Lecture 6

Main topic: Elliptic curve discrete logarithm problem (ECDLP)

Problem: Given an elliptic curve E defined over a finite field $\mathbb{F}_q$, a point $P \in E(\mathbb{F}_q)$ of order n, a point $Q \in \{P, 2P, 3P, \ldots, nP\}$

(Order means that $nP = O$ & $mP \neq 0$ for $m < n$)

Find l s.t $Q = lP$.

(In multiplicative notation, we can think of $Q = P^l$ $\log_P Q = l$)

Let us discuss some attacks on this.

1. Pohlig – Hellman attack

(Tackle this one prime at a time)

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

Fundamental idea is to compute l_i's s.t

$$l \equiv l_i \pmod{p_i^{e_i}} \quad i \in \{1, 2, \ldots, r\}$$

Then use Chinese remainder thm to find l.

Suppose (Base p expansion)

$$l_i = z_0 + z_1 p_i + z_2 p_i^2 + \cdots + z_{e_i - 1} p_i^{e_i - 1}$$

$$\boxed{0 \le z_i \le p-1}$$

Idea is to compute z_j's & then find l_i

① Computation of z_0

$$P_0 := \left(\frac{n}{p_i}\right) P \qquad Q_0 := \left(\frac{n}{p_i}\right) Q.$$

Order of $P_0 \ge 1$

$$p_i P_0 = p_i \left(\frac{n}{p_i}\right) P = nP = \mathcal{O}$$

Order of $P_0 = P_1$

$$Q_0 = \left(\frac{n}{P_1}\right) Q = l\left(\frac{n}{P_1} P\right)$$

$$= l P_0$$

$$= (z_0 + z_1 P + \cdots) P_0$$

$$= z_0 P_0$$

(2) Computation of z_1

$$Q_1 := \left(\frac{n}{P_1^2}\right)(Q - z_0 P)$$

$$= \left(\frac{n}{P_1^2}\right)(l - z_0) P$$

$$= (l - z_0)\left(\frac{n}{P_1^2}\right) P$$

(Order P_1^2)

$$= (z_1 P_1 + z_2 P_1^2 + \cdots)\left(\frac{n}{P_1^2}\right) P$$

$$= z_1 P_1 \left(\frac{n}{p_1 2}\right) P$$

$$= z_1 \left(\frac{n}{p_1}\right) P$$

$$Q_1 = z_1 P_0$$

- - - -

Example: $E: y^2 = x^3 + 100x + 75 \in \mathbb{F}_{7919}$

$P = (4023, 6036) \in E(\mathbb{F}_{7919})$

$n = 7889 = 7^3 \cdot 23$ (Order of P)

$Q = (4135, 3169)$, want to find l s.t $lP = Q$

Let's determine $l \bmod 7^3$, say l_7

$$l_7 = z_0 + z_1 7 + z_2 7^2$$

$$P_0 = \left(\frac{7^3 \cdot 23}{7}\right)P = 7^2 \cdot 23\, P$$

$$= (7801, 2071)$$

$$Q_0 = 7^2 \cdot 23\, Q = (7801, 2071)$$

$$Q_0 = P_0 \Rightarrow z_0 = 1$$

$$Q_1 = 7 \cdot 23\,(Q - P) = (7285, 14)$$

$$Q_1 = z_1 P_0 \Rightarrow z_1 = 3$$

$$Q_2 = 23(Q - P - 3 \cdot 7P)$$

$$= (7285, 7905) = 4P_0$$

$$\Rightarrow z_2 = 4$$

$$\ell_1 = 1 + 3 \cdot 7 + 4 \cdot 7^2 = 218$$

$$\ell \equiv 218 \pmod{7^3}$$

Mod 23 computation

$$P_0 = 7^3 P = (7190, 7003)$$

$$Q_0 = 7^3 Q = (2599, 759)$$

$$\text{lo } P_0 = Q_0 \qquad l_2 = 10$$

$$\left.\begin{aligned} l &\equiv 218 \pmod{7^3} \\ l &\equiv 10 \pmod{23} \end{aligned}\right\}$$

