SQIsign, the number theorists' great crypto heist

Luca De Feo
IBM Research Zürich

June 28, 2023
Recent Trends in Computer Algebra 2023

Hi, it’s me!

- Started into research working on (essentially) counting points of elliptic curves.

Hi, it's me!

- Started into research working on (essentially) counting points of elliptic curves.
- Very quickly got distracted by efficient computations in finite fields.

Hi, it's me!

- Started into research working on (essentially) counting points of elliptic curves.
- Very quickly got distracted by efficient computations in finite fields.
- I was using Magma and NTL. Got very frustrated with Magma's finite fields.

Hi, it's me!

- Started into research working on (essentially) counting points of elliptic curves.
- Very quickly got distracted by efficient computations in finite fields.
- I was using Magma and NTL. Got very frustrated with Magma's finite fields.
- Never counted a single point, ended up with a thesis on computing isogenies of elliptic curves for the sake of computing them.

Hi, it's me!

- Started into research working on (essentially) counting points of elliptic curves.
- Very quickly got distracted by efficient computations in finite fields.
- I was using Magma and NTL. Got very frustrated with Magma's finite fields.
- Never counted a single point, ended up with a thesis on computing isogenies of elliptic curves for the sake of computing them.
- Postdoc in Waterloo. David Jao shows me his new cute idea to make an encryption system out of isogenies of supersingular curves, asks me if I can make it fast.

Hi, it's me!

- Started into research working on (essentially) counting points of elliptic curves.
- Very quickly got distracted by efficient computations in finite fields.
- I was using Magma and NTL. Got very frustrated with Magma's finite fields.
- Never counted a single point, ended up with a thesis on computing isogenies of elliptic curves for the sake of computing them.
- Postdoc in Waterloo. David Jao shows me his new cute idea to make an encryption system out of isogenies of supersingular curves, asks me if I can make it fast.
- I could.

Hi, it's me!

- Started into research working on (essentially) counting points of elliptic curves.
- Very quickly got distracted by efficient computations in finite fields.
- I was using Magma and NTL. Got very frustrated with Magma's finite fields.
- Never counted a single point, ended up with a thesis on computing isogenies of elliptic curves for the sake of computing them.
- Postdoc in Waterloo. David Jao shows me his new cute idea to make an encryption system out of isogenies of supersingular curves, asks me if I can make it fast.
- I could.
- That's also when I started seriously working with Sage and Flint.

Hi, it's me!

- Started into research working on (essentially) counting points of elliptic curves.
- Very quickly got distracted by efficient computations in finite fields.
- I was using Magma and NTL. Got very frustrated with Magma's finite fields.
- Never counted a single point, ended up with a thesis on computing isogenies of elliptic curves for the sake of computing them.
- Postdoc in Waterloo. David Jao shows me his new cute idea to make an encryption system out of isogenies of supersingular curves, asks me if I can make it fast.
- I could.
- That's also when I started seriously working with Sage and Flint.
- Went back to France and finite fields, but never stayed too far from elliptic curves.

…continued

2015–2019 Member of OpenDreamKit, I start digging into the gory depths of Sage & friends.

…continued

2015–2019 Member of OpenDreamKit, I start digging into the gory depths of Sage & friends.

2016 Our little encryption system (SIDH/SIKE) starts getting more attention than expected.

…continued

2015–2019 Member of OpenDreamKit, I start digging into the gory depths of Sage & friends.

2016 Our little encryption system (SIDH/SIKE) starts getting more attention than expected.

2017 People start talking a lot about post-quantum cryptography, for some reason think isogenies are the way forward.

…continued

2015–2019 Member of OpenDreamKit, I start digging into the gory depths of Sage & friends.

2016 Our little encryption system (SIDH/SIKE) starts getting more attention than expected.

2017 People start talking a lot about post-quantum cryptography, for some reason think isogenies are the way forward.

2018–now I become more interested in making new cryptography, end up inventing a few more isogeny-based systems. Some are even sort of efficient.

…continued

2015–2019 Member of OpenDreamKit, I start digging into the gory depths of Sage & friends.

2016 Our little encryption system (SIDH/SIKE) starts getting more attention than expected.

2017 People start talking a lot about post-quantum cryptography, for some reason think isogenies are the way forward.

2018–now I become more interested in making new cryptography, end up inventing a few more isogeny-based systems. Some are even sort of efficient.

2019 Move to IBM Research. I guess I'm a cryptographer, now.

…continued

2015–2019 Member of OpenDreamKit, I start digging into the gory depths of Sage & friends.

