FAST — (Harder Better) FAster STronger Cryptography

2018/09/18 — LIRIMA Meeting, Paris, France

Damien Robert

Équipe LFANT, Inria Bordeaux Sud-Ouest

Goal

Cryptology:

- Encryption;
- Authenticity;
- Integrity.

Public key cryptology is based on a one way (trapdoor) function $\Rightarrow$ asymmetric encryption, signatures, zero-knowledge proofs...

Goal: Improve and extend elliptic curve cryptography to

- Secure the Internet of Things;
- Prepare the next generation of cryptosystems able to resist to quantum computers.

Organisation

- Joint team between LFANT (Lithe and fast algorithmic number theory) https://lfant.math.u-bordeaux.fr/ and PREMA (the Pole of Research in Mathematics and Applications in Africa) http://prmasi.org/;
- Project coordinators: Tony Ezome, Senior Lecturer/Researcher (Cames), University of Sciences and Technology of Masuku (USTM), and Damien Robert (CR Inria).
- PREMA is a Simon's fundation project involving researchers in Cameroun, Gabon, Madagascar, Sénégal along with members in Cote d'Ivoire, Maroc, South Africa and international collaborators in Canada, France, the Netherlands, Singapore.

Results

- Efficiency
  - Improving randomness extractions ([KSC+17; CS17]), pseudo-random generators and pseudo-random functions [MV17b].
  - Improving arithmetic and pairing on elliptic curves [GF18; FD17].
- Post quantum cryptography
  - Pairing based signatures [MV17a]
  - Isogenies: modular polynomials for cyclic isogenies between abelian surfaces [MR17], cyclic isogenies given their kernels [DJR+17].
- Work in progress:
  - Constructing normal basis [ES].
  - Attribute based credentials for IoT [CS]
  - Computing canonical lift of genus 2 curves;
  - Computing the kernel between two isogenous genus 2 curves.
- Diffusion
  - Book chapter "Pairings" of the book "Guide to Pairing-Based Cryptography" [EJ17].
  - T. M. Nountu. "Pseudo-Random Generators and Pseudo-Random Functions: Cryptanalysis and Complexity Measures". PhD thesis. Paris Sciences et Lettres, 2017

Scientific activities for the years 2017–2018

- Participation to the organization of Eurocrypt 2017 (from 30 April to 4th May 2017 in Paris);
- EMA “Mathématiques pour la Cryptographie Post-quantique et Mathématiques pour le Traitement du Signal” at the École Polytechnique de Thiès (Sénégal) from May 10 to May 23 2017.
- Kickstart workshop in Bordeaux (from September 04 to September 08 2017). Slides or proceedings available at `https://lfant.math.u-bordeaux.fr/index.php?category=seminar&page=2017`.
- Ecole Mathématique Africaine (from April 02 to 04 2018 at Franceville), `http://prmasi.org/african-mathematical-school-ams-from-april-02-to-april-14-2018`
    - Jacobian varieties, discrete logarithm, Diffie-Hellman key exchange, Elgamal cryptosystem and an introduction to semi-algebraic geometry
    - p-adic fields and number fields
    - Initiation to Pari-GP.

An introduction to public key cryptography: key exchange

- How to exchange a secret key across a public channel?
- Diffie-Helmann (1976): let $g \in G$ be an element of a group
- Alice uses a random a and sends g^a;
- Bob uses a random b and sends g^b;
- Common secret key: $g^{ab} = g^{ab} = g^{ba}$
- Attack: Diffie-Helmann problem: recover g^{ab} from (g, g^a, g^b).
- Easy when the Discrete Logarithm Problem (DLP) is easy;
- In a generic group can be reduced to the DLP.

