Number theory for post-quantum cryptography

2024/02/20 — Conseil scientifique de l'Imb

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: $n \mapsto n.P$, 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: $n \mapsto n.P$, 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)

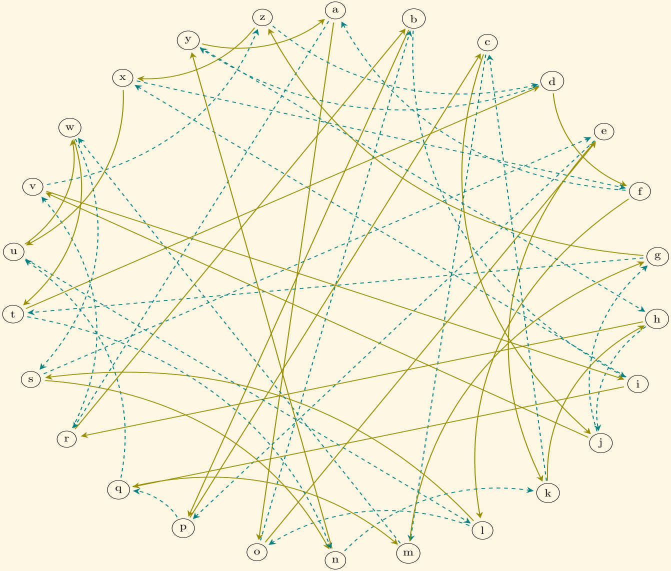
Diffie-Hellman Key Exchange

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

Post-quantum Diffie-Hellman Key exchange:

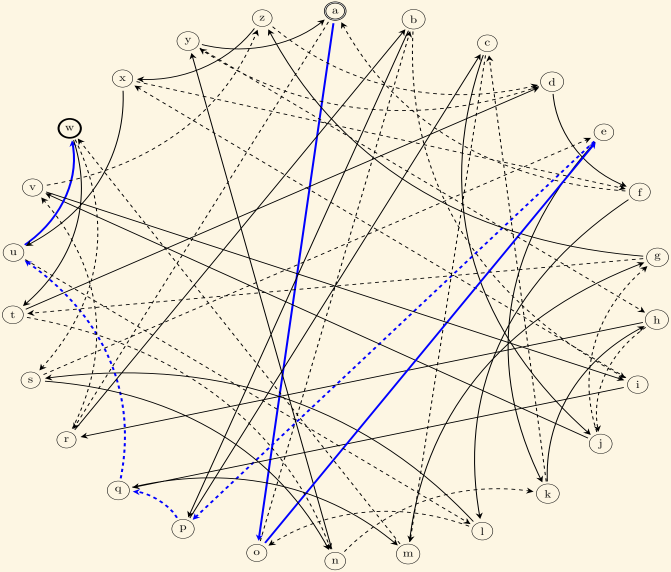
1. Noisy version (codes, lattices)
2. Group action: commutative group G acting on X ($a, b \in G$, $P \in X$).

