A new algorithm for the effective Deuring correspondence: making SQISign faster.

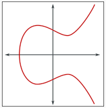
Antonin Leroux, joint work with Luca De Feo, Patrick Longa, Benjamin Wesolowski

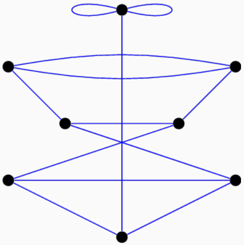
Isogeny Club, October 25, 2022

DGA, France

The Deuring correspondence

The supersingular 2-isogeny graph in char. p.

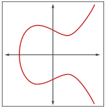




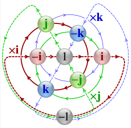
Credits to Luca De Feo and Cmglee

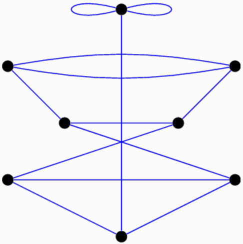
The Deuring correspondence

The supersingular 2-isogeny graph in char. p.



2-Ideal graph in quaternion algebra ramified at p and ∞.

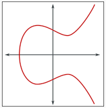




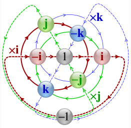
Credits to Luca De Feo and Cmglee

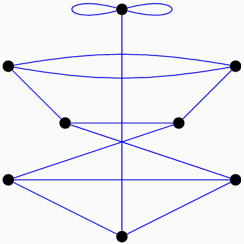
The Deuring correspondence

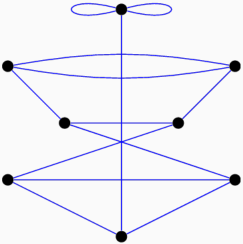
The supersingular 2-isogeny graph in char. p.



2-Ideal graph in quaternion algebra ramified at p and ∞.







Credits to Luca De Feo and Cmglee

The rest of this talk

The plan:

- Introduction to the Deuring correspondence
- Algorithmic aspects: theory.
- Algorithm aspects: practice, the ideal to isogeny translation.
- Application to SQISign.

Mathematical Background

Quaternion algebra definitions

The quaternion algebra $\mathcal{B}(a, b)$ over $\mathbb{Q}$ with $a, b \in \mathbb{Z}$ is

$$\mathcal{B}(a, b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = a$, $j^2 = b$ and $k = ij = -ji$.

Quaternion algebra definitions

The quaternion algebra $\mathcal{B}(a, b)$ over $\mathbb{Q}$ with $a, b \in \mathbb{Z}$ is

$$\mathcal{B}(a, b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = a$, $j^2 = b$ and $k = ij = -ji$.

An **order** $\mathcal{O}$ is a $\mathbb{Z}$-lattice of rank 4 inside $\mathcal{B}(a, b)$ which is also a ring, it is **maximal** when not contained in another order.

Quaternion algebra definitions

The quaternion algebra $\mathcal{B}(a, b)$ over $\mathbb{Q}$ with $a, b \in \mathbb{Z}$ is

$$\mathcal{B}(a, b) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$$

with $i^2 = a$, $j^2 = b$ and $k = ij = -ji$.

An **order** $\mathcal{O}$ is a $\mathbb{Z}$-lattice of rank 4 inside $\mathcal{B}(a, b)$ which is also a ring, it is **maximal** when not contained in another order.

Orders are rings: so we have ideals. In a non-commutative algebra, ideals have distinct left and right orders.

There is $n : \mathcal{B}(a, b) \to \mathbb{Q}$, and the norm is integral over orders, so we can define **ideal norm** as $\{\gcd(n(\alpha)), \alpha \in I\}$.

Elliptic curve and isogeny notations

Elliptic Curve over $\mathbb{F}_{p^k}$:

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_{p^k}$$

Elliptic curve and isogeny notations

Elliptic Curve over $\mathbb{F}_{p^k}$:

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_{p^k}$$

Isogeny: rational map between elliptic curves.

When separable, the **degree** is $\deg(\varphi) = \# \ker(\varphi)$.

