A look at isogeny-based cryptography

2025/11/06 — **9th Franco-Japanese Cybersecurity Workshop** — Tokyo

Damien Robert

Inria

Post-Quantum Cryptography

- Cryptography: defense (military secrets), security, economy (e-commerce, blockchains), privacy...

- **Risk**: quantum computers break classical cryptography
- **Solution**: switch to post-quantum cryptography

The challenge of Post-Quantum Cryptography

We want a secure cryptosystem which is:

1. Fast
2. Compact
3. Post-Quantum

Pick two out of these three!

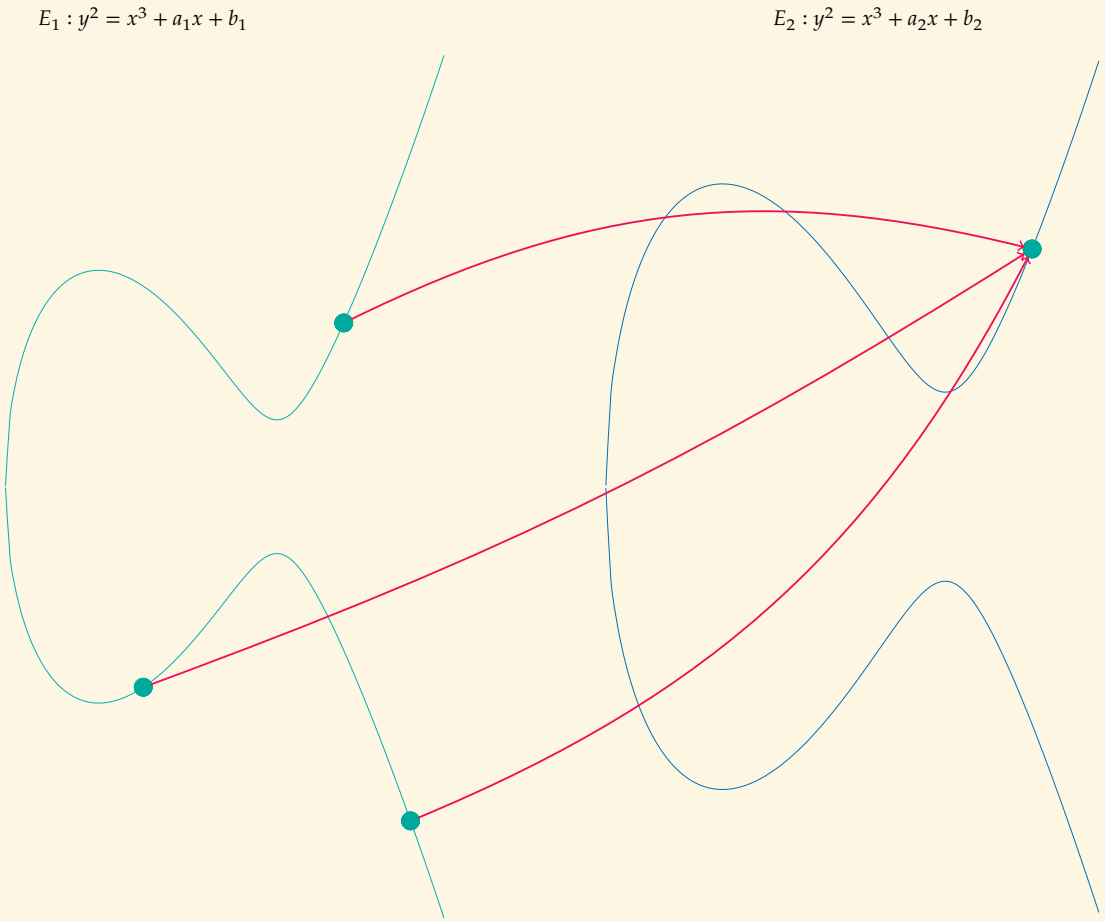
- Elliptic Curve Cryptography: Fast+Compact
- Noisy Linear Algebra (codes/lattices): Fast+Post-Quantum
- Isogenies: Compact+Post-Quantum

Why isogenies?

