Isogeny based cryptography: from the fall of SIKE to the rise of higher dimensional isogenies

2024/02/22 — Workshop Inria – University of Waterloo – Université de Bordeaux

Damien Robert

Équipe Canari, Inria Bordeaux Sud-Ouest

Classical public key cryptography

- One way function:
- Multiplication: $p, q \mapsto pq$, vs Factorisation
- Exponentiation in an elliptic curve: $n \mapsto n \cdot P$, vs Discrete Logarithm

☺ Everybody can encrypt

☹ Nobody can decrypt

Classical public key cryptography

- Trapdoor one way function
- Multiplication: $p, q \mapsto pq$, vs Factorisation
- Exponentiation in an elliptic curve: $n \mapsto n \cdot P$, vs Discrete Logarithm

☺ Everybody can encrypt

☺ The secret trapdoor allows to decrypt

Elliptic curves vs RSA

- RSA 2048 bits: `ssh-rsa`

`AAAAB3NzaC1yc2EAAAADAQABAAABgQC1c6zqJctqMRoYWVjovfPzwKGoFgv8j6y1W6f2zGbvOif`
`9hdw6X1u+ooI6IwkQWr9kPrM8xl9EJ/Q1ajeESPknLUHkqrVmrfFrYsyr6DKDapdAztCfT72IXy`
`4Fq12PzPKTfUw67vZTqEsGH2L5x0kYrWD+P/vA/+CQpwjMq9IZ7GRE2Yf6EHpcV6ifDqRSVlyGN`
`z/NzBDWBQNxdCORI7DG+L3tV0xODJKqXbvw/edVo6StAiWr0b67SYrxeUMhmvLgqFWWtq9Gayt/`
`4bLotah081RBUqVNQr9bSaLTY0ke/sEiOeHxiXfG3Uh7fLkVWYd+mwDcyRBGReNAik6u4ZKcCCU`
`y7P9UXuhLnBGpzjhUu/zuqckBR4NJDx+icq37cni1S9AaO/ftb8L2ryGRMeiy89HPYhQBPzBaif`
`xpQ7XA6Vyv8VhE5an9Bewv7spHtQ50xlXkAu6BJtNcIwbt6O1Wu6PuXDAc4gnyqa1MI3XIh36oE`
`ONIwRrrqvig0mixl0k=`

- ECC 256 bits: `ssh-ed25519`

`AAAAC3NzaC1lZDI1NTE5AAAAIFQDOTtvWadRfCXTXuT2pT7E5KWJZjPH4gOJyWvmiSJm`

- ☺ ECC: very fast and compact
- ☺ Signatures: 64B. Pairings: 32B

- ☹ ECC and RSA broken by quantum computers [Shor 1994]
- NIST post-quantum call (2017), further call for post-quantum signatures (2023)

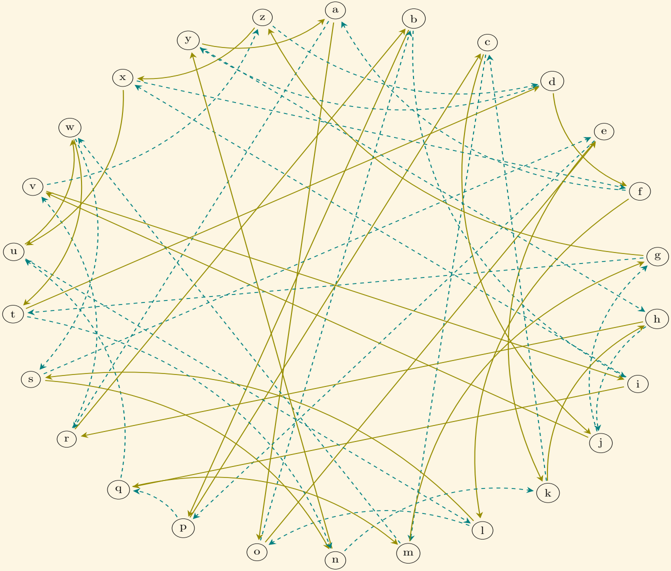
Diffie-Hellman Key Exchange

- $P \in G$ an abelian group, e.g. $G = E(\mathbb{F}_q)$ an elliptic curve
- Alice: $P_A = a \cdot P$,
- Bob: $P_B = b \cdot P$,
- Common secret key: $S = ab \cdot P = ba \cdot P$.