Elliptic curve and isogeny notations

Elliptic Curve over $\mathbb{F}_{p^k}$:

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_{p^k}$$

Isogeny: rational map between elliptic curves.

When separable, the **degree** is $\deg(\varphi) = \# \ker(\varphi)$.

The Vélu formulas (1971) are used to compute an isogeny from its kernel.

Can make it efficient when $\deg \varphi$ is smooth by factoring the isogeny.

Elliptic curve and isogeny notations

Elliptic Curve over $\mathbb{F}_{p^k}$:

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_{p^k}$$

Isogeny: rational map between elliptic curves.

When separable, the **degree** is $\deg(\varphi) = \# \ker(\varphi)$.

The Vélu formulas (1971) are used to compute an isogeny from its kernel.

Can make it efficient when $\deg \varphi$ is smooth by factoring the isogeny.

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

Supersingular curves $\Leftrightarrow$ $\mathrm{End}(E)$ is a max. *order* in a quaternion algebra.

The Deuring Correspondence

p : prime characteristic, $\mathcal{B}(-q,-p)$ where $q > 0$ depends only on p.

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

The Deuring Correspondence

p : prime characteristic, $\mathcal{B}(-q,-p)$ where $q>0$ depends only on p.

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

Example: $p \equiv 3 \mod 4$, $q = 1$.

The Deuring Correspondence

p : prime characteristic, $\mathcal{B}(-q,-p)$ where $q > 0$ depends only on p.

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

Example: $p \equiv 3 \mod 4$, $q = 1$.

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

The Deuring Correspondence

p : prime characteristic, $\mathcal{B}(-q,-p)$ where $q>0$ depends only on p.

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

Example: $p \equiv 3 \mod 4$, $q = 1$.

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

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

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

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

Kernel ideals

Let $\varphi : E \to E'$ be an isogeny of degree D. The kernel ideal I_φ of I is defined as

$$I_\varphi = \{\alpha \in \mathrm{End}(E), \alpha(\ker \varphi) = 0\}.$$

Alternatively, we have

$$I_\varphi = \mathrm{Hom}(E', E)\varphi.$$

Kernel ideals

Let $\varphi : E \to E'$ be an isogeny of degree D. The kernel ideal I_φ of I is defined as

$$I_\varphi = \{\alpha \in \mathrm{End}(E), \alpha(\ker \varphi) = 0\}.$$

Alternatively, we have

$$I_\varphi = \mathrm{Hom}(E', E)\varphi.$$

Conversely, the kernel of an $\mathcal{O}$-ideal I (for $\mathcal{O} \cong \mathrm{End}(E)$)

$$E[I] = \{P, \alpha(P) = 0 \text{ for all } \alpha \in I\} = \bigcap_{\alpha \in I} \ker \alpha.$$

We define $\varphi_I : E \to E/E[I]$.

A new hard 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 $e \in \mathbb{N}^\star$.

Quaternion ℓ-Isogeny Path Problem: Given a prime number p, two maximal orders $\mathcal{O}_1, \mathcal{O}_2$ of $\mathcal{B}(-q, -p)$, 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 hard 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 $e \in \mathbb{N}^\star$.

Quaternion ℓ-Isogeny Path Problem: Given a prime number p, two maximal orders $\mathcal{O}_1, \mathcal{O}_2$ of $\mathcal{B}(-q, -p)$, find an ideal J of norm ℓ^e for $e \in \mathbb{N}^\star$ with $\mathcal{O}_L(J) \cong \mathcal{O}_1$, $\mathcal{O}_R(J) \cong \mathcal{O}_2$.

Kohel, Lauter, Petit, and Tignol (2014): heuristic *polynomial-time* algorithm `KLPT` for quaternion path problem.

Complexity proven under GRH by Wesolowski (2022).

A new hard 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 $e \in \mathbb{N}^\star$.

$\downarrow$ Endomorphism ring problem

Quaternion ℓ-Isogeny Path Problem: Given a prime number p, two maximal orders $\mathcal{O}_1, \mathcal{O}_2$ of $\mathcal{B}(-q,-p)$, find an ideal J of norm ℓ^e for $e \in \mathbb{N}^\star$ with $\mathcal{O}_L(J) \cong \mathcal{O}_1$, $\mathcal{O}_R(J) \cong \mathcal{O}_2$.