2016 Our little encryption system (SIDH/SIKE) starts getting more attention than expected.

2017 People start talking a lot about post-quantum cryptography, for some reason think isogenies are the way forward.

2018–now I become more interested in making new cryptography, end up inventing a few more isogeny-based systems. Some are even sort of efficient.

2019 Move to IBM Research. I guess I'm a cryptographer, now.

June 2022 SIKE is selected for the 4th round of NIST's competition.

…continued

2015–2019 Member of OpenDreamKit, I start digging into the gory depths of Sage & friends.

2016 Our little encryption system (SIDH/SIKE) starts getting more attention than expected.

2017 People start talking a lot about post-quantum cryptography, for some reason think isogenies are the way forward.

2018–now I become more interested in making new cryptography, end up inventing a few more isogeny-based systems. Some are even sort of efficient.

2019 Move to IBM Research. I guess I'm a cryptographer, now.

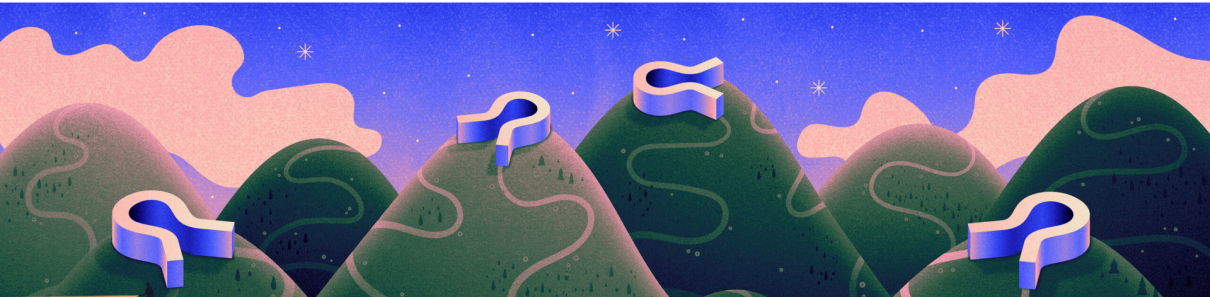
June 2022 SIKE is selected for the 4th round of NIST's competition.

July 2022 …

CRYPTOGRAPHY

‘Post-Quantum’ Cryptography Scheme Is Cracked on a Laptop

Two researchers have broken an encryption protocol that many saw as a promising defense against the power of quantum computing.



Why am I here today?

- To share my experience implementing cryptography.

Why am I here today?

- To share my experience implementing cryptography.
- To show you some cool maths.

Why am I here today?

- To share my experience implementing cryptography.
- To show you some cool maths.
- To know if msolve can run on a quantum computer.

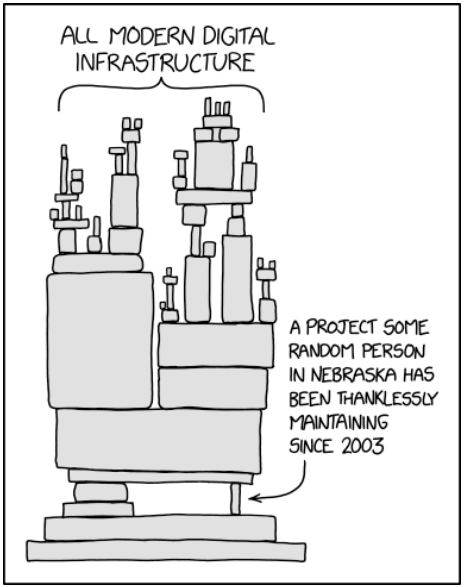
Implementing Crypto

A different game…

- Quite the opposite of general purpose.
- Old salty dogs write C/C++, cool kids write Rust.
- Must fit in all sorts of strange platforms (e.g., smartphones, smartcards).
- The more code, the more trouble.
- Code must be easily auditable.
- Misunderstanding the spec of a function can be fatal!
- Randomness is a pain. Always.

and yet, some familiarity…

- Most code open source. Good for auditability.
- Mostly developed by volunteers on their spare time.
- E.g.: OpenSSL (50% market share) has only 2 full-time developers and 1M$ budget.



with some unique rules: Secure coding

- Avoid external dependencies as much as possible.
- Dynamic memory allocation shunned.
- Constant time: running time must be independent from secrets.
- Code must be robust against errors (incl. cosmic rays).

Computer algebra in pre-quantum crypto

RSA

- Multi-precision integers.
  - Bit-sizes: 2048, 3072, 4096, 7680, 15360, ...

