New algorithms for the effective Deuring correspondence: Towards practical and secure SQISign signatures.

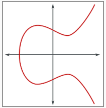
Antonin Leroux, joint work with Luca De Feo, Patrick Longa, Benjamin Wesolowski

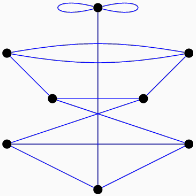
EUROCRYPT 2023, April 26

DGA, Ecole Polytechnique, INRIA, and Université de Rennes

The Deuring correspondence: a picture

The
supersingular
2-isogeny graph
in char. p.

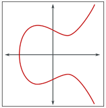




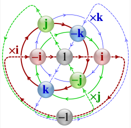
Credits to Luca De Feo and Cmglee

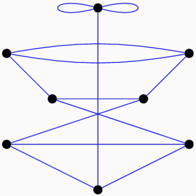
The Deuring correspondence: a picture

The supersingular 2-isogeny graph in char. p.



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

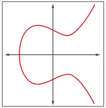


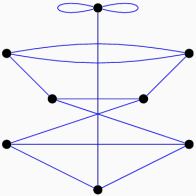


Credits to Luca De Feo and Cmglee

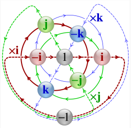
The Deuring correspondence: a picture

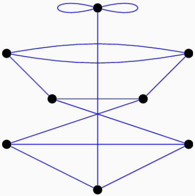
The supersingular 2-isogeny graph in char. p.





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

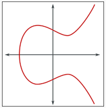




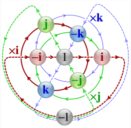
Credits to Luca De Feo and Cmglee

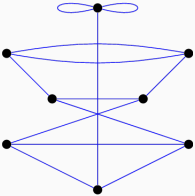
The Deuring correspondence: a picture

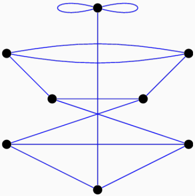
The supersingular 2-isogeny graph in char. p.



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







Our Contribution: A new algorithm for ideal to isogeny translation.

Credits to Luca De Feo and Cmglee

The Deuring Correspondence: an example

Supersingular elliptic curves over $\mathbb{F}_{p^2}$ E (up to Galois conjugacy)	Maximal Orders in $\mathcal{B}(p)$ $\mathcal{O} \cong \mathrm{End}(E)$
Isogeny with $\varphi : E_1 \to E_2$	Ideal I_φ left $\mathcal{O}_1, \mathcal{O}_2$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

The Deuring Correspondence: an example

Supersingular elliptic curves over $\mathbb{F}_{p^2}$ E (up to Galois conjugacy)	Maximal Orders in $\mathcal{B}(p)$ $\mathcal{O} \cong \mathrm{End}(E)$
Isogeny with $\varphi : E_1 \to E_2$	Ideal I_φ left $\mathcal{O}_1, \mathcal{O}_2$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

Example: $p \equiv 3 \mod 4$, $\mathcal{B}(p) \cong \mathbb{Q}\langle 1, i, j, ij \rangle$ where $i^2 = -1, j^2 = -p$.

The Deuring Correspondence: an example

Supersingular elliptic curves over $\mathbb{F}_{p^2}$ E (up to Galois conjugacy)	Maximal Orders in $\mathcal{B}(p)$ $\mathcal{O} \cong \mathrm{End}(E)$
Isogeny with $\varphi : E_1 \to E_2$	Ideal I_φ left $\mathcal{O}_1, \mathcal{O}_2$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

Example: $p \equiv 3 \mod 4$, $\mathcal{B}(p) \cong \mathbb{Q}\langle 1, i, j, ij \rangle$ where $i^2 = -1, j^2 = -p$.

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

The Deuring Correspondence: an example

Supersingular elliptic curves over $\mathbb{F}_{p^2}$ E (up to Galois conjugacy)	Maximal Orders in $\mathcal{B}(p)$ $\mathcal{O} \cong \mathrm{End}(E)$
Isogeny with $\varphi : E_1 \to E_2$	Ideal I_φ left $\mathcal{O}_1, \mathcal{O}_2$-ideal
Degree $\deg(\varphi)$	Norm $n(I_\varphi)$

Example: $p \equiv 3 \mod 4$, $\mathcal{B}(p) \cong \mathbb{Q}\langle 1, i, j, ij \rangle$ where $i^2 = -1, j^2 = -p$.

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

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

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

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

Hard and easy problems

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 $\mathcal{B}(p)$, find an ideal J of norm ℓ^e for $e \in \mathbb{N}^\star$ with $\mathcal{O}_L(J) \cong \mathcal{O}_1$, $\mathcal{O}_R(J) \cong \mathcal{O}_2$.

Hard and easy problems

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 $\mathcal{B}(p)$, find an ideal J of norm ℓ^e for $e \in \mathbb{N}^\star$ with $\mathcal{O}_L(J) \cong \mathcal{O}_1$, $\mathcal{O}_R(J) \cong \mathcal{O}_2$.

[KLPT14]: polynomial time alg. for the quaternion path problem.