Kohel, Lauter, Petit, and Tignol (2014): heuristic *polynomial-time* algorithm `KLPT` for quaternion path problem.

Complexity proven under GRH by Wesolowski (2022).

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.

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

Algorithmic summary of effective Deuring Correspondence

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

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

Algorithmic summary of effective Deuring Correspondence

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

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

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

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

Algorithmic summary of effective Deuring Correspondence

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

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

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

Algorithmic summary of effective Deuring Correspondence

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

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

[EHLMP18; W22]: 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.

Ideal to isogeny: theory vs practice.

Ideal to isogeny translation

Input: A supersingular *curve* E, a *maximal order* $\mathcal{O}$ with $\mathcal{O} \cong \mathrm{End}(E)$, and an $\mathcal{O}$*-ideal* I of norm D (both given as 16 coefficients over $\mathcal{B}(-q,-p)$).

Output: The isogeny $\varphi_I : E \to E_I$.

Poly-time in theory when D is smooth...

Ideal to isogeny: theory vs practice.

Ideal to isogeny translation

Input: A supersingular *curve* E, a *maximal order* $\mathcal{O}$ with $\mathcal{O} \cong \mathrm{End}(E)$, and an $\mathcal{O}$-*ideal* I of norm D (both given as 16 coefficients over $\mathcal{B}(-q,-p)$).

Output: The isogeny $\varphi_I : E \to E_I$.

Poly-time in theory when D is smooth...

Motivation: make the computation efficient in practice for a big smooth degree D (application to SQISign).

Effective ideal to isogeny: the solution from Galbraith, Petit and Silva

Ideal to isogeny translation

Input: A supersingular *curve* E, a *maximal order* $\mathcal{O}$ with $\mathcal{O} \cong \mathrm{End}(E)$, and an $\mathcal{O}$-*ideal* I of norm D (both given as 16 coefficients over $\mathcal{B}(-q,-p)$).

Output: The isogeny $\varphi_I : E \to E_I$.

Effective ideal to isogeny: the solution from Galbraith, Petit and Silva

Ideal to isogeny translation

Input: A supersingular *curve* E, a *maximal order* $\mathcal{O}$ with $\mathcal{O} \cong \mathrm{End}(E)$, and an $\mathcal{O}$-*ideal* I of norm D (both given as 16 coefficients over $\mathcal{B}(-q, -p)$).

Output: The isogeny $\varphi_I : E \to E_I$.

An algorithm from Galbraith, Petit and Silva [GPS17]:

1. Evaluate the elements of $I \hookrightarrow \mathrm{End}(E)$ on the D-torsion.
2. Find the common kernel $E[I]$ (DLP computations)
3. Compute φ_I from $\ker \varphi_I = G$.

Complexity: polynomial in some nice cases...

Generalizing the approach

Ideal to isogeny translation

Input: A supersingular *curve* E, a *maximal order* $\mathcal{O}$ with $\mathcal{O} \cong \mathrm{End}(E)$, and an $\mathcal{O}$-*ideal* I of norm D (both given as 16 coefficients over $\mathcal{B}(-q, -p)$).

Output: The isogeny $\varphi_I : E \to E_I$.

Two main obstacles for an efficient generic solution:

1. The field of definition of the kernel might be very big.
2. No nice formula to evaluate the elements of $\mathrm{End}(E)$ when represented as elements in $\mathcal{B}(-q, -p)$ in general.

Generalizing the approach

Ideal to isogeny translation

Input: A supersingular *curve* E, a *maximal order* $\mathcal{O}$ with $\mathcal{O} \cong \mathrm{End}(E)$, and an $\mathcal{O}$-*ideal* I of norm D (both given as 16 coefficients over $\mathcal{B}(-q,-p)$).

Output: The isogeny $\varphi_I : E \to E_I$.

