ECC Cryptography

Team Details

Sunny Kumar Pandit CSE/22105/959

Sunny Kumar CSE/22104/958

Sourav Roy CSE/22099/XXX

Mentor - Dr. Soumen Pandit

Modular Point Addition

Elliptic Curve Over a Finite Field

An elliptic curve over a finite field F is defined by an equation of the form:

$$y^2 \equiv x^3 + ax + b \mod p$$

where a,b are constants satisfying the condition:

$$4a^3 + 27b^2 \not\equiv 0 \mod p$$

This condition ensures that the curve has no singularities.

Types of Singularities

Cusp: A sharp point where the curve does not have a well-defined tangent.

Node: A self-intersection point where two branches of the curve meet.

Isolated Point: A point that satisfies the curve equation but does not connect smoothly to the rest of the curve.

Modular Point Addition Example

Example 1

Given the elliptic curve:

$$y^2 \equiv x^3 + 2x + 3 \mod 5$$

Lets add two points a=(1, 1) and b=(0, 2)

- Compute the slope :

$$\lambda = \frac{2-1}{0-1} \equiv \frac{1}{-1} \equiv -1 \equiv 4 \mod 5$$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \mod p$$

- Compute x3 and y3:

$$x_3 = 4^2 - 1 - 0 \equiv 16 - 1 \equiv 15 \equiv 0 \mod 5$$

$$y_3 = 4(1-0) - 1 \equiv 4 - 1 \equiv 3 \mod 5$$

$$x_3 = \lambda^2 - 2x_1 \mod p$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \mod p$$

Thus, $P + Q = (0, 3)$.

Example 2

Given the elliptic curve:

$$y^2 \equiv x^3 + 2x + 3 \pmod 5$$

Lets add two points p=(1, 1) and q=(1, 1), this is an example of point doubling :

- Compute the slope :

$$m = \frac{3+2}{2} = \frac{5}{2} \pmod 5$$ m=0 $$m = \frac{3x_1^2 + a}{2y_1} \pmod p$$

- Compute x3 and y3 :

$$x_3 = 0^2 - 2(1) \equiv -2 \equiv 3 \pmod 5$$ $$x_3 = m^2 - 2x_1 \pmod p$$

$$y_3 = 0(1-3) - 1 = -1 \equiv 4 \pmod 5$$ $$y_3 = m(x_1 - x_3) - y_1 \pmod p$$

- Thus :

$$2P = (3,4) \pmod 5$$