Kryptografia na báze eliptických kriviek

Katedra matematiky a teoretickej informatiky, FEI TU

Elliptic Curve Cryptography (ECC)

- nový a perspektívny smer v modernej kryptografii
- umožňuje dosiahnuť rovnakú kryptografickú bezpečnosť pri menšej dĺžke kľuča

Kryptografické systémy na báze ECC:

- predstavujú alternatívu k systémom na báze RSA a DSA
- väčšia rýchlosť a menšie nároky na technické prostriedky

Bezpečnosť (v Bitoch)	RSA dĺžka kľúča	ECC dĺžka kľúča
80	1024	160-223
112	2048	224-255
192	7680	384-511
256	15360	512+

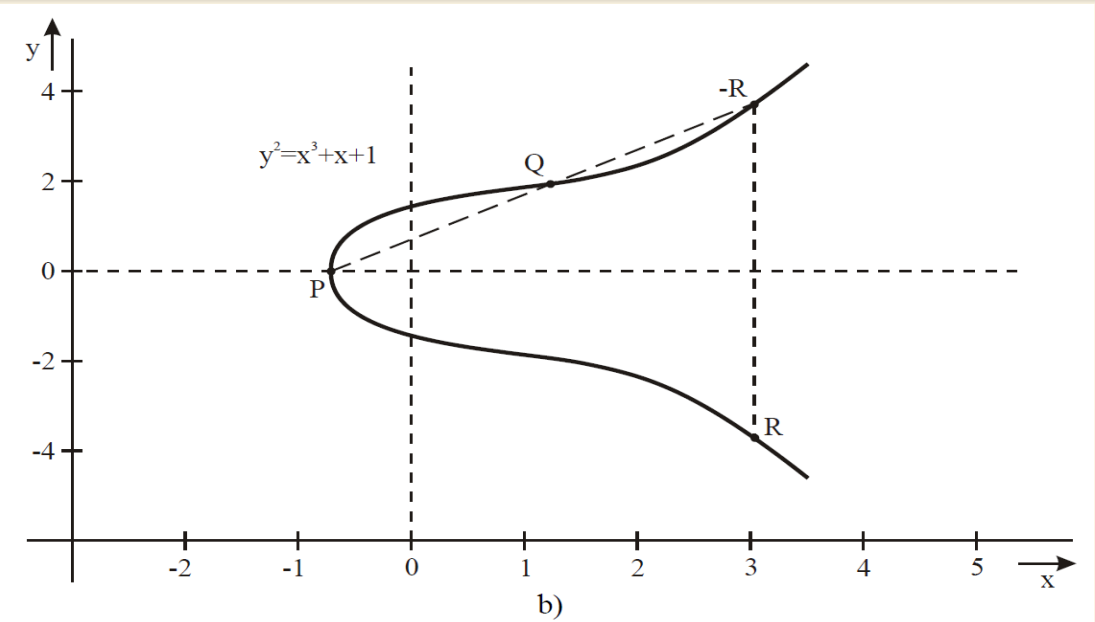
Tabuľka: Tabuľka porovnaní dĺžky kľúčov

Eliptické krivky nad reálnymi číslami $E(a, b)$

- sú špeciálnou triedou kubických kriviek
- eliptická krivka je množina bodov, ktoré vyhovujú eliptickej rovnici

$$y^2 = x^3 + ax + b$$

- definícia eliptickej krivky zahŕňa tiež špeciálny bod označovaný ako bod O, ktorý sa nazýva bod v nekonečne alebo nulový bod
- eliptická krivka je symetrická podľa osi x



b)

Geometrická interpretácia sčítania

Majme základnú množinu grupy $E(a, b)$, kedy prvky a, b vyhovujú podmienke

$$4a^3 + 27b^2 \neq 0$$

Taktiež definujeme nulový bod (bod v nekonečne) O.

Definícia

Ak tri body eliptickej krivky ležia na jednej priamke, ich súčet je rovný O.

