Elliptic curves over finite fields and point counting

Alexandre Benoist

University of Luxembourg

PhD seminar, Belval - May 19, 2025

Introduction: The Discrete Logarithm Problem (DLP)

- Let G be a cyclic group of order n generated by an element g.

Introduction: The Discrete Logarithm Problem (DLP)

- Let G be a cyclic group of order n generated by an element g.
- For every $k \in \mathbb{Z}/n\mathbb{Z}$, it is easy to compute g^k (time complexity $O(\log(n))$.

Introduction: The Discrete Logarithm Problem (DLP)

- Let G be a cyclic group of order n generated by an element g.
- For every $k \in \mathbb{Z}/n\mathbb{Z}$, it is easy to compute g^k (time complexity $O(\log(n))$.
- But going in the other direction is much harder ...

Introduction: The Discrete Logarithm Problem (DLP)

- Let G be a cyclic group of order n generated by an element g.
- For every $k \in \mathbb{Z}/n\mathbb{Z}$, it is easy to compute g^k (time complexity $O(\log(n))$.
- But going in the other direction is much harder ...

Definition (Discrete Logarithm Problem)

Given g and g^k, the Discrete Logarithm Problem consists in finding $k \in \mathbb{Z}/n\mathbb{Z}$.

Attacks on the DLP

Examples:

- If $G = \mathbb{Z}/n\mathbb{Z}$, then solving the DLP is easy ...

Attacks on the DLP

Examples:

- If $G = \mathbb{Z}/n\mathbb{Z}$, then solving the DLP is easy ...
- If $G = (\mathbb{Z}/19\mathbb{Z})^*$ and $g = 3$, what is k such that $3^k = 10$?

Attacks on the DLP

Examples:

- If $G = \mathbb{Z}/n\mathbb{Z}$, then solving the DLP is easy ...
- If $G = (\mathbb{Z}/19\mathbb{Z})^*$ and $g = 3$, what is k such that $3^k = 10$?
- (Answer: 11)

Attacks on the DLP

Examples:

- If $G = \mathbb{Z}/n\mathbb{Z}$, then solving the DLP is easy ...
- If $G = (\mathbb{Z}/19\mathbb{Z})^*$ and $g = 3$, what is k such that $3^k = 10$?
- (Answer: 11)

Notation: $n = \#G$ and p is the larger prime factor of n

- The time complexity of the best generic attacks on the DLP is $O(\sqrt{p} \cdot \mathrm{poly}(\log(n)))$.
- There are specific attacks for $G = (\mathbb{Z}/p\mathbb{Z})^*$, but not for elliptic curves ...

Summary

1. Elliptic curves
   - Definition and the group law
   - One application to cryptography
2. Point counting methods for elliptic curves over finite fields
   - Schoof's algorithm
   - The SEA algorithm

Elliptic curves: definition

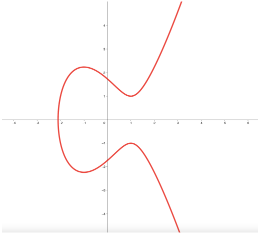
Let k be a field of characteristic p.

Definition

An elliptic curve E over k is given by the solutions $(x, y) \in k^2$ of an equation of the form

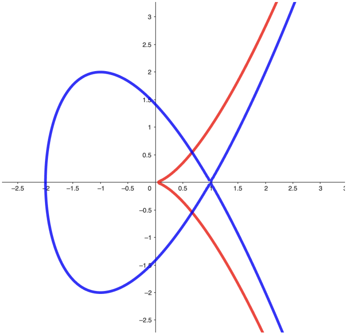
$$y^2 = x^3 + ax + b$$

with an additional point O called the "point at infinity", where $(a, b) \in k^2$ satisfy $4a^3 + 27b^2 \neq 0$. We denote by $E(k)$ the set of points of E.



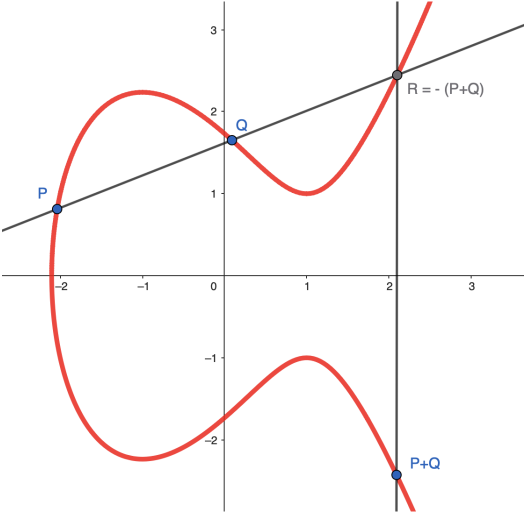
Singularity

The condition $4a^3 + 27b^2 \neq 0$ ensures that the curve is smooth.



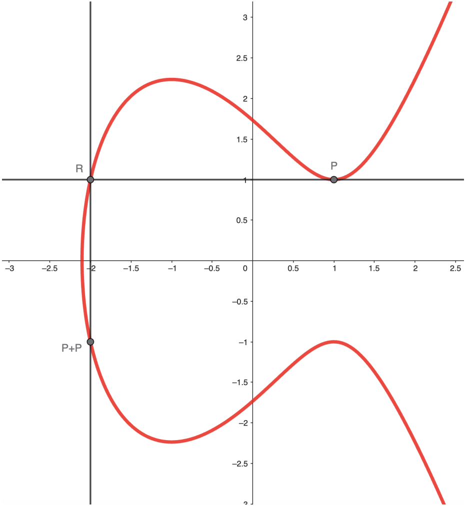
$y^2 = x^3$ (cusp); $y^2 = x^3 - 3x + 2$ (node)

The group law



Thus, elliptic curves are both algebraic and geometric objects.

Duplication of a point



Morphisms of elliptic curves: isogenies

Let E, E' be two elliptic curves over k. An isogeny $\phi : E \to E'$ is a map which respects the algebraic and geometric structures of E and E'. Concretely, it is a morphism of algebraic varieties such that

$$\phi(P + Q) = \phi(P) + \phi(Q)$$

for every points $P, Q \in E$.

Morphisms of elliptic curves: isogenies

Let E, E' be two elliptic curves over k. An isogeny $\phi : E \to E'$ is a map which respects the algebraic and geometric structures of E and E'. Concretely, it is a morphism of algebraic varieties such that

$$\phi(P+Q) = \phi(P) + \phi(Q)$$

for every points $P, Q \in E$.
Example: the multiplication-by-m map $[m]P = \underbrace{P + \ldots + P}_{m \text{ terms}}$.

Morphisms of elliptic curves: isogenies

Let E, E' be two elliptic curves over k. An isogeny $\phi : E \to E'$ is a map which respects the algebraic and geometric structures of E and E'. Concretely, it is a morphism of algebraic varieties such that

$$\phi(P + Q) = \phi(P) + \phi(Q)$$

for every points $P, Q \in E$.
Example: the multiplication-by-m map $[m]P = \underbrace{P + \ldots + P}_{m \text{ terms}}$.

Definition/Proposition (torsion)

Let $m > 0$ be an integer. The m-torsion subgroup of E is

$$E[m] := \{P \in E(\overline{k}) : [m]P = O\}.$$

If m is coprime to $\mathrm{char}(k)$, then $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

The Diffie-Hellman protocol (1976)

Let $k = \mathbb{F}_q$ be a finite field, and assume that $E(\mathbb{F}_q)$ is cyclic of order n, generated by a point P.

Alice		Bob
chooses a random $a \in \mathbb{Z}/n\mathbb{Z}$	$\xrightarrow{[a]P}$	chooses a random $b \in \mathbb{Z}/n\mathbb{Z}$
computes $[a]P$	$\xleftarrow{[b]P}$	computes $[b]P$
$[ab]P = [a]([b]P)$		$[ab]P = [b]([a]P)$

The Diffie-Hellman protocol (1976)

Let $k = \mathbb{F}_q$ be a finite field, and assume that $E(\mathbb{F}_q)$ is cyclic of order n, generated by a point P.

Alice		Bob
chooses a random $a \in \mathbb{Z}/n\mathbb{Z}$	$\xrightarrow{[a]P}$	chooses a random $b \in \mathbb{Z}/n\mathbb{Z}$
computes $[a]P$	$\xleftarrow{[b]P}$	computes $[b]P$
$[ab]P = [a]([b]P)$		$[ab]P = [b]([a]P)$

Given $P, [a]P, [b]P$, computing $[ab]P$ is not easy. The security of the Diffie-Hellman protocol relies on the difficulty to solve the DLP when $\#E(\mathbb{F}_q)$ is a large prime number.

The Diffie-Hellman protocol (1976)

Let $k = \mathbb{F}_q$ be a finite field, and assume that $E(\mathbb{F}_q)$ is cyclic of order n, generated by a point P.

Alice		Bob
chooses a random $a \in \mathbb{Z}/n\mathbb{Z}$	$\xrightarrow{[a]P}$	chooses a random $b \in \mathbb{Z}/n\mathbb{Z}$
computes $[a]P$	$\xleftarrow{[b]P}$	computes $[b]P$
$[ab]P = [a]([b]P)$		$[ab]P = [b]([a]P)$

Given $P, [a]P, [b]P$, computing $[ab]P$ is not easy. The security of the Diffie-Hellman protocol relies on the difficulty to solve the DLP when $\#E(\mathbb{F}_q)$ is a large prime number.

$\rightsquigarrow$ We have to find elliptic curves such that $\#E(\mathbb{F}_q)$ is a large prime.

The endomorphism of Frobenius

Let E be an elliptic curve over $\mathbb{F}_q$ given by a Weierstrass equation

$$y^2 = x^3 + ax + b.$$

The endomorphism of Frobenius of E is:

$$\phi_q : \begin{cases} E \to E \\ (x, y) \mapsto (x^q, y^q). \end{cases}$$

The endomorphism of Frobenius

Let E be an elliptic curve over $\mathbb{F}_q$ given by a Weierstrass equation

$$y^2 = x^3 + ax + b.$$

The endomorphism of Frobenius of E is:

$$\phi_q : \begin{cases} E \to E \\ (x, y) \mapsto (x^q, y^q). \end{cases}$$

There is an integer t_E, called trace of Frobenius of E, such that

$$\phi_q^2 - t_E \phi_q + [q] = 0.$$

The endomorphism of Frobenius

Let E be an elliptic curve over $\mathbb{F}_q$ given by a Weierstrass equation

$$y^2 = x^3 + ax + b.$$

The endomorphism of Frobenius of E is:

$$\phi_q : \begin{cases} E \to E \\ (x, y) \mapsto (x^q, y^q). \end{cases}$$

There is an integer t_E, called trace of Frobenius of E, such that

$$\phi_q^2 - t_E \phi_q + [q] = 0.$$

We have $\#E(\mathbb{F}_q) = q + 1 - t_E$. Hasse bound : $|t_E| \leq 2\sqrt{q}$.

Schoof's algorithm (1985)

Time complexity: $\widetilde{O}(\log(q)^5)$ (quite impossible to use in prcatice for cryptographic sizes...)

- The main idea of Schoof's algorithm: compute t_E modulo small primes $\ell \leq \ell_{max}$ such that

$$\prod_{\ell \leq \ell_{max}} \ell > 4\sqrt{q}$$

and use the Chinese Remainder Theorem.

Schoof's algorithm (1985)

Time complexity: $\widetilde{O}(\log(q)^5)$ (quite impossible to use in prcatice for cryptographic sizes...)

- The main idea of Schoof's algorithm: compute t_E modulo small primes $\ell \leq \ell_{max}$ such that

$$\prod_{\ell \leq \ell_{max}} \ell > 4\sqrt{q}$$

  and use the Chinese Remainder Theorem.
- The trace of ϕ_q seen as an endomorphism of $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ is t_E mod ℓ.

Schoof's algorithm (1985)

Time complexity: $\widetilde{O}(\log(q)^5)$ (quite impossible to use in prcatice for cryptographic sizes...)

- The main idea of Schoof's algorithm: compute t_E modulo small primes $\ell \leq \ell_{max}$ such that

$$\prod_{\ell \leq \ell_{max}} \ell > 4\sqrt{q}$$

  and use the Chinese Remainder Theorem.
- The trace of ϕ_q seen as an endomorphism of $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ is t_E mod ℓ.

How to compute t_E mod ℓ ?

- Evaluating the characteristic equation of Frobenius at $P = (x, y) \in E[\ell]$, we get $(x^{q^2}, y^{q^2}) - [t_E](x^q, y^q) + [q](x, y) = 0$.

How to compute t_E mod ℓ ?

- Evaluating the characteristic equation of Frobenius at $P = (x, y) \in E[\ell]$, we get $(x^{q^2}, y^{q^2}) - [t_E](x^q, y^q) + [q](x, y) = 0$.
- Since $P \in E[\ell]$, we have $[t_E](x^q, y^q) = [n_\ell](x^q, y^q)$ where $t_E \equiv n_\ell \bmod \ell$ and $0 \leq n_\ell < \ell$ (we also define q_ℓ the same way).

How to compute t_E mod ℓ ?

- Evaluating the characteristic equation of Frobenius at $P = (x, y) \in E[\ell]$, we get $(x^{q^2}, y^{q^2}) - [t_E](x^q, y^q) + [q](x, y) = 0$.
- Since $P \in E[\ell]$, we have $[t_E](x^q, y^q) = [n_\ell](x^q, y^q)$ where $t_E \equiv n_\ell \bmod \ell$ and $0 \leq n_\ell < \ell$ (we also define q_ℓ the same way).
- We test whether the equality $(x^{q^2}, y^{q^2}) - [k](x^q, y^q) + [q_\ell](x, y) = 0$ is satisfied for $k = 0, \dots, \ell - 1$. The only k such that the last equality holds is n_ℓ.