Two main obstacles for an efficient generic solution:

1. The field of definition of the kernel might be very big.
2. No nice formula to evaluate the elements of $\mathrm{End}(E)$ when represented as elements in $\mathcal{B}(-q,-p)$ in general.

For 1: Factor φ_I and apply the algorithm on the factor isogenies of small degrees. This means several intermediate curves: we really need to find a solution to 2.

For 2...

Evaluating the elements of an arbitrary endo. ring: a first approach

$\mathcal{O} \cong \mathsf{End}(E)$, a point $P \quad \rightarrow \quad \alpha(P)$ for some $\alpha \in \mathsf{End}(E)$.

[FK**L**PW20]: any $\alpha \in \mathsf{End}(E)$.

Idea: use a nice curve E_0 where we can evaluate endomorphisms.

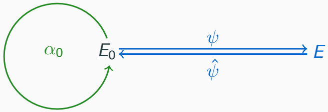
Evaluating the elements of an arbitrary endo. ring: a first approach

$\mathcal{O} \cong \mathrm{End}(E)$, a point $P \quad \rightarrow \quad \alpha(P)$ for some $\alpha \in \mathrm{End}(E)$.

[FK**L**PW20]: any $\alpha \in \mathrm{End}(E)$.

Idea: use a nice curve E_0 where we can evaluate endomorphisms.

$$\alpha = \frac{1}{[\deg \psi]} \psi \circ \alpha_0 \circ \hat{\psi}$$



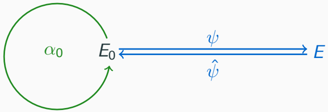
Evaluating the elements of an arbitrary endo. ring: a first approach

$\mathcal{O} \cong \mathrm{End}(E)$, a point P $\quad\rightarrow\quad$ $\alpha(P)$ for some $\alpha \in \mathrm{End}(E)$.

[FK**L**PW20]: any $\alpha \in \mathrm{End}(E)$.

Idea: use a nice curve E_0 where we can evaluate endomorphisms.

$$\alpha = \frac{1}{[\deg \psi]} \psi \circ \alpha_0 \circ \hat{\psi}$$



1. Compute $\psi : E_0 \rightarrow E$ with KLPT and the algorithm from [GPS17] (need $T = \deg \psi$ coprime to D!).
2. Express α from ψ and some $\alpha_0 \in \mathrm{End}(E_0)$ (lollipop endomorphism).
3. Evaluate ψ, α_0 to derive $\alpha(P)$.

Evaluating the elements of an arbitrary endo. ring: improvement.

$\mathcal{O} \cong \mathrm{End}(E)$, a point $P \quad \rightarrow \quad \alpha(P)$ for some $\alpha \in \mathrm{End}(E)$.

[F**L**LW22]: we can restrict to α of smooth norm T coprime with D.
Idea: if α is in the Eichler order $\mathrm{End}(E_0) \cap \mathrm{End}(E)$, we will first find the version of $\alpha \in \mathrm{End}(E_0)$ and then use an isogeny $\varphi : E_0 \rightarrow E$ to compute the version in $\mathrm{End}(E)$. If $n(\alpha)$ is coprime with D, φ can be the isogeny we are translating!

1. Compute $\alpha \in \mathcal{B}(-p, -q)$ of smooth norm in $\mathrm{End}(E_0) \cap \mathrm{End}(E)$.
2. Compute α as an isogeny in $\mathrm{End}(E_0)$ from its kernel.
3. Compute α as an isogeny in $\mathrm{End}(E)$ from its kernel with $\varphi : E_0 \rightarrow E$.
4. Evaluate $\alpha(P)$.

KLPT and generalizations

Goal of KLPT: find an ideal of smooth norm connecting two maximal orders $\mathcal{O}_1, \mathcal{O}_2$. Takes another connecting ideal I in input.

Goal of KLPT: find an ideal of smooth norm connecting two maximal orders $\mathcal{O}_1, \mathcal{O}_2$. Takes another connecting ideal I in input.