1. Bod O je vzhľadom na sčítanie neutrálny prvok, teda $O = -O$ a $P - O = P$
2. Existuje opačný bod $-P = (x, -y)$ k bodu $P = (x, y)$, ktorý má odlišnú iba súradnicu y.
   Pre tieto body platí, že ležia na vertikálnej priamke a $P + (-P) = P - P = O$

Geometrická interpretácia sčítania

Majme základnú množinu grupy $E(a, b)$, kedy prvky a, b vyhovujú podmienke

$$4a^3 + 27b^2 \neq 0$$

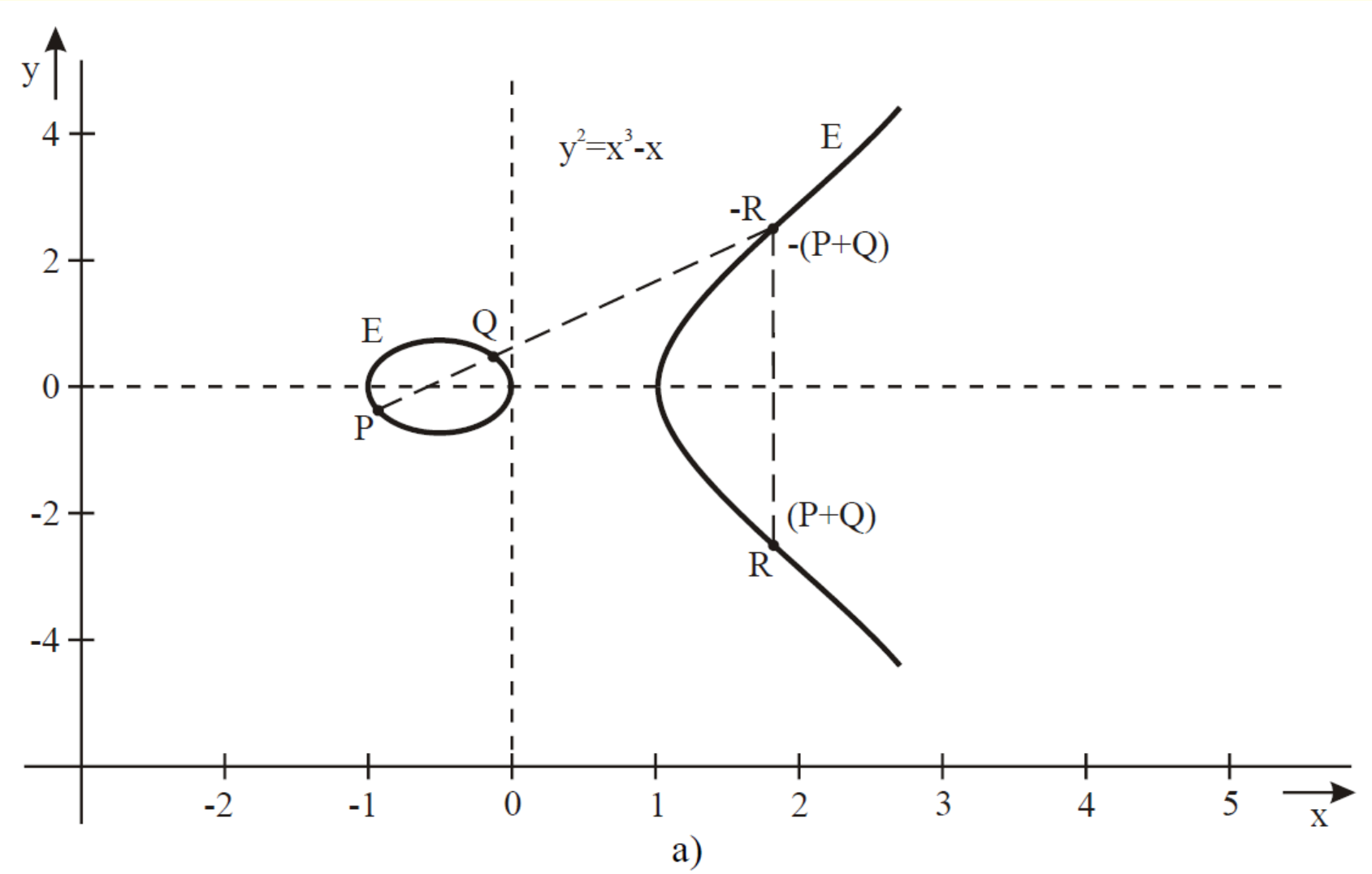
Taktiež definujeme nulový bod (bod v nekonečne) O.

Definícia

Ak tri body eliptickej krivky ležia na jednej priamke, ich súčet je rovný O.

1. Sčítanie dvoch rôznych bodov P a Q realizujeme tak, že bodmi P a Q preložíme priamku, ktorej priesečník s eliptickou krivkou označíme $-R$. Platí teda $P + Q = R$. Bod R je symetrickým bodom k bodu $-R$ podľa osi x.
2. Body P a $-P$ možno spojiť vertikálnou priamkou, ktorá pretína eliptickú krivku v nekonečne, teda $P + (-P) = O$.

