Tutorial 8 ENG

03 November 2021 14:00

Elliptic curve cryptography

→ Mathematics of elliptic curves

→ Elliptic curve version of discrete logarithm problem

→ ECC El Gamal protocols

$\mathbb{Z}_p^*$ - for a large prime this is a large cyclic group $(p-1)$ which can be used to formulate discrete log problem.

There multiple ways to construct large cyclic groups.

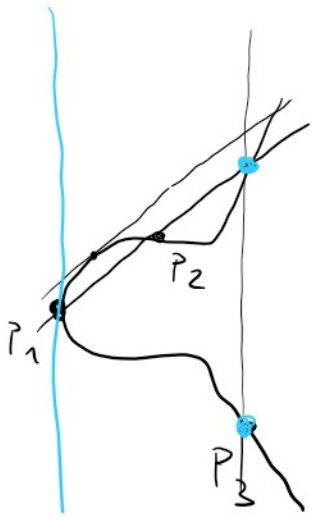
Elliptic curves is one of them.

Elliptic curve $\boxed{E: y^2 \equiv x^3 + ax + b} \mod p$

Non-singular if $-16(4a^3 + 27b^2) \neq 0 \mod p$

Point (x, y) lies on E $(P = (x, y) \in E)$

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



$P_1 = (x_1, y_1)$

$P_2 = (x_2, y_2)$

$P_1 + P_2 = P_3 = (x_3, y_3)$

$P_1 + P_2 = P_3 = (x_3, y_3)$

$$x_3 = \lambda^2 - x_1 - x_2$$

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

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & P_1 \neq P_2 \\ \frac{3x_1^2 + a}{2y_1} & P_1 = P_2 \end{cases}$$

Examples: $3P = (P + P + P)$ $\quad P = (0,1)$

$E: y^2 \equiv x^3 + 4x + 1 \mod 5$

1.) E is non-singular

$$-16(4 \cdot 4^3 + 27 \cdot 1^2) \mod 5$$

$$-1((-1)^4 + 2)$$

$$-1(3) \equiv -3 \equiv 2 \mod 5$$

$$\neq 0 \mod 5$$

2.) $P \in E$

$$1^2 \equiv 0^3 + 4 \cdot 0 + 1 \mod 5 \quad \checkmark$$

$P = (0,1)$

$P + P = (x_3, y_3) = (4,1)$ $\quad = 2P$

$$\lambda \equiv \frac{3x_1^2 + a}{2y_1} \equiv \frac{3 \cdot 0 + 4}{2 \cdot 1}$$

$$\equiv \frac{4}{2} \equiv 4 \cdot 2^{-1} \equiv 4 \cdot 3 \equiv 2 \mod 5$$

$$x_3 \equiv \lambda^2 - x_1 - x_2 \mod 5$$

$$\equiv 2^2 - 0 - 0$$

$$y_3 \equiv \lambda (x_1 - x_3) - y_1 \mod 5$$

$$2(0 - 4) - 1$$

$2P = 2P + P = (x_3, y_3)$ $\quad (1,4)$

$(4,1) + (0,1)$ $\quad x_1 y_1 \quad x_2 y_2$

$3P = 2P + P = (x_3, y_3)$ $\quad (1,4)$

$(4,1) + (0,1)$ $\quad x_1 y_1 \quad x_2 y_2$

$x_3 = \lambda^2 - x_1 - x_2 \mod 5$

$= 0 - 4 - 0 \equiv 1 \mod 5$

$y_3 = \lambda (x_1 - x_3) - y_1 \mod 5$

$0 - 1 \equiv 4 \mod 5$

$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{1-1}{0-4} = 0 \mod 5$

What if λ is not defined?

$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ $\quad P_1 \neq P_2$ $\quad x_1 = x_2$ but $y_1 \neq y_2$

$P_1 = (x, y)$

$-P_1 = P_2 = (x, -y)$

$\lambda = \frac{3x_1^2 + a}{2y_1}$ $\quad P_1 = P_2$ $\quad$ und $\quad y_1 = 0$

In such cases $P_1 + P_2 = \infty \quad (0,0) \ldots$

↑ neutral additive element

$P + \infty = \infty + P = P$

We know E is closed under addition ↑

$(P+Q)+R = P+(Q+R)$

For every P there is $-P$, s.t. $P + (-P) = \infty$

$P = (x, 0) \qquad -P = (x, 0)$

$P = (x, 3) \qquad -P = (x, -3)$

We know $(E, +)$ is a group ↑

$P + Q = Q + P$

we know $(E, +)$ is a commutative (Abelian) group

Every finite commutative group is isomorphic to

$[(\mathbb{Z}_{i_1} \times \mathbb{Z}_{i_2} \times \dots \times \mathbb{Z}_{i_2}), +]$

of

$(\mathbb{Z}_i, +)$

Size is $\prod_{j=0}^{\varepsilon} i_j$

$(\mathbb{Z}_4, +)$

$[(\mathbb{Z}_2 + \mathbb{Z}_2), +]$

$\{0, 1, 2, 3\}, +$ mod 4

$1 + 1 + 1 + 1$

$0 + 0 = 0$

$1 + 1 = 2$

$2 + 2 = 0$

$3 + 3 = 2$

$[(0,0), (0,1), (1,0), (1,1)]$

$(0,1) + (1,1) = (0+1, 1+1)$ mod 2

$(0,0) + (0,0) = (0,0)$

$(0,1) + (0,1) = (0,0)$

$(1,0) + (1,0) = (0,0)$

$(1,1) + (1,1) = (0,0)$

Elliptic curve discrete logarithm problem

$\mathbb{Z}_p^*$

$(E, +)$

p

q - generator of $\mathbb{Z}_p^*$

$\{q, q^2, q^3, \dots, q^{p-1}\} < \mathbb{Z}_p^*$

$y = q^x \bmod p$

Solve for x given y and p

P - generator of $(E, +)$

$\{P, 2P, 3P, \dots, \star P\} = E$ (order of $(E,+)$ = size if isomorphic to $(\mathbb{Z}_\ell, +)$)

$Q = x \cdot P$

Solve for x given Q, P and $(E, +)$

Computationally hard.

