Day 24 – Elliptic Curve Cryptography

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

$$E_p : y^2 = x^3 + Ax + B \quad (mod\ p)$$

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

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 mod 23

<table>
<thead>
<tr>
<th>y^2</th>
<th>1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18</th>
</tr>
</thead>
<tbody>
<tr>
<td>y</td>
<td>1 5 7 2 11 10 3 9 6 4 8 22 18 16 21 12 13 20 14 17 19 15</td>
</tr>
</tbody>
</table>

- Table of $x \mapsto x^3 + 16x + 14 \pmod{23}$

The "points" of the "curve"

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

For continuous version

$E$
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

\[
\begin{align*}
\alpha &= (y_Q - y_P) \cdot (x_Q - x_P)^{-1} \pmod{p} \\
\frac{\alpha}{x_R} &= x_Q - x_P \pmod{p} \\
y_R &= y_P + \alpha(x_R - x_P) \pmod{p}.
\end{align*}
\]

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

\[
\begin{align*}
\alpha &= (3x_P^2 + A) \cdot (2y_P)^{-1} \pmod{p} \\
x_R &= \alpha^2 - 2x_P \pmod{p} \\
y_R &= y_P + \alpha(x_R - x_P) \pmod{p}.
\end{align*}
\]

The following results hold for both elliptic curve over real numbers and elliptic curve \( \pmod{p} \):

- 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 \( kP = P + P + \cdots + P(k \text{ times}) \) (scalar multiplication)
- For any two integers \( k, h \), we have \( h(kP) = (hk)P = k(hP) \) (scalar multiplication is associative)
Example. In modulo $p = 23$, given the curve $y^2 = x^3 + 13x + 7 \pmod{23}$ 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

\[
A = 13; \quad B = 7; \quad p = 23
\]

\[
4A^3 + 27B^2 \pmod{23} = 4(13)^3 + 27(7)^2 \pmod{23} = 0
\]

(Easy)

To check $P = (x_P, y_P)$ is on the curve, show

\[
y_P^2 = x_P^3 + Ax_P + B \pmod{p}
\]

2. Find $P + Q$

\[
\alpha = \frac{y_Q - y_P}{x_Q - x_P} \pmod{p}
\]

\[
= \frac{14 - 9}{17 - 14} \pmod{23}
\]

\[
= \frac{5}{3} \pmod{23}
\]

\[
= \ldots = 17
\]

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

\[
= 17^2 - 17 - 14 \pmod{23}
\]

\[
= 5
\]

\[
P + Q = (5, 6)
\]

3. Now let $S = (9, 5)$ and $T = (9, 18)$. Find $S + T$

\[
y_S + y_T = 0 \pmod{23} \Rightarrow S \& T are symmetry \Rightarrow S + T \text{ is @ } (0, 0)
\]

about $x$-axis

\[S
\]

\[T
\]

\[R
\]

\[O\]
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 \( 2P \).

\[
\begin{align*}
\alpha &= \left( 3 \cdot (3^2 + 5) \cdot (2 \cdot 2)^{-1} \pmod{23} \\
&= \left( 32 \cdot 4^{-1} \pmod{23} \\
&= 9 \cdot 6 \pmod{23} \\
&= 8
\end{align*}
\]

\[
\begin{align*}
x_R &= \alpha^2 - 2x_P \pmod{p} = 64 - (2 \cdot 3) \pmod{23} = 12, \\
y_R &= y_P + \alpha(x_R - x_P) = 2 + 8(12 - 3) \pmod{23} = 8
\]

\[
\begin{array}{c}
2P = (12, 18)
\end{array}
\]
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

$$N_AQ_B = N_A(N_BQ) = (N_AN_B)Q = (N_BN_A)Q = N_B(N_AQ) = N_BQ_A$$

---

<table>
<thead>
<tr>
<th>Alice</th>
<th>Public</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large prime $p = \text{modulo}$</td>
<td>$E_p : y^2 = x^3 + Ax + B \pmod{p}$</td>
<td>Pick $Q \in E_p.$</td>
</tr>
<tr>
<td>private: $N_A$</td>
<td>$Q_A = N_A \cdot Q$</td>
<td>public: $Q_B = N_B \cdot Q$</td>
</tr>
</tbody>
</table>

Known to be NP-hard

```latex
\begin{align*}
\Rightarrow \text{Enemy has to solve} & \quad Q_A = N_A \cdot Q \quad \text{for } N_A \quad \text{or} \quad Q_B = N_B \cdot Q \quad \text{for} \quad N_B
\end{align*}
```
Represent plaintext
(as a point on the curve $E_p$)

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:
- Should not use $M^3 + A\cdot M + B \pmod{p}$
  b/c this may not be a quad. residue.
- How can I know that I will get an $x_j$ on the curve
  (i.e. $x_j^3 + Ax_j + B$ is a quadratic residue)?

  There are $\frac{p-1}{2}$ quadratic residues

  Prob. that none of $x_j^3 + Ax_j + B$ is quad. residue

- To recover $M$ from $x_j$; $M = \left\lfloor \frac{x_j}{k} \right\rfloor$
Elliptic Curve El Gamal

1. As the receiver, Bob chooses a large prime $p$ and an elliptic curve $E_p : y^2 = x^3 + Ax + B \pmod{p}$. 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

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