ECC

- Arithmetic in $\mathbb{Z}/p\mathbb{Z}$.
  - Bit-sizes: 256, 384, 512, ...
- Elliptic curve addition/duplication formulas

Computer algebra in post-quantum crypto

CRYSTALS – Kyber/Dilithium (lattice based)

- Arithmetic in $(\mathbb{Z}/p\mathbb{Z})[X]/(X^{256}+1)$,
  - where $p = 3329, 8380417$ (FFT friendly).
- Matrix operations
  - from 2×2 to 8×7.

Multi-quadratics (UOV, etc.)

- Multivariate dense polynomials over $\mathbb{Z}/p\mathbb{Z}$.
- Linear system solving.
  - e.g.: $p = 31$, dimension $\approx 50 \times 150$.

Computer algebra in post-quantum crypto

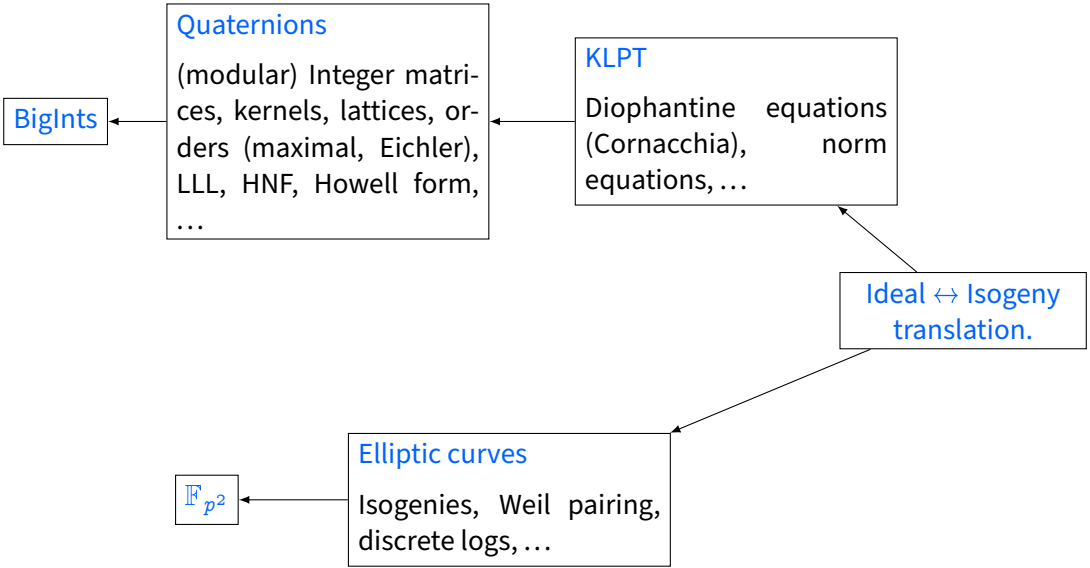
Code based (McEliece, etc.)

- Matrices over binary fields
  - dimensions in the hundreds to thousands.
- (List) decoding algorithms.

SIKE (isogeny based)

- Arithmetic in $\mathbb{F}_p[i]/(i^2+1)$
  - bit-sizes $434, 503, 610, 751$
- Elliptic curve arithmetic.
- Isogeny formulas.
- Isogeny composition.
- Optional: Weil pairing, discrete logs in $C_{2^e} \times C_{2^e}$.

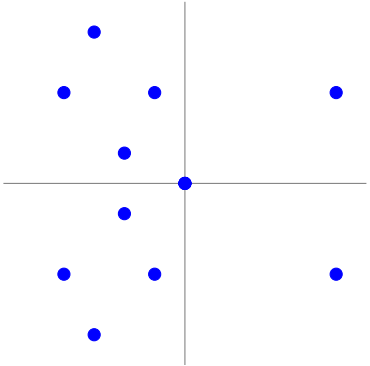
SQIsign


Quaternions
(modular) Integer matrices, kernels, lattices, orders (maximal, Eichler), LLL, HNF, Howell form, …
BigInts
KLPT
Diophantine equations (Cornacchia), norm equations, …
Ideal ↔ Isogeny translation.
Elliptic curves
Isogenies, Weil pairing, discrete logs, …
$\mathbb{F}_{p^2}$