How do we know which commutative group is $(E, +)$ isomorphic to?

1.) How many points does $(E, +)$ have?

Hasse's theorem $E \bmod p$ with N points

$$|N - p - 1| \leq 2\sqrt{p}$$

$N - p - 1 \leq 2\sqrt{p}$

$N \leq 2\sqrt{p} + p + 1$

$-(N - p - 1) \leq 2\sqrt{p}$

$N \geq p - 2\sqrt{p} + 1$

$E: \quad y^2 = x^3 + 4x + 1 \quad \bmod 5$

$5 - 2\sqrt{5} + 1 \leq N \leq 5 + 2\sqrt{5} + 1$

2. ... 10. ... Euler's criterion $a^{\frac{p-1}{2}} = 1 \bmod p$

x	$x^3 + 4x + 1$	QR?	Points
0	1	✓	(0,1) (0,-1)
1	1	✓	(1,1) (1,-1)
2	2	X	— —
3	0	-	(3,0)
4	1	✓	(4,1) (4,-1)

∞

8 points

$\{\}$ $\{\}$ $\{\}$

$(\mathbb{Z}_8, +)$ $\{(\mathbb{Z}_4 + \mathbb{Z}_2), +\}$ $\{(\mathbb{Z}_2 + \mathbb{Z}_2 + \mathbb{Z}_2), +\}$

n	nP
1	(0,1)
2	(4,1)
3	(1,4)
4	(3,0)
5	(1,1)
6	(4,4)
7	(0,4)
8	∞

$\Rightarrow$ $(E, +)$ is isomorphic to $(\mathbb{Z}_8, +)$

isomorphism $f: E \to \mathbb{Z}_8$

$f(P_1) + f(P_2) = f(P_1 + P_2)$

$f: aP \to a$

$aP + bP = (a+b)P$

$a + b = a + b$

Example of curves with same number of points but different group structure:

Example of curves with same number of points but different group structure:

$y^2 = x^3 + 6x + 6 \mod 7 \quad \{(3,3),(3,4),(5,0),\infty\} \cong (\mathbb{Z}_4, +)$

$y^2 = x^3 + 6 \mod 7 \quad \{(1,0),(2,0),(3,0),\infty\} \cong ((\mathbb{Z}_2 \times \mathbb{Z}_2), +)$

Why is EC discrete logarithm advantageous?

$E \mod p$ uses $(\log_2 p + 1)$ bit numbers

$/\mathbb{Z}_p^*$ uses $\log_2 p$ bit numbers

$|\mathbb{Z}_p^*| = p - 1$

$|(E, +)| = p + 1 + 2\lfloor\sqrt{p}\rfloor \equiv$ EC problem is larger

---

$\mathbb{Z}_p^*$ uses exponentiation $\Rightarrow$ expensive operation

---

El Gamal encryption

$\mathbb{Z}_p^*$	$(E, +) \mod p$
Public: p - large prime	$(E, +) \mod p$
q - generator of $\mathbb{Z}_p^*$	P a generator of $(E, +)$ of order K
$b = q^x \mod p$	(k is the smallest number for which $k \cdot P = \infty$)
Private: x	$Q = x \cdot P$
	Private: $x \in \{1, \dots, \varepsilon\}$

Encrypt m

choose a random $r \in \mathbb{Z}_{p-1}$

$$a = g^r \bmod p$$

$$b = m \cdot y^r \bmod p$$

Decrypt (a, b)

$$m = b \cdot a^{-x} \bmod p$$

$$m \cdot g^{rx} \cdot g^{-rx} \bmod p$$

$$m \cdot (g^x)^r \cdot (g^r)^{-r} \bmod p$$

$$m$$

Encrypt M

Choose random $r \in \{1, \ldots, \}$

$$A = r \cdot P$$

$$B = M + r \cdot Q$$

Decrypt (A, B)

$$M = B + (-x A)$$

$$= M + r \cdot Q - x \cdot r \cdot P$$

$$= M + r \cdot x \cdot P - x \cdot r \cdot P$$

$$= M$$

✓

How to map messages to points on Elliptic curve?

El Gamal Signatures

$\mathbb{Z}_p^*$

$(E, +) \bmod p$

Public: p - large prime

g - generator of $\mathbb{Z}_p^*$

$y = g^x \bmod p$

$(E, +) \bmod p$

$P \in E$ - generator $(E, +)$

↳ order of P is $\}$

$Q = \textcircled{x} \cdot P$

Private: x

x

Sign: m

1.) Choose r from $\mathbb{Z}^*_{p-1}$

$$a = a^r \mod p$$

$$b = r^{-1}(m - ax) \mod (p-1)$$

m

1.) Choose r randomly from $\mathbb{Z}_k^*$

$$A = r \cdot P = (a_1, a_2)$$

$$b = r^{-1} \cdot (m - a_1 x) \mod k$$

Verification:

$$b^a a^b \overset{!}{=} q^m \mod p$$

$$(q^r)^a (q^r)^{r^{-1}(m-ax)} \overset{?}{=} q^m \mod p$$

$$q^m \overset{?}{=} q^m \mod p$$

Homework