How to compute t_E mod ℓ ?

- Evaluating the characteristic equation of Frobenius at $P = (x, y) \in E[\ell]$, we get $(x^{q^2}, y^{q^2}) - [t_E](x^q, y^q) + [q](x, y) = 0$.
- Since $P \in E[\ell]$, we have $[t_E](x^q, y^q) = [n_\ell](x^q, y^q)$ where $t_E \equiv n_\ell \bmod \ell$ and $0 \leq n_\ell < \ell$ (we also define q_ℓ the same way).
- We test whether the equality $(x^{q^2}, y^{q^2}) - [k](x^q, y^q) + [q_\ell](x, y) = 0$ is satisfied for $k = 0, \ldots, \ell - 1$. The only k such that the last equality holds is n_ℓ.

Fast exponentiation

We know that $E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$. So, the x-coordinates of the ℓ-torsion points of E are the roots of a polynomial ψ_ℓ of degree $\frac{\ell^2-1}{2}$. Computations are performed in the ring

$$R_\ell = \frac{\mathbb{F}_q[x,y]}{(\psi_\ell(x), y^2 - x^3 - ax - b)}.$$

The SEA algorithm (90s)

The SEA algorithm (90s): $t_E \bmod \ell$ can be computed faster if there is a subgroup $K \subset E[\ell]$ of order ℓ defined over $\mathbb{F}_q$, described by a polynomial f_ℓ which is a factor of ψ_ℓ. It exists if and only if $t_E^2 - 4q$ is a square modulo ℓ.

The SEA algorithm (90s)

The SEA algorithm (90s): $t_E \bmod \ell$ can be computed faster if there is a subgroup $K \subset E[\ell]$ of order ℓ defined over $\mathbb{F}_q$, described by a polynomial f_ℓ which is a factor of ψ_ℓ. It exists if and only if $t_E^2 - 4q$ is a square modulo ℓ.

Definition

A prime $\ell \neq \mathrm{char}(\mathbb{F}_q)$ is said to be Elkies for E if and only if

$$\left(\frac{t_E^2 - 4q}{\ell}\right) = 0 \text{ or } 1.$$

Otherwise, it is said to be Atkin.

Heuristic: The number of Elkies and Atkin primes is approximately the same. If true, the complexity of the SEA algorithm is $\widetilde{O}(\log(q)^4)$.

Average results for the distribution of Elkies primes

Shparlinski and Sutherland have shown that the number of Elkies and Atkin primes is roughly the same, in average, over these two families:

- All elliptic curves defined over a finite field $\mathbb{F}_q$, when $q \to +\infty$

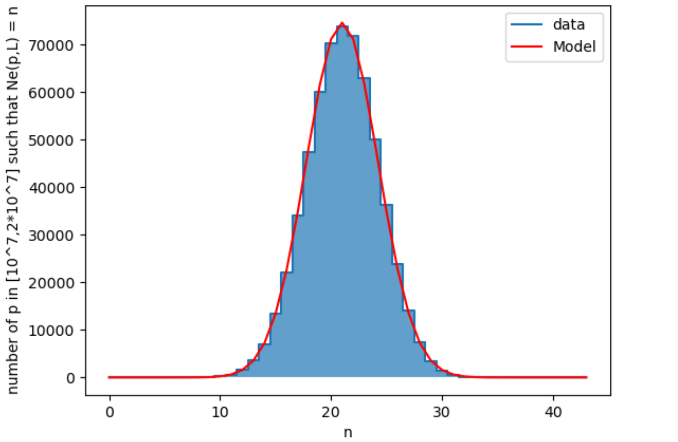
Average results for the distribution of Elkies primes

Shparlinski and Sutherland have shown that the number of Elkies and Atkin primes is roughly the same, in average, over these two families:

- All elliptic curves defined over a finite field $\mathbb{F}_q$, when $q \to +\infty$
- Reductions modulo p of a given elliptic curve E defined over $\mathbb{Q}$

The distribution of Elkies primes is Gaussian

For an elliptic curve $E/\mathbb{Q}$, let $N_e(p, L)$ be the number of Elkies primes in $(L, 2L)$ for the elliptic curve E mod p.



A word about Abelian varieties

- The SEA algorithm has been generalized for Abelian varieties (analogues of elliptic curves in higher dimension)

A word about Abelian varieties

- The SEA algorithm has been generalized for Abelian varieties (analogues of elliptic curves in higher dimension)
- Elkies primes have also been generalized

A word about Abelian varieties

- The SEA algorithm has been generalized for Abelian varieties (analogues of elliptic curves in higher dimension)
- Elkies primes have also been generalized
- Results about the distribution of Elkies primes are (partially) generalized

Questions ?

Thank you !