Hard and easy problems

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 $\mathcal{B}(p)$, find an ideal J of norm ℓ^e for $e \in \mathbb{N}^\star$ with $\mathcal{O}_L(J) \cong \mathcal{O}_1$, $\mathcal{O}_R(J) \cong \mathcal{O}_2$.

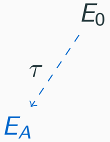
[KLPT14]: polynomial time alg. for the quaternion path problem.

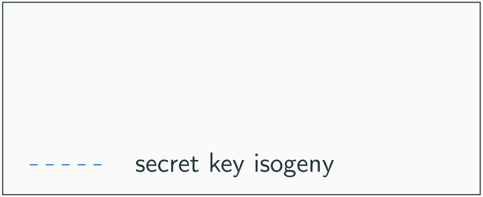
SQISign Identification Scheme [FKLPW20]

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 solving the isogeny problem.

SQISign Identification Scheme [FKLPW20]

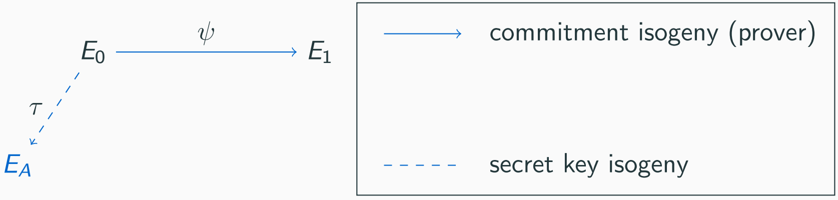
Main idea: public key is a curve E_A and secret key is $\mathrm{End}(E_A)$. Proving knowledge of $\mathrm{End}(E_A)$ by solving the isogeny problem.





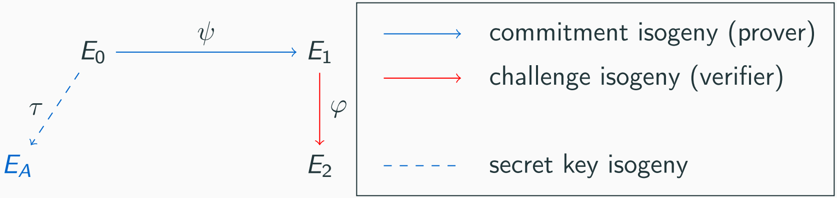
SQISign Identification Scheme [FKLPW20]

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 solving the isogeny problem.



SQISign Identification Scheme [FKLPW20]

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 solving the isogeny problem.



SQISign Identification Scheme [FKLPW20]

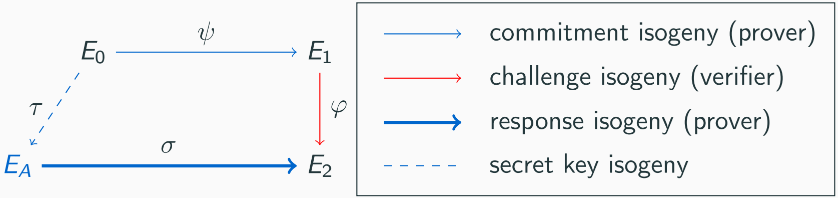
Main idea: public key is a curve E_A and secret key is $\mathrm{End}(E_A)$. Proving knowledge of $\mathrm{End}(E_A)$ by solving the isogeny problem.

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

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

SQISign Identification Scheme [FKLPW20]

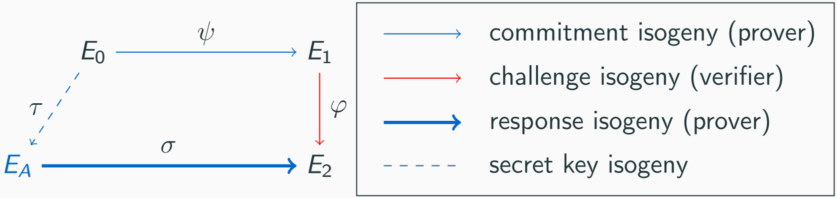
Main idea: public key is a curve E_A and secret key is $\mathrm{End}(E_A)$. Proving knowledge of $\mathrm{End}(E_A)$ by solving the isogeny problem.



Response computation:

SQISign Identification Scheme [FKLPW20]

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 solving the isogeny problem.

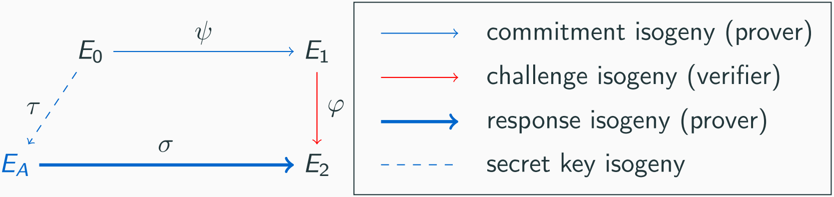


Response computation:

1. Compute $\mathrm{End}(E_2)$ from ψ, φ.

SQISign Identification Scheme [FKLPW20]

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 solving the isogeny problem.