An introduction to public key cryptography: key exchange

- How to exchange a secret key across a public channel?
- Diffie-Helmann (1976): let $g \in G$ be an element of a group
- Alice uses a random a and sends g^a;
- Bob uses a random b and sends g^b;
- Common secret key: $g^{ab} = g^{ab} = g^{ba}$
- Attack: Diffie-Helmann problem: recover g^{ab} from (g, g^a, g^b).
- Easy when the Discrete Logarithm Problem (DLP) is easy;
- In a generic group can be reduced to the DLP.

An introduction to public key cryptography: key exchange

- How to exchange a secret key across a public channel?
- Diffie-Helmann (1976): let $g \in G$ be an element of a group
- Alice uses a random a and sends g^a;
- Bob uses a random b and sends g^b;
- Common secret key: $g^{ab} = g^{a\,b} = g^{b\,a}$
- Attack: Diffie-Helmann problem: recover g^{ab} from (g, g^a, g^b).
- Easy when the Discrete Logarithm Problem (DLP) is easy;
- In a generic group can be reduced to the DLP.

An introduction to public key cryptography: key exchange

- How to exchange a secret key across a public channel?
- Diffie-Helmann (1976): let $g \in G$ be an element of a group
- Alice uses a random a and sends g^a;
- Bob uses a random b and sends g^b;
- Common secret key: $g^{ab} = g^{a\,b} = g^{b\,a}$
- Attack: Diffie-Helmann problem: recover g^{ab} from (g, g^a, g^b).
- Easy when the Discrete Logarithm Problem (DLP) is easy;
- In a generic group can be reduced to the DLP.

An introduction to public key cryptography: El Gamal encryption

- Public key of Alice: (g, g^a), Secret key of Alice: a.
- Encryption: choose a random r and send $(g^r, m \times g^{ar})$;
- Decryption: Alice compute g^{ar} from which she recovers m.

Choice of the base group

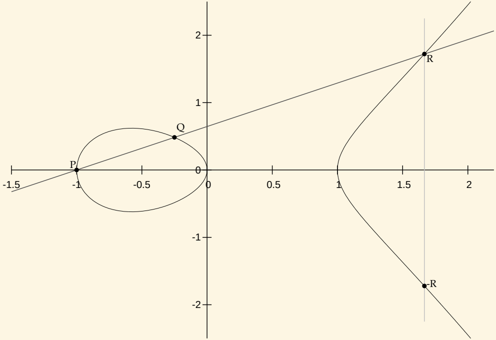
- $G = \mathbb{Z}/n\mathbb{Z}$: polynomial attack in $O(\log n^2)$;
- $G = \mathbb{F}_q^*$: subexponential attack in $\widetilde{O}(2^{\log q^{1/3}})$;
- $G = E(\mathbb{F}_q)$ (for a suitable elliptic curve over $\mathbb{F}_q$): exponential attack in $\widetilde{O}(\sqrt{q})$

Elliptic curves

Definition (char $k \neq 2,3$)

An elliptic curve is a plane curve

$$y^2 = x^3 + ax + b \qquad 4a^3 + 27b^2 \neq 0.$$



Exponentiation:

$$(\ell, P) \mapsto \ell P$$

DLP:

$$(P, \ell P) \mapsto \ell$$

ECC vs RSA for 128 bits of security

- ECC (Curve25519) 256 bits:

AAAAC3NzaC1lZDI1NTE5AAAAIMoNrNYhU7CY1Xs6v4Nm1V6oRHs/FEE8P+XaZ0PcxPzz

- RSA 3248 bits:

MIIHRgIBAAKCAZcAvlGW+b5L2tmqb5bUJMrfLHgr2jga/Q/8IJ5QJqeSsB7xLVT/
ODN3KNSPxyjaHmDNdDTwgsikZvPYeyZWWFLP0B0vgwDqQugUGHVfg4c73ZolqZk6
1nA45XZGHUPt98p4+ghPag5JyvAVsf1cF/VlttBHbu/noyIAC4F3tHP81nn+lOnB
eilEALbdmvGTTZ5jcRrt4IDT5a4IeI9yTe0aVdTsUJ6990hpKrVzyTOu1eoxp5eV
KQ7aIX6es9Xjnr8widZunM8rqhBW9EMmLqabnXZItPQoV3rUAnwKzDLV7E56viJk
S2xU5+95IctYu/RTTbf3wTxnkDOqxId0MONHyBJsukXgYKxVB1fWhBKZ4tWui1gw
UCIiKTqLml2zJhLn4WovaxrvvTx0082S0xncEfYDXYu4xbRnJn+ZsTTguqufwC1M
U4MYRdWy7uj+H1EmIGul69Fw9NkuCitWI9dFpcDtSP+/1eEN7wc2FlxhDIRwer0F
6I1P4StWn1uQyHzsTLVdcP+rqA1AsvbWBCKL4ravEO2CEQIDAQABAoIBllWt5YoJ
YZzk4RXbkSX/LvmWICfdmkjTKW6F1w+P4TnotCr0WPG0ObDoANJoUcnbSqNGMgCu
01SF8q9+UuDwZx4KBZm0j8IPOPzJ2nYcK5dYDhyMHzDq1LJ4zJfgPQGQ5WWq2BWm
2RHDhADdTth6YZArs/z9hAqtA9gqMPnMPcdQpIvlsHSOn06zBJD8sJQA+kOxG+Y2
GS8NakLcUVlDpNd/Q+QHkv4AW1ge2EF8QvmKtU/9rekOBqWNm2Tapd6RtAhZwPJX
UhD9yiesTF6rjZ1ZcMGXUaN5Rt0zD3D4zowRz2JLtCe4GkiJmtc3waN6hu1IaIqz
boI11evqnbatqnC4rCq8sf21yZqaLUIbwH4lW2G3K8xMJNh3iy8cgHTYneNYa+/d
7xyNWlMO9SKlHsyaPcWv98BdD+At0x/6R6YPYkeR+qXJ9ETGFKW4U6iNbBQXOMbh
kZb1Ry8vfMH8vsYIzh8Edg6aq00ScU57KiDS/Gc8KuqI6vmf2leCdCa487kVCgw6
cGXQ2bLZGYBiMZFfOOlpCQECgcwA5ZUh3/8yS0duNhsDz3sgC2u40HwHUbxuSOUa
a5t4CoUY9iuF7b7qhBEcvdLgIOiXA5xo+r4p0xgbLvDUTsRR1mrDM2+wRcjjwXcW
pFaMFRl2Rr72yLUC7N0WNcoUshrNL4X/1j8T4WLRcannpXcor+/kn1rwdLEbRCC+
zRTAdJlgMPt4kwJeHtE9Mzw2/O3GX3MeLvzvJklzvpCGw20N/2Yqjs++V5hXoHPs
21y6y6/FV097dvFctf7NahS04JsjubfnjOMx89AUNZsCgcwA1DfabCGJSCkmQ+mg
2q9lDPJz6r29wmBtYyT20oZ2kd4QBHrOp0t59yG4bvdRqcZG/Dr5LjuVDWMPyetV
dksK7hVYQz2B7Nzy7W3waPVrhA0N4fqbIFGxih5QiSFG7/oroZ8PdZDcfVRKroh1
/JJ7rIz/ZBQCLRS5t7/G2B0kBDOMMM+02wR60CTmxUhmgvsoDZWRp5KKha5PSvZa
WAu2CN3mXNK72RLF3RFUvuhNYnkOEj5Oau1RaGgpZoB0JTKYI9nffbe8up+DV8MC
gcwA18be28Ti5FXyg+/IGQ3EBHfucCTiTDQqA2Ew/8pTfK+z0kr9yYISsKXUuaSk
+skghkhPcrugW8LgabH4GT/zGu+lH4btyekSBxeCtFqTtpED1WJOWD2ozi7NXSjd
YrhF+VCcMCWA7ekOqSHjkmT4XMO/wPab4VFEKzgLnHzQlcZB3ke7/4/OHnDScIE7
vWVNeRCdYdRggT+wBX+Y6bxp142Smj8uyu1oDmpmR5ZUCnTdqT4O8K/RT0x4jCeC
CUhGv5rVillO7bS4CdkCgctXvnQwCzmwvVrV744TfTuhu8lTwHnqGWaA/LKU3wW9
T/x9ba1uHFXkaWvRba61LIcDGPsYM4hwTYokqYnfbC2rvOWOf6rtnXlP1An3y6lV
ovQfgDeNiFmIyvnviPPEm0JZA+QnburLYwOx4DgwYvyBnpal8WPo8c3L/J4hkwLm
Pc30DJ0xhUumLevAnCyOcjvgSfw8NenSVfzw+KToDIeKaP0rWfJTUWDAA79yY6tD

