Recent advances in isogeny based cryptography

2023/11/29 — 8th Franco-Japanese Cybersecurity Workshop, Bordeaux

Damien Robert

Équipe Canari, Inria Bordeaux Sud-Ouest

Isogeny based cryptography

Elliptic curve cryptography

- ☺ Compact
- ☺ Fast
- ☹ Not Post-Quantum

Isogeny based cryptography

- ☺ Post-quantum
- ☺ Compact keys. SQISign signatures = 177 Bytes
- ☹ Slow. SQISign (NIST submission): Signature = 550 ms, Verification = 8 ms
- 😐 Very new field (<10 years)

Isogeny based cryptography

Elliptic curve cryptography

- ☺ Compact
- ☺ Fast
- ☹ Not Post-Quantum

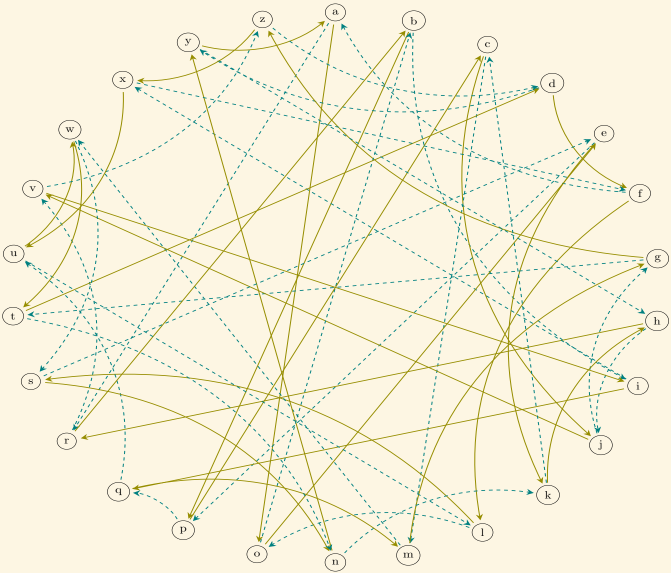
Isogeny based cryptography

- ☺ Post-quantum
- ☺ Compact keys. SQISign signatures = 177 Bytes
- ☹ Slow. SQISign (NIST submission): Signature = 550 ms, Verification = 8 ms
- 😐 Very new field (<10 years)

This talk:

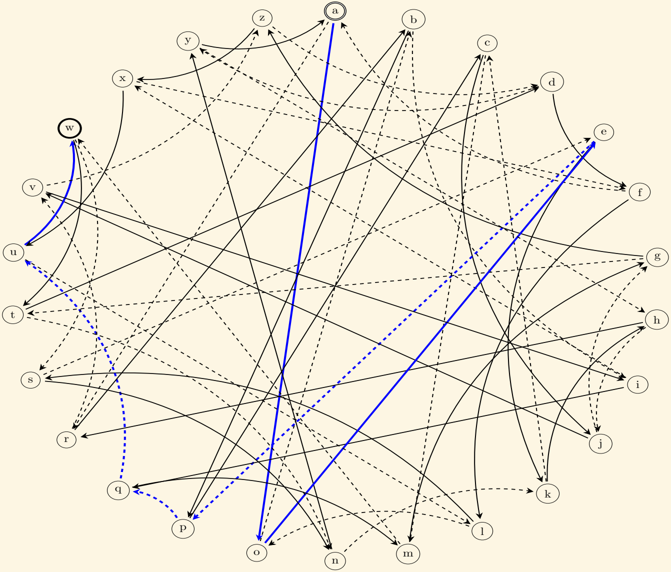
- The state of isogeny based cryptography before 2022
- Recent advances since 2022
- How to improve the efficiency of isogeny based cryptography
- SQISignHD: Signatures of 109 Bytes in 28 ms