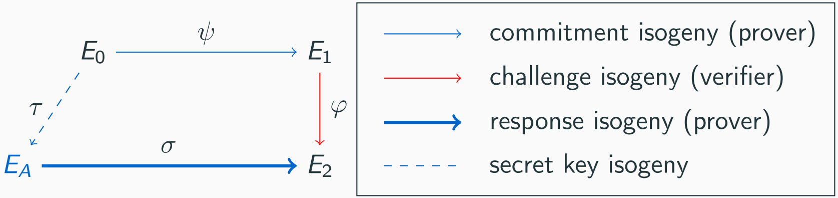


Response computation:

1. Compute $\mathrm{End}(E_2)$ from ψ, φ.
2. Compute I_σ connecting $\mathrm{End}(E_A)$ and $\mathrm{End}(E_2)$.

SQISign Identification Scheme [FKLPW20]

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 solving the isogeny problem.



Response computation:

1. Compute $\mathrm{End}(E_2)$ from ψ, φ.
2. Compute I_σ connecting $\mathrm{End}(E_A)$ and $\mathrm{End}(E_2)$.
3. Translate I_σ into σ.

SQISign Identification Scheme [FKLPW20]

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 solving the isogeny problem.

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

- commitment isogeny (prover)
- challenge isogeny (verifier)
- response isogeny (prover)
- secret key isogeny

Response computation:

1. Compute $\mathrm{End}(E_2)$ from ψ, φ.
2. Compute I_σ connecting $\mathrm{End}(E_A)$ and $\mathrm{End}(E_2)$.
3. Translate I_σ into σ. Need efficient ideal to isogeny translation!

Effective Deuring Correspondence: Ideal to isogeny

Ideal to isogeny translation problem

Input: A ss. *curve* E, a *max. order* $\mathcal{O} \cong \mathrm{End}(E)$, and an $\mathcal{O}$-*ideal* I[1] of norm D.

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

Algorithm from [GPS16] : $O(\mathrm{poly}(\max_{\ell | D} \ell))$ operations over $\mathbb{F}_{p^k}$ when $\ker \varphi_I \in E[\mathbb{F}_{p^k}]$.

[1] given as 16 coefficients of $O(pD)$ over $\mathbb{Q}$

Effective Deuring Correspondence: Ideal to isogeny

Ideal to isogeny translation problem

Input: A ss. *curve* E, a *max. order* $\mathcal{O} \cong \mathrm{End}(E)$, and an $\mathcal{O}$*-ideal* I[1] of norm D.

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

Algorithm from [GPS16] : $O(\mathrm{poly}(\max_{\ell | D} \ell))$ operations over $\mathbb{F}_{p^k}$ when $\ker \varphi_I \in E[\mathbb{F}_{p^k}]$.

We need to take D smooth, but then D is too big to have a small k!

[1] given as 16 coefficients of $O(pD)$ over $\mathbb{Q}$

Dividing the problem

For SQISign, $D = 2^f$.

Idea introduced in [FK**L**PW20]: Cut the isogeny in small pieces of degree 2^e where kernels are defined over $\mathbb{F}_{p^2}$.

But we need to "refresh" the 2^e-torsion after each step. In initial SQISign : alternate path of smooth odd degree T.

$$\begin{tikzcd}
E_0 \arrow[r, "2^e"] \arrow[r, bend right, "T"'] & E_1 \arrow[r, "2^e"] \arrow[r, bend right, "T"'] & E_2 \arrow[r, dashed] & {}
\end{tikzcd}$$

Dividing the problem

For SQISign, $D = 2^f$.

Idea introduced in [FK**L**PW20]: Cut the isogeny in small pieces of degree 2^e where kernels are defined over $\mathbb{F}_{p^2}$.

But we need to "refresh" the 2^e-torsion after each step. In initial SQISign : alternate path of smooth odd degree T.

$$
\begin{tikzcd}
E_0 \arrow[r, "2^e"] \arrow[r, bend right, "T"'] & E_1 \arrow[r, "2^e"] \arrow[r, bend right, "T"'] & E_2 \arrow[r, dashed] & {}
\end{tikzcd}
$$

To have $E[2^e T]$ defined over $\mathbb{F}_{p^2}$, we need $2^e T | p^2 - 1$. The problem is $T \approx p^{3/2}$.

Endomorphisms instead of isogenies

Main new idea : smooth odd degree endomorphisms are enough to "refresh" the torsion.

$$\begin{tikzcd} E_0 \arrow[r, "2^e"] & E_1 \arrow[r, "2^e"] \arrow[loop below, "T"] & E_2 \arrow[r, dashed] \arrow[loop below, "T"] & {} \end{tikzcd}$$

Endomorphisms are easier to find than isogenies : we need $T \approx p^{5/4}$.

Example: p_{6983} vs p_{3923}

For the original SQISign we add p_{6983}

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

For the new algorithm, we have p_{3923}

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

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 various improvements: new algorithms accounts for $\times 2$ speed-up.

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 various improvements: new algorithms accounts for $\times 2$ speed-up.

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

Table 1: Performance of SQISign in milliseconds, on an Intel core i7 Skylake @ 3.40 GHz CPU

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