KLPT [KLPT14] $\Rightarrow$ resolution of norms equations in I.
Solutions of size $\approx p^2 N^2 = (p/N)pN^3$ where N is the norm of the smallest element in I. In general, we expect $N \approx \sqrt{p}$ and so we have a solution of size p^3.

Goal of KLPT: find an ideal of smooth norm connecting two maximal orders $\mathcal{O}_1, \mathcal{O}_2$. Takes another connecting ideal I in input.

KLPT [KLPT14] $\Rightarrow$ resolution of norms equations in I.
Solutions of size $\approx p^2 N^2 = (p/N)pN^3$ where N is the norm of the smallest element in I. In general, we expect $N \approx \sqrt{p}$ and so we have a solution of size p^3.

In [FK**L**PW20,F**L**LW22]: generalization of KLPT to Eichler orders of the form $\mathbb{Z} + I = \mathcal{O}_R(I) \cap \mathcal{O}_L(I)$.
Solutions of size $\approx pN^3 \approx p^{5/2}$.

KLPT and generalizations

Goal of KLPT: find an ideal of smooth norm connecting two maximal orders $\mathcal{O}_1, \mathcal{O}_2$. Takes another connecting ideal I in input.

KLPT [KLPT14] $\Rightarrow$ resolution of norms equations in I.
Solutions of size $\approx p^2 N^2 = (p/N)pN^3$ where N is the norm of the smallest element in I. In general, we expect $N \approx \sqrt{p}$ and so we have a solution of size p^3.

In [FK**L**PW20,F**L**LW22]: generalization of KLPT to Eichler orders of the form $\mathbb{Z} + I = \mathcal{O}_R(I) \cap \mathcal{O}_L(I)$.
Solutions of size $\approx pN^3 \approx p^{5/2}$.

The second algorithm is better because smaller torsion requirement.

A specific choice of parameters

In both cases, we need some $D' \mid D$ torsion and some powersmooth T-torsion defined over $\mathbb{F}_{p^2}$.

A specific choice of parameters

In both cases, we need some $D' \mid D$ torsion and some powersmooth T-torsion defined over $\mathbb{F}_{p^2}$.

Need a prime p with $TD' \mid p^2 - 1$ with $T \approx p^\beta$ for some $1 < \beta < 2$ (β is half the exponent in norm equation output sizes).

A specific choice of parameters

In both cases, we need some $D' \mid D$ torsion and some powersmooth T-torsion defined over $\mathbb{F}_{p^2}$.

Need a prime p with $TD' \mid p^2 - 1$ with $T \approx p^\beta$ for some $1 < \beta < 2$ (β is half the exponent in norm equation output sizes).

We sieve through families of primes where a portion of the torsion requirement is forced.

A smaller T helps a lot finding a good smoothness bound on T.

Example: p_{6983} vs p_{3923}

For algorithm 1 we have p_{6983}

$$\begin{aligned} p+1 &= 2^{33} \cdot 5^{21} \cdot 7^2 \cdot 11 \cdot 31 \cdot 83 \cdot 107 \cdot 137 \cdot 751 \cdot 827 \cdot 3691 \cdot 4019 \cdot 6983 \\ &\quad \cdot 517434778561 \cdot 26602537156291\,, \\ p-1 &= 2 \cdot 3^{53} \cdot 43 \cdot 103^2 \cdot 109 \cdot 199 \cdot 227 \cdot 419 \cdot 491 \cdot 569 \cdot 631 \cdot 677 \cdot 857 \cdot 859 \\ &\quad \cdot 883 \cdot 1019 \cdot 1171 \cdot 1879 \cdot 2713 \cdot 4283 \end{aligned}$$

For algorithm 2 we have p_{3923}

$$\begin{aligned} p+1 &= 2^{65} \cdot 5^2 \cdot 7 \cdot 11 \cdot 19 \cdot 29^2 \cdot 37^2 \cdot 47 \cdot 197 \cdot 263 \cdot 281 \cdot 461 \cdot 521 \\ &\quad \cdot 3923 \cdot 62731 \cdot 96362257 \cdot 3924006112952623\,, \\ p-1 &= 2 \cdot 3^{65} \cdot 13 \cdot 17 \cdot 43 \cdot 79 \cdot 157 \cdot 239 \cdot 271 \cdot 283 \cdot 307 \cdot 563 \cdot 599 \\ &\quad \cdot 607 \cdot 619 \cdot 743 \cdot 827 \cdot 941 \cdot 2357 \cdot 10069\,. \end{aligned}$$