Key exchange on a (commutative) graph



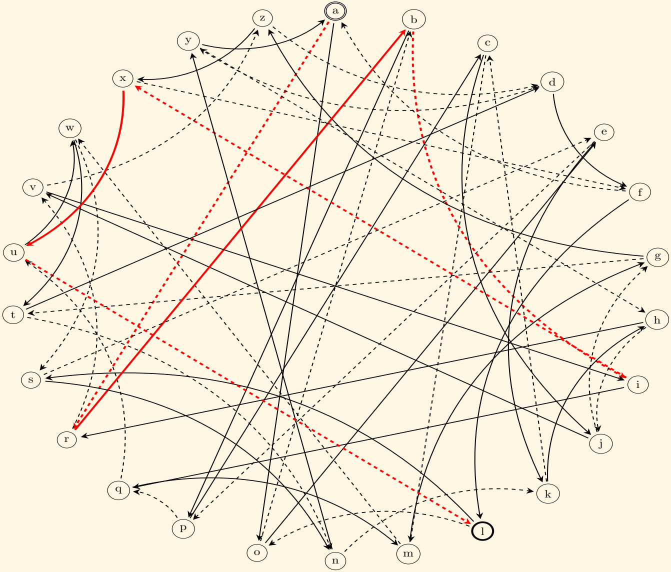
Key exchange on a (commutative) graph

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



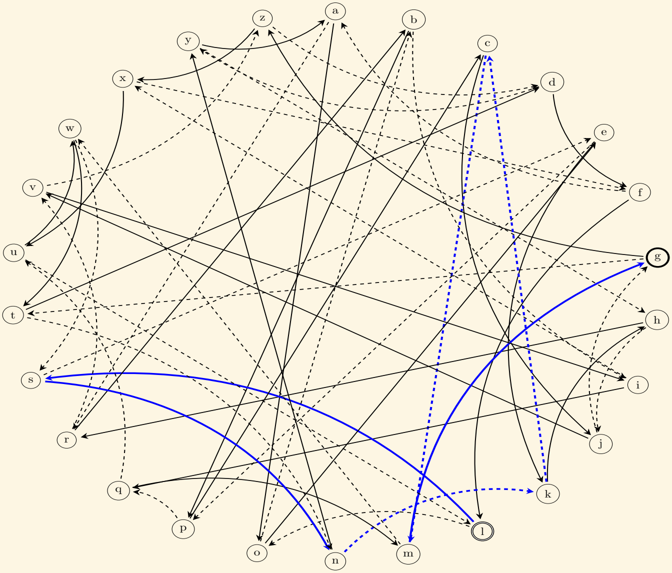
Key exchange on a (commutative) graph

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



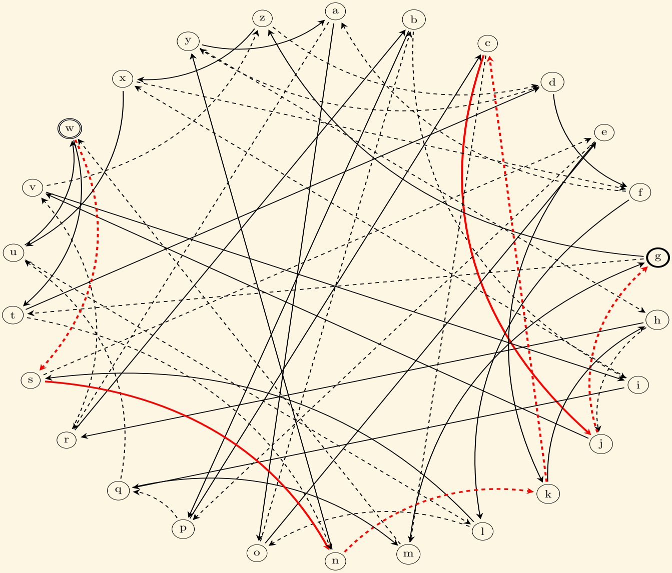
Key exchange on a (commutative) graph

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



