Tutorial VIII group 2

07 November 2019 16:05

Elliptic Curve Cryptography

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

There are other ways to construct large cyclic groups

Elliptic curves are one of them

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

$$\left.\begin{array}{l} P_1 = (x_1, y_1) \\ P_2 = (x_2, y_2) \end{array}\right\} \in E$$

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

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

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

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

$y_3 \quad \ldots \quad 0/1 \quad \ldots \quad \frac{\ldots}{2y_1}$

POINT ADDITION

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

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

1.) E is non-singular $\quad -16\left(4(4)^3 + 27\cdot 5^2\right) \bmod 5$

$$= -16\,(1+2) \bmod 5$$

✓ $$= -3 \neq 0 \bmod 5$$

2.) P lies on E

$$1^2 = 0^3 + 4\cdot 0 + 1 \bmod 5 \quad ✓$$

$P = (\overset{x_1}{0}, \overset{y_1}{1})$

$P+P = (x_3, y_3) = (4,1) \qquad 1^2 = 4^3 + 4\cdot 4 + 1$
$\qquad\qquad -1 - 4 + 1 \equiv 1 \bmod 5$

$$x_3 = \lambda^2 - x_1 - x_1 \qquad \lambda = \frac{3x_1^2 + a}{2y_1} = \frac{0+4}{2\cdot 1} \quad (\bmod 5)$$

$$= \lambda^2 = 4 \quad \bmod 5 \qquad\qquad = 2 \quad \bmod 5$$

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

$$= 2(0-4) - 1 \quad \bmod 5$$

$$= 1 \quad \bmod 5$$

$2P + P = (4,1) + (0,1) = (x_3, y_3) = (1,4) \qquad 4^2 = 1^3 + 4\cdot 1 + 1 \quad ✓$
$\qquad\qquad 1 = 5 + 1 \equiv 1 \bmod 5$

$$x_3 \ldots \qquad \lambda = \frac{y_2 - y_1}{\ldots} = \frac{1-1}{\ldots} \ldots$$

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

$$x_3 = \lambda^2 - x_1 - x_2$$
$$= 0 - 4 - 0 = 1 \mod 5$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \mod 5$$
$$= 0 - 1 = 4 \mod 5$$

When is λ not defined?

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

1.) $x_1 = x_2$ but $y_1 \neq y_2$
$\Downarrow$
$P_1 = (x, y)$ $P_2 = (x, -y)$

$$= \frac{3x_1^2 + a}{2y_1} \qquad P_1 = P_2$$

2.) $P_1 = P_2$ but $y_1 = 0$

in such cases $P_1 + P_2 = O$ (∞, O)

$$P + \infty = P$$

We now know that E is closed under addition

$(P+Q)+R = P+(Q+R)$ ✓

For every P there is a point Q, such that

$P+Q = \infty$ ✓

We now know that E is a group

$P+Q = Q+P$

$P + Q = Q + P$

We now know that E is a commutative group (Abelian)

Every finite commutative group is isomorphic to

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

How many elements?

$$\prod_{j \in \{1,\dots,k\}} i_j$$

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

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

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

$0 + 0 = 0 \mod 4$

$1 + 1 = 2 \mod 4$

$2 + 2 = 0 \mod 4$

$3 + 3 = 2 \mod 4$

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

$\{(0,0), (0,1), (1,0), (1,1)\}, +$

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

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

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

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

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

Elliptic curve discrete log problem

$\mathbb{Z}_p^*$

$(E, +)$

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

P - generator of $(E, +)$

$\{g, g^2, \boxed{g^3}, \dots, g^{p-1}\} = \mathbb{Z}_p^*$

$\{P, 2P, 3P, \dots, kP\} = E$

order of $(E, +)$

$y = g^x \mod p$

Solving for $\boxed{x}$ given y, g, p is discrete log and it is computationally hard

$Q = xP$

Solving for x given Q and P and $(E,+)$ is EC discrete log and it is computationally hard

---

How do we know what $(E,+)$ is isomorphic to?