- ECC: key exchange = 32B, signatures = 64B/32B (pairings)
- Lattices: ≈10000B
- Structured lattices: ≈1000B
- Isogenies: key exchange = 64B (WIP), signatures = 150B

- Structured lattices: Standardised by NIST
- Structure reduces key size, but adds a big security risk

Isogenies and isogeny graphs

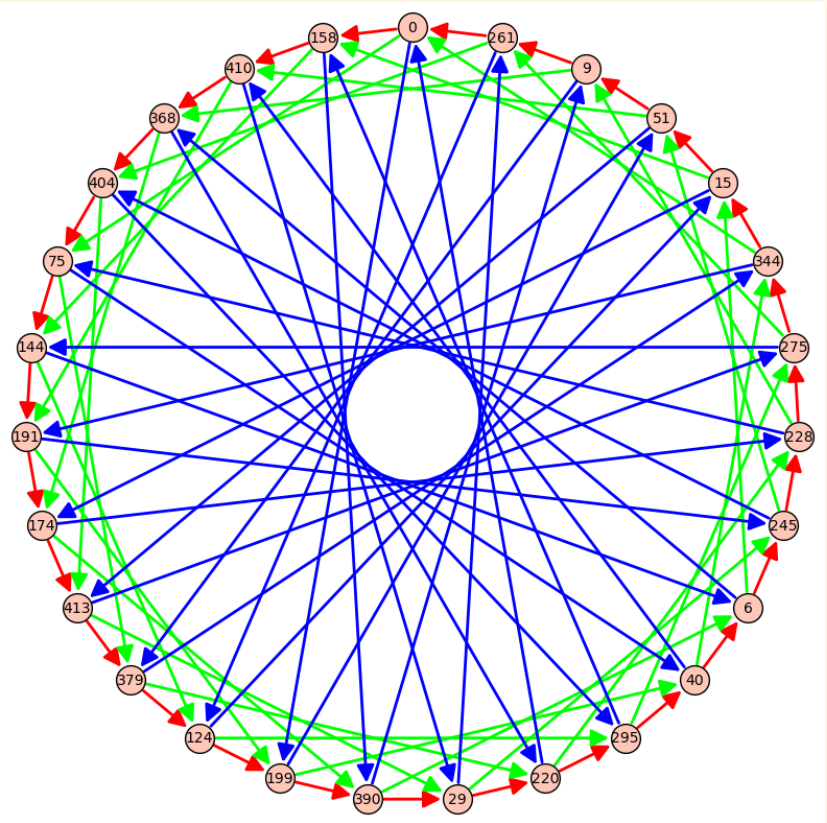


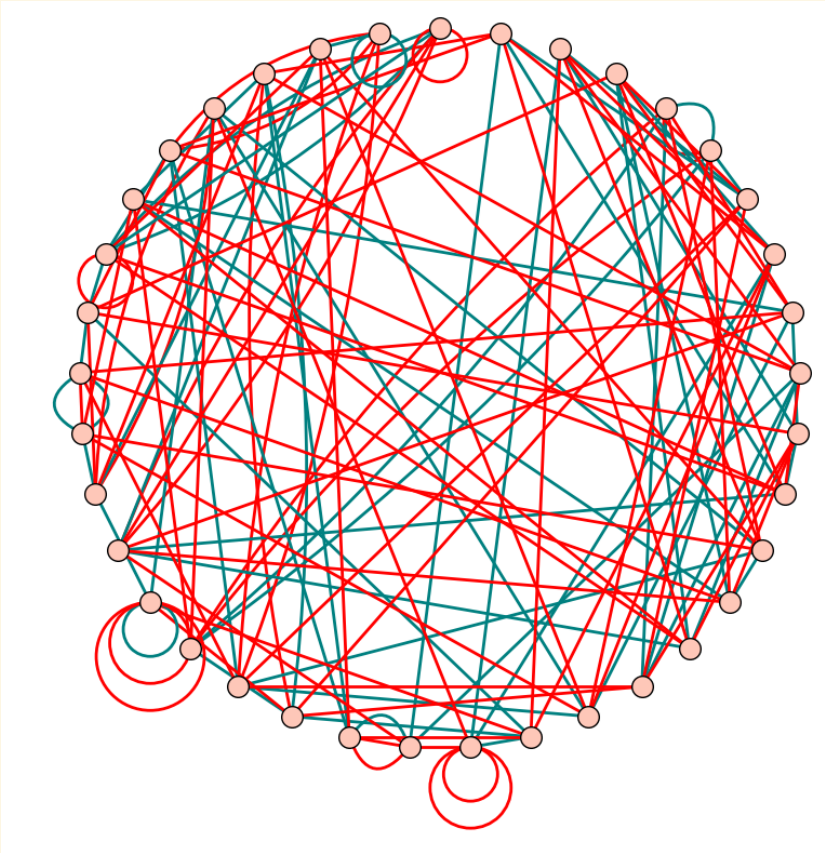
A 3-isogeny between elliptic curves.