Eliptická krivka $E(-1, 0)$



a)

Algebraická interpretácia sčítania

Majme body $P = (x_P, y_P)$ a $Q = (x_Q, y_Q)$ na eliptickej krivke $y^2 = x^3 + ax + b$, ktoré nie sú navzájom opačné, potom smernica spájajúca tieto body je daná vzťahom:

$$s = \frac{y_Q - y_P}{x_Q - x_P}$$

Navyše, ak platí, že $R = P + Q$, potom súradnice bodu $R = (x_R, y_R)$ určíme ako:

$$x_R = s^2 - x_P - x_Q$$
$$y_R = -y_P + s(x_P - x_R)$$

Algebraická interpretácia sčítania

Pre sčítanie dvoch rovnakých bodov P platí $P + P = 2P = R$ a smernica priamky je daná predpisom

$$s = \frac{3x_P^2 + a}{2y_P}$$

Súradnice bodu R potom možno vyjadriť vzťahmi

$$x_R = s^2 - 2x_P$$
$$y_R = s \cdot (x_P - x_R) - y_P$$

Eliptické krivky nad konečnými poľami

ECC používa eliptické krivky, ktorých premenné a koeficienty sú prvkami konečných polí - rozdeľujú sa do dvoch skupín:

1. **binárne eliptické krivky**
   - definované nad konečným poľom $GF(2^n)$
   - výhodnejšie pre hardvérové riešenia
2. **prvočíselné eliptické krivky**
   - definované nad konečným poľom $GF(p)$
   - výhodnejšie pre softvérové aplikácie
   - opísané kubickou rovnicou, v ktorej premenné nadobúdajú hodnoty z intervalu $< 0; p - 1 >$
   - operácie sa realizujú pomocou modulo p, teda rovnica prechádza na tvar

$$y^2 mod\, p = (x^3 + ax + b)\, mod\, p \tag{1}$$

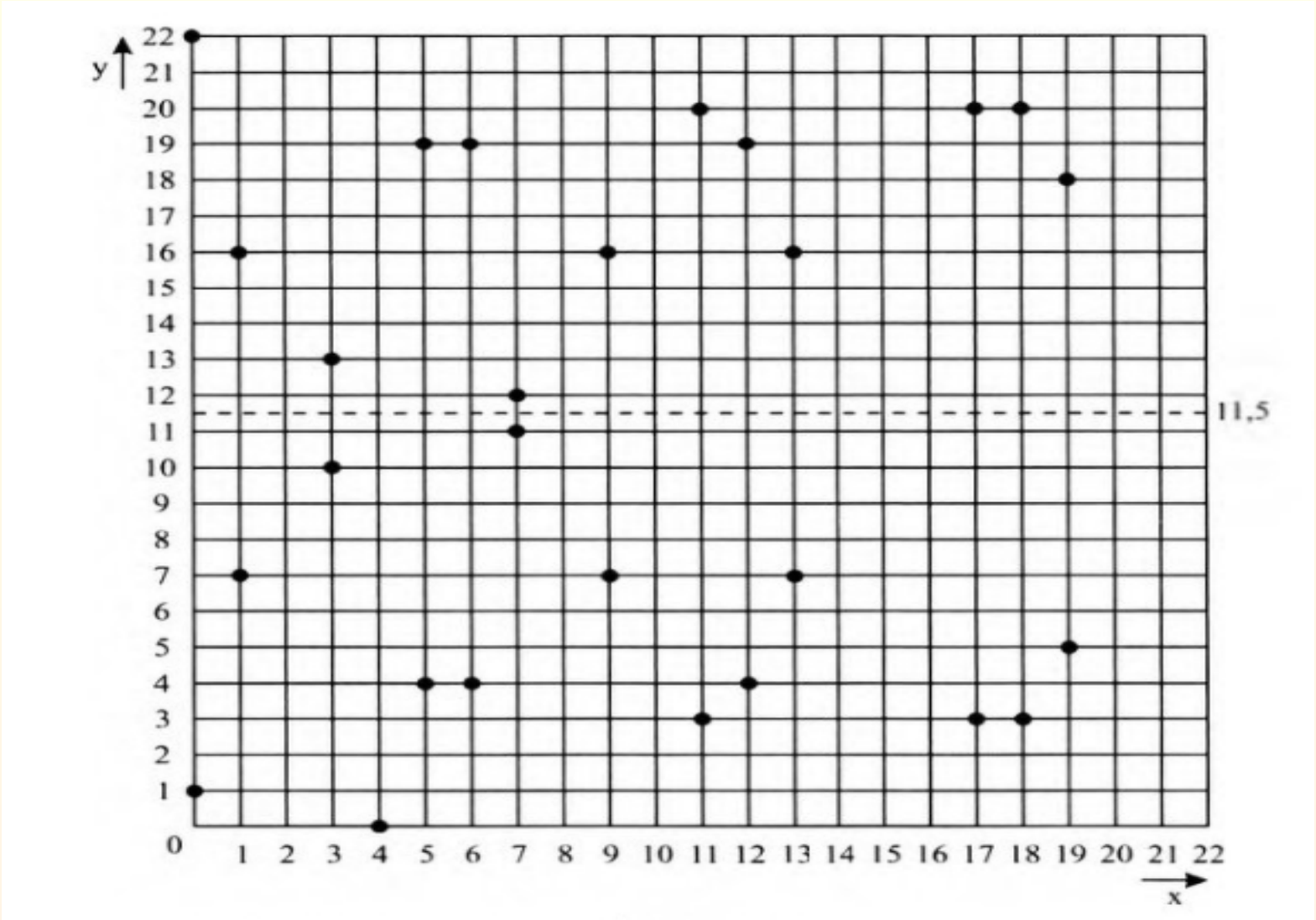
PR.1. Uvažujme $E_{23}(1,1)$: $y^2 mod\, 23 = (x^3 + x + 1)\, mod\, 23$