Key exchange on a (commutative) graph



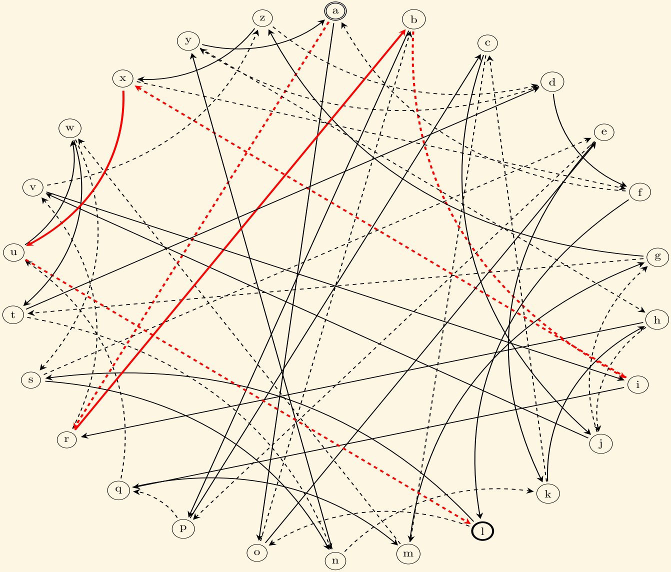
Key exchange on a (commutative) graph

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



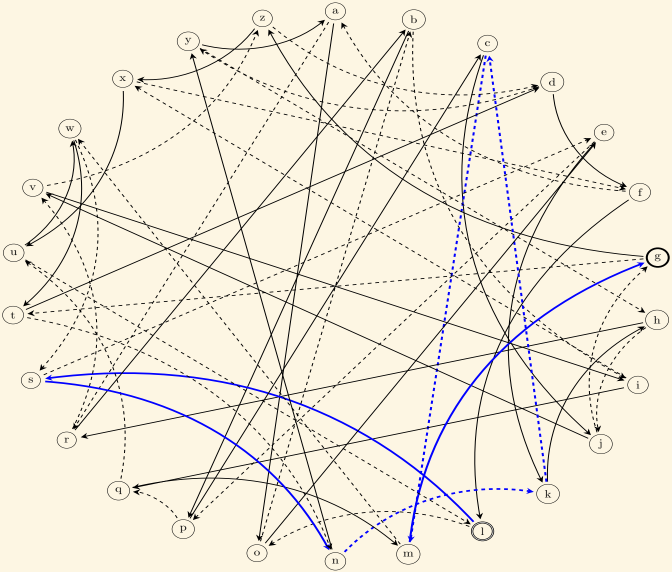
Key exchange on a (commutative) graph

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



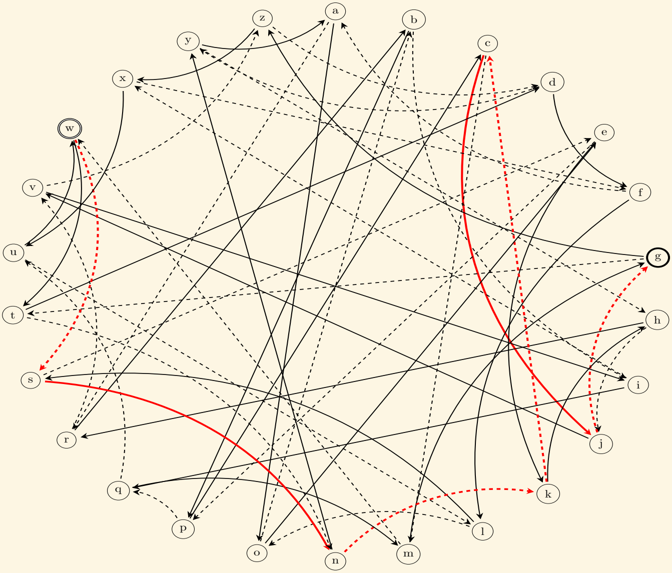
Key exchange on a (commutative) graph

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



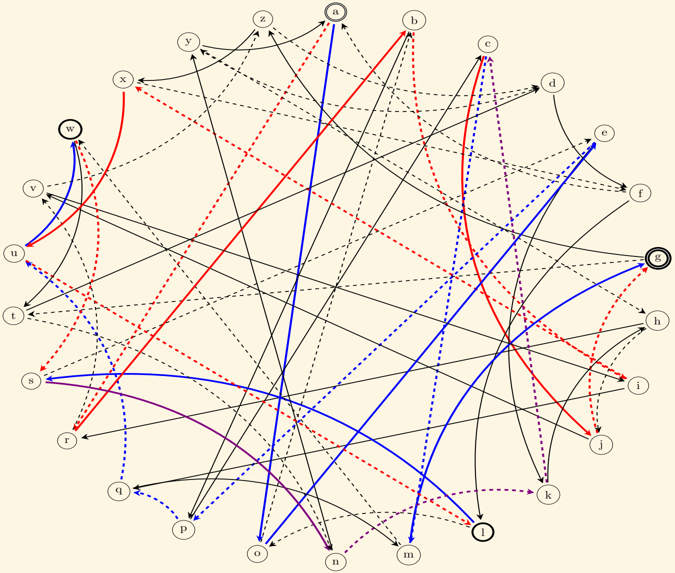
Key exchange on a (commutative) graph

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