Quantum algorithms: Hidden subgroup problem

- Hidden subgroup problem:

$$f : G \to X$$

Goal: recover the largest subgroup H such that

$$f : G \to G/H \to X$$

- Polynomial time quantum algorithm for solving HSP over finite Abelian groups based on the quantum Fourier transform.
- Exemple: let $f : \mathbb{Z}/N\mathbb{Z} \to X$ be a function periodic with period r. Classical algorithm to find r: $O(N)$. Quantum algorithm: $O(\log N^2)$.

⇒ Break factorisation;

⇒ Break the DLP.

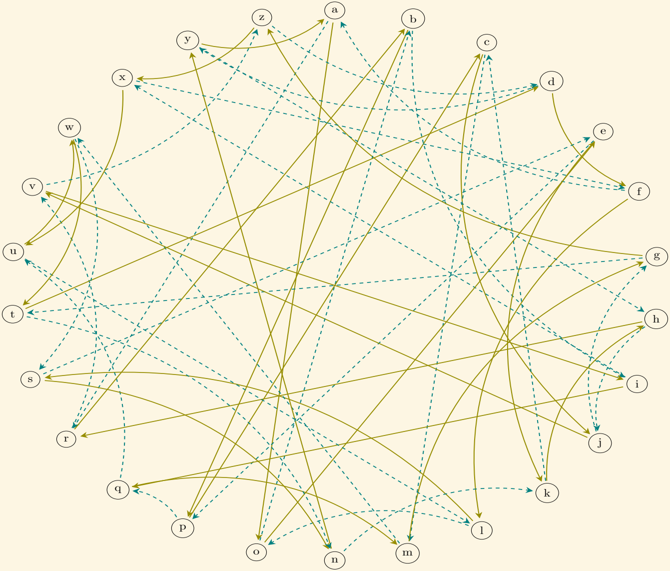
Extending DH key exchange

- Let G be an abelian group acting on X.
- Fix a base point $x \in X$.
- Alice chooses a secret $a \in G$ and sends $a.x$;
- Bob chooses a secret $b \in G$ and sends $b.x$;
- The common key is $ab.x = ba.x \in X$.

Example

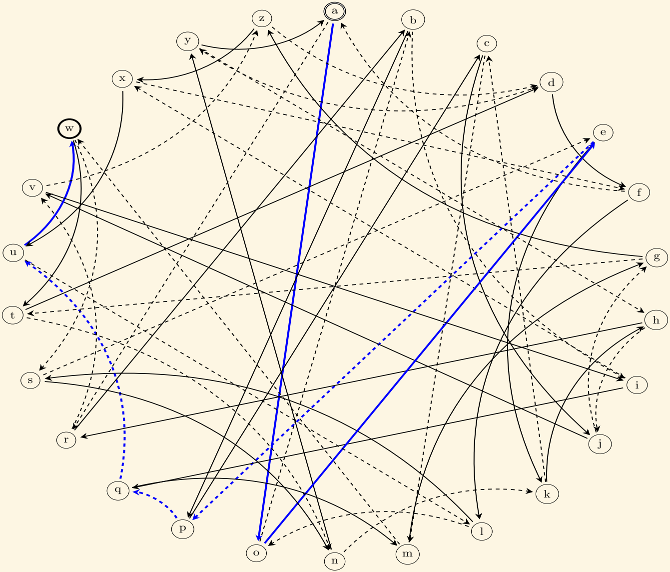
Key exchange on the Cayley graph of an abelian group.

