Algorithmic number theory and cryptography

2013/12/05 — Comité des projets, Bordeaux

Damien Robert

Équipe LFANT, Inria Bordeaux Sud-Ouest

Public key cryptology

Cryptology:

- Encryption;
- Authenticity;
- Integrity.

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

Applications:

- Military;
- Privacy;
- Communications (internet, mobile phones...)
- E-commerce...

Paranoia is healthy…

The Prism program collects stored Internet communications based on demands made to Internet companies (Microsoft, Yahoo!, Google, Facebook, Paltalk, YouTube, AOL, Skype, Apple…)

"The NSA has been:

- Tampering with national standards (NIST is specifically mentioned) to promote weak, or otherwise vulnerable cryptography.
- Influencing standards committees to weaken protocols.
- Working with hardware and software vendors to weaken encryption and random number generators.
- Attacking the encryption used by "the next generation of 4G phones".
- Obtaining cleartext access to "a major internet peer-to-peer voice and text communications system"
- Identifying and cracking vulnerable keys.
- Establishing a Human Intelligence division to infiltrate the global telecommunications industry.
- decrypting SSL connections.

" (Matthew Green on Bullrun – http://blog.cryptographyengineering.com/2013/09/on-nsa.html)

LFANT: Lithe and fast algorithmic number theory

- Algorithmic number theory and algebraic geometry;
- Head: **Andreas Enge**;
- Strong focus on efficiency and correctness (certificates...) (We frequently deal with very large objects, like polynomials of degree ≈ 20000 and precision ≈ 8000000 bits);
- Star software: `PARI/GP`, but also `mpc`, `mpfrcx`, `cme`, `cmh`, `avisogenies`, `cubic`, `euclid`, `kleinian`...

My role in the team: apply the tools from number theory and algebraic geometry to cryptography.

- ERC Antics: Algorithmic Number Theory in Computer Science;
- ANR Peace: Parameter spaces for Efficient Arithmetic and Curve security Evaluation;
- ANR Simpatic: SIM and PAiring Theory for Information and Communications security;
- Scientific coordinator of team MACISA – Mathematics applied to cryptology and information security in Africa (Lirima);
- Idex CPU: Numerical certification and reliability;
- LFANT Seminar.

RSA system

Example (RSA 2048 bits)

- Public key: $N =$

$$
\begin{aligned}
&6463401214262201460142975337733990392088820533943096806426069 08\\
&\quad 5504931027773578178639440282304582692737743592184379603898823 9118\\
&\quad 3009818421901763047728965662412617547346019921835003955007793 0421\\
&\quad 3592115276768135136553584437285239512323676188676952340941163 2917\\
&\quad 0407261008577515178308213161721510479824786077154125035719573 9496\\
&\quad 5100686958644522827818065821439888727917366458821083663392380 8561\\
&\quad 6504873936830006403891242313041069135357067992614094086246516 2358\\
&\quad 0589147661573801247602443817897855584010180507546603761358052 4358\\
&\quad 2452549325783007903147486271992478399020780673351167464392246 6646\\
&\qquad\qquad 898327931186654267129234738109026 7.
\end{aligned}
$$

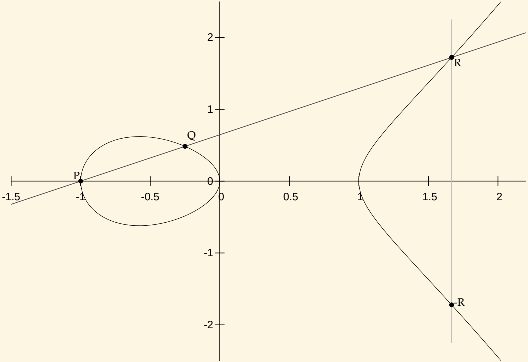
- Private key: The primes number p and q such that $N = pq$.

Elliptic curves

Definition ($\mathrm{char}\, k \neq 2,3$)

An elliptic curve is a plane curve with equation

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



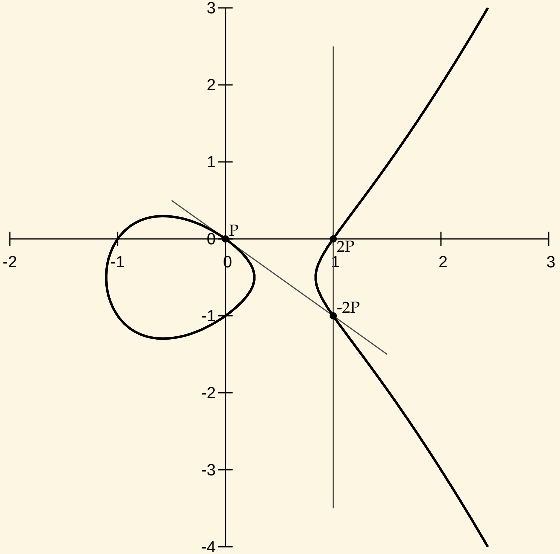
Exponentiation:

