Tutorial VIII

27 November 2020 13:49

Elliptic curve cryptography

- → Mathemathics of elliptic curves
- → Elliptic curve version of discrete logarithm
- → ECC El Gamal protocols

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

There are multiple ways to construct large cyclic groups. Elliptic Curves is one of them.

Elliptic curve $y^2 = x^3 + ax + b \mod p$

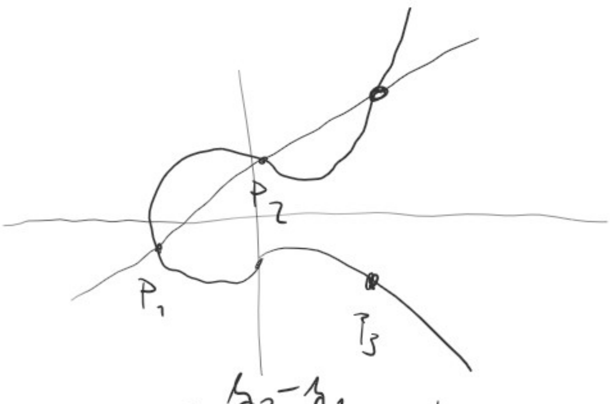
Non-singular if $-16(4a^3 + 27b^2) \neq 0 \mod p$

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

iff $\quad y^2 = x^3 + \boxed{a}x + b \mod p$

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

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



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

$y_3 = \lambda(x_1 - x_2) - y_1$

$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & P_1 \neq P_2 \end{cases}$

$y_3 = \lambda(x_1 - x_2) - y_1$ $\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \\ \frac{3x_1^2 + \boxed{a}}{2y_1} \end{cases}$

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

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

1.) E is non-singular $-16(4\cdot(4)^3 + 27\cdot(1)^2)$

$= -16(1+2)$ ✓

$= -3 \neq 0 \mod 5$

2.) P lies on E

$1^2 = 0^3 + 4\cdot 0 + 1 \mod 5$ ✓

$P = (0,1)$

$P+P = (x_3, y_3) = \overset{2P}{(4,1)}$ $\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{0+4}{2} = 4\cdot 2^{-1} = 4\cdot 3 = 12 = 2 \mod 5$

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

$= 2^2 - 0 - 0 = 4$

$1^2 = 4^3 + 4\cdot 4 + 1$ ✓

$-1 + 1 + 1 = 1$

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

$2(0-4) - 1 = 1 \mod 5$

$2P + P = (x_3, y_3)$ $\overset{x_1 y_1}{(4,1)} + \overset{x_2 y_2}{(0,1)}$

$= (1,4)$

$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{1-1}{0-4} = 0\cdot(-4)^{-1}$

$= 0 \mod 5$

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

$= 0 - 4 - 0 = \boxed{1} \mod 5$

$4^2 = 1^3 + \overbrace{4\cdot 1 + 1}^{5}$

$1 = 1$ ✓

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

$y_3 = \lambda(x_1 - x_3) - y_1 \mod 5$ $\qquad 1 = 1$ ✓

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

What if λ is not defined?

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

$P_1 = (x_1, y)$

$P_2 = (x_1, -y)$

$\lambda = \dfrac{3x_1^2 + a}{2y_1 b}$ $\quad P_1 = P_2$ $\qquad P_1 = P_2$ and $y_1 = 0$

In such cases $\quad P_1 + P_2 = \infty$

neutral additive element

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

We know that E is closed under addition.

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

For every point P there is a point $-P$ such that

$P + (-P) = \infty$

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

$P = (x, y) \quad -P = (x, -y) \qquad (y \neq 0)$

We now know that $(E, +)$ is a group

$P + Q = Q + P$

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

Every finite commutative group is isomorphic to

Every finite commutative group is isomorphic to

$[(\mathbb{Z}_{i_1} \times \mathbb{Z}_{i_2} \times \dots \times \mathbb{Z}_{i_k}), +]$ → how many elements?

