Elliptic Curve Cryptography

Definition 1. Given a modulo $p$, a (discrete) elliptic curve mod $p$ is the collection of all integer points $(x, y)$ that satisfy the equation

\[ E_p : y^2 = x^3 + Ax + B \pmod{p} \]

where $A, B$ are integers in $[0, p - 1]$ and $4A^3 + 27B^2 \neq 0 \pmod{p}$.

Messages are encoded into pairs of integers and encryption is obtained by transforming the pairs using arithmetic based on the curve.
HOW DO WE CONSTRUCT THE PAIRS?

Table of square roots \( \text{mod } 23 \)

\[
\begin{pmatrix}
1 & 2 & 3 & 4 & 6 & 8 & 9 & 12 & 13 & 16 & 18 \\
1 & 5 & 7 & 2 & 11 & 10 & 3 & 9 & 6 & 4 & 8 \\
22 & 18 & 16 & 21 & 12 & 13 & 20 & 14 & 17 & 19 & 15
\end{pmatrix}
\]

Table of \( x \mapsto x^3 + 16x + 14 \pmod{23} \)

\[
\begin{pmatrix}
6 & 8 & 20 & 4 & 12 & 4 & 9 & 10 & 13 & 1 & 3 & 2 & 4 & 15 & 18 & 19 & 1 & 16 & 1 & 8 & 20 & 20
\end{pmatrix}
\]

The “points” of the “curve”

\[
\{(1, 10), (1, 13), (2, 10), (2, 13), (4, 2), (4, 21), (5, 9), (5, 14), (6, 2), (6, 21), (7, 3), (7, 20), (9, 6), (9, 17), (10, 1), (10, 22), (11, 7), (11, 16), (12, 5), (12, 18), (13, 2), (13, 21), (15, 8), (15, 15), (17, 1), (17, 22), (18, 4), (18, 19), (19, 1), (19, 22), (20, 10), (20, 13)\}
\]
Addition on elliptic curve

Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be two points on the curve $E_p : y^2 = x^3 + Ax + B \pmod{p}$. Then $P + Q = (x_R, -y_R)$ where

$$\alpha = (y_Q - y_P) \cdot (x_Q - x_P)^{-1} \pmod{p}$$
$$x_R = \alpha^2 - x_P - x_Q \pmod{p}$$
$$y_R = y_P + \alpha(x_R - x_P) \pmod{p}.$$

Point doubling on elliptic curve

Let $P = (x_P, y_P)$ be a point on the curve $y^2 = x^3 + Ax + B$. Then $2P = (x_R, -y_R)$ where

$$\alpha = (3x_P^2 + A) \cdot (2y_P)^{-1} \pmod{p}$$
$$x_R = \alpha^2 - 2x_P \pmod{p}$$
$$y_R = y_P + \alpha(x_R - x_P) \pmod{p}.$$

The following results hold for both elliptic curve over real numbers and elliptic curve mod $p$:

- Curve addition is associative: $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$
- Curve addition is commutative: $P_1 + P_2 = P_2 + P_1$
- For a point $P = (x, y)$ and an integer $k$, we set
  $$kP = P + P + \cdots + P (k \text{ times})$$
- For any two integers $k, h$, we have $h(kP) = (hk)P = k(hP)$
Example. In modulo \( p = 23 \), given the curve \( y^2 = x^3 + 13x + 7 \mod 23 \) and two points \( P = (14, 9) \) and \( Q = (17, 14) \)

1. Check that the curve is valid and that \( P, Q \) are two points on the curve

2. Find \( P + Q \)

3. Now let \( S = (9, 5) \) and \( T = (9, 18) \). Find \( S + T \)
Point doubling on elliptic curve Let \( P = (x_P, y_P) \) be a point on the curve \( y^2 = x^3 + Ax + B \). Then \( 2P = (x_R, -y_R) \) where

\[
\alpha = (3x_P^2 + A) \cdot (2y_P)^{-1} \pmod{p}
\]

\[
x_R = \alpha^2 - 2x_P \pmod{p}
\]

\[
y_R = y_P + \alpha(x_R - x_P) \pmod{p}.
\]

**Example.** In modulo \( p = 23 \), given the curve \( y^2 = x^3 + 5x + 8 \pmod{23} \) and a point \( P = (3, 2) \) on this curve. Find \( 2P \).
Elliptic Curve Diffie-Hellman Key Exchange

1. Alice and Bob agree on a modulo $p$ and choose a point $Q$ on an elliptic curve $E_p : y^2 = x^3 + Ax + B \pmod{p}$.

2. Alice chooses a random integer $N_A$ and Bob chooses a random integer $N_B$. Both keep these choices secret.

3. Alice computes $Q_A = N_A \cdot Q$ and sends it to Bob.

4. Bob computes $Q_B = N_B \cdot Q$ and sends it to Alice.

5. Upon receiving $Q_A$, Bob computes $N_B \cdot Q_A$.

6. Upon receiving $Q_B$, Alice computes $N_A \cdot Q_B$.

7. Now they share the secret key $N_A Q_B = N_A (N_B Q) = (N_A N_B) Q = (N_B N_A) Q = N_B (N_A Q) = N_B Q_A$
Represent plaintext
Suppose we want to use the elliptic curve $y^2 = x^3 + Ax + B \pmod{p}$, for large prime $p$.

Suppose that the plaintext is converted into an integer $M \in [1, p - 1]$.

1. Pick a large integer $k$ and successively compute
   \[ x_j = M \cdot k + j \text{ for } j = 0, 1, 2, \ldots, k - 1. \]

2. Each time we compute an $x_j$, we test whether $x_j^3 + Ax_j + B$ is a quadratic residue modulo $p$.

3. The first time that $x_j^3 + Ax_j + B$ is a quadratic residue modulo $p$, we shall encrypt $M$ by the point
   \[ U = \left( x_j, \sqrt{x_j^3 + Ax_j + B} \right) \pmod{p} \]

Remarks:
Elliptic Curve El Gamal

1. As the receiver, Bob chooses a large prime $p$ and an elliptic curve $E_p : y^2 = x^2 + Ax + B (\text{mod} \ p)$. He also chooses a point $P$ and a positive integer $k$. He computes $Q = kP = P + \cdots + P (k \text{ times})$.

2. He publishes $E_p, P, Q$ and keeps $k$ secret.

3. As the sender, Alice encrypts her message as a point $U$ on $E_p$ and selects a random integer $h$. She then computes 

$$Y_1 = hP \quad \text{and} \quad Y_2 = U + hQ.$$ 

4. Alice sends $(Y_1, Y_2)$ to Bob.

5. To decrypt, Bob computes 

$$Y_2 - kY_1 = U + hQ - k(hP) = U + hQ - h(kP) = U + hQ - hQ = U.$$