Algorithmic number theory and cryptography

2016/01/07 — Inria Bordeaux

Damien Robert

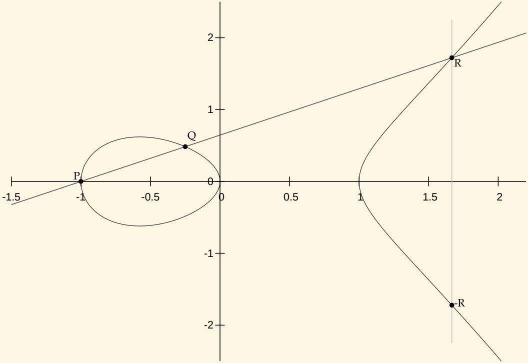
Équipe LFANT, Inria Bordeaux Sud-Ouest

Elliptic curves

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

An elliptic curve is a plane curve with equation

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



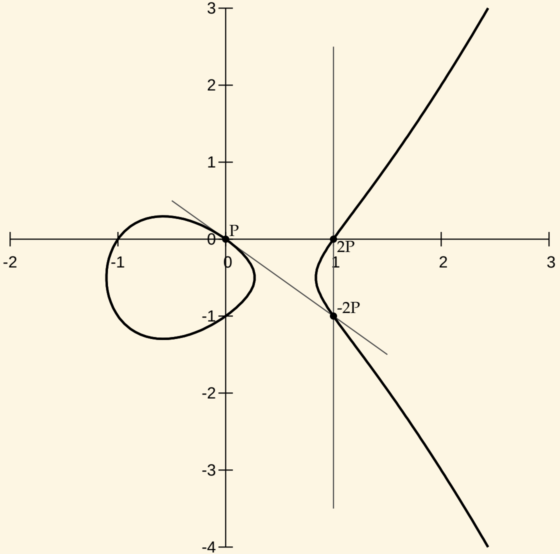
Exponentiation:

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

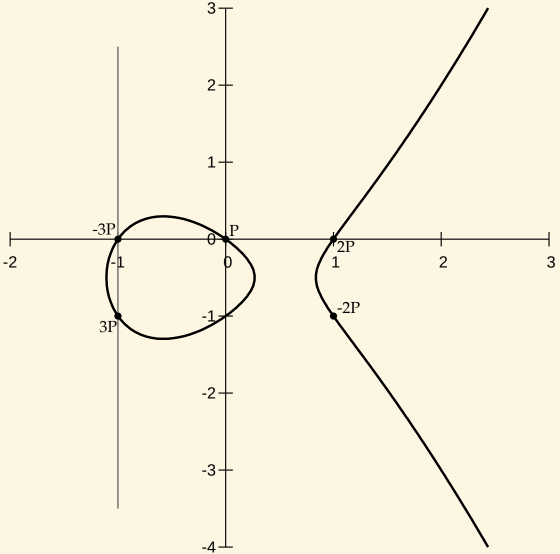
Discrete logarithm:

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

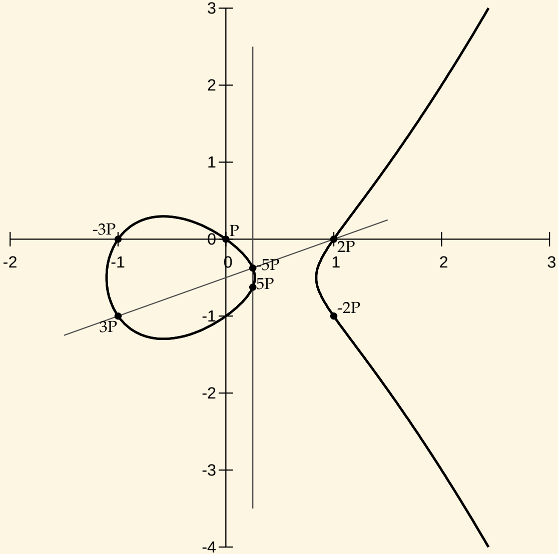
Scalar multiplication on an elliptic curve



Scalar multiplication on an elliptic curve



Scalar multiplication on an elliptic curve



ECC (Elliptic curve cryptography)

Example (NIST-p-256)

- E elliptic curve
  $y^2 = x^3 - 3x + 41058363725152142129326129780047268409114441015993725554835256314039467401291$
  over $\mathbb{F}_{115792089210356248762697446949407573530086143415290314195533631308867097853951}$
- Public key:
  $$P = (48439561293906451759052585252797914202762949526041747995844080717082404635286,\\ 36134250956749795798585127919587881956611106672985015071877198253568414405109),$$
  $$Q = (76028141830806192577282777898750452406210805147329580134802140726480409897389,\\ 85583728422624684878257214555223946135008937421540868848199576276874939903729)$$
- Private key: ℓ such that $Q = \ell P$.