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

$(\mathbb{Z}_{i_1}, +)$

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

$\{0,1,2,3\}, +\ \mathrm{mod}\ 4$ $\quad$ $\{(0,0), (0,1), (1,0), (1,1)\}$

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

$0+0 = 0 \mod 4$

$1+1 = 2 \mod 4$

$2+2 = 0 \mod 4$

$3+3 = 2 \mod 4$

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

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

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

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

Elliptic curve discrete logarithm problem

$\mathbb{Z}_p^*$ $\quad$ $(E, +)$

g – generator of $\mathbb{Z}_p^*$ $\quad$ P – generator of $(E,+)$

$\{g, g^2, g^3, \dots, g^{p-1}\} = \mathbb{Z}_p^*$ $\quad$ $\{P, 2P, 3P, \dots, \overset{\text{order of } (E,+)}{k}P\} = (E)$ $\quad$ a (size) if isomorphic to $(\mathbb{Z}_a, +)$

$y = g^x \mod p$ $\quad$ $Q = xP$

Solving for x given y, g, p is a discrete logarithm problem

Computationally hard

Solving for x given $Q, P, (E,+)$ is a EC discrete logarithm

Computationally hard

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

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

Hesse's theorem $\quad E \bmod p$ with N points

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

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

$N \le p+2\sqrt{p}+1$ $\qquad\qquad$ $N \ge p-2\sqrt{p}+1$

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

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

$2{,}0\ldots$ $\qquad\qquad$ $10{,}\ldots$

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

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

∞

$\boxed{8 \text{ points}}$

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

n	nP
1	$(0,1)$
2	$(4,1)$
3	$(1,4)$

$P=(0,1)$

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

isomorphism $E \longrightarrow \mathbb{Z}_8$

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

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

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

Each point can be written as $k \cdot P$

$$f: aP \to a$$

$$a + b = (a+b)$$

$$\boxed{aP + bP = (a+b)P}$$

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

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

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

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

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

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

$\infty + \infty = \infty$

Why is EC discrete logarithm advantageous?

$E \mod p$ uses $\log_2 p$ bit numbers

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

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

$|(E,+)| \sim p + 1 + 2\sqrt{p}$ = EC log problem is harder

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

$\mathbb{Z}_p^*$ uses exponentiation which is computationally expensive!

El Gamal Encryption

$\mathbb{Z}_p^*$

Public: p - large prime

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

$y = g^x \mod p$

Private: x

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

P generator of $(E,+)$ (of order k)

k is the smallest k, such that $k.P = \infty$

$Q = x P$

Private: x

Encrypt m

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

$a = g^r \mod p$

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

Encrypt M

Choose random $r \in \{1, \dots, k\}$

$A = r.P$

$B = M + r.Q$

Decrypt (a,b)

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

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

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

Decrypt (A,B)

$M = (B - x.A)$

$P = (x,y)$

$-P = (x,-y)$

$= M + r.Q - x.r.P$

$M + r.x.P - x.r.P$

$= M$

A How to map messages to points on the curve

El Gamal signatures

$\mathbb{Z}_p^*$

Public: p – large prime

g – generator of $\mathbb{Z}_p^*$

$y = g^x \bmod p$ order of g is $p-1$

Private: x

Sign m

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

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

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

Verification (m, a, b)

$$y^a a^b \stackrel{?}{=} g^m \bmod p$$

$$(g^x)^a \, g^{r \cdot (r^{-1}(m-ax))} \bmod p$$

$$g^m \bmod p$$

$(E, +) \bmod p$

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

$P \in E$ – generator $(E, +)$

↳ order of P

$k \Rightarrow$ the smallest k, such that $k.P = \infty$

$Q = xP$

Private: x

Sign m

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

$$A = r.P = (a_1, a_2)$$

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

Verification (m, A, b)

$$a_1 Q + b.A \doteq m.P$$

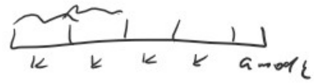
$$a_1 x.P + \{(m - a_1 x).r^{-1}.r\} P$$

$$a_1 x P + (m - a_1 x) P$$

$$\cancel{a_1 x P} + mP - \cancel{a_1 x P}$$

$$mP$$

$aP = (a \bmod k) P$



$$a.P = (k + k + \dots + k + a \bmod k).P$$

$$= \underbrace{k.P}_{\infty} + \underbrace{k.P}_{\infty} + \dots + k.P + (a \bmod k).P$$

$m\, r$

$$= k.P + k.P + \cdots + k.P + (a \bmod k).P$$

$$\underset{\infty}{\overset{\shortparallel}{}} \qquad \underset{\infty}{\overset{\shortparallel}{}}$$

$$(a \bmod k).P$$