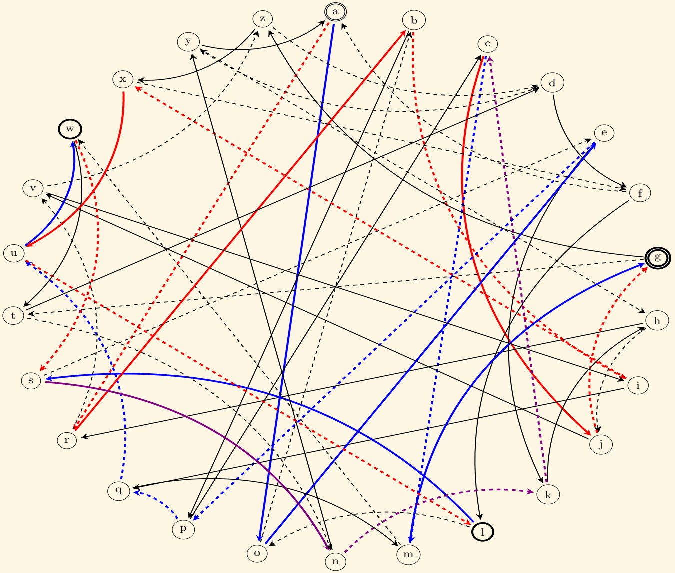
Key exchange on a (commutative) graph

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



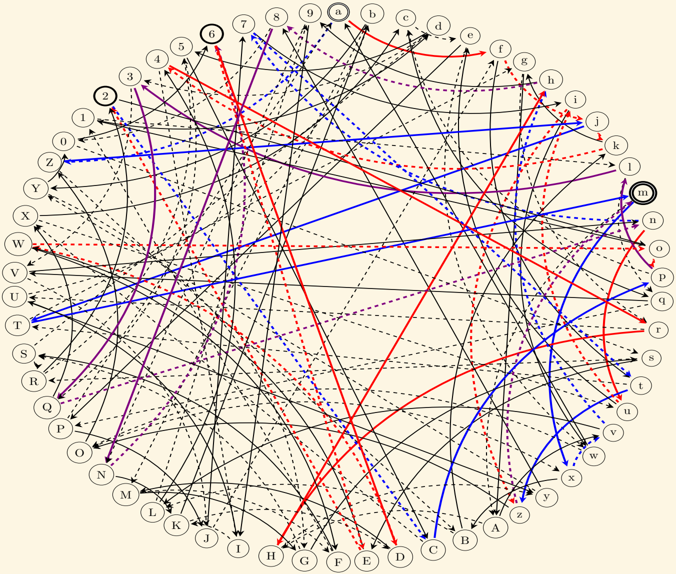
Key exchange on a (commutative) graph

The full exchange:



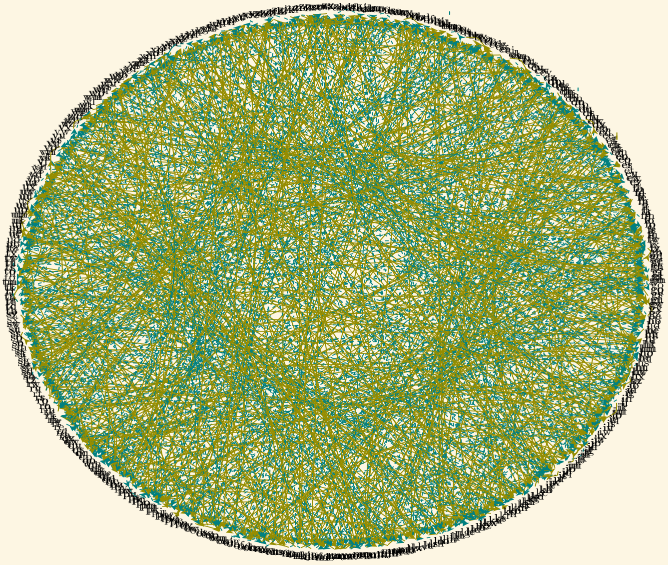
Key exchange on a (commutative) graph

Bigger graph (62 nodes)



Key exchange on a (commutative) graph

Even bigger graph (676 nodes)