Post-quantum Diffie-Hellman Key exchange:

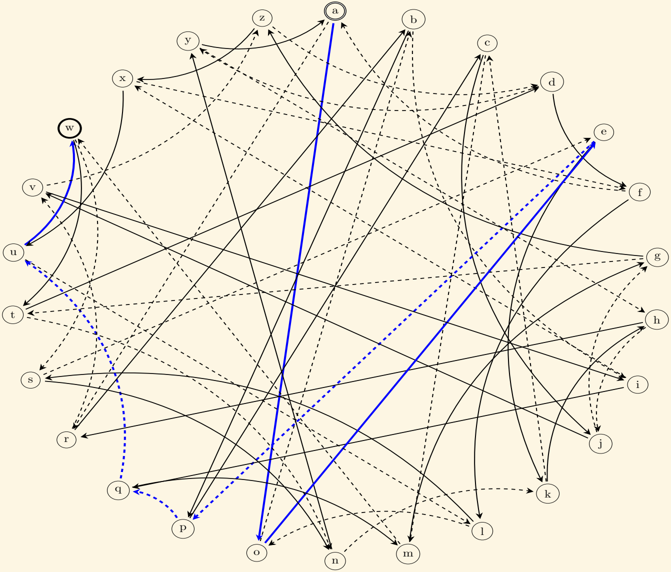
1. Noisy version (codes, lattices)
2. Group action: commutative group G acting on X ($a, b \in G$, $P \in X$).