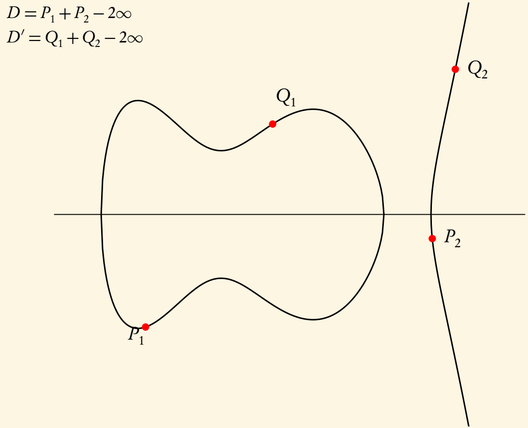
- Used by the NSA;
- Used in Europeans biometric passports.

Higher dimension

Dimension 2:

Addition law on the Jacobian of an hyperelliptic curve of genus 2:

$$y^2 = f(x), \deg f = 5.$$



Higher dimension

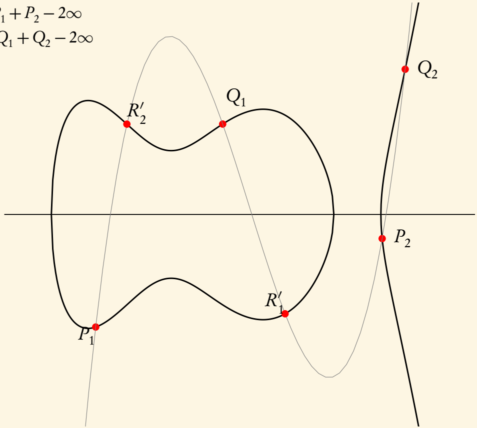
Dimension 2:

Addition law on the Jacobian of an hyperelliptic curve of genus 2:

$$y^2 = f(x), \deg f = 5.$$

$D = P_1 + P_2 - 2\infty$

$D' = Q_1 + Q_2 - 2\infty$

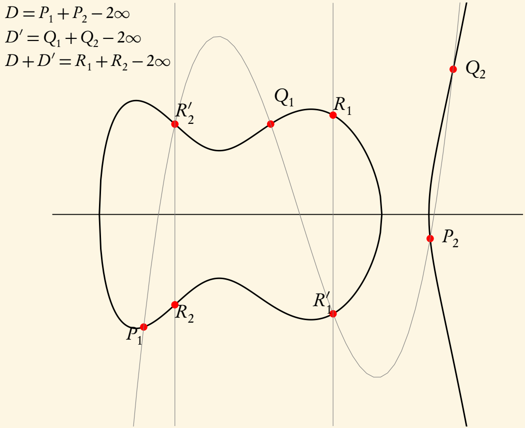


Higher dimension

Dimension 2:

Addition law on the Jacobian of an hyperelliptic curve of genus 2:

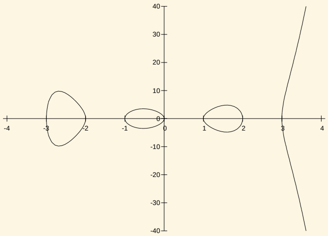
$$y^2 = f(x), \deg f = 5.$$



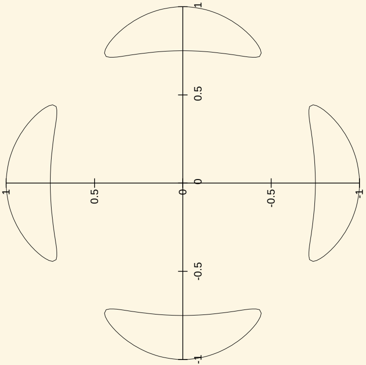
Higher dimension

Dimension 3

Jacobians of hyperelliptic curves of genus 3.



Jacobians of quartics.



Abelian surfaces

- For the same level of security, abelian surfaces need fields half the size as for elliptic curves (good for embedded devices);
- The moduli space is of dimension 3 compared to $1 \Rightarrow$ more possibilities to find efficient parameters;
- Potential speed record (the record holder often change between elliptic curves and abelian surfaces);
- But lot of algorithms still lacking compared to elliptic curves!

Security of elliptic curves cryptography

The security of an elliptic curve $E/\mathbb{F}_q$ depends on its number of points $\#E(\mathbb{F}_q)$. But

- Endomorphisms acts on (the points of) E;
- Isogenies map an elliptic curve to another one;
- Pairings map an elliptic curve to $\mathbb{F}_{q^e}^*$;
- E can be lifted to an elliptic curve over a number field (where we can compute elliptic integrals);
- The Weil restriction maps $E/\mathbb{F}_{q^d}$ to an abelian variety over $\mathbb{F}_q$ of higher dimension.

Security of elliptic curves cryptography

Most important question

How to assess the security of a particular elliptic curve?

- Point counting;
- Endomorphism ring computation (finer, more expensive);
- Relations to surrounding (isogenous) elliptic curves.

Main research theme

Consider elliptic curves and higher dimensional abelian varieties as families, via their moduli spaces.

Remark

- The geometry of the moduli space of elliptic curves is incredibly rich (Wiles' proof of Fermat's last theorem);
- This rich structure explain why elliptic curve cryptography is so powerful.

Moduli spaces

- If $E: y^2 = x^3 + ax + b$ is an elliptic curve, its isomorphism class is given by the j-invariant
$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$
The (coarse) moduli space of elliptic curves is isomorphic via the j-invariant to the projective line $\mathbb{P}^1$;
- The modular curve $X_0(3) \subset \mathbb{P}^2$ cut out by the modular polynomial
$$\begin{aligned}\varphi_3(X,Y) = X^4 + Y^4 - X^3Y^3 + 2232X^2Y^3 + 2232X^3Y^2 - 1069956X^3Y - 1069956XY^3 \\ + 36864000X^3 + 36864000Y^3 + 2587918086X^2Y^2 + 8900222976000X^2Y \\ + 8900222976000XY^2 + 452984832000000X^2 + 452984832000000Y^2 \\ -770845966336000000XY + 1855425871872000000000X + 1855425871872000000000Y\end{aligned}$$
describes the pairs of 3-isogenous elliptic curves (j_{E_1}, j_{E_2});
- The moduli space of abelian surfaces is of dimension 3;
- The class polynomials
$$128i_1^2 + 4456863i_1 - 7499223000 = 0$$
$$(256i_1 + 4456863)i_2 = 580727232i_1 - 1497069297000$$
$$(256i_1 + 4456863)i_3 = 230562288i_1 - 421831293750$$
describe the (dimension 0) moduli space of abelian surfaces with complex multiplication by $\mathbb{Q}(X)/(X^4 + 13X^2 + 41)$.

Isogeny graphs on elliptic curves

Definition

Isogenies are morphisms between elliptic curves.

Isogenies give links between

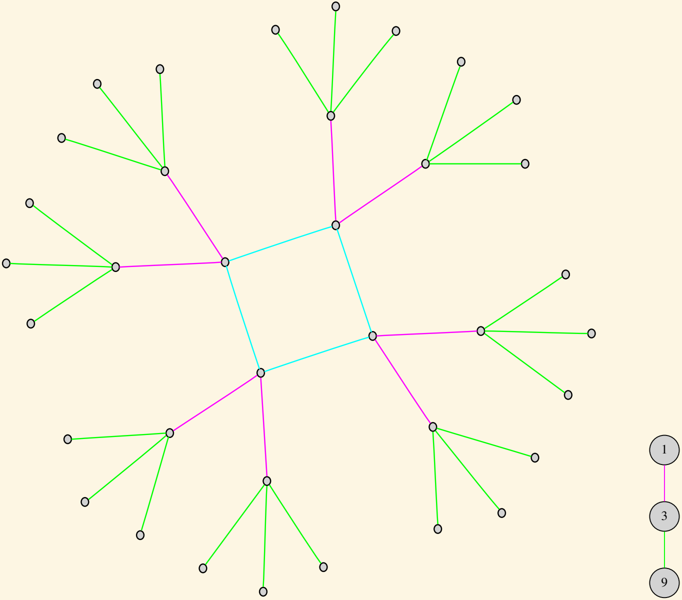
- arithmetic;
- endomorphism rings;
- class polynomials;
- modular polynomials;
- point counting;
- canonical lifting;
- moduli spaces;
- transfering the discrete logarithm problem.

Isogeny graphs on elliptic curves

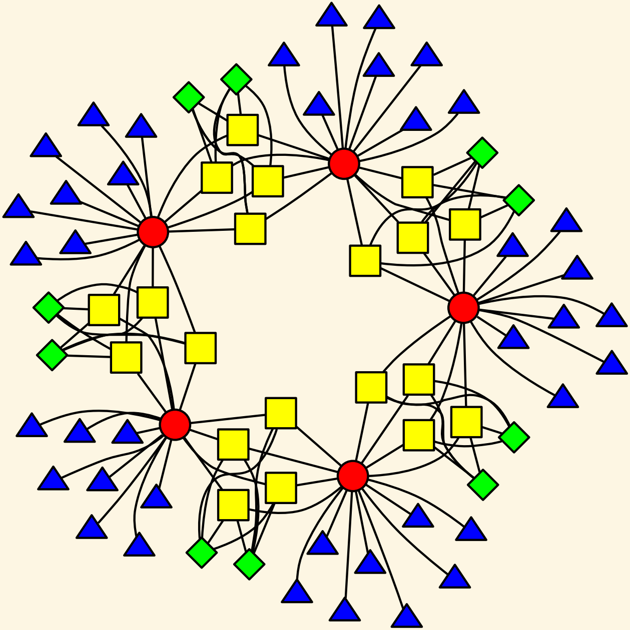
	Dimension 1	Dimension 2
$\#\mathbb{F}_q$	2^{256}	2^{128}
$\#\mathscr{M}_g(\mathbb{F}_q)$	2^{256}	2^{384}
#Isogeny graph	2^{128}	2^{192}

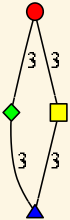
Table: Orders of magnitudes for 128 bits of security

Isogeny graphs on elliptic curves

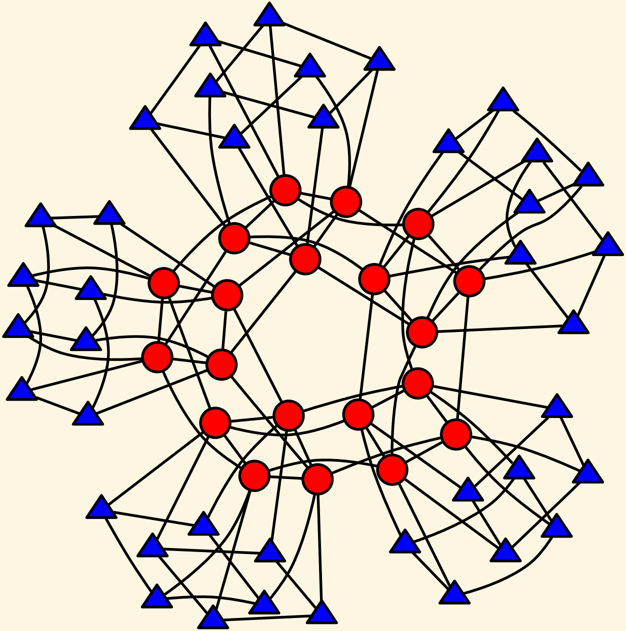


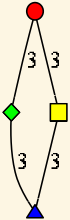
Isogeny graphs in dimension 2



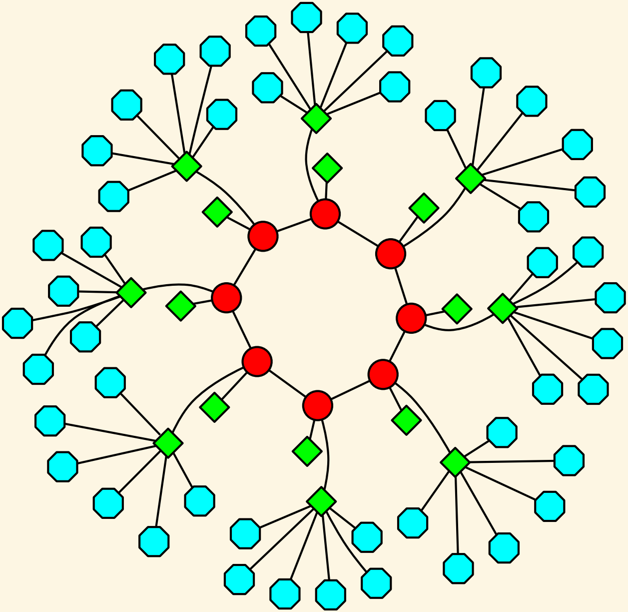


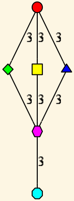
Isogeny graphs in dimension 2





Isogeny graphs in dimension 2





Isogeny graphs in dimension 2