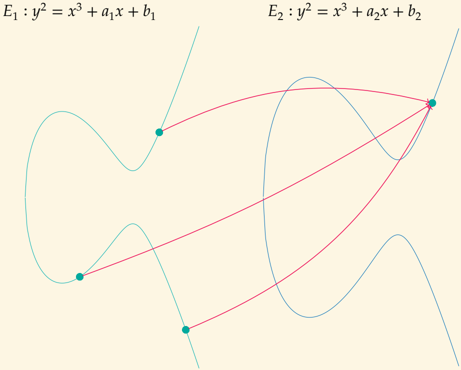


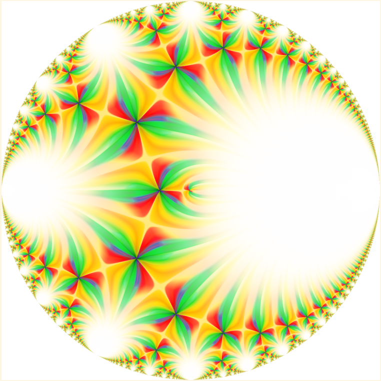
Commutative isogeny graphs for key exchange

- 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.

Commutative isogeny graphs for key exchange

- Isogeny graph of ordinary (or oriented) elliptic curves $E/\mathbb{F}_p$ [Couveignes (1997)], [Rostovtsev–Stolbunov (2006)]
- Graph of size $N \approx \sqrt{p}$.





Commutative isogeny graphs for key exchange

- ☺ Commutative graph!
- ☺ Key exchange from a commutative group action of G on X:
  $G = \mathrm{Cl}(\mathrm{End}(E)), X = \{\text{oriented elliptic curves}\}$
  1. Alice selects $\mathfrak{a} \in G$ and publish $\mathfrak{a} \cdot x$
  2. Bob selects $\mathfrak{b} \in G$ and publish $\mathfrak{b} \cdot x$
  3. The shared secret key is $\mathfrak{a}\mathfrak{b} \cdot x$.
- ☺ Signatures, PRFs, threshold signatures, oblivious signatures…
- 😐 Can only compute a restricted group action
- ☹ Hidden shift problem solvable in quantum subexponential $L(1/2)$ time for an abelian group action via Kuperberg's algorithm.

Supersingular isogeny graphs

- Deuring's correspondance: supersingular isogenies = ideals in non commutative quaternion algebras
- Supersingular isogeny path problem: given two supersingular elliptic curves $E_1, E_2/\mathbb{F}_{p^2}$, find an isogeny $\phi : E_1 \to E_2$.

☺ Best algorithm is exponential $\widetilde{O}(p^{1/2})$ (almost no progress made on improving it)

☺ Well understood security reductions between the isogeny path problem and various related problems like computing endomorphisms [Wesolowski et al.]

😐 No commutative group action anymore

☹☹ Supersingular isogeny cryptographic protocols often rely on ad-hoc assumptions rather than just the isogeny path problem

Supersingular isogeny graphs

Dimension 1 isogenies

- $E : y^2 = x^3 + Ax^2 + x, T = (u : \_ : v) \in E[2]$
- Isogeny: $E \to E' = E/\langle T \rangle, (X : \_ : Z) \mapsto (X(uX - vZ) : \_ : Z(vX - uZ))$ of degree 2.
  $E' : y^2 = x^3 + A'x^2 + x, A' = \frac{2(v^2 - 2u^2)}{v^2}$
- Compose several isogenies of this type: isogeny of degree 2^n
- Similar formulas for isogenies of degree $3, 5, \ldots$ and (by composition) for isogenies of smooth degree $N = 2^a \cdot 3^b \cdot 5^c \ldots$
- Complexity increases with the size of the largest ℓ dividing N.