Isogenies and isogeny graphs

The moduli space of elliptic curves over $\mathbb{C}$.

Isogenies and isogeny graphs





An example of a commutative supersingular isogeny graph over $\mathbb{F}_{419}$, and of a non-commutative maximal supersingular isogeny graph over $\mathbb{F}_{431^2}$.

Isogenies and isogeny graphs

Fundamental hard problem: given two supersingular curves E_1, E_2, find an isogeny $\phi : E_1 \to E_2$.

Two flavors of isogeny graphs

Commutative isogeny graphs:

- Isogeny graphs of supersingular elliptic curves over $\mathbb{F}_p$
- Commutative group action
- ☺ Easy to build protocols, e.g: a NIKE (non interactive key exchange) via a Diffie-Helmann like key exchange
- But also advanced protocols: oblivious PRFs, threshold signatures, blind signatures, group and ring signatures, updatable schemes, Verifiable Random Functions, Password Authenticated Key Exchange...
- ☹ Extra structure leads to subexponential attacks [Kuperberg] ⇒ needs increased parameters size

Non-commutative isogeny graphs:

- Isogeny graph of maximal supersingular elliptic curves over $\mathbb{F}_{p^2}$.
- ☺ Very unstructured graph ⇒ very small parameters
- ☹ Hard to build protocols on top of it. May need to add back extra structure by publishing extra informations in the protocol.
- ☹☹ This extra information may lead to attacks: the SIDH attacks from 2022!

A partial history of isogeny based cryptography

- [Couveignes (1997)], [Rostovtsev–Stolbunov (2006)]: Commutative isogeny graphs of ordinary elliptic curves for key exchange.
- [Charles, Goren, Lauter 2006]: Switch to non commutative supersingular graphs to build hash functions.

- [De Feo, Jao (2011)],[De Feo, Jao, Plût (2014)]: SIDH, a key exchange on non commutative graphs ⇒ the key exchange needs extra informations.
- [Castryck, Lange, Martindale, Panny, Renes (2018)]: CSIDH, a key exchange on commutative graphs.
  Use supersingular graphs over $\mathbb{F}_p$, same commutative properties as ordinary graphs but much easier to find optimised parameters.
- [De Feo, Kohel, Leroux, Petit, Wesolowski (2020)]: SQISign: signatures on non commutative graphs.

- 2022-07: SIKE advances to fourth round of the NIST's PQC call
- 2022-07: SIDH attacks ☹
- 2022–2025: Higher dimensional renaissance ☺
  Exploits the attacks against SIDH constructively, by using isogenies in higher dimension

Higher dimensional isogenies

- 2022: Big revolution in isogeny based cryptography
- Switch from dimension 1 to higher dimension (dimension 2, 4 or 8)
- Destructive application: breaking SIDH [Castryck-Decru; Maino-Martindale-Panny-Pope-Wesolowski; R. 2022]
  The attacks use the extra SIDH information in the key exchange, the pure path finding graph problem still secure.

- [R.] constructive application: can evaluate any isogeny in polynomial time (before: only very special isogenies).
- **Intuition**: higher dimensional isogenies as wormholes in the dimension one isogeny graph.

Main applications:

- For non commutative graphs: Improved versions of SQISign: SQISignHD, SQISign2d (Much faster, better security proofs, slightly more compact keys)
- For commutative graphs: evaluating arbitrary group action in polynomial time: CLAPOTIS [Page-R 2023] ⇒ much more flexible protocols
  (previously restricted to restricted group actions)

NIST Post-Quantum Cryptography: Additional Digital Signature Schemes

- SQISignHD [Dartois-Leroux-R.-Wesolowski] Eurocrypt 2024 Best Paper
- SQISign2d [Basso-De Feo-Dartois-Leroux-Maino-Pope-R.-Wesolowski] Asiacrypt 2024

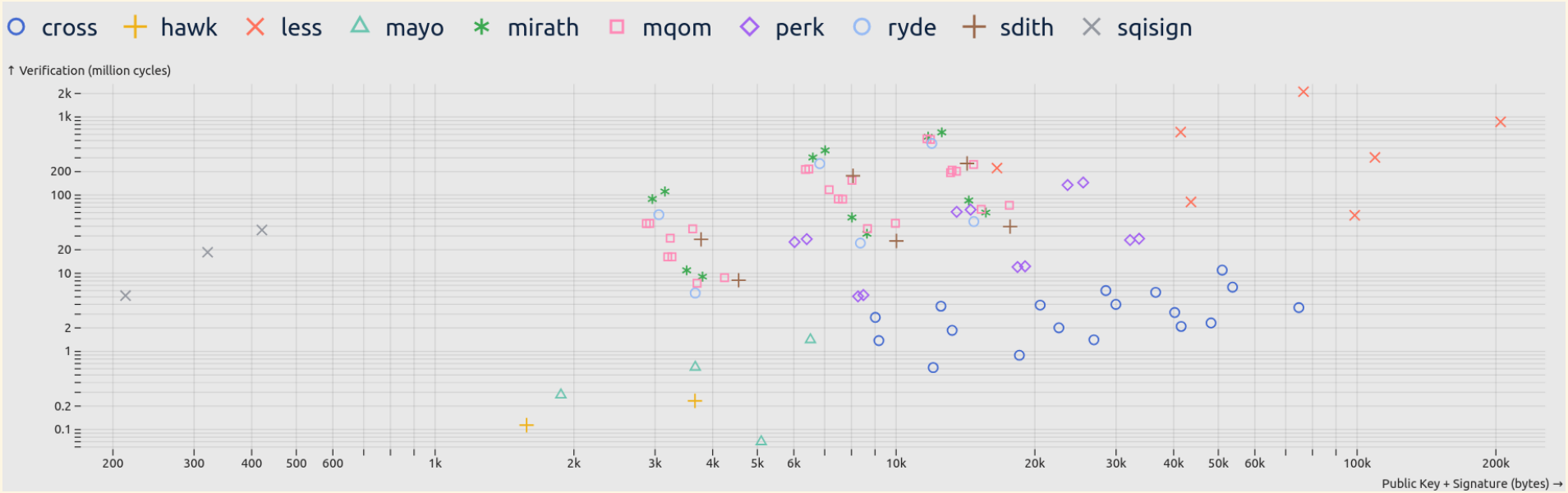
SQISign v1 (June 2023)

	Sizes (bytes)		Timing (ms)		
Security	Public Key	Signature	Keygen	Sign	Verify
NIST-1	64	177	1,864	2,890	54
NIST-3	96	263	11,867	21,880	327
NIST-5	128	335	45,525	79,272	1,089

SQISign v2 (June 2025)

	Sizes (bytes)		Timing (ms)		
Security	Public Key	Signature	Keygen	Sign	Verify
NIST-1	66	148	25	60	3
NIST-3	98	222	67	161	9
NIST-5	130	294	119	300	18

NIST Post-Quantum Cryptography: Additional Digital Signature Schemes



Summary

Why isogeny based cryptography?

- Increased resilience in Post-Quantum Cryptography
- European Autonomy. How much do we trust NIST? How much do we trust structured noisy linear algebra?
- Provides a strong and worthwhile alternative
- By far the most compact post-quantum schemes

Current status: higher dimensional isogenies

- Non commutative isogeny graphs: very compact, much faster than before, but only used by signature schemes SQISign (or PRISM)
- Commutative isogeny graphs: can now evaluate arbitrary group actions: very powerful for protocols (NIKE, threshold, blind signatures, ...), but needs larger parameters.

In the future:

- MIKE (Module isogeny key exchange) [R. 2024]
- A very compact NIKE using only the unstructured isogeny graph
- Via an higher dimensional module action

Tools: Elliptic curves, Polarised abelian varieties, Moduli spaces, Quaternion algebras, Hermitian modules, Pairings, Biextension and Cubical torsor structures...