Key exchange on a (commutative) graph



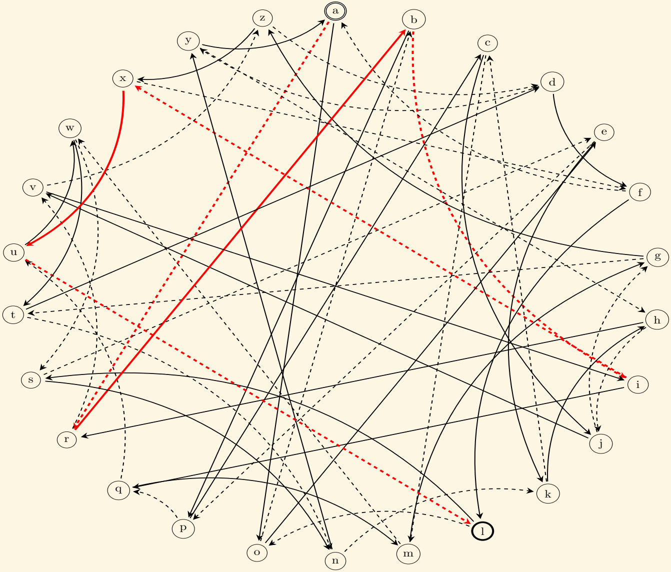
Key exchange on a (commutative) graph

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



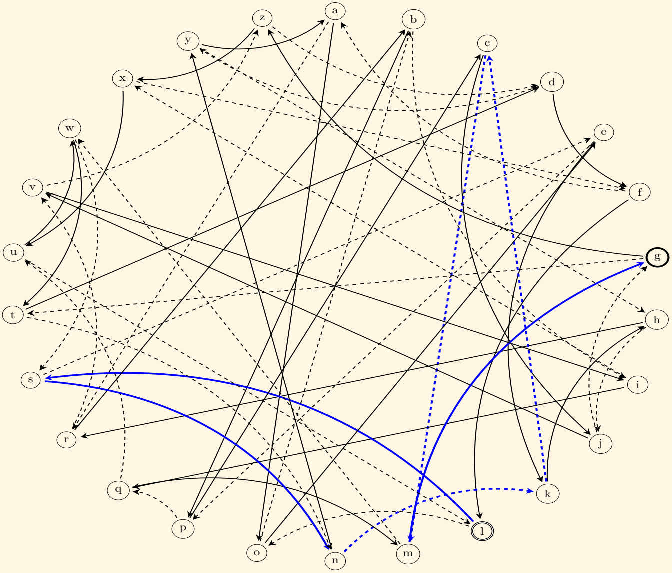
Key exchange on a (commutative) graph

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



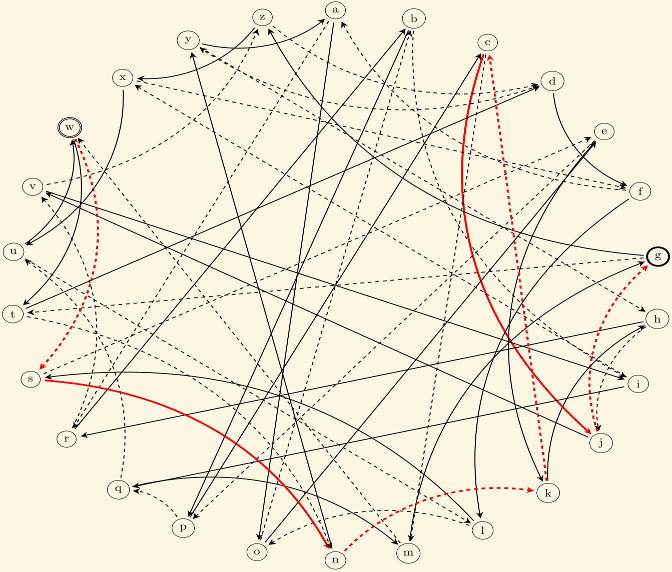
Key exchange on a (commutative) graph

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



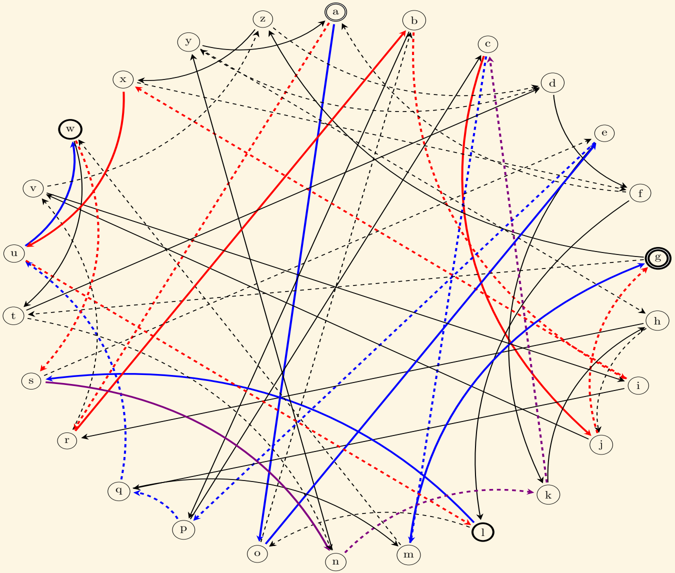
Key exchange on a (commutative) graph

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



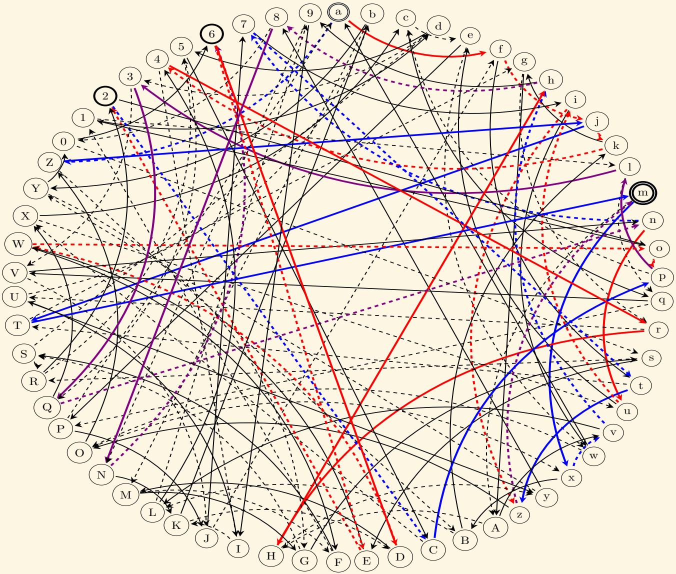
Key exchange on a (commutative) graph

The full exchange:



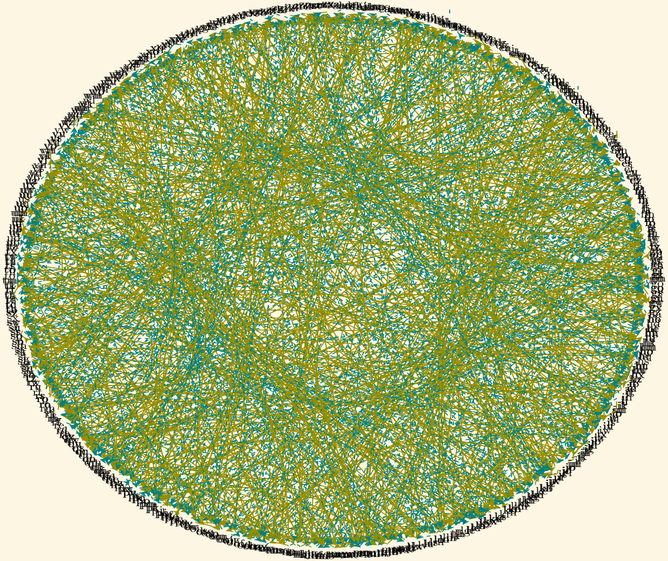
Key exchange on a (commutative) graph

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.
- Does not fit in memory $(N = 2^{256})$.