- ukážte, že daná rovnica je splnená pre hodnoty $x = 6$, $y = 4$
- aké hodnoty môžu nadobúdať x a y?
- určte body, ktoré tvoria množinu $E_{23}(1,1)$, pre $x = 0$ a $x = 1$
- okolo ktorého bodu je množinu $E_{23}(1,1)$ symetrická?
- ktorý bod je výnimkou z tejto symetrie a prečo?
- množina $E_{23}(1,1)$ obsahuje celkovo 28 bodov (párny počet). Ako je to vzhľadom na symetriu s 1 výnimkou možné?

(0,1)	(6,4)	(12,19)	(0,22)
(6,19)	(13,7)	(1,7)	(7,11)
(13,16)	(1,16)	(7,12)	(17,3)
(3,10)	(9,7)	(17,20)	(3,13)
(9,16)	(18,3)	(4,0)	(11,3)
(18,20)	(5,4)	(11,20)	(19,5)
(5,19)	(12,4)	(19,18)	???

Tabuľka: Zoznam bodov množiny $E_{23}(1,1)$

$E_{23}(1,1)$: $y^2 mod\, 23 = (x^3 + x + 1)\, mod\, 23$



Pravidlá sčítania nad množinou $E_p(a,b)$

Zodpovedajú pravidlám, ktoré boli definované pre eliptické krivky nad reálnymi číslami. Pre všetky body $P, Q \in E_p(a,b)$ teda platí:

1. $P + O = P$
2. ak $P = (x_P, y_P)$ a $-P = (x_P, -y_P)$, potom $P + (-P) = O$ a $-P$ je opačný bod k bodu P
3. ak $P = (x_P, y_P)$ a $Q = (x_Q, y_Q)$, pričom $P \neq -Q$, potom $P + Q = R = (x_R, y_R)$ a platí:
   - $x_R = (s^2 - x_P - x_Q) mod\, p$, ak $P \neq Q$
   - $x_R = (s^2 - x_P - x_P) mod\, p$, ak $P = Q$
   - $y_R = [s(x_P - x_R) - y_P] mod\, p$
   - $s = \left(\frac{y_Q - y_P}{x_Q - x_P}\right) mod\, p$, ak $P \neq Q$
   - $s = \left(\frac{3x_P^2 + a}{2y_P}\right) mod\, p$, ak $P = Q$
4. násobenie bodu skalárom je definované ako opakované sčítanie, napr. $2P = P + P, 4P = 2P + 2P = P + P + P + P$

Eliptické krivky nad konečným poľom $GF(2^n)$

V kryptografických algoritmoch sa pre eliptické krivky nad $GF(2^n)$ používajú kubické rovnice, ktoré sa odlišujú od rovníc pre eliptické krivky nad GF(p).

Rovnice týchto kriviek majú tvar

$$\mathbf{y^2 + xy = x^3 + ax^2 + b} \tag{2}$$

kde premenné x, y a koeficienty a, b sú prvkami konečného poľa $GF(2^n)$
a operácie sú realizované v $GF(2^n)$.