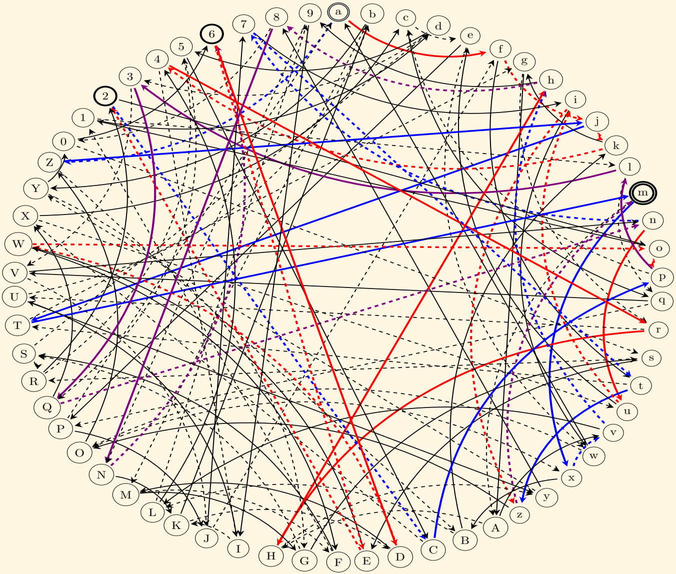
Key exchange on a (commutative) graph

The full exchange:



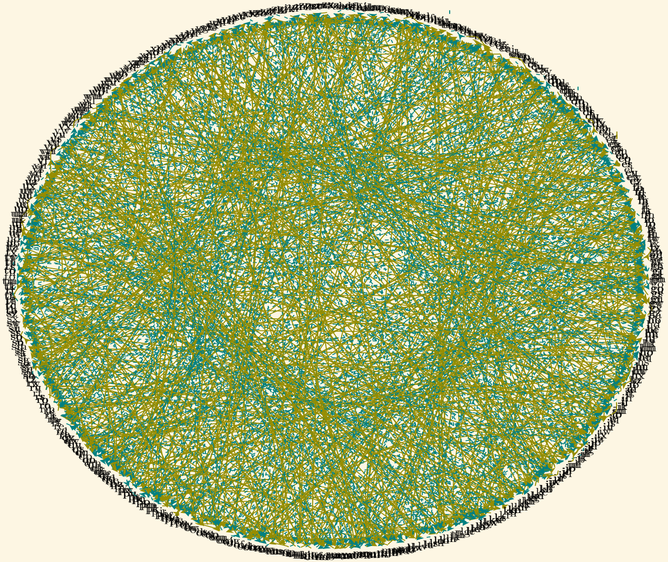
Key exchange on a (commutative) graph

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.
- 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 based cryptography

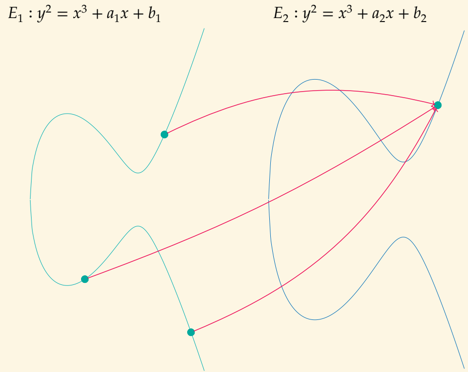
- ☺ Post-quantum
- ☺ Compact keys. SQISign signatures = 177 Bytes (Lattices 666B–2420B)
- ☹ Slow. SQISign (NIST submission): Signature = 550 ms, Verification = 8 ms
- 😐 Very new field (<10 years)
- ☹ Flagship protocol SIKE (post quantum key exchange) broken in 2022.