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

Hesse's theorem $E \mod p$ with N points

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

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

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

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

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

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

Euler's criterion $\boxed{a^{\frac{p-1}{2}} = 1 \mod p}$

$$2.\ldots \leq N \leq \underset{6}{5} + 2\sqrt{5} + 1 = 10.\ldots$$

is this a Quadratic Residue?

x	x^3+4x+1	QR	y
		✓	(1,4) 2
0	1	✓	(1,4) 2
1	1		
2	2	×	—

1	1	×	—
2	2	—	0 1
3	0	✓	(1,4) 2
4	1		

∞ 1

8 points

$P = (0,1)$

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

$P_1 + P_2 = P_3$

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

P

Each point can be written as $k.P$

$a.P + b.P = (a+b).P$ ✓

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

$(5,0)+(5,0)=\infty$

$0 + \infty = 8$

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

$y^2 = x^3 + 6 \mod 7 \quad \{(1,0),(2,0),(4,0),\infty\} = (\mathbb{Z}_2 \times \mathbb{Z}_2,+)$

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

$(2,0)+(2,0)=\infty$

$(4,0)+(4,0)=\infty$

$(4,0)+(4,5)=\infty$

$\gamma+\infty=\infty$

We are going to build cryptographic protocols using discrete log on EC.

WHY?

E mod p uses $\log_2 p$ bit numbers

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

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

$|(E,+)| = p+1+2\sqrt{p}$ = better security

El Gamal Encryption

$\mathbb{Z}_p^*$

Public: p - a large prime

q - generator of $\mathbb{Z}_p^*$ (order of q $p-1$)

$y = q^x \bmod p$

Private: x

Encrypt m

choose a random $r \in \mathbb{Z}_p^*$

$a = q^r \bmod p$

$(E,+)$

Public: $(E,+) \bmod p$

P - generator of $\mathbb{Z}_p^*$ (order of P is k)

(k is smallest number such that $k.P=\infty$)

$Q = xP$

Private: x

Encrypt M

choose a random $r \in \{1, \dots, k\}$

$A = r.P$

$a = g^r \mod p$

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

Decrypt (a, b)

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

$= m \cdot y^r \cdot (g^r)^{-x} \mod p$

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

$= m$

$A = r \cdot P$

$B = M + r \cdot Q$

$P = (x, y)$

$-P = (x, -y)$

Decrypt (A, B)

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

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

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

$= M$

How to choose M to represent a message?

El Gamal Signatures

$\mathbb{Z}_p^*$

Public: p - a large prime

g - generator of $\mathbb{Z}_p^*$ (order of g $p-1$)

$y = g^x \mod p$

Private: x

Sign m

$(E, +)$

Public: $(E, +) \mod p$

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

$\rightarrow$ (order of P is k)

(k is smallest number such that $k \cdot P = \infty$)

$Q = x P$

Private: x

Sign m

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

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

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

Verify(m, a, b)

$$y^a \cdot a^b \overset{?}{=} g^m \mod p$$

$$g^{xa} \cdot g^{r(r^{-1}(m-ax))} \mod p$$

$$g^m$$

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

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

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

Verify(m, A, b)

$$a_1 \cdot Q + b \cdot A \overset{?}{=} m \cdot P$$

$$a_1 x \cdot P + (m - a_1 x) \cdot \underbrace{r^{-1} \cdot r}_{=1} \cdot P$$

$$= m \cdot P$$

$$r^{-1} \cdot r \equiv 1 \mod k$$

$$r^{-1} \cdot r = \ell \cdot k + 1$$

$$r^{-1} \cdot r \cdot P = \ell \cdot k + 1$$
$$= \ell \cdot k \cdot P + P$$
$$= \ell \cdot \infty + P$$
$$= \infty + P$$
$$= P$$

$$\overbrace{\underbrace{P + P + P}_{k = \infty} + \underbrace{\ldots + P}_{k = \infty} + \underbrace{P}_{n \bmod k}}^{n}$$

$$P + P + \ldots + P$$

HW 2b $\rightsquigarrow$ Pollard $p-1$ algorithm

$$k = \prod q^{\lfloor \log_q B \rfloor}$$

$\lfloor \log_q n \rfloor$ instead — wrong

$$\boxed{m = \prod_{q \mid q \text{ is a prime}} q^{\lfloor \log_q B \rfloor}}$$ ← correct

$\lfloor \log_q n \rfloor$ instead $\lfloor \log_q B \rfloor$

b the smallest number s.t. $\forall i < B \;\; i \mid m$