Elliptic Curve Cryptography (ECC)

Theory

Elliptic Curve Cryptography (ECC) is a type of public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC provides the same level of security as traditional public-key cryptography (like RSA) but with smaller key sizes, making it faster and more efficient.

Elliptic Curve Equation:

An elliptic curve over a finite field F_p is defined as: $y^2 \equiv x^3 + ax + b \pmod{p}$

Where:

- $a, b \in F_p$
- $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$ (to avoid singular curves)
- p is a prime number representing the field

Points on the Curve

A point P = (x, y) satisfies the curve equation. There is a special 'point at infinity', denoted O, which acts as the identity element for addition.

Point Addition

Given two points P = (x1, y1) and Q = (x2, y2) on the curve:

1. Distinct points ($P \neq Q$):
   $m = (y2 - y1)/(x2 - x1) \pmod{p}$

2. Point doubling ($P = Q$):
   $m = (3x1^2 + a)/(2y1) \pmod{p}$

3. Resulting point $R = P + Q = (xr, yr)$:
   $xr = m^2 - x1 - x2 \pmod{p}$
   $yr = m(x1 - xr) - y1 \pmod{p}$

Scalar Multiplication

Scalar multiplication is the repeated addition of a point: $kP = P + P + ... + P$ (k times)
Efficient computation uses the double-and-add method, analogous to exponentiation by squaring.

Example

Consider the elliptic curve:
$y^2 \equiv x^3 + 2x + 3 \pmod{97}$
and the point P = (3, 6) on the curve.

Point Addition Example

Let Q = (80, 10). To compute R = P + Q:
1. Calculate slope:
   m = (10 - 6)/(80 - 3) (mod 97) = 4/77 (mod 97)
2. Compute modular inverse of 77 mod 97: $77^{-1} \equiv 63 \pmod{97}$
3. Slope: m = 4 * 63 (mod 97) = 252 mod 97 = 58
4. Compute resulting point:
   xr = 58^2 - 3 - 80 (mod 97) = 30
   yr = 58*(3 - 30) - 6 (mod 97) = 95

So, P + Q = (30, 95).

Scalar Multiplication Example

Compute 3P = P + P + P:
1. Double P: 2P = P + P
   m = (3*3^2 + 2)/(2*6) (mod 97) = 29/12 (mod 97)
   Modular inverse of 12 mod 97 = 89
   m = 29*89 mod 97 = 61
   x2P = 61^2 - 3 - 3 (mod 97) = 2
   y2P = 61*(3 - 2) - 6 (mod 97) = 55
   So, 2P = (2, 55)
2. Add P again: 3P = 2P + P = (2, 55) + (3, 6)

Procedure:

Colab Notebook Link for this lab: Lab 7 - ECC [Summer 2025]

Submission form: https://forms.gle/rwnFtVFcAqCHKmPp8