$$l = 4334 \pmod{7^3 \cdot 23}$$

Chinese remainder thm:

$$\left.\begin{aligned} X &\equiv a \pmod{m} \\ X &\equiv b \pmod{n} \end{aligned}\right\} \quad \boxed{\gcd(m, n) = 1}$$

$$X \equiv 1 \pmod 9$$
$$X \equiv 2 \pmod 3$$
↳ no solution

$$\boxed{X = a(ny_1) + b(my_2)}$$

$$ny_1 \equiv 1 \pmod m$$
$$my_2 \equiv 1 \pmod n$$

Pollard's Rho attack

$P \in E(\mathbb{F}_q)$ Order n

$Q = lP$ Want to find $l \pmod n$

Idea is to find two distinct pairs

(c', d') & (c'', d'') s.t

$$c'P + d'Q = c''P + d''Q$$

$$\Rightarrow (c' - c'')P = (d'' - d')Q$$

$$\Rightarrow (c' - c'')P = (d'' - d')(lP)$$

$$\Rightarrow (c' - c'') \equiv (d'' - d')l \pmod n$$

$$\Rightarrow l \equiv \frac{(c' - c'')}{(d'' - d')} \pmod n$$

$\left(\frac{1}{3} \pmod 7 = 5 \pmod 7 \right)$

Observation: Expected time for this algorithm to finish $\approx \sqrt{\frac{\pi n}{2}}$

Example: $E: y^2 = x^3 + x + 44$ over $\mathbb{F}_{229}$

$P = (5, 116)$ $\quad Q = (155, 166)$

$n = 239$

$H: \{P, 2P, 3P, \ldots, nP\} \to \{1, 2, 3, 4\}$

↓

Partition

$H(x, y) = (x \bmod 4) + 1$

Choice of 4 triples

$(a_1, b_1, \underset{R_1}{a_1 P + b_1 Q}) = (79, 163, (135, 117))$

$(a_2, b_2, R_2) = (206, 19, (96, 97))$

$= (87, 109, (84, 62))$

$= (219, 68, (72, 134))$

Algorithm

Select c', d' mod n & $X' = c'P + d'Q$

$$X'' = X' \quad c'' = c' \quad d'' = d'$$

Iterations

① $$\begin{cases} j = H(X') \\ X' = X' + R_j & c' = c' + q_j \pmod n \\ & d' = d' + b_j \pmod n \end{cases}$$

Repeat this twice

$$\begin{cases} j = H(X'') \\ X'' = X'' + R_j \\ c'' = c'' + q_j \pmod n \\ d'' = d'' + b_j \pmod n \end{cases}$$

For our example

In 6th iteration $(c'', d'') = (192, 24)$

$$c''P + d''Q = (57, 105)$$

In 12th iteration $(c', d') = (213, 104)$

$$c'P + d'Q = (57, 105)$$

$$192P + 24Q = 213P + 104Q$$

$$192P - 213P = 104Q - 24Q$$

$$-21P = 80Q$$

$$l = 176 \pmod{239}$$

—

Isomorphism attacks

E over $\mathbb{F}_q$

P order n

Q find l s.t. $lP = Q$

Suppose n is prime

$$\psi: \{P, 2P, 3P, \ldots, nP\} \xrightarrow{\cong} G$$

$\{P, 2P, 3P, \ldots, nP\}$: cyclic group of order p

G: group of order n

If we can compute ψ, then

$$Q = lP$$

Apply ψ

$$\psi(Q) = \psi(lP)$$
$$= l\,\psi(P)$$

Solving DLP in first group is equivalent to solving DLP in G_φ

Suppose $\gcd(m, q) = 1$

then we can use Weil Pairing & Tate Pairing to given an isomorphism.

Next week: discuss Weil Pairing