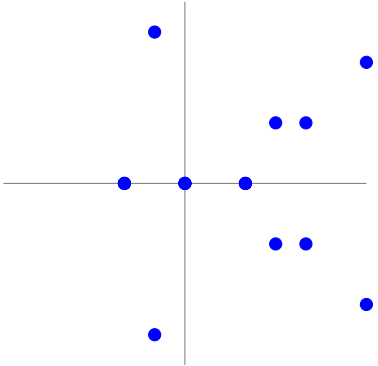
An overview of SQlsgin

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

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

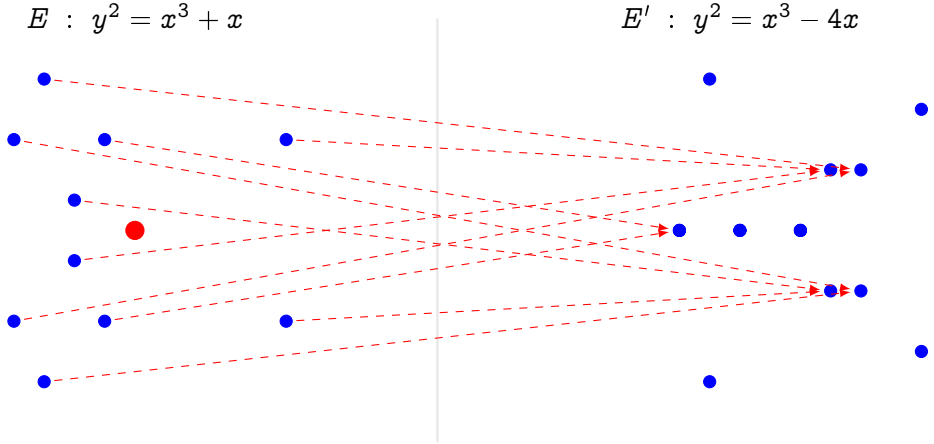


$E' : y^2 = x^3 - 4x$



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

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



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

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

Supersingular isogeny graphs

- There is a unique isogeny class of supersingular curves over $\bar{\mathbb{F}}_p$ of size $\approx p/12$.
- The graph of isogenies of degree ℓ is $(\ell+1)$-regular.
- It is a Ramanujan graphs, i.e., an optimal expander.
- Related to Hecke operators, modular forms, Brandt matrices…

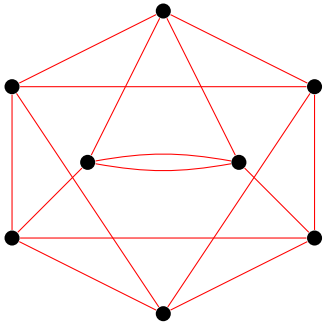


Figure: 3-isogeny graph on $\mathbb{F}_{97^2}$.

A loose analogy: Signing based on factoring

$$N = pq$$

	$\mathbb{Z}/N\mathbb{Z}$	$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$
multiplication	easy	easy
inversion	easy	easy
square roots	hard	easy
n-th roots	hard	easy

Rabin's signature

Sign: $s \leftarrow \sqrt{H(m;r)} \mod N$,

Verify: $s^2 \stackrel{?}{=} H(m;r) \mod N$.

The endomorphism ring of a supersingular curve

Theorem (Deuring)

Let E be a supersingular elliptic curve, then

- E is isomorphic to a curve defined over $\mathbb{F}_{p^2}$;
- Every isogeny of E is defined over $\mathbb{F}_{p^2}$;
- Every endomorphism of E is defined over $\mathbb{F}_{p^2}$;
- Every endomorphism ω satisfies a quadratic equation $\omega^2 - t\omega + n = 0$ with $t, n \in \mathbb{Z}$.
- $\mathtt{End}(E)$ is isomorphic to a maximal order in a quaternion algebra ramified at p and ∞.

An example

The curve of j-invariant 1728

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

is supersingular over $\mathbb{F}_p$ iff $p = -1 \mod 4$.

Endomorphisms

$\mathrm{End}(E) \subset \mathbb{Q}\langle \iota, \pi \rangle$, with:

- π the Frobenius endomorphism, s.t. $\pi^2 = -p$;
- ι the map

$$\iota(x, y) = (-x, iy),$$

where $i \in \mathbb{F}_{p^2}$ is a 4-th root of unity. Clearly, $\iota^2 = -1$.

And $\iota\pi = -\pi\iota$.

Quaternion algebras

(Assume $p = 3 \bmod 4$) The quaternion algebra $B_{p,\infty}$ is:

- A 4-dimensional $\mathbb{Q}$-vector space with basis $(1, i, j, k)$.
- A non-commutative division algebra[1] $B_{p,\infty} = \mathbb{Q}\langle i, j \rangle$ with the relations:

$$i^2 = -1, \quad j^2 = -p, \quad ij = -ji = k.$$

Properties

- All elements of $B_{p,\infty}$ are quadratic algebraic numbers.
- $B_{p,\infty} \otimes \mathbb{Q}_\ell \simeq \mathcal{M}_{2\times 2}(\mathbb{Q}_\ell)$ for all $\ell \neq p$.
- $B_{p,\infty} \otimes \mathbb{R}$ is isomorphic to Hamilton's quaternions.
- $B_{p,\infty} \otimes \mathbb{Q}_p$ is a division algebra.