Uvažujme, že množina $E_{2^n}(a, b)$ obsahuje všetky dvojice celých čísel (x, y), ktoré spĺňajú rovnicu 2 spoločne s bodom O. Nad množinou $E_{2^n}(a, b)$ možno definovať abelovskú grupu, pričom pre všetky body $P, Q \in E_{2^n}(a, b)$ platia pre sčítanie nasledujúce pravidlá.

Pravidlá sčítania nad množinou $E_{2^n}(a, b)$

1. $P + 0 = P$
2. ak $P = (x_P, y_P)$, potom $P + (x_P, x_P + y_P) = O$. Bod $(x_P, x_P + y_P)$ je opačný bod k bodu P a označuje sa ako $-P$
3. ak $P = (x_P, y_P)$ a $Q = (x_Q, y_Q)$ pričom $P \neq -Q$ a $P \neq Q$, potom pre súčet $P + Q = R$ a $R = (x_R, y_R)$ platí

$$x_R = s^2 + s + x_P + x_Q + a$$
$$y_R = s(x_P + x_R) + x_R + y_R$$

kde $s = \frac{y_Q + y_P}{x_Q + x_P}$

4. ak $P = (x_P, y_P)$, potom $R = P + P = 2P$ platí

$$x_R = s^2 + s + a$$
$$y_R = x_P^2 + (s + 1)x_R$$

kde $s = x_P + \frac{y_P}{x_P}$

Eliptické krivky nad konečným poľom $GF(2^n)$

Výber prvkov konečného poľa $GF(2^n)$ možno v porovnaní s $GF(p)$ realizovať rôznymi spôsobmi:

štandardná resp. polynomiálna báza - prvky sú určené binárnymi polynómami menšieho stupňa než n a operácie sú realizované modulo ireducibilný polynóm stupňa n

optimálna normálna báza - prvky telesa $GF(2^n)$ sú reprezentované ako lineárne kombinácie prvkov množiny $(\beta^{2^0}, \beta^{2^1}, \beta^{2^2}, ..., \beta^{2^{n-1}})$, kde β je vhodne zvolený prvok poľa

reprezentácia telesom typu "veža" - prvky sú určené polynómami nad $GF(2^r)$, kde r je deliteľom n

ECC využíva **náročnosť výpočtu diskrétnych algoritmov**. Ak pre určitý bod P na eliptickej krivke postupne vypočítame body $2P, 3P, 4P, ...$, dostaneme postupnosť rôznych bodov na tejto eliptickej krivke. Po určitom počte n krokov dosiahneme bod O. V ďalšom kroku sa realizuje výpočet $n \cdot P + P = O + P = P$ a postupnosť sa opakuje.

P	2P	3P	4P	5P	6P	7P	8P=P
(13,7)	(5,4)	(17,3)	(17,20)	(5,19)	(13,16)	O	(13,7)

Tab. Viacnásobné sčítanie rovnakého bodu $P = (13, 7)$ na eliptickej krivke $E_{23}(1, 1)$, ktorá je daná rovnicou $y^2 = x^3 + x + 1$ nad $GF(23)$.

Najmenšie číslo n, pre ktoré platí $n \cdot P = O$ sa nazýva **rád bodu P**, pričom rôzne body na eliptickej krivke majú rôzny rád. **Rád eliptickej krivky** je počet bodov na krivke. Rád každého bodu P delí rád krivky.

Rády n bodov na eliptickej krivke $E_{23}(1,1)$:

Bod	n	Bod	n	Bod	n	Bod	n
(0,1)	28	(6,4)	14	(12,19)	14	(0,22)	28
(6,19)	14	(13,7)	7	(1,7)	28	(7,11)	14
(13,16)	7	(1,16)	28	(7,12)	14	(17,3)	7
(3,10)	28	(9,7)	28	(17,20)	7	(3,13)	28
(9,16)	28	(18,3)	28	(4,0)	4	(11,3)	4
(18,20)	28	(5,4)	7	(11,20)	4	(19,5)	28
(5,19)	7	(12,4)	14	(18,18)	28	O	

Šifrovanie a podpisovanie v ECC je založené na náročnosti výpočtu diskrétnych logaritmov, pri ktorom sa volí bod P a tajné číslo n a potom sa vypočíta bod $Q = n \cdot P$. Body P a Q sú súčasťou verejného kľúča a môžu sa zverejniť.

Problém diskrétneho logaritmu je úloha, ako zo známych bodov P a Q určiť tajné číslo n tak, aby $Q = n \cdot P$. Pre malé n je úloha triviálna, avšak pre veľké n (napr. 2^{256}) je úloha obťažná.

Výmena tajného kľúča na báze ECