Post-Quantum Cryptography: a survey of isogeny based cryptography 2024/10/08 — Inria-Simula Workshop

Damien Robert

Équipe Canari, Inria Bordeaux Sud-Ouest









Alice starts from 'a', follows the path 001110, and get 'w'.



Bob starts from 'a', follows the path 101101, and get 'l'.



Alice starts from 'l', follows the path 001110, and get 'g'.



Bob starts from 'w', follows the path 101101, and get 'g'.



The full exchange:



Bigger graph (62 nodes)



Even bigger graph (676 nodes)



Graphs for key exchange

- Needs a graph with good mixing properties: A path of length $O(\log N)$ gives a uniform node \Rightarrow Ramanujan/expander graph.
- The graph does not fit in memory $(N = 2^{256})$.
- Needs an algorithm taking a node as input and giving the neighbour nodes as output.
- ⇒ Isogeny graphs of elliptic curves



Isogeny based cryptography

- ③ Very compact keys!
- Signature: SQISignHD
 Public key: 64B, signature 109B
 Lattices: 666B-2420B
 ECDSA: 32B
- NIKE (Non Interactive Key Exchange): ⊗-MIKE: 64B Lattices: 220KB
- VRF (Verifiable Random Function): DeuringVRF Public key 192B, Proof 256B Lattices: 2.6KB-39KB
- Very slow
- But lot of progress on efficiency recently! (see later)

Isogeny based cryptography brings **diversity** to our other post-quantum schemes like lattice based cryptography or code cryptography who rely on **noisy linear algebra** (over \mathbb{Z} or \mathbb{F}_2 respectively)

Graphs in Isogeny based cryptography

Security:

- Random walking in the graph is easy
- Finding a path between two curves is hard
 Even for a quantum computer! ⇒ Post-Quantum Cryptography!

Two kind of isogeny graphs

- Ordinary (or oriented) isogeny graphs
- The graph is commutative
- ③ Key exchange is easy
- © Path finding easier than for a general graph (Kuperberg's quantum subexponential algorithm)
- Supersingular isogeny graphs
- The graph is non commutative
- © Best known algorithm for path finding is quantum exponential
- Sey exchange is not obvious

Part 1 (1997–2010) — The prehistory: ordinary isogeny graphs

- [Couveignes 1997]: <u>Hard Homogeneous Spaces</u> First suggestion to use isogeny graphs of ordinary elliptic curves for key exchange. Commutative graphs!
- Rediscovered in [Rostovtsev–Stolbunov (2006)]: Public-key cryptosystem based on isogenies
- [De Feo, Kieffer, Smith 2018]: Towards practical key exchange from ordinary isogeny graphs Huge computationally intensive search for "optimised parameters" 520s for a key exchange (512b=64B)

Part 2 (2011 – 2022) — The history: supersingular isogeny graphs

- [Charles, Goren, Lauter 2006] Cryptographic hash functions from expander graphs Switch from commutative ordinary graphs to non commutative supersingular graphs over \mathbb{F}_{n^2}
- [De Feo, Jao (2011)],[De Feo, Jao, Plût (2014)]: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies

SIDH: Supersingular Isogeny Diffie-Hellman

Non commutative graph \Rightarrow the key exchange needs extra informations

Not a pure path finding graph problem anymore!

- [Costello, Longa, Naehrig 2016]: Efficient algorithms for supersingular isogeny Diffie-Hellman \approx 50MCycles \approx 25ms, 564B
- [Galbraith, Petit, Shani, Ti 2016]: On the security of supersingular isogeny cryptosystems Active adaptative attack against SIDH, can no longer be used as a NIKE Replaced by SIKE: a PKE (Public Key Encapsulation) scheme
- © NIST PQC Round 4, 5 July 2022: SIKE advances to fourth round
- [Castryck, Lange, Martindale, Panny, Renes 2018]: <u>CSIDH: An Efficient Post-Quantum</u> Commutative Group Action

Use supersingular graphs over \mathbb{F}_p , same commutative properties as ordinary graphs but much easier to find optimised parameters

pprox 100MCycles pprox 50ms, 64B

• [De Feo, Kohel, Leroux, Petit, Wesolowski 2020]: <u>SQISign: compact post-quantum signatures from</u> quaternions and isogenies

Part 3 (2022) — The downfall of isogeny based cryptography

• [Peikert 2019]: He Gives C-Sieves on the CSIDH

"This strongly invalidates its claimed NIST level 1 quantum security [...] Moreover, under analogous assumptions for CSIDH-1024 and -1792, which target higher NIST security levels [...] even these instantiations fall short of level 1." Key size recommendation for CSIDH: from 512b to 2000b-5000b...

- 2022-07-05: SIKE advances to fourth round of the NIST PQC call
- 2022-07-30: [Castryck, Decru], "An efficient key recovery attack on SIDH"
- 2022-08-08: [Maino, Martindale], "An attack on SIDH with arbitrary starting curve"
- 2022-08-10: [R.], "Breaking SIDH in polynomial time" Use objects in higher dimension (2, 4 and 8) to break SIDH.
- \odot SIDH/SIKE, and many protocols derived from it, are completely dead (full attacks in pprox 100ms)
- The attacks use the extra SIDH information in the key exchange, the pure path finding graph problem still secure
- Only SQISign remains (and CSIDH with increased parameter sizes)

Part 3 (2022) — The downfall of isogeny based cryptography

• [Peikert 2019]: He Gives C-Sieves on the CSIDH

"This strongly invalidates its claimed NIST level 1 quantum security [...] Moreover, under analogous assumptions for CSIDH-1024 and -1792, which target higher NIST security levels [...] even these instantiations fall short of level 1." Key size recommendation for CSIDH: from 512b to 2000b-5000b...

- 2022-07-05: SIKE advances to fourth round of the NIST PQC call
- 2022-07-30: [Castryck, Decru], "An efficient key recovery attack on SIDH"
- 2022-08-08: [Maino, Martindale], "An attack on SIDH with arbitrary starting curve"
- 2022-08-10: [R.], "Breaking SIDH in polynomial time" Use objects in higher dimension (2, 4 and 8) to break SIDH.
- \odot SIDH/SIKE, and many protocols derived from it, are completely dead (full attacks in \approx 100ms)
- The attacks use the extra SIDH information in the key exchange, the pure path finding graph problem still secure
- Only SQISign remains (and CSIDH with increased parameter sizes)

Part 4 (2022–) — the higher dimensional renaissance

- The attacks against SIDH exploited higher dimensional isogenies. These add considerable flexibility, and they were quickly exploited constructively: [R. 2022]: Evaluating isogenies in polylogarithmic time
- [Dartois, Leroux, R., Wesolowski (2023)]: <u>SQISignHD: New Dimensions in Cryptography</u> Improvement of SQISign using dimension 4 for verification Best paper award (Eurocrypt 2024)
- [Basso, De Feo, Dartois, Leroux, Maino, Pope, R., Wesolowski (2024)]: <u>SQIsign2D-West: The Fast,</u> <u>the Small, and the Safer</u> Improvement of SQISign using dimension 2 for signature and verification
- [R. (October 2024)]: <u>The module action for isogeny based cryptography</u> Uses rank 2 modules to build a new NIKE: OMIKE (Module Isogeny Key Exchange), with keys of only 64B

See Castryck's invited talk at Eurocrypt 2024: "An attack became a tool: Isogeny based cryptography 2.0"

SQISign2d (West) and SQISignHD

	SQlsign	SQIsign2d
Public key	64B	64B
Signatures	177B	148B
Clean security proof	٢	٢
Keygen (Mcycles)	400	60
Sign (Mcycles)	1880	160
Verify (Mcycles)	29	9

SQIsignHDv2: Signature size: 109B, $\approx 5 \times$ faster than SQIsign2d Verification expected $\approx 8 \times$ slower