SQIsign: Short Quaternion and Isogeny signature

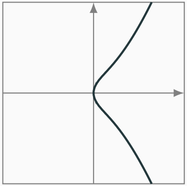
Antonin Leroux, *DGA-MI, and Université de Rennes*

Oxford PQ workshop, September 27, 2023

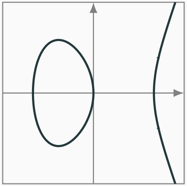
joint work with J. Chavez-Saab, M. Corte-Real Santos, L. De Feo, J. Komada Eriksen, B. Hess, D. Kohel, P. Longa, M. Meyer, L. Panny, S. Patranabis, C. Petit, F. Rodríguez Henríquez, S. Schaeffler, and B. Wesolowski

A quick overview of mathematical notions

Elliptic curves and isogenies

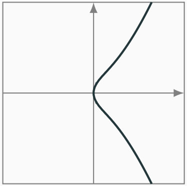


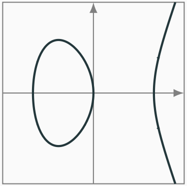
$y^2 = x^3 + x$



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

Elliptic curves and isogenies

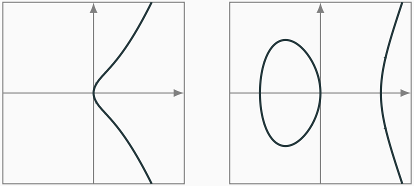




$$\begin{tikzcd} y^2 = x^3 + x \arrow[r, bend right] & y^2 = x^3 - 4x \end{tikzcd}$$

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

Elliptic curves and isogenies



$$\begin{tikzcd} y^2 = x^3 + x \arrow[rr, bend right, "{\varphi(x,y) = \left(\frac{x^2+1}{x}, \quad y\frac{x^2-1}{x^2}\right)}"'] & & y^2 = x^3 - 4x \end{tikzcd}$$

The Isogeny Problem: Given two elliptic curves E_1 and E_2, find an isogeny $\varphi : E_1 \to E_2$.

The supersingular isogeny graph

Over $\mathbb{F}_{p^2}$, supersingular curves with degree ℓ isogenies create a graph that is

1. connected
2. $\ell + 1$-regular
3. Ramanujan
4. of size $O(p)$

The supersingular isogeny graph

Over $\mathbb{F}_{p^2}$, supersingular curves with degree ℓ isogenies create a graph that is

1. connected
2. $\ell + 1$-regular
3. Ramanujan
4. of size $O(p)$

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 $e \in \mathbb{N}^\star$.

The supersingular isogeny graph

Over $\mathbb{F}_{p^2}$, supersingular curves with degree ℓ isogenies create a graph that is

1. connected
2. $\ell + 1$-regular
3. Ramanujan
4. of size $O(p)$

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 $e \in \mathbb{N}^\star$.

Best known attack: requires random walk in the isogeny graph. Complexity is polynomial in the size of the graph.

Endomorphisms

An **endomorphism** is an isogeny $\varphi : E \to E$.

Supersingular curves/$\mathbb{F}_{p^2}$ $\Leftrightarrow$ End(E) is a maximal order in a quaternion algebra $\mathcal{B}(p)$.

Endomorphisms

An **endomorphism** is an isogeny $\varphi : E \to E$.

Supersingular curves/$\mathbb{F}_{p^2}$ $\Leftrightarrow$ End(E) is a maximal order in a quaternion algebra $\mathcal{B}(p)$.

Endomorphisms are a bit like coordinates. With computations over the quaternions we can get our position in the graph. This is what is called the Deuring correspondence.

In particular, when we know the endomorphism ring of E_1 and E_2, we can solve the isogeny problem!

Endomorphisms

An **endomorphism** is an isogeny $\varphi : E \to E$.

Supersingular curves/$\mathbb{F}_{p^2}$ $\Leftrightarrow$ End(E) is a maximal order in a quaternion algebra $\mathcal{B}(p)$.

Endomorphisms are a bit like coordinates. With computations over the quaternions we can get our position in the graph. This is what is called the Deuring correspondence.

In particular, when we know the endomorphism ring of E_1 and E_2, we can solve the isogeny problem!

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

The signature scheme

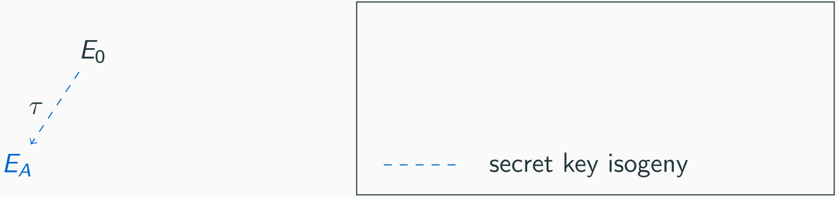
SQIsign: the protocol

Signature based on the Deuring correspondence and algorithms to translate from quaternion to isogenies. Built from an identification scheme with Fiat-Shamir.

SQIsign: the protocol

Signature based on the Deuring correspondence and algorithms to translate from quaternion to isogenies. Built from an identification scheme with Fiat-Shamir.

