm and the Zero-knowledge

Zero-Knowledge: It is possible to generate a transcript indistinguishable from a valid one with the *sole knowledge* of the public key.

$$\begin{tikzcd} & E_0 \arrow[r, "\psi"] \arrow[dl, dashed, "\tau"'] & E_1 \arrow[d, "\varphi"] \\ E_A \arrow[rr, "\sigma"] & & E_2 \end{tikzcd}$$

$\longrightarrow$	commitment isogeny (prover)
$\longrightarrow$	challenge isogeny (verifier)
$\boldsymbol{\longrightarrow}$	response isogeny (prover)
$- - - - -$	secret key isogeny

Show that σ is a random isogeny $\Rightarrow$ depends on the alg. to compute σ.

Solution from [Koh+14]: σ reveal a path to E_0.

The KLPT algorithm and the Zero-knowledge

Zero-Knowledge: It is possible to generate a transcript indistinguishable from a valid one with the *sole knowledge* of the public key.

$$\begin{tikzcd} & E_0 \arrow[r, "\psi"] \arrow[dl, dashed, "\tau"'] & E_1 \arrow[d, "\varphi"] \\ E_A \arrow[rr, "\sigma"] & & E_2 \end{tikzcd}$$

- $\longrightarrow$ commitment isogeny (prover)
- $\longrightarrow$ challenge isogeny (verifier)
- $\boldsymbol{\longrightarrow}$ response isogeny (prover)
- $- - - - -$ secret key isogeny

Show that σ is a random isogeny $\Rightarrow$ depends on the alg. to compute σ.

Solution from [Koh+14]: σ reveal a path to E_0.

We propose a new `SigningKLPT` algorithm.

A New Security Assumption

Lemma: Fix D as σ's degree. There exists $\mathcal{P}_{\deg(\tau)}$ a set of isogenies of degree D such that:

A New Security Assumption

Lemma: Fix D as σ's degree. There exists $\mathcal{P}_{\mathsf{deg}(\tau)}$ a set of isogenies of degree D such that: `SigningKLPT` outputs an *uniform element* in $\{\rho, \rho = [\tau]_*\iota, \iota \in \mathcal{P}_{\mathsf{deg}(\tau)}\}$.

$$\begin{tikzcd}
 & E_0 \arrow[r, "\iota"] \arrow[dl, dashed, "\tau"'] & E_1 \\
E_A \arrow[r, "\sigma = [\tau]_*\iota"] & E_2 &
\end{tikzcd}$$

A New Security Assumption

Lemma: Fix D as σ's degree. There exists $\mathcal{P}_{\mathsf{deg}(\tau)}$ a set of isogenies of degree D such that: `SigningKLPT` outputs an *uniform element* in $\{\rho, \rho = [\tau]_*\iota, \iota \in \mathcal{P}_{\mathsf{deg}(\tau)}\}$.

$$
\begin{tikzcd}
 & E_0 \arrow[rr, "\iota"] \arrow[dl, dashed, "\tau"'] & & E_1 \\
E_A \arrow[rr, "\sigma = [\tau]_*\iota"] & & E_2 &
\end{tikzcd}
$$

ZK reduces to the distinguishing problem between:

1. σ is uniformly random isogeny of degree D;

A New Security Assumption

Lemma: Fix D as σ's degree. There exists $\mathcal{P}_{\mathsf{deg}(\tau)}$ a set of isogenies of degree D such that: `SigningKLPT` outputs an *uniform element* in $\{\rho, \rho = [\tau]_* \iota, \iota \in \mathcal{P}_{\mathsf{deg}(\tau)}\}$.

$$\begin{tikzcd}
& E_0 \arrow[r, "\iota"] \arrow[dl, dashed, "\tau"'] & E_1 \\
E_A \arrow[r, "\sigma = [\tau]_* \iota"] & E_2 &
\end{tikzcd}$$

ZK reduces to the distinguishing problem between:

1. σ is uniformly random isogeny of degree D;
2. σ is uniformly random in $[\tau]_* \mathcal{P}_{\mathsf{deg}(\tau)}$.

$\mathcal{P}_{\mathsf{deg}(\tau)}$ can be computed from $\deg(\tau)$ only and has exponential size.

The effective Deuring Correspondence: algorithmic challenges

From Ideals to Isogenies

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

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!

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 $\mathbb{F}_{p^2}$.

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]).

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 SQISign

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

Choice of Parameters for SQISign

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 SQISign

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 SQISign

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

GPS and SQISign are the first applications of constructive Deuring correspondence but there is still lot of room for improvements and new discoveries. Some follow-up work and future direction:

Conclusion and Important Problems

GPS and SQISign are the first applications of constructive Deuring correspondence but there is still lot of room for improvements and new discoveries. Some follow-up work and future direction:

- Improve the `KLPT` algorithm and ideal to isogeny translation mechanism.

Conclusion and Important Problems

GPS and SQISign are the first applications of constructive Deuring correspondence but there is still lot of room for improvements and new discoveries. Some follow-up work and future direction:

- Improve the `KLPT` algorithm and ideal to isogeny translation mechanism.
- Study the new ZK assumption.

Conclusion and Important Problems

GPS and SQISign are the first applications of constructive Deuring correspondence but there is still lot of room for improvements and new discoveries. Some follow-up work and future direction:

- Improve the `KLPT` algorithm and ideal to isogeny translation mechanism.
- Study the new ZK assumption.
- "SETA: Supersingular Encryption from Torsion Attacks", DDFK**L**PSW, ASIACRYPT 2021

Conclusion and Important Problems

GPS and SQISign are the first applications of constructive Deuring correspondence but there is still lot of room for improvements and new discoveries. Some follow-up work and future direction:

- Improve the `KLPT` algorithm and ideal to isogeny translation mechanism.
- Study the new ZK assumption.
- "SETA: Supersingular Encryption from Torsion Attacks", DDFK**L**PSW, ASIACRYPT 2021
- "A New Isogeny Representation and Applications to Cryptography", **L** (preprint).