$\Rightarrow$ Needs an algorithm taking a node as input and giving the neighbour nodes as output.

Isogeny based cryptography

☺ Post-quantum

☺ Compact keys. SQISign signatures = 177 Bytes (Lattices 666B–2420B)

☹ Slow. SQISign (NIST submission): Signature = 550 ms, Verification = 8 ms

😐 Very new field (<10 years)

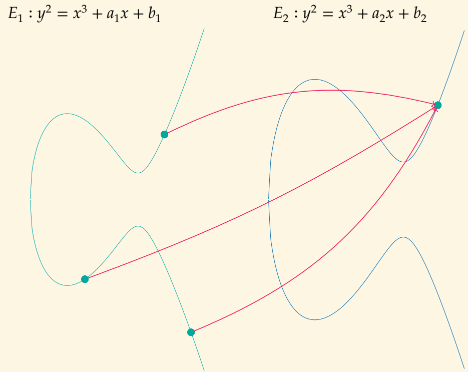
☹ Flagship protocol SIKE (post quantum key exchange) broken in 2022.

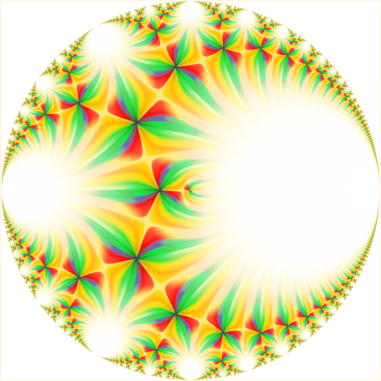
This talk:

- Recent advances since 2022
- How to improve the efficiency of isogeny based cryptography
- SQISignHD: Signatures of 109 Bytes in 28 ms [Dartois, Leroux, R., Wesolowski 2023]

Isogeny based cryptography

Isogeny graph of elliptic curves $E/\mathbb{F}_q$ (Graph of size $N \approx \sqrt{q}$):





Isogeny based cryptography

Ordinary (or oriented) elliptic curves $E/\mathbb{F}_p$ [Couveignes (1997)], [Rostovtsev–Stolbunov (2006)]

- ☺ Key exchange from a commutative group action of G on X: $G = \mathrm{Cl}(\mathrm{End}(E)), X = \{\text{oriented elliptic curves}\}$
- ☺ Signatures, PRFs, threshold signatures, oblivious signatures…
- ☹ Hidden shift problem solvable in quantum subexponential $L(1/2)$ time for an abelian group action via Kuperberg's algorithm.

Supersingular isogeny graphs $E/\mathbb{F}_{p^2}$ [De Feo, Jao, Plut 2011]

- Deuring's correspondance: supersingular isogenies = ideals in non commutative quaternion algebras
- ☺ Isogeny path problem: exponential quantum security (best known algorithm in $\widetilde{O}(p^{1/2})$)
- 😐 No commutative group action anymore

Isogeny based cryptography

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.
  $E' : y^2 = x^3 + A'x^2 + x, A' = \frac{2(v^2 - 2u^2)}{v^2}$

☺ Isogeny of large degree 2^n: decomposes as n isogenies of degree 2

☹ Isogeny of large prime degree ℓ: no such decomposition!

☹ Inefficiencies, Restricted group action

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"
  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: any isogeny of large degree can be decomposed into a product of isogenies of small degree by going to higher dimension ($g = 8$ and sometimes $g = 4$ or $g = 2$).

☺ Considerable flexibility

☺ New algorithmic tools: canonical lifts, dividing an isogeny, point counting, endomorphism rings…[R. 2022]

😐 Algorithms for higher dimensional isogenies (of small degree) less understood than in dimension 1

- [Lubicz, R. et al.] 15+ years of work
- `AVIsogenies` [Bisson, Cosset, R.]: software to compute any N-isogeny in any dimension
- [Dartois, Maino, Pope, R. 2023]: $10\times$ speed up for 2^n-isogenies in dimension 2.
  Low level constant time Rust implementation: $40\times$ speed-up ($400\times$ speed up in total!)
- 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): unrestricted 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