For id: public key is a curve E_A and secret key is $\mathrm{End}(E_A)$. The knowledge of $\mathrm{End}(E_A)$ is proven by using quaternions to solve the isogeny problem.



SQIsign: the protocol

Signature based on the Deuring correspondence and algorithms to translate from quaternion to isogenies. Built from an identification scheme with Fiat-Shamir.

For id: public key is a curve E_A and secret key is $\text{End}(E_A)$. The knowledge of $\text{End}(E_A)$ is proven by using quaternions to solve the isogeny problem.

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

$\longrightarrow$ commitment isogeny (prover)

- - - - - secret key isogeny

SQIsign: the protocol

Signature based on the Deuring correspondence and algorithms to translate from quaternion to isogenies. Built from an identification scheme with Fiat-Shamir.

For id: public key is a curve E_A and secret key is $\mathrm{End}(E_A)$. The knowledge of $\mathrm{End}(E_A)$ is proven by using quaternions to solve the isogeny problem.

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

$\longrightarrow$ commitment isogeny (prover)

$\longrightarrow$ challenge isogeny (verifier)

$- - - - -$ secret key isogeny

SQIsign: the protocol

Signature based on the Deuring correspondence and algorithms to translate from quaternion to isogenies. Built from an identification scheme with Fiat-Shamir.

For id: public key is a curve E_A and secret key is $\mathrm{End}(E_A)$. The knowledge of $\mathrm{End}(E_A)$ is proven by using quaternions to solve the isogeny problem.

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

→ commitment isogeny (prover)

→ challenge isogeny (verifier)

⟶ response isogeny (prover)

- - - - - secret key isogeny

SQIsign: analysis

Pros

1. **Compact**: thanks to the good mixing property of the isogeny graph, there is always a short response path σ that we can find.
2. **Easy and efficient** to verify (for isogenies): one simple isogeny computation.
3. **Stable security** (for isogenies): soundness relies on a well-understood problem. ZK is more ad hoc, but not affected by recent attacks.

Cons

1. The signature is **involved and slow**: the Deuring correspondence requires a lot of complex algorithms.
2. A **costly** parameter selection process.

SQIsign: sizes

Most compact PQ signature scheme: PK + Signature combined.

SQIsign: sizes

Most compact PQ signature scheme: PK + Signature combined.

Parameter set	`Public key`	`Secret key`	`Signature`
NIST-I	64	782	177
NIST-III	96	1138	263
NIST-V	128	1509	335

Table 1: SQIsign key and signature sizes in bytes for each security level.

Slight improvement in signature size since the research papers. Signatures could be even more compact ($\approx 5\%$) with more work. Secret keys are big due to precomputation.

History of SQIsign implementation

1. AC20 paper: first implementation at NIST-I with pari-gp for quaternions.
2. EC23 paper: improved implementation at NIST-I (improved algorithms, better finite field arithmetic), still with pari-gp.
3. NIST submission: reference implementation based on gmp and without pari-gp at NIST-I,III,V. Clean inner heuristic algorithms. A partly optimized implementation at NIST-I (performances are currently worse than EC23 paper).

SQIsign: performances

Parameter set	KeyGen	Sign	Verify
Reference implementation (with default GMP installation)			
NIST-I	2'834	4'781	103
NIST-III	21'359	38'84'84	687
NIST-V	84'944	160'458	2'051
Assembly-optimized implementation for Intel Broadwell or later			
NIST-I	1'661	2'370	37

Table 2: SQIsign performance in 10^6 CPU cycles on an Intel Xeon Gold 6338 CPU (Ice Lake), compiled on Ubuntu with clang version 14. Results are the median of 10 benchmark runs.

Future work

A lot of work needs to be done:

1. Obtain a **fully optimized implementation** for all three levels (a lot of open research questions remains). Going faster than EC23 paper is definitely possible. On-going reasearch: some ideas for bigger improvements.
2. **Constant time implementation** (in particular for the quaternion part). Hard due to a lot of heuristics in the quaternion computations.
3. **Side-channel analysis** in general.
4. Various **trade-offs** to explore. Some variants are possible.
5. Continue **cryptanalysis** and gain confidence in the hardness of isogeny-based cryptography.

The material

1. *SQISign: Compact Post-Quantum Signatures from Quaternions and Isogenies*, **ASIACRYPT 2020**

   L. de Feo, D. Kohel, A. Leroux C. Petit and B. Wesolowski

2. *New algorithms for the Deuring correspondence: toward practical and secure SQISign signatures*, **EUROCRYPT 2023**

   L. De Feo, A. Leroux, P. Longa and B. Wesolowski

3. *SQIsign specification*, **NIST Submission**

   J. Chavez-Saab, M. Corte-Real Santos, L. De Feo, J. Komada Eriksen, B. Hess, D. Kohel, A. Leroux, P. Longa, M. Meyer, L. Panny, S. Patranabis, C. Petit, F. Rodríguez Henríquez, S. Schaeffler, and B. Wesolowski

4. Website: `https://sqisign.org`

Thank you for listening!