CIAO — Cryptography, Isogenies and Abelians varieties

Overwhelming

2019/11/06 — ANR Meeting, Paris, France

Damien Robert

Équipe LFANT, Inria Bordeaux Sud-Ouest

Elliptic curve cryptography

Currently, the best standard public key cryptography system:

- ☺ Extremely small parameters (256 bits);
- ☺ Extremely fast;
- ☺ More powerful than RSA;
- ☹ Broken by quantum computers.

Goal: Post quantum elliptic cryptography

Elliptic curve cryptography

Currently, the best standard public key cryptography system:

- ☺ Extremely small parameters (256 bits);
- ☺ Extremely fast;
- ☺ More powerful than RSA;
- ☹ Broken by quantum computers.

Goal: Post quantum elliptic cryptography

Public 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.

Public 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.

Public 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.

Public 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: $g^{ab} = g^{a\,b} = g^{b\,a}$

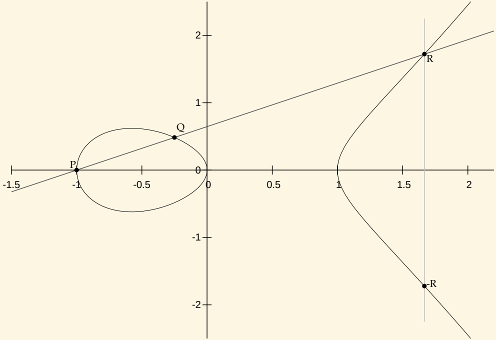
- Attack: Diffie-Helmann problem: recover g^{ab} from (g, g^a, g^b).
- Easy when the Discrete Logarithm Problem (DLP) is easy;
- In a generic group can be reduced to the DLP.

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

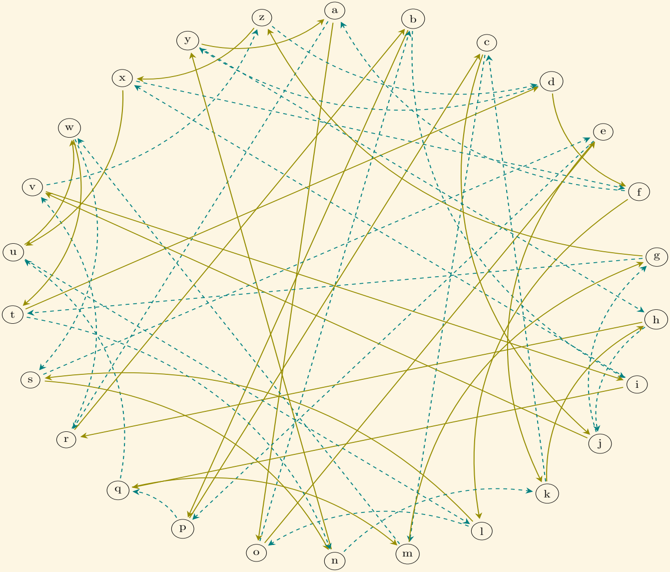
- ECC (Curve25519) 256 bits:

AAAAC3NzaC1lZDI1NTE5AAAAIMoNrNYhU7CY1Xs6v4Nm1V6oRHs/FEE8P+XaZ0PcxPzz

- RSA 3248 bits:

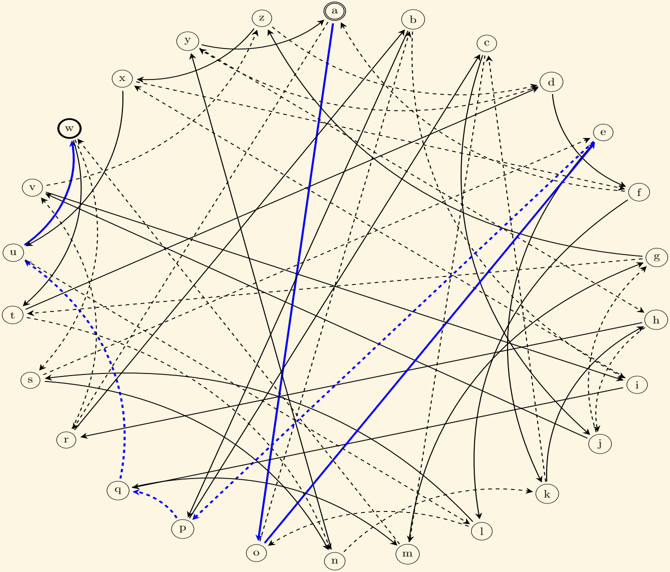
MIIHRgIBAAKCAZcAvlGW+b5L2tmqb5bUJMrfLHgr2jga/Q/8IJ5QJqeSsB7xLVT/
ODN3KNSPxyjaHmDNdDTwgsikZvPYeyZWWFLP0B0vgwDqQugUGHVfg4c73ZolqZk6
1nA45XZGHUPt98p4+ghPag5JyvAVsf1cF/VlttBHbu/noyIAC4F3tHP81nn+lOnB
eilEALbdmvGTTZ5jcRrt4IDT5a4IeI9yTe0aVdTsUJ6990hpKrVzyTOu1eoxp5eV
KQ7aIX6es9Xjnr8widZunM8rqhBW9EMmLqabnXZItPQoV3rUAnwKzDLV7E56viJk
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
Pc30DJ0xhUumLevAnCvOcjvgSfw8NenSVfzw+KToDIeKaP0rWfJTUWDAA79vY6tD

Key exchange on a graph



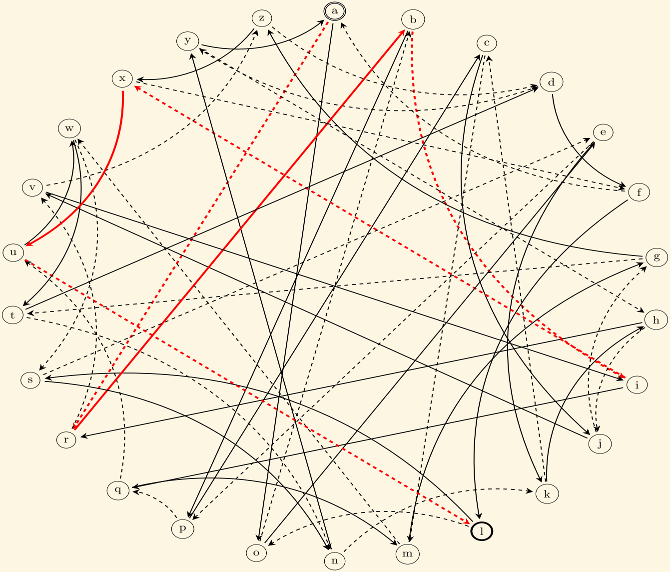
Key exchange on a graph

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



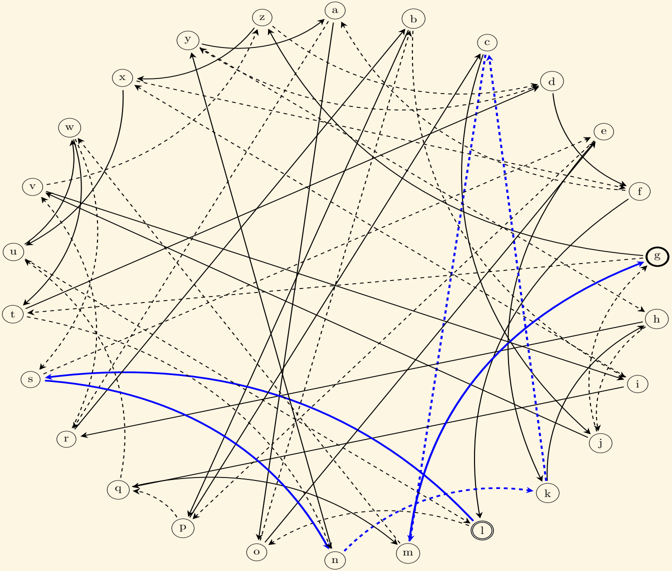
Key exchange on a graph

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

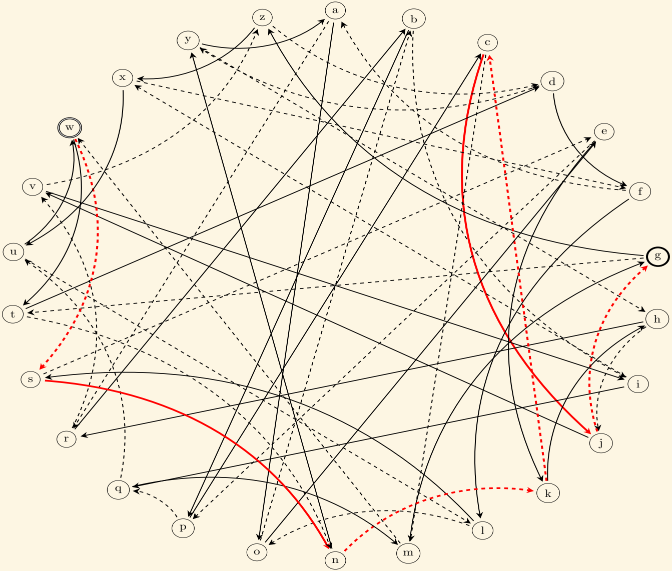


Key exchange on a graph

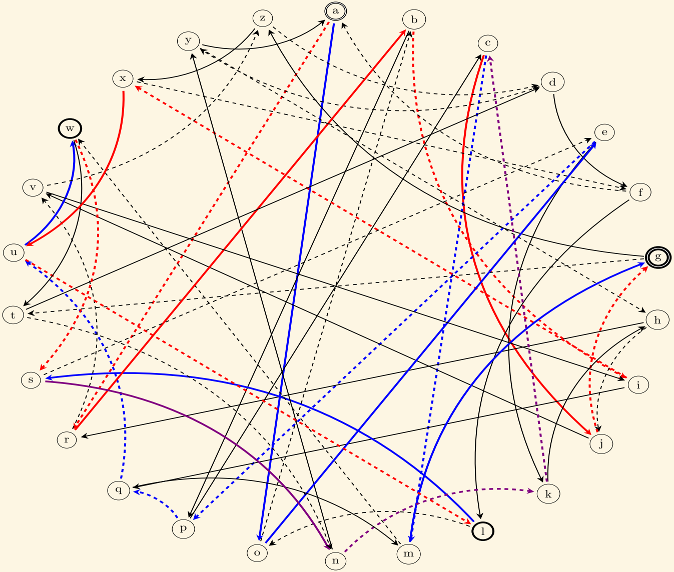
Alice starts from ‘l’, follows the path 001110, and get ‘g’.



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

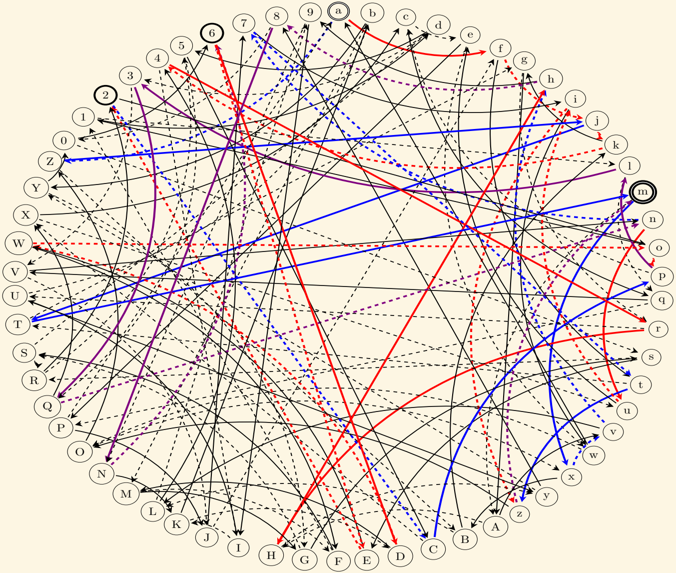


The full exchange:



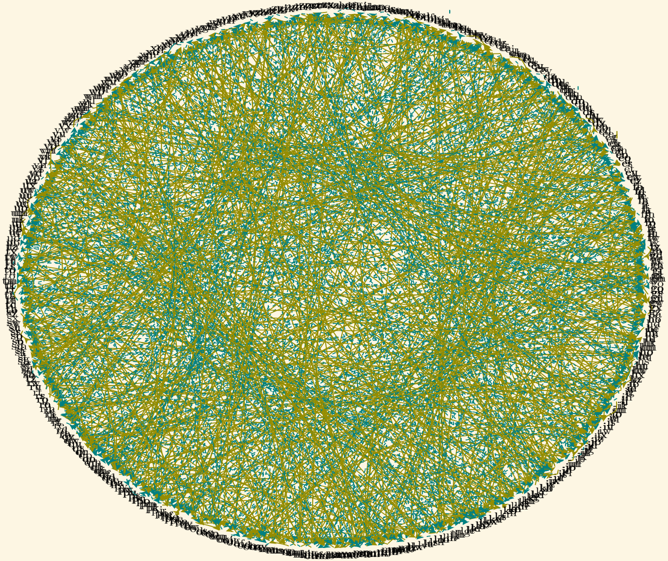
Key exchange on a graph

Bigger graph (62 nodes)



Key exchange on a graph

Even bigger graph (676 nodes)



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:

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

⇒ Needs p of 512 bits, and total key size is 2048 bits.

Organisation

- Project coordinator: Damien Robert (CR Inria Bordeaux).
- Members in Bordeaux: Bill Allombert, Jean-Marc Couveignes, Jean Kieffer, Aurel Page
- Exterior members: Luca De Feo, Benjamin Smith (Paris), Cyril Bouvier, Laurent Imbert (Montpellier)
- Temporary members: Jean Kieffer (PhD student), one year postdoc.

Work program

- Computational aspects of isogenies: arithmetic over finite fields, efficient isogenies, models for elliptic curves, implementations.
- Cryptographic protocols related to isogenies: Key exchange and encryption, Signatures and authentication, Verifiable Delay Functions
- Higher dimensional isogenies: isogenies for abelian varieties, moduli spaces, isogeny graphs, Higher dimensional supersingular isogeny Diffie–Hellman
- Security of isogeny-based cryptosystems: security reductions and security parameters, point counting and endomorphism rings computation, security in the wild