Introduction to Elliptic Curve Cryptography

Christophe Clavier

University of Limoges

Master 2 Cryptis

What is an Elliptic Curve

Characteristic of a Field

When a field $\mathbb{K}$ is finite, it is always of the form $\mathbb{K} = \mathbb{F}_q$ where $q = p^m$
The integer p is called the characteristic of the field, denoted $\mathrm{char}(\mathbb{K})$.
When $\mathrm{char}(\mathbb{K}) = 2, 3$ the field is said to be of *small characteristic*.
Otherwise it is said to be of *large characteristic*. (this includes infinite fields)

In the sequel we only consider fields of large characteristic.

Weierstraß Equation

Let $\mathbb{K}$ a field of large characteristic and $a, b \in \mathbb{K}$ such that $4a^3 + 27b^2 \neq 0$.

The elliptic curve $\mathcal{E}$ of parameters a and b defined over $\mathbb{K}$ is $\mathcal{E} = \mathcal{S} \cup \mathcal{O}$ where :

- $\mathcal{S}$ is the set of points $(x, y) \in \mathbb{K}^2$ verifying

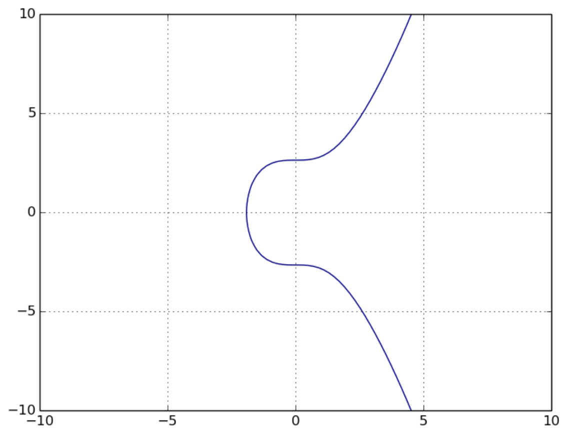
$$y^2 = x^3 + ax + b$$

- $\mathcal{O}$ is a special point called 'point at infinity'. (may be viewed as the point $(0, \infty)$)

Université de Limoges

An Elliptic Curve over $\mathbb{R}$

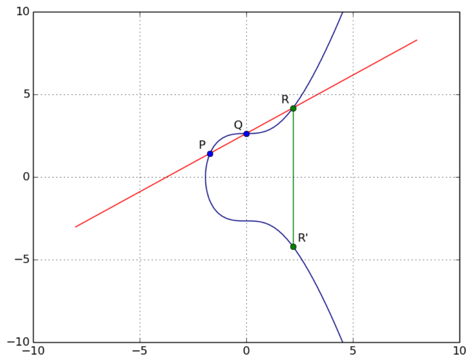
Defined over the real numbers ($\mathbb{K} = \mathbb{R}$), an elliptic curve may look like this:



Notice the symmetry with respect to the X axis.

The Addition Law

Given two points P and Q, the straight line passing between these two points always crosses the curve on a third point R:

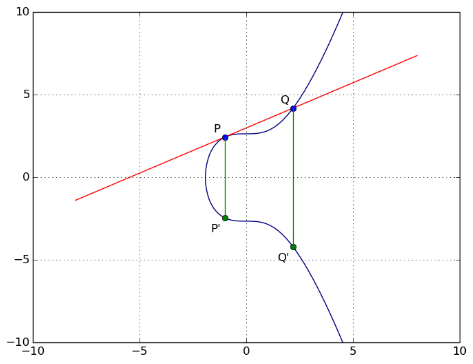


$$P + Q = R'$$

The sum of P and Q is defined as R' the symmetric point of R with respect to the X axis.