SQISign Identification Scheme

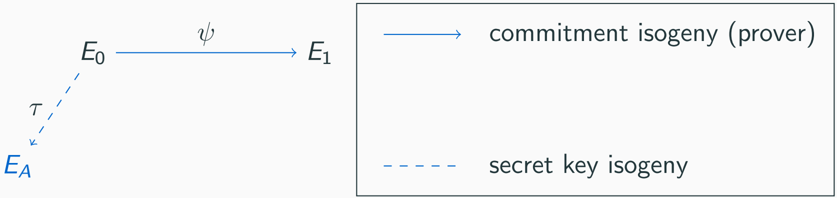
Main idea: public key is a curve E_A and secret key is $\text{End}(E_A)$. Proving knowledge of $\text{End}(E_A)$ by using KLPT to solve the isogeny problem.

SQISign Identification Scheme

Main idea: public key is a curve E_A and secret key is $\mathrm{End}(E_A)$. Proving knowledge of $\mathrm{End}(E_A)$ by using KLPT to solve the isogeny problem.

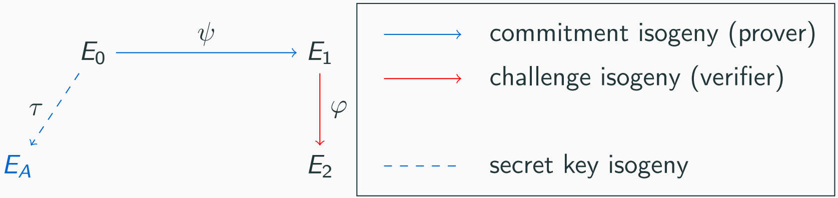
SQISign Identification Scheme

Main idea: public key is a curve E_A and secret key is $\mathrm{End}(E_A)$. Proving knowledge of $\mathrm{End}(E_A)$ by using KLPT to solve the isogeny problem.



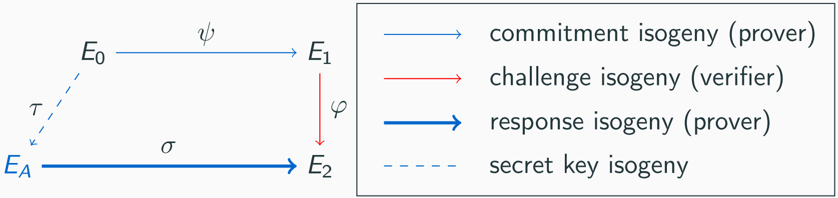
SQISign Identification Scheme

Main idea: public key is a curve E_A and secret key is $\mathrm{End}(E_A)$. Proving knowledge of $\mathrm{End}(E_A)$ by using `KLPT` to solve the isogeny problem.



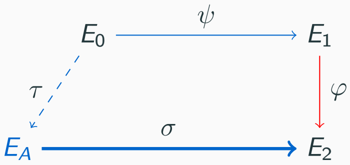
SQISign Identification Scheme

Main idea: public key is a curve E_A and secret key is $\mathrm{End}(E_A)$. Proving knowledge of $\mathrm{End}(E_A)$ by using `KLPT` to solve the isogeny problem.



SQISign Identification Scheme

Main idea: public key is a curve E_A and secret key is $\mathrm{End}(E_A)$. Proving knowledge of $\mathrm{End}(E_A)$ by using KLPT to solve the isogeny problem.



⟶ (thin blue)	commitment isogeny (prover)
⟶ (thin red)	challenge isogeny (verifier)
⟶ (thick blue)	response isogeny (prover)
- - - - -	secret key isogeny

Response computation:

1. Compute $\mathrm{End}(E_2)$ from ψ, φ.
2. Apply KLPT to compute I_σ connecting $\mathrm{End}(E_A)$ and $\mathrm{End}(E_2)$. For security, need generic version of the algorithm!
3. Translate I_σ into σ.

