Tutorial 8 SVK

03 November 2021 18:04

KRYPTOGRAFIA S ELIPTICKÝMI KRIVKAMI

- Matematika Eliptických kriviek (EC)
- Eliptická varianta diskrétneho logaritmu
- EC ElGamal protokoly

Z_p^* - pretože p je tento objekt cyklická komutatívna grupa $(p-1)$

ktorú sa dá použiť na definíciu diskrétneho logaritmu.

Existujú iné spôsoby ako nadefinovať cyklické komutatívne grupy.

Eliptické krivky sú jedna takáto možnosť

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

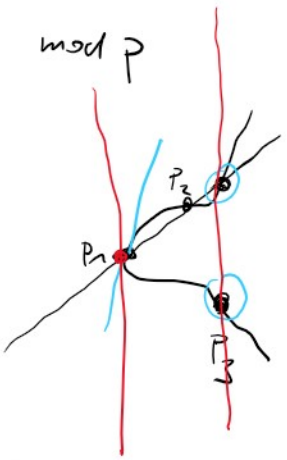
Nesingulárne $-16(4a^3 + 27b^2) \not\equiv 0 \mod p$

Bod (x,y) leží na krivke E $(P = (x,y) \in E)$

práve vtedy keď $y^2 = x^3 + ax + b \mod p$

$P_1 = (x_1, y_1)$

$P_2 = (x_2, y_2) \in E$



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

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

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

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

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

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

Čo ak λ nie je dobre definované?

1.) $P_1 \neq P_2$ a $x_1 = x_2$ $\quad P_1 = (x, y)$ $\quad P_2 = (x, -y)$ $\quad P_1 + P_2 = \infty$

2.) $P_1 = P_2$ a $y_1 = 0$ $\quad P_1 = (x, 0)$ $\quad P_1 + P_1 = \infty$

∞ ... neutrálne vo sčítaní

$\forall P \quad P + \infty = \infty + P = P$

$\infty + \infty = \infty$

E so symbolom ∞ je uzavretá na sčítanie

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

Pre každý bod P existuje inverzný prvok $-P$, t.ž. $P + (-P) = \infty$

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

$P = (x, y) \quad -P = (x, -y)$

$(E, +)$ je grupa

$P + Q = Q + P$

$(E, +)$ je komutatívna grupa

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

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

1.) Nesingularita ✓ $\quad -16(4 \cdot (4)^3 + 27 \cdot 1^2) \neq 0 \mod 5$

$-1 \; (-1(-1)^3 + 2 \cdot 1) \neq$

$-1\,(-1(-1)^3 + 2\cdot 1) \neq$

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

2.) $1^2 = 0 + 4\cdot 0 + 1$ ✓

$P = (0,1)$

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

$x_3 = \lambda^2 - x_1 - x_2 \equiv 4 \mod 5 \equiv 4-3 \equiv 2 \mod 5$

$4 - 0 - 0$

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

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

$2P + P = (x_3, y_3) = (1,4)$ $(4,1) + (0,1)$

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

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

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

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

$= -1 \equiv 4 \mod 5$

Každá komutatívna grupa je izomorfná nejakej grupe tvaru $\{(\mathbb{Z}_{i_1} \times \mathbb{Z}_{i_2} \times \dots \times \mathbb{Z}_{i_2}), +\}$

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

veľkosť $\prod_{j=1}^{2} i_j$

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

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

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

$0+0$	$=0$
$1+1$	$=2$
$2+2$	$=0$
$3+3$	$=2$

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

$\{(0,0), (0,1), (1,0), (1,1)\}$ $(i,j) + (k,l)$

$= (i+k, j+l) \bmod 2$

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

Eliptická varianta diskrétneho logaritmu

$\mathbb{Z}_p^*$

g - generátor $\mathbb{Z}_p^*$

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

$y = g^x \bmod p$

Pre y, g a p nájdi x

$(E, +)$

P - generátor $(E, +)$

$\{P, 2P, 3P, \ldots, \underline{\ell}P\} = E$

$Q = xP$

Pre Q, P a E nájdi x

Výpočtovo náročné

Ako veľká je Eliptická krivka $(E, +)$?

Hasseho teoréma: Pre $E \bmod p$ s N bodmi platí

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

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

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

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

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

2. ... $\qquad$ 10. ... $\qquad$ Eulers criterion $a^{\frac{p-1}{2}} \equiv 1 \mod p$

X	$x^3+4x+1 \mod$	QR mod 5	Body
0	1	✓	(0,1), (0,4)
1	1	✓	(1,1), (1,4)
2	2	X	—
3	0	✓	(3,0)
4	1	✓	(4,1) (4,4)
	1		∞

8 bodov

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

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

P = (0,1)

$67352\,P \equiv (67352 \mod 8)\,P$

$3P+5P = 8P$

$= \infty$

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

6 | (4,4)
7 | (0,4)
8 | ∞

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

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

$f: aP \to a$

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

Príklad dvoch kriviek s rovnakým počtom bodov a inou štruktúrou

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

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

Prečo EC diskrétny logaritmus?

E mod p pracuje s číslami veľkosti $\log_2 p$

$\mathbb{Z}_p^*$ ——— " ——— $\log_2 p$

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

$|(E,+)| = p+1+2\sqrt{p}$ $\Rightarrow$ rovnaké krivky väčšia bezpečnosť

$\mathbb{Z}_p^*$ používa modulárnu exponenciáciu $\Rightarrow$ výpočetne náročné

El Gamal šifrovanie

$\mathbb{Z}_p^*$

p- veľké prvočíslo

$(E,+)$

Krivka $= (E,+)$, kde krivky (E)

Verejné

Verejné: p - veľké prvočíslo, q - generátor $\mathbb{Z}_p^*$, $y = q^x \bmod p$

Tajné: x

Šifrovanie správy m

Zvoľ náhodné číslo $r \in \mathbb{Z}_p^*$

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

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

Desifrovanie (a, b)

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

$$= m \cdot y^r \cdot (q^r)^{-x} \bmod p$$

$$= m \cdot q^{x \cdot r} \cdot q^{-xr} \bmod p$$

$$= m$$

El Gamal podpisy

$\mathbb{Z}_p^*$

Verejné: p - veľké prvočíslo, q - generátor $\mathbb{Z}_p^*$, $y = q^x \bmod p$

Tajné: x

Krivka $= (C, +)$, ktorá existuje

P - generátor $(E, +)$ (veľkosť $E, +$)

$Q = x P$ $\quad$ $\xi, P > \infty$

x

Šifrovanie správy M

Zvoľ náhodné číslo $r \in \mathbb{Z}_k^*$

$$A = x \cdot P$$

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

(A, B)

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

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

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

$$= M + \infty = M$$

$(E, +)$

Krivka $= (E, +)$, ktorá existuje

P - generátor $(E, +)$ (veľkosť $E, +$)

$Q = x P$ $\quad$ $\xi, P > \infty$

x

Podpis m

Zvol r z $\mathbb{Z}_{p-1}^*$

$a = g^r \bmod p$

$b = r^{-1}(m - a \cdot x) \bmod (p-1)$

Verifikácia m, a, b

$g^a \cdot a^b = g^m \bmod p$

$\equiv 1 \bmod (p-1)$

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

$g^m \cdot g^{x a} \cdot g^{-a x} \equiv g^m \bmod p$

Podpis m

Zvol r zo $\mathbb{Z}_\varphi^*$

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

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

$(a_2 - m \cdot x)$

Verifikácia m, A, b

HOMEWORK