☺ Smooth degree isogenies are fast to compute

☹ General isogenies are too expensive

☹ Restricted group action

☹ Inefficiencies

Isogeny based cryptosystems in 2022

Commutative group action:

- CRS, CSIDH: key exchange
- SiGamal: public key encryption
- SeaSign, CSI-Fish, …: signatures

Supersingular isogenies:

- SIDH/SIKE, BSIDH, k-SIDH, SHealS: key exchange
- Séta: public key encryption
- SQISign: signatures via the effective Deuring correspondance

The Break

- 2011 [De Feo, Jao, Plût]: SIDH (Supersingular Isogeny Key-Exchange)
- 2017: SIKE (Supersingular Isogeny Key Encapsulation) submitted to NIST's PQC competition
- 2022-07-05: SIKE goes to fourth round

The Break

- 2011 [De Feo, Jao, Plût]: SIDH (Supersingular Isogeny Key-Exchange)
- 2017: SIKE (Supersingular Isogeny Key Encapsulation) submitted to NIST's PQC competition
- 2022-07-05: SIKE goes to fourth round
- 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"

The Break

- 2011 [De Feo, Jao, Plût]: SIDH (Supersingular Isogeny Key-Exchange)
- 2017: SIKE (Supersingular Isogeny Key Encapsulation) submitted to NIST's PQC competition
- 2022-07-05: SIKE goes to fourth round

- 2022-07-30: [Castryck, Decru], "An efficient key recovery attack on SIDH"
  Heuristic polynomial break on a special supersingular curve, using dimension 2 isogenies
- 2022-08-08: [Maino, Martindale], "An attack on SIDH with arbitrary starting curve"
  Heuristic subexponential break on any supersingular curve, using dimension 2 isogenies
- 2022-08-10: [R.], "Breaking SIDH in polynomial time"
  Proven polynomial break on any supersingular curve, using dimension $2, 4$ or 8 isogenies

Remaining isogeny based cryptosystems after the break

Commutative group action:

- CRS, CSIDH: key exchange
- SiGamal: public key encryption
- SeaSign, CSI-Fish, …: signatures

Supersingular isogenies:

- ~~SIDH/SIKE, BSIDH, k-SIDH, SHealS~~: key exchange
- ~~Séta~~: public key encryption
- SQISign: signatures via the effective Deuring correspondance

The rise of higher dimensional isogenies

- [R. 2022] embedding lemma: for all $N' > N$, an N-isogeny $f : E_1 \to E_2$ can always be efficiently embedded into an N'-isogeny $F : A_1 \to A_2$ in dimension $g = 8$ (and sometimes $g = 4$, $g = 2$)
- Build on earlier theoretical work by [Zarhin 1975], [Kani 1997]
- Take N' smooth or even $N' = 2^n$: can now efficiently evaluate any N-isogeny by going to higher dimension

☺ Considerable flexibility

☺ New algorithmic tools (canonical lifts, dividing an isogeny, …[R. 2022])

😐 Algorithms for higher dimensional isogenies much less understood than in dimension 1

Computing higher dimensional isogenies

- [Lubicz, R. et al.] 15+ years of work
- `AVIsogenies`: compute any isogeny in any dimension
- [Dartois, Maino, Pope, R. 2023]: $10\times$ speed up for 2^n-isogenies in dimension 2
- Constant time implementation in Rust
- A 2^{126}-isogeny in dimension 2 over a field of 500 bits in 2.85 ms

The current state of isogeny based cryptography

Commutative group action:

- CRS, CSIDH, SeaSign, CSI-Fish, SCALLOP (dimension 1)
- SCALLOP-HD (dimension 2)
  CLAPOTIS [Page-R. 2023] (dimension 2 or 4): non restricted group action!

Supersingular isogenies:

- Key exchange: M-SIDH, ter-SIDH (dimension 1), IS-CUBE (dimension 2)
- Public key cryptography: FESTA, QFESTA, FESTA-HD (encryption in dimension 1 or 2, decryption in dimension 2 or 4)
- Signatures: SQISign (dimension 1)
  SQISignHD [Dartois, Leroux, R., Wesolowski 2022] (signature in dimension 1 or 2, verification in dimension 2 or 4)
  Signatures of 109 bytes in 28 ms, Better security proof, Upcoming: faster verification
- VRFs (Evaluation in dimension 1 or 2, Verification in dimension 2 or 4)

Future directions:

- Extremely recent (1 year), still finding new ways to exploit higher dimensional isogenies
- Challenge: exploit higher dimensional isogeny graphs
  (Rather than just using higher dimensional isogenies to compute efficiently dimension 1 isogenies)