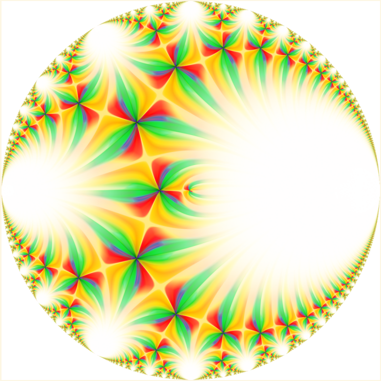
This talk:

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

- Compose several isogenies of this type: isogeny of degree 2^n
- Complexity increases with the size of the largest ℓ dividing N $\quad (O(\ell)$ for an ℓ-isogeny).

☺ Smooth degree isogenies: fast to compute

☹ General isogenies: too expensive

☹ Restricted group action

☹ Inefficiencies

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

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 (polylogarithmic time in the degree)

☺ Considerable flexibility

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

☺ [Page-R. 2023]: Unrestricted group action

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

- [Lubicz, R. et al.] 15+ years of work ($O(\ell^g)$ for an ℓ-isogeny)
- `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

Some mathematical tools

- Moduli spaces: Shimura varieties of PEL type, Algebraic stacks, Hilbert-Blumenthal stacks, Complex Multiplication, Compactifications
  Modular forms: $\phi \in \Lambda^g \pi_* \Omega^1_{\mathcal{X}_g/\mathcal{A}_g} = \sum_n a_n e^{2\pi i \operatorname{Tr}(n\tau)}$, Modular correspondances:
  $\Phi_N : \overline{\mathcal{A}}_g(N) \to \overline{\mathcal{A}}_g \times \overline{\mathcal{A}}_g$ ($\mathcal{A}_g$: moduli of principally polarised abelian schemes)
- Deformations: Heat equation: $2\pi i(1+\delta_{jk})\frac{\partial\theta(z,\tau)}{\partial\tau_{jk}} = \frac{\partial^2\theta(z,\tau)}{\partial z_j \partial z_k}$,
  Kodaira-Spencer isomorphism: $T_{\mathcal{A}_g} \simeq R^1\pi_* T_{\mathcal{X}_g/\mathcal{A}_g} \simeq \operatorname{Lie}_{\mathcal{A}_g}(\mathcal{X}_g) \otimes_{\mathcal{O}_{\mathcal{A}_g}} \operatorname{Lie}_{\mathcal{A}_g}(\mathcal{X}_g^\vee)$,
  Gauss-Manin connection: $R^n f_* \Omega_{X/S} \to \Omega^1_S \otimes R^n f_* \Omega_{X/S}$,
  Picard-Fuchs equation: $(\lambda^3 - 27)\frac{\partial^2\omega_\lambda}{\partial\lambda^2} + 3\lambda^2 \frac{\partial\omega_\lambda}{\partial\lambda} + \lambda\omega_\lambda = 0$,
- Lifting and reductions: p-divisible groups $A(p)$ and their crystals $\mathbb{D}(A(p))$, Serre-Tate + Grothendieck-Messing theory, canonical lifts, Hoge-Tate decomposition, Néron models, semi-stability, semi-abelian varieties
- Point counting and L-functions: étale cohomology: $H^1_{et}(A_{\overline{k}}, \mathbb{Z}_\ell) = \operatorname{Hom}(T_\ell(A_{\overline{k}}), \mathbb{Z}_\ell)$, crystalline cohomology: $H^1_{crys}(A/W(k)) \simeq \mathbb{D}(A(p))_{W(k)}$, Monsky-Washnitzer/rigid cohomology, De Rham cohomology, Hodge filtration: $0 \to H^0(A, \Omega^0_{A/k}) \to H^1_{dR}(A) \to H^1(A, O_A) \to 0$
- Coordinates: Heisenberg groups and representations, algebraic theta functions, Fourier-Mukai transform: $R\Phi_{P_A} : D^b_{coh}(O_A) \to D^b_{coh}(O_{A^\vee})$
- Pairings: biextensions, cubical torsors. Curves: hyperelliptic curves, minimal models
- Heights: Néron-Tate height, Faltings-Raynaud isogeny formula, intersections
- Equivalences of categories: Hermitian modules