Particular Case

The three intersection points may be a simple one (Q) and a double one (P):

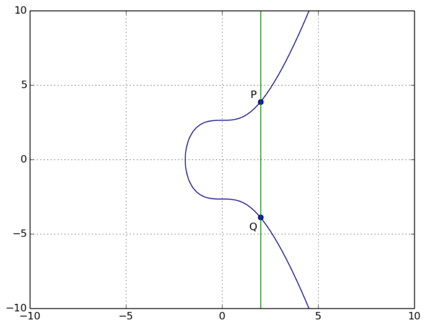


$$P + P = Q'$$
$$P + Q = P'$$

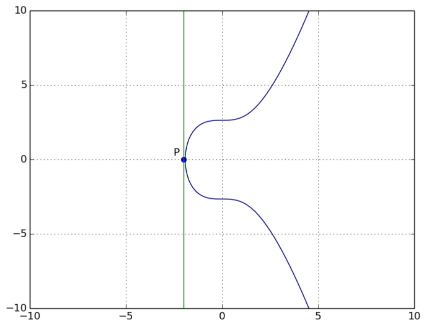
We consider the tangent point as two distinct points.

Particular Case

If the intersection line between P and Q is vertical, the virtual third point is the point at infinity:



$P + Q = \mathcal{O}$



$P + P = \mathcal{O}$

The Group Structure

The addition of points of $\mathcal{E}$ gives to the elliptic curve the structure of a commutative group $(\mathcal{E}, +)$:

$(\mathcal{E}, +)$ is a Group

commutativity for all $P, Q \in \mathcal{E}$, $P + Q = Q + P$

associativity for all $P, Q, R \in \mathcal{E}$, $(P + Q) + R = P + (Q + R)$

neutral element for all $P \in \mathcal{E}$, $P + \mathcal{O} = \mathcal{O} + P = P$

inverse for all $P \in \mathcal{E}$, the symmetric of P w.r.t. X axis is its own inverse $-P$: $P + (-P) = \mathcal{O}$

Multiple of a Point P

For any point $P \in \mathcal{E}$, the scalar multiplication by any positive integer k is defined as

$$k \cdot P = \underbrace{P + P + \ldots + P}_{k \text{ times}}$$

Addition and Doubling Formulae

Addition Formula

Given two different points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$, with $x_P \neq x_Q$, the addition point $R = (x_R, y_R) = P + Q$ is given by:

- $\lambda = \frac{y_Q - y_P}{x_Q - x_P}$
- $x_R = \lambda^2 - x_P - x_Q$
- $y_R = \lambda(x_P - x_R) - y_P$

Doubling Formula

Given $P = (x_P, y_P)$, the double point $R = (x_R, y_R) = 2.P$ is given by:

- $\lambda = \frac{3x_P^2 + a}{2y_P}$ (a is the curve equation parameter)
- $x_R = \lambda^2 - 2x_P$
- $y_R = \lambda(x_P - x_R) - y_P$

Université de Limoges

Order of an Elliptic Curve, Order of a Point

Elliptic curves used for cryptography are always defined on a finite field $\mathbb{K} = \mathbb{F}_q$ which is either:

- $\mathbb{K} = \mathbb{F}_q = \mathbb{F}_p$, with p a large prime, (large characteristic)
- or $\mathbb{K} = \mathbb{F}_q = \mathbb{F}_{2^m}$. (small, or even, characteristic)

When $\mathbb{K}$ is a finite field, the number of points of $\mathcal{E}$ is also finite.

Order of an Elliptic Curve

The order of an elliptic curve $\mathcal{E}$ is its number of points, and is denoted $\#\mathcal{E}$.

Order of a Point

The order of a point P on an elliptic curve $\mathcal{E}$, denoted as $\text{ord}(P)$, is the least integer $k > 0$ such that $k.P = \mathcal{O}$.

By Euler's theorem, one always have $\text{ord}(P) \mid \#\mathcal{E}$.

Université de Limoges

Elliptic Curves defined over $\mathbb{F}_p$

When $\mathbb{K} = \mathbb{F}_p$ all arithmetic operations in the field are defined modulo p.