Key exchange on a graph



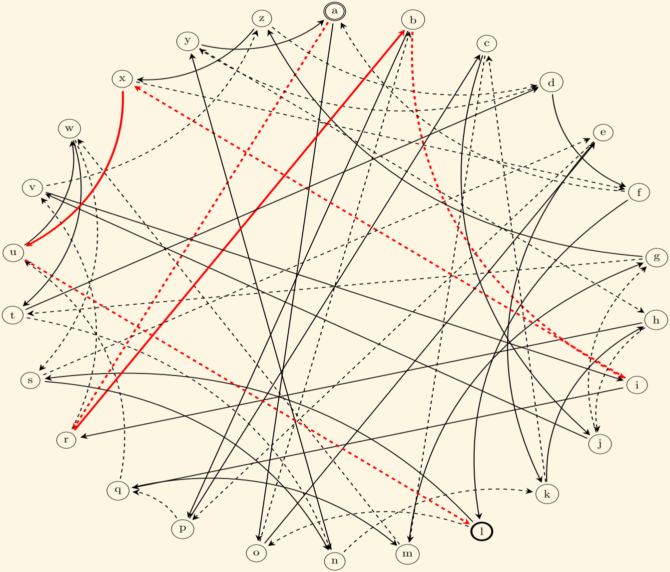
Key exchange on a graph

Alice starts from ‘a’, follow the path 001110, and get ‘w’.



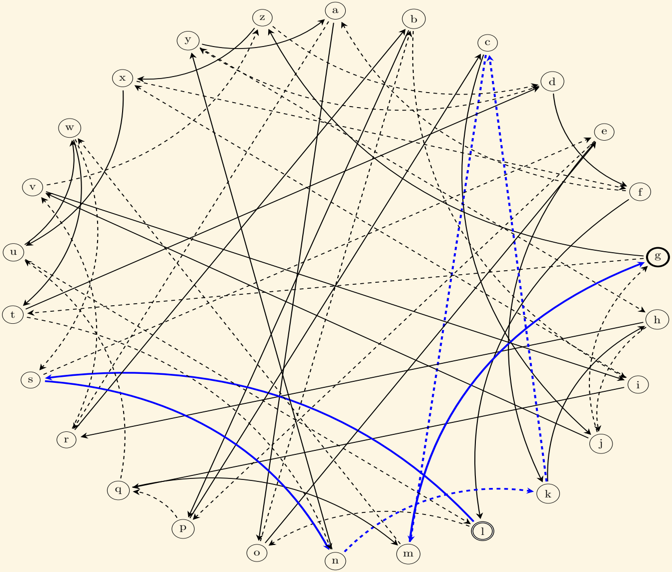
Key exchange on a graph

Bob starts from ‘a’, follow the path 101101, and get ‘l’.



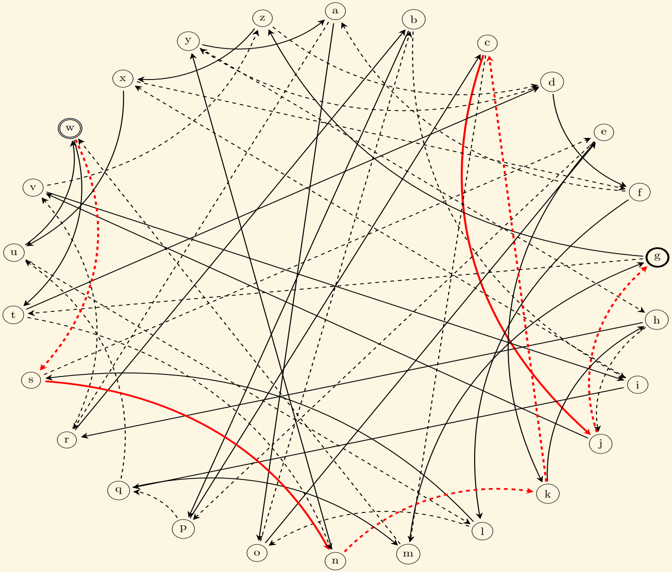
Key exchange on a graph

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



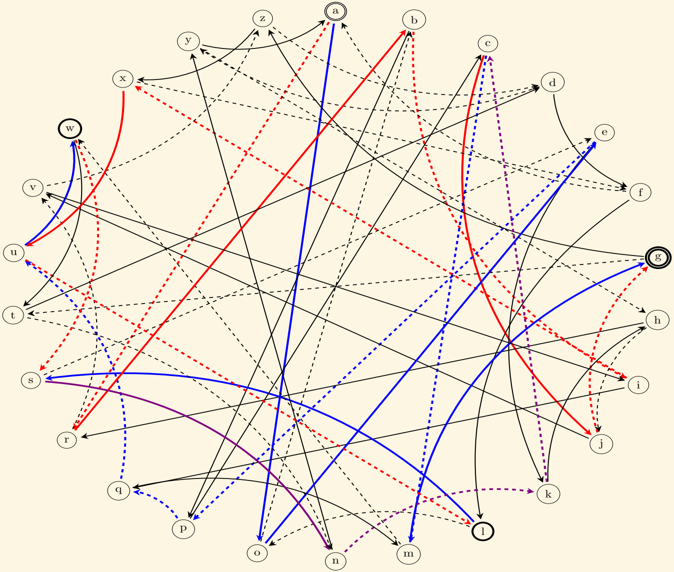
Key exchange on a graph

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



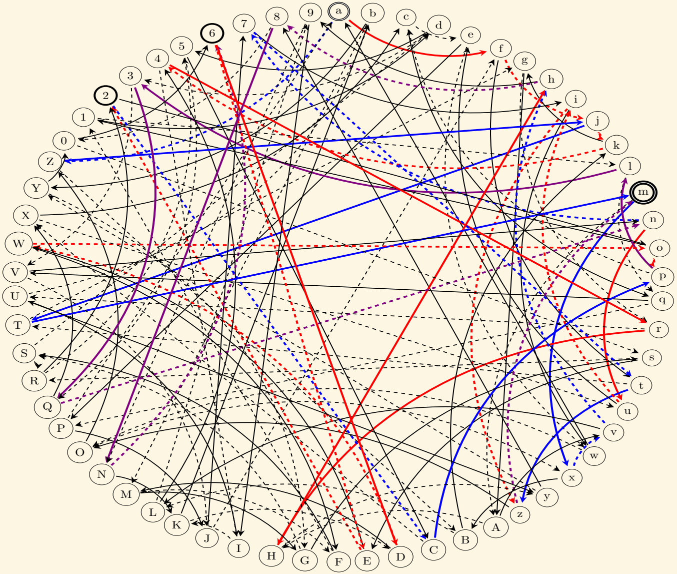
Key exchange on a graph

The full exchange:



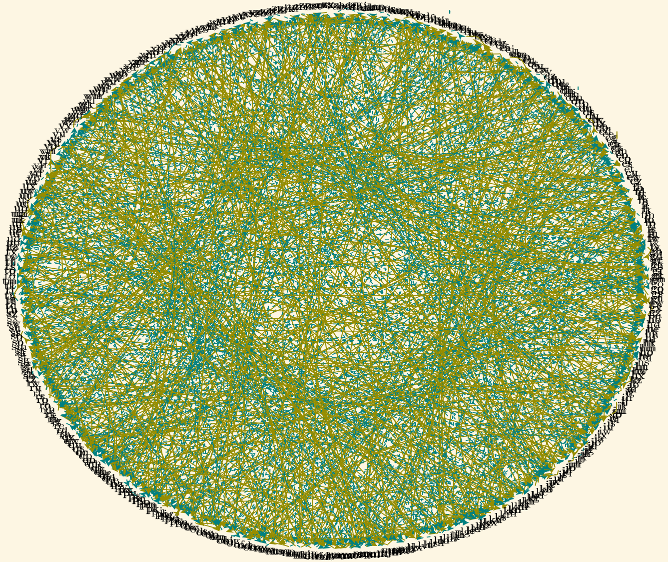
Key exchange on a graph

Bigger graph (62 nodes)



Key exchange on a graph

Even bigger graph (676 nodes)



Elliptic curves isogeny key exchange (Couveignes, Rostovtsev and Stolbunov)

- Use the horizontal isogeny graph of an ordinary elliptic curve E over $\mathbb{F}_q$.
- This is in fact the Cayley graph of the class group of the endomorphism ring of E, which is an imaginary quadratic order.
- For cryptography, choose a curve such that the graph has 2^{256} nodes.
- Unlike standard Diffie-Helmann, the cryptosystem is not restricted to one curve, it is now all the curves in the isogeny class! In other words the base point is not a rational point in an elliptic curve, but an elliptic curve seen as a point in its moduli space.

Quantum algorithms: Hidden shift problem

- G acts on X, f, g two functions $X \to Y$ such that

$$\exists s \in G \mid \forall x \in X, f(x) = g(s.x).$$

- Goal: recover s.
- Polynomial quantum algorithms if G is cyclic;
- Subexponential quantum algorithms if G is abelian;
- No subexponential quantum algorithm known if G is not abelian;

SIDH: supersingular elliptic curve Diffie-Helmann (De Feo, Jao, Plût)

- Use the isogeny graph of a supersingular elliptic curve E over $\mathbb{F}_{p^2}$.
- There are $O(p)$ nodes and the graph is an expander graph.
- The endomorphism ring is a quaternion algebra (ramified at p and infinity), which is non commutative.
- The isogeny graph is a Cayley graph for the groupoid class group.
- The key exchange can be seen as a pushforward:

$$E/K_A \otimes_E E/K_B = E/(K_A + K_B)$$

- Problem: to compute this pushforward, Alice and Bob need to send more informations (the image of some points by the isogeny). Can this extra information be used by an attacker?
- Best currently known attack: find a path to a supersingular elliptic curve defined over $\mathbb{F}_p$ (where the rational endomorphism ring is commutative). There are $O(\sqrt{p})$ such curves, so Grover's algorithm find such a path in time $O(p^{1/4})$.

$\Rightarrow$ Needs p of 1024 bits.

SIDH: supersingular elliptic curve Diffie-Helmann (De Feo, Jao, Plût)

- Use the isogeny graph of a supersingular elliptic curve E over $\mathbb{F}_{p^2}$.
- There are $O(p)$ nodes and the graph is an expander graph.
- The endomorphism ring is a quaternion algebra (ramified at p and infinity), which is non commutative.
- The isogeny graph is a Cayley graph for the groupoid class group.
- The key exchange can be seen as a pushforward:

$$E/K_A \otimes_E E/K_B = E/(K_A + K_B)$$

- Problem: to compute this pushforward, Alice and Bob need to send more informations (the image of some points by the isogeny). Can this extra information be used by an attacker?
- Best currently known attack: find a path to a supersingular elliptic curve defined over $\mathbb{F}_p$ (where the rational endomorphism ring is commutative). There are $O(\sqrt{p})$ such curves, so Grover's algorithm find such a path in time $O(p^{1/4})$.

$\Rightarrow$ Needs p of 1024 bits.

Using SIDH

- Key exchange: starting with E, Alice sends E/K_A (+ extra informations), Bob sends E/K_B, the common secret key is $E/(K_A+K_B)$.
- The curves E, E/K_A, E/K_B are public, the secrets are the kernel K_A and K_B (alternatively the secrets are the paths in the isogeny graph).
- If $\alpha : E \rightarrow E/K_A$ and $\beta : E/K_B$ are the isogenies (which are secrets), the extra informations allow Alice to compute $\beta(K_A)$ and the common key $E/(K_A+K_B) = (E/K_B)/\beta(K_A)$;
- Likewise Bob computes the common key $E/(K_A+K_B) = (E/K_A)/\alpha(K_B)$.

- Zero knowledge authentification: Alice has a secret K_A. She wants to prove she knows K_A without revealing it.
- She publish $(E, E/K_A)$. Bob does several challenges:
- Alice take a random K_B and publish $(E/K_B, E/(K_A+K_B))$.
- Bob either asks for K_B and checks that E/K_B is correct;
- Or Bob asks for $\beta(K_A) \subset E/K_B$ and checks that $E/(K_A+K_B) = (E/K_B)/\beta(K_A)$.

Bibliography

A. A. Ciss and I. Sène. "Efficient Attribute based credentials for IoT". (Cit. on p. 4).

A. A. Ciss and D. Sow. "Two-Source Randomness Extractors for Elliptic Curves for Authenticated Key Exchange". In: *International Conference on Codes, Cryptology, and Information Security*. Springer. 2017, pp. 85–95 (cit. on p. 4).

A. Dudeanu, D. Jetchev, D. Robert, and M. Vuille. "Cyclic Isogenies for Abelian Varieties with Real Multiplication". working paper or preprint. Nov. 2017. URL: https://hal.inria.fr/hal-01629829 (cit. on p. 4).

N. El Mrabet and M. Joye. *Guide to Pairing-Based Cryptography*. CRC Press, 2017 (cit. on p. 4).

T. Ezome and M. Sall. "Normal Bases using 1-dimensional Algebraic Groups". (Cit. on p. 4).

E. Fouotsa and O. Diao. "A Theta Model for Elliptic Curves". In: *Mediterranean Journal of Mathematics* 14.2 (2017), p. 65 (cit. on p. 4).

L. Ghammam and E. Fouotsa. "Improving the computation of the optimal ate pairing for a high security level". In: *Journal of Applied Mathematics and Computing* (2018), pp. 1–16 (cit. on p. 4).

D. Kolyang, D. Sow, A. A. Ciss, and H. B. Tchapgnouo. "Two-sources randomness extractors in finite fields and in elliptic curves". In: *REVUE AFRICAINE DE LA RECHERCHE EN INFORMATIQUE ET MATHÉMATIQUES APPLIQUÉES* 24 (2017) (cit. on p. 4).

T. Mefenza and D. Vergnaud. "Lattice Attacks on Pairing-Based Signatures". In: *IMA International Conference on Cryptography and Coding*. Springer. 2017, pp. 352–370 (cit. on p. 4).

T. Mefenza and D. Vergnaud. "Polynomial interpolation of the Naor–Reingold pseudo-random function". In: *Applicable Algebra in Engineering, Communication and Computing* 28.3 (2017), pp. 237–255 (cit. on p. 4).

E. Milio and D. Robert. "Modular polynomials on Hilbert surfaces". working paper or preprint. Sept. 2017. URL: https://hal.archives-ouvertes.fr/hal-01520262 (cit. on p. 4).

T. M. Nountu. "Pseudo-Random Generators and Pseudo-Random Functions: Cryptanalysis and Complexity Measures". PhD thesis. Paris Sciences et Lettres, 2017 (cit. on p. 4).