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

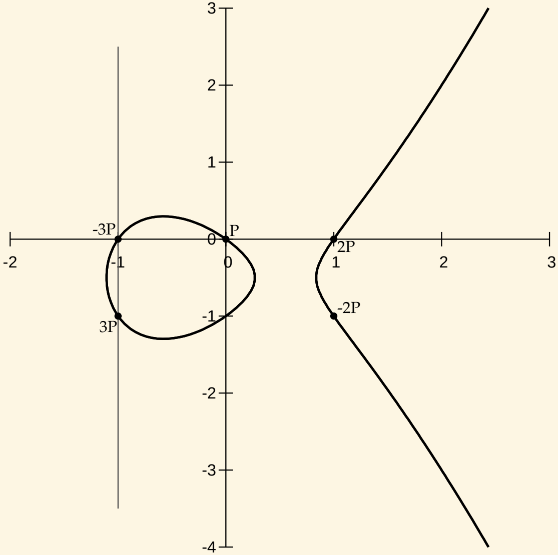
Discrete logarithm:

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

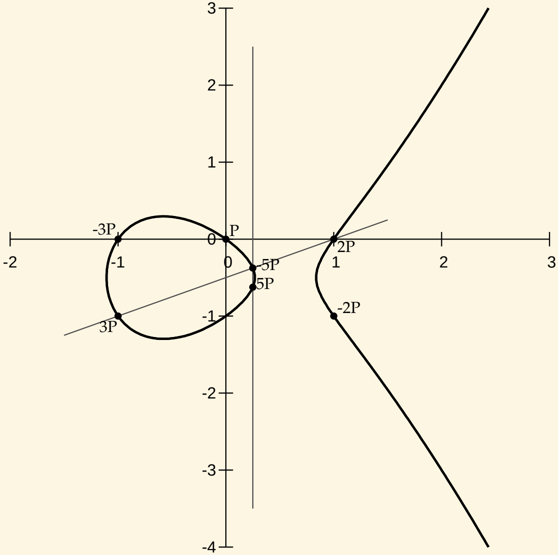
Scalar multiplication on an elliptic curve



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 $Q = \ell P$.

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

Why elliptic curves?

With the same security level, compared to RSA, elliptic curve cryptography is

- faster;
- more compact;
- more powerful.

Example (Pairings)

- On an elliptic curve, from one master public key, we can generate many other public keys, but generating the corresponding private keys requires the master private key.

$\Rightarrow$ Identity-based cryptography, short signatures, one way tripartite Diffie–Hellman, self-blindable credential certificates, attribute based cryptography, broadcast encryption…

Maps... Maps everywhere!

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.

Remark

This rich structure explain why elliptic curve cryptography is so powerful.

How to choose an elliptic curve?

- Take one at random;
- Generate one with carefully tweaked parameters (Complex Multiplication method);
- Use one standardized (☹NIST-p-256, ☺Curve25519).

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 incredibly rich (Wiles' proof of Fermat's last theorem).

Moduli spaces

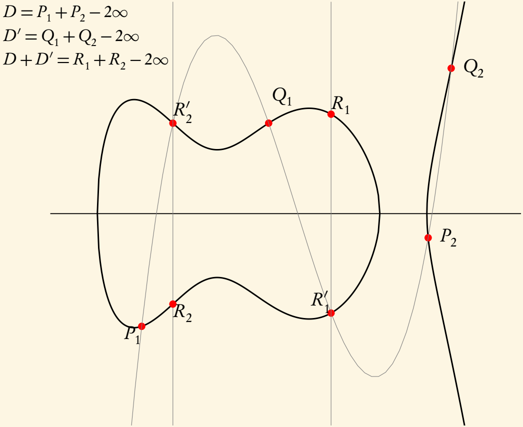
- If $E: y^2 = x^3 + ax + b$ is an elliptic curve, its isomorphism class is given by the j-invariant
$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$
The (coarse) moduli space of elliptic curves is isomorphic via the j-invariant to the projective line $\mathbb{P}^1$;
- The modular curve $X_0(3) \subset \mathbb{P}^2$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

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:

5 quadratic equations in $\mathbb{P}^7$:

$$(4a_1a_2+4a_5a_6)X_1X_6+(4a_1a_2+4a_5a_6)X_2X_5=$$
$$(4a_3a_44a_4a_3)X_3X_4+(4a_3a_44a_4a_3)X_7X_8;$$
$$(2a_1a_5+2a_2a_6)X_1^2+(2a_1a_5+2a_2a_6)X_2^2+(-2a_3^2-2a_4^2-2a_3^2-2a_4^2)X_3X_3=$$
$$(2a_3^2+2a_4^2+2a_3^2+2a_4^2)X_4X_8+(-2a_1a_5-2a_2a_6)X_5^2+(-2a_1a_5-2a_2a_6)X_6^2;$$
$$(4a_1a_6+4a_2a_5)X_1X_2+(-4a_3a_4-4a_3a_4)X_3X_8=$$
$$(4a_3a_4+4a_3a_4)X_4X_7+(-4a_1a_6-4a_2a_5)X_5X_6;$$
$$(2a_1^2+2a_2^2+2a_5^2+2a_6^2)X_1X_5+(2a_1^2+2a_2^2+2a_5^2+2a_6^2)X_2X_6+(-2a_3a_3-2a_4a_4)X_3^2=$$
$$(2a_3a_3+2a_4a_4)X_4^2+(2a_3a_3+2a_4a_4)X_7^2+(2a_3a_3+2a_4a_4)X_8^2;$$
$$(2a_1^2-2a_2^2+2a_5^2-2a_6^2)X_1X_5+(-2a_1^2+2a_2^2-2a_5^2+2a_6^2)X_2X_6+(-2a_3a_3+2a_4a_4)X_3^2=$$
$$(-2a_3a_3+2a_4a_4)X_4^2+(2a_3a_3-2a_4a_4)X_7^2+(-2a_3a_3+2a_4a_4)X_8^2;$$

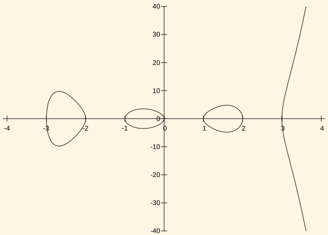
where the parameters live in the (fine) moduli space of abelian surfaces with a level $(2,4)$-structure described by 2 quartics equations in $\mathbb{P}^5$:

$$a_1^3a_5+a_1^2a_2a_6+a_1a_2^2a_5+a_1a_5^3+a_1a_5a_6^2+a_2^3a_6+a_2a_5^2a_6+a_2a_6^3-2a_3^4-4a_3^2a_4^2-2a_4^4=0;$$
$$a_1^2a_2a_6+a_1a_2^2a_5+a_1a_5a_6^2+a_2a_5^2a_6-4a_3^2a_4^2=0$$

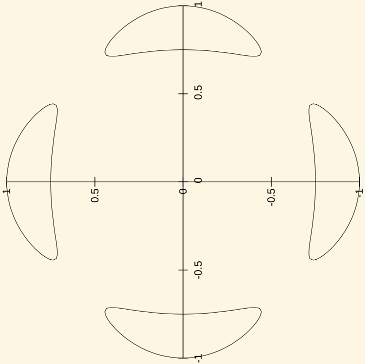
Higher dimension

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;
- Pairings on a space of rank 4 rather than $2 \Rightarrow$ more powerful;
- Potential speed record (the record holder often change between elliptic curves and abelian surfaces);
- But lot of algorithms still lacking compared to elliptic curves!

Isogeny graphs on elliptic curves

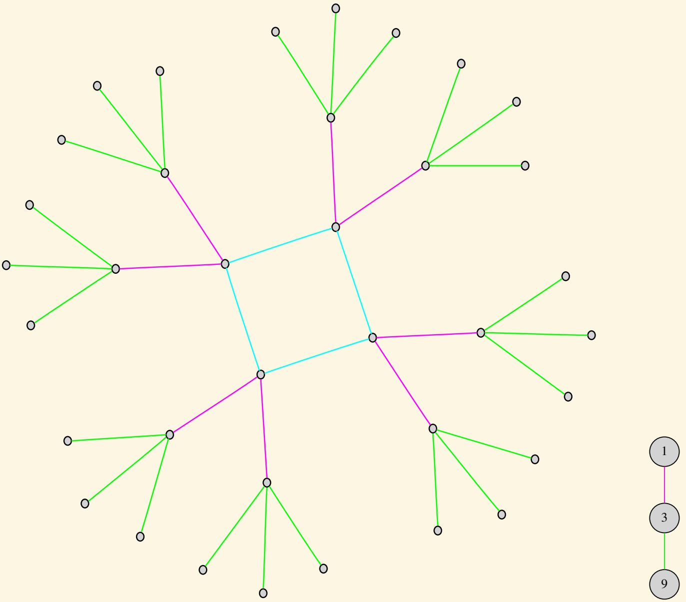
Definition

Isogenies are morphisms between elliptic curves.

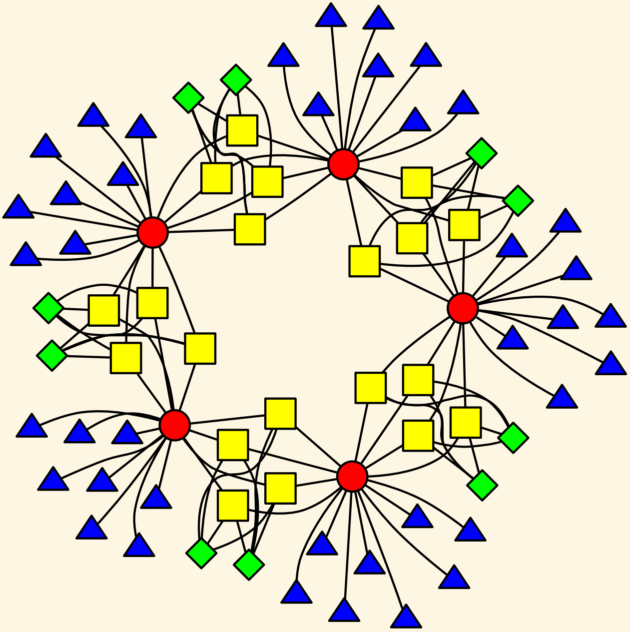
Isogenies give links between

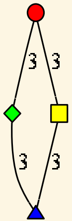
- arithmetic;
- endomorphism rings;
- class polynomials;
- modular polynomials;
- point counting;
- canonical lifting;
- moduli spaces;
- transfering the discrete logarithm problem.

Isogeny graphs on elliptic curves

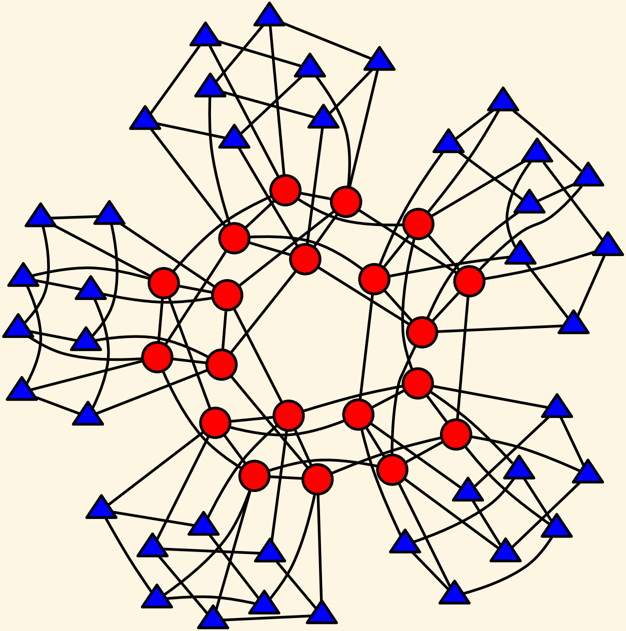


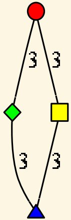
Isogeny graphs in dimension 2



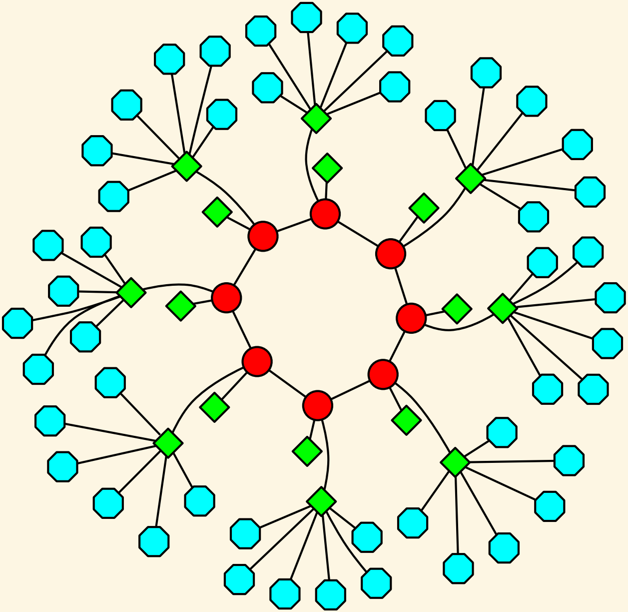


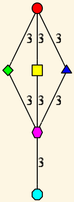
Isogeny graphs in dimension 2





Isogeny graphs in dimension 2





Isogeny graphs in dimension 2