[1] All elements have inverses.

Oh, no! Not again lattices!

We define the reduced norm of $B_{p,\infty} = \mathbb{Q}\langle i, j \rangle$ as

$$N(\alpha) = N(a + b \cdot i + c \cdot j + d \cdot ij) = a^2 + b^2 + p(c^2 + d^2)$$

Properties

- The norm is multiplicative.
- $\sqrt{N(\alpha - \beta)}$ defines a metric.
- If $N(\alpha)$ and $2a$ are integers, α is called an algebraic integer.

Ideals, orders

Ideals

- A full rank ($= 4$) lattice $\mathfrak{a} \subset B_{p,\infty}$ is called a fractional ideal.
- If all elements of $\mathfrak{a}$ are integers, it is called an (integral) ideal.
- If $\mathfrak{a}$ is a subring of $B_{p,\infty}$, it is called an order.
- We define $N(\mathfrak{a})$ as the gcd of $N(\alpha)$ for all $\alpha \in \mathfrak{a}$.

Orders

Let $\mathfrak{a} \subset B_{p,\infty}$ be an ideal, its left order is

$$\mathcal{O}_L(\mathfrak{a}) := \{\alpha \in B_{p,\infty} \mid \alpha\mathfrak{a} \subset \mathfrak{a}\}.$$

The right order $\mathcal{O}_R(\mathfrak{a})$ is defined analogously.

The Deuring correspondence

Let $\mathcal{O}, \mathcal{O}' \subset B_{p,\infty}$ be two maximal orders. They have the same type if there exists α s.t.

$$\mathcal{O} = \alpha \mathcal{O}' \alpha^{-1}.$$

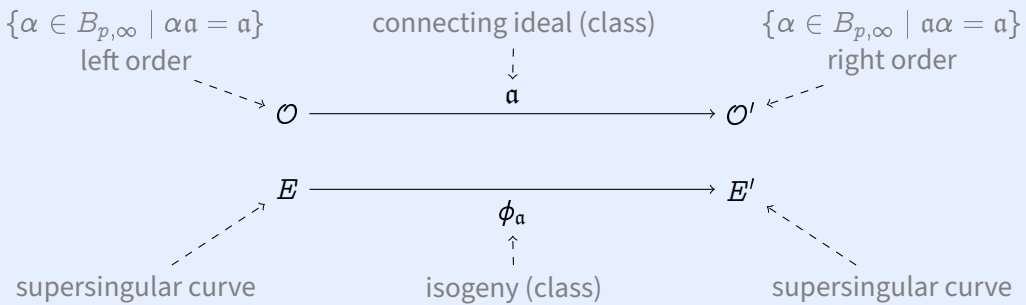
Theorem (Deuring)

Maximal order types of $B_{p,\infty}$ are in one-to-one correspondence with supersingular curves up to Galois conjugation in $\mathbb{F}_{p^2}/\mathbb{F}_p$.

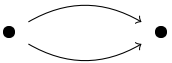
The Deuring correspondence

Two left ideals $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}$ are in the same class if there exists β s.t. $\mathfrak{a} = \mathfrak{b}\beta$.

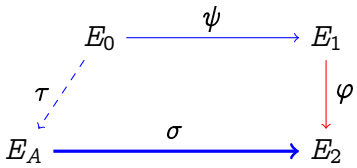
An equivalence of categories (Kohel, roughly)



The Deuring correspondence

Supersingular curves	Orders
Endomorphisms	Integers of $B_{p,\infty}$
Endomorphism ring	Maximal order
Isogeny	Ideal
Isogeny degree	Ideal norm
Isogenies 	Ideal classes
Dual isogeny	Conjugate ideal

SQIsign: Signatures from the effective Deuring correspondence



commitment isogeny (prover)

challenge isogeny (verifier)

response isogeny (prover)

secret key isogeny

Most compact PQ signature scheme: PK + Signature combined **5**$\times$**smaller** than Falcon.

Secret Key (bytes)	Public Key (bytes)	Signature (bytes)	Security
782	64	177	NIST-1
1138	96	263	NIST-3
1509	128	335	NIST-5


Thank you
https://defeo.lu/
@luca_defeo