Definition

Let $a, b \in \mathbb{F}_p$ such that $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$.

The elliptic curve $\mathcal{E}$ of parameters a and b defined over $\mathbb{F}_p$ is $\mathcal{E} = \mathcal{S} \cup \mathcal{O}$ where:

- $\mathcal{S}$ is the set of points $(x, y) \in \mathbb{F}_p^2$ verifying

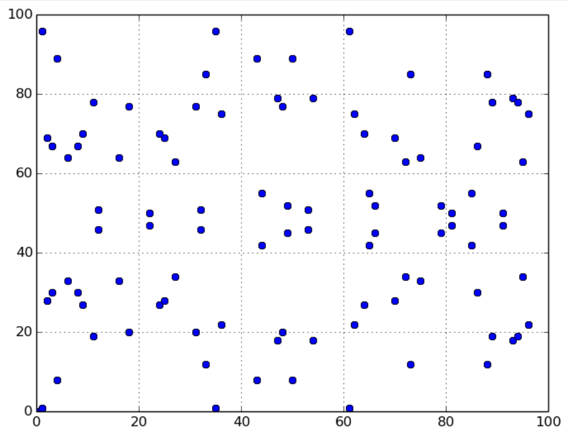
$$y^2 \equiv x^3 + ax + b \pmod{p}$$

- $\mathcal{O}$ is a special point called ‘point at infinity’. (may be viewed as the point $(0, \infty)$)

Another consequence is that the set of points is discrete. Visual aspect of the curve is totally different than with $\mathbb{K} = \mathbb{R}$.

A Toy Example: $\mathcal{E}$ defined over $\mathbb{F}_{97}$

When $p = 97$ the elliptic curve may look like this:



The symmetry with respect to the X axis still holds.

Affine Coordinates

The natural 2-coordinates system is called affine coordinates.

Beside its simplicity, its main drawback is the quite time-consuming modular inversion required both for addition and for doubling.

Cost of Addition

Input: $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$
Output: $R = (x_R, y_R) = P + Q$

- $\lambda = \frac{y_Q - y_P}{x_Q - x_P}$
- $x_R = \lambda^2 - x_P - x_Q$
- $y_R = \lambda(x_P - x_R) - y_P$

Cost: $I + 2M + S + 6A$

Cost of Doubling

Input: $P = (x_P, y_P)$
Output: $R = (x_R, y_R) = 2.P$

- $\lambda = \frac{3x_P^2 + a}{2y_P}$
- $x_R = \lambda^2 - 2x_P$
- $y_R = \lambda(x_P - x_R) - y_P$

Cost: $I + 2M + 2S + 8A$

Typical ratios are: $I/M \approx 100$ $\quad S/M = 0.8$ to 1 $\quad A/M = 0.1$ to 0.3

Homogeneous Projective Coordinates

Denoting $x = X/Z$ and $y = Y/Z$, $Z \neq 0$, we obtain homogeneous projective Weierstraß equation of $\mathcal{E}$:

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

- Each affine point (x, y) is represented by homogeneous projective coordinates $(\lambda x : \lambda y : \lambda)$ with $\lambda \in \mathbb{F}_q^\star$.
- Conversely, every point represented by $(X : Y : Z)$, $Z \neq 0$, has affine coordinates $(x, y) = (X/Z, Y/Z)$.
- The opposite of a point $(X : Y : Z)$ is $(X : -Y : Z)$.
- The point at infinity $\mathcal{O}$ is $(0 : \lambda : 0)$, $\lambda \in \mathbb{F}_q^\star$.