SQISign: Short Quaternion Isogeny Signature

Most compact PQ signature scheme with PK + Signature combined.

Name	Public Key (bytes)	Signature (bytes)	Security
SQISign	64	204	NIST-1
Falcon-512	897	666	NIST-1
Dilithium2	1312	2420	NIST-1

SQISign: Short Quaternion Isogeny Signature

Most compact PQ signature scheme with PK + Signature combined.

Name	Public Key (bytes)	Signature (bytes)	Security
SQISign	64	204	NIST-1
Falcon-512	897	666	NIST-1
Dilithium2	1312	2420	NIST-1

Implementation in C with recent finite field arithmetic from Patrick Longa: Efficient *verification* and reasonably efficient *signature* for isogenies. But $\approx 10^3$ times slower than Falcon or Dilithium.

SQISign: Short Quaternion Isogeny Signature

Most compact PQ signature scheme with PK + Signature combined.

Name	Public Key (bytes)	Signature (bytes)	Security
SQISign	64	204	NIST-1
Falcon-512	897	666	NIST-1
Dilithium2	1312	2420	NIST-1

Implementation in C with recent finite field arithmetic from Patrick Longa: Efficient *verification* and reasonably efficient *signature* for isogenies. But $\approx 10^3$ times slower than Falcon or Dilithium.

	Keygen	Sign	Verify	method	article
Mcycles	1823	7020	143	SQISign	[FK**L**PW20]
Mcycles	421	1987	30	New Id-to-Iso	[F**L**LW22]

Signature: $\approx 400ms$ Verification: $\approx 6ms$

SQISign: Short Quaternion Isogeny Signature

Most compact PQ signature scheme with PK + Signature combined.

Name	Public Key (bytes)	Signature (bytes)	Security
SQISign	64	204	NIST-1
Falcon-512	897	666	NIST-1
Dilithium2	1312	2420	NIST-1

Implementation in C with recent finite field arithmetic from Patrick Longa: Efficient *verification* and reasonably efficient *signature* for isogenies. But $\approx 10^3$ times slower than Falcon or Dilithium.

	Keygen	Sign	Verify	method	article
Mcycles	1823	7020	143	SQISign	[FK**L**PW20]
Mcycles	421	1987	30	New Id-to-Iso	[F**L**LW22]

Signature: $\approx 400ms$ Verification: $\approx 6ms$

Non-standard security assumption but safe from recent attacks!

Future work and open problems

Isogeny-based cryptography is not dead! It is an exciting time to work on isogenies and the Deuring correspondence.

Future work and open problems

Isogeny-based cryptography is not dead! It is an exciting time to work on isogenies and the Deuring correspondence.

- Norm equations have a role to play.
  1. Smaller solutions mean:
     1.1 Speed-up: SQISign and the ideal-to-isogeny translation.
     1.2 Security analysis: understanding the link between the endomorphism ring problem and all the other problems.

Future work and open problems

Isogeny-based cryptography is not dead! It is an exciting time to work on isogenies and the Deuring correspondence.

- Norm equations have a role to play.
    1. Smaller solutions mean:
        1.1 Speed-up: SQISign and the ideal-to-isogeny translation.
        1.2 Security analysis: understanding the link between the endomorphism ring problem and all the other problems.
- Work on SQISign (NIST submission):
    1. Finding good parameters for SQISign.
    2. Understanding the security of SQISign.

Future work and open problems

Isogeny-based cryptography is not dead! It is an exciting time to work on isogenies and the Deuring correspondence.

- Norm equations have a role to play.
  1. Smaller solutions mean:
     - 1.1 Speed-up: SQISign and the ideal-to-isogeny translation.
     - 1.2 Security analysis: understanding the link between the endomorphism ring problem and all the other problems.
- Work on SQISign (NIST submission):
  1. Finding good parameters for SQISign.
  2. Understanding the security of SQISign.
- Find constructive applications of the new attacks (on-going work).