Addition in Homogeneous Projective Coordinates

The sum of $P = (X_P : Y_P : Z_P)$ and $Q = (X_Q : Y_Q : Z_Q)$, with $Z_P, Z_Q \neq 0$ and $P \neq \pm Q$, is the point $R = (X_R : Y_R : Z_R)$ such that:

Addition Formula (Homogeneous Projective Coordinates)

- $X_R = BC$
- $Y_R = A(B^2 X_P Z_Q - C) - B^3 Y_P Z_Q$
- $Z_R = B^3 Z_P Z_Q$

with $A = Y_Q Z_P - Y_P Z_Q \quad B = X_Q Z_P - X_P Z_Q$

$C = A^2 Z_P Z_Q - B^3 - 2B^2 X_P Z_Q$

Cost: $12M + 2S + 7A$

Mixed Affine-Projective Addition

Three multiplications are saved if P is given in affine coordinates (i.e. $Z = 1$).

Doubling in Homogeneous Projective Coordinates

The double of $P = (X_P : Y_P : Z_P)$, with $Z_P \neq 0$, is the point $R = (X_R : Y_R : Z_R)$ such that:

Doubling Formula (Homogeneous Projective Coordinates)

- $X_R = EB$
- $Y_R = A(D - E) - 2C^2$
- $Z_R = B^3$

with $A = 3X_P^2 + aZ_P^2 \quad B = 2Y_PZ_P \quad C = BY_P$

$D = 2CX_P \quad E = A^2 - 2D$

Cost: $7M + 5S + 10A$

Fast Doubling Trick $(a = -3)$

When the curve parameter a is equal to -3, A can be computed as $A = 3(X_P + Z_P)(X_P - Z_P)$ which saves two squarings. (with one more addition)

Jacobian Projective Coordinates

Denoting $x = X/Z^2$ and $y = Y/Z^3$, $Z \neq 0$, we obtain the Jacobian projective Weierstraß equation of $\mathcal{E}$:

$$Y^2 = X^3 + aXZ^4 + bZ^6$$

- Each affine point (x, y) is represented by homogeneous projective coordinates $(\lambda^2 x : \lambda^3 y : \lambda)$ with $\lambda \in \mathbb{F}_q^\star$.
- Conversely, every point represented by $(X : Y : Z)$, $Z \neq 0$, has affine coordinates $(x, y) = (X/Z^2, Y/Z^3)$.
- The opposite of a point $(X : Y : Z)$ is $(X : -Y : Z)$.
- The point at infinity $\mathcal{O}$ is $(\lambda^2 : \lambda^3 : 0)$, $\lambda \in \mathbb{F}_q^\star$.

Addition in Jacobian Projective Coordinates

The sum of $P = (X_P : Y_P : Z_P)$ and $Q = (X_Q : Y_Q : Z_Q)$, with $Z_P, Z_Q \neq 0$ and $P \neq \pm Q$, is the point $R = (X_R : Y_R : Z_R)$ such that:

Addition Formula (Jacobian Projective Coordinates)

- $X_R = F^2 - E^3 - 2AE^2$
- $Y_R = F(AE^2 - X_R) - CE^3$
- $Z_R = Z_P Z_Q E$

with $A = X_P Z_Q^2 \quad B = X_Q Z_P^2 \quad C = Y_P Z_Q^3 \quad D = Y_Q Z_P^3$

$E = B - A \quad F = D - C$

Cost: $12M + 4S + 7A$

Mixed Affine-Projective Addition

One squaring and four multiplications are saved if P is given in affine coordinates (i.e. $Z = 1$).

Doubling in Jacobian Projective Coordinates

The double of $P = (X_P : Y_P : Z_P)$, with $Z_P \neq 0$, is the point $R = (X_R : Y_R : Z_R)$ such that:

Doubling Formula (Jacobian Projective Coordinates)

- $X_R = C^2 - 2B$
- $Y_R = C(B - X_R) - 2A^2$
- $Z_R = 2Y_P Z_P$

with $A = 2Y_P^2 \quad B = 2AX_P \quad C = 3X_P^2 + aZ_P^4$

Cost: $4M + 6S + 11A$

Fast Doubling Trick $(a = -3)$

When the curve parameter a is equal to -3, C can be computed as $C = 3(X_P + Z_P^2)(X_P - Z_P^2)$ which saves two squarings. (with one more addition)

Cost Comparison

Representation	Addition	Mixte Add.	Doubling	Fast Doub.
Affine	I + 2M + S + 6A		I + 2M + 2S + 8A	I + 2M + 2S + 8A
Hom. Proj.	12M + 2S + 7A	9M + 2S + 7A	7M + 5S + 10A	7M + 3S + 11A
Jac. Proj.	12M + 4S + 7A	8M + 3S + 7A	4M + 6S + 11A	4M + 4S + 12A

- When computing a scalar multiplication $k.P$ one uses methods like *double-and-add* which are equivalent to exponentiation methods in $\mathbb{Z}_n$.
- With projective coordinates, a unique modular inversion $(1/Z)$ is still required at the end of the scalar multiplication to convert back to affine coordinates.
- Jacobian projective representation has faster doubling but slower addition than the homogeneous projective one $\rightarrow$ interesting as *double-and-add* uses more doublings than additions.
- Whatever the representation, signed digit scalar multiplication methods are interesting as $-P$ can be computed for free.

Université de Limoges

Curve Parameters and Key Generation

An elliptic curve is characterized by the following parameters:

- p, the prime number which defines the field $\mathbb{K} = \mathbb{F}_p$
- a, b, the two integer coefficients which define the curve
- a *base point* G on the curve ; all point computations will be done in the subgroup $\langle G \rangle$ generated by G (the multiples of G),
- $n = \mathrm{ord}(G)$ which is the cardinal of $\langle G \rangle$

Key Generation

Computing a key pair is quite easy:

1. pick a random integer d between 1 and $n - 1$ $\rightarrow$ this is the private key
2. compute $Q = d.G$ $\rightarrow$ this is the public key

Elliptic Curve Diffie-Hellman (ECDH)

Alice and Bob want to agree on some common secret value (e.g. for using as an AES key):

ECDH Protocol

1. They first agree on some domain and curve parameters (p, a, b, G, n)
2. They compute their own private/public key pairs (d, Q) and exchange their public keys Q_A and Q_B
3. Alice computes $S = d_A.Q_B$ and Bob computes $S = d_B.Q_A$

Note that S is actually an elliptic curve point. The AES secret key can be taken e.g. as the least significant bits of x_s.

Elliptic Curve Digital Signature Algorithm (ECDSA)

Alice want to sign a message m with her private key d_A.

Everyone should be able to check the signature thanks to Alice's public key Q_A.

ECDSA Signature Generation

1. compute $z = H(m)$ the hash of the message (truncated to the size of n)
2. take k at random between 1 and $n - 1$
3. compute $P = k.G$
4. compute $r = x_P \bmod n$ (if $r = 0$ then choose another k and try again)
5. compute $s = k^{-1}(z + rd_A) \bmod n$ (if $s = 0$ then choose another k and try again)

The pair (r, s) is the signature of m.

Note that $k^{-1} \bmod n$ can be computed only if n is prime (k is arbitrary).

$\Rightarrow$ ECDSA works only on curves with a subgroup $\langle G \rangle$ of prime order.

Elliptic Curve Digital Signature Algorithm (ECDSA)

ECDSA Signature Generation

1. compute $z = H(m)$ the hash of the message (truncated to the size of n)
2. take k at random between 1 and $n-1$
3. compute $P = k.G$
4. compute $r = x_P \bmod n$ (if $r = 0$ then choose another k and try again)
5. compute $s = k^{-1}(z + rd_A) \bmod n$ (if $s = 0$ then choose another k and try again)

The pair (r, s) is the signature of m.

ECDSA Signature Verification

Input: the truncated hash z, the signature (r, s), and the public key Q_A

1. compute $u_1 = s^{-1}z \bmod n$
2. compute $u_2 = s^{-1}r \bmod n$
3. compute $P = u_1.G + u_2.Q_A$

The signature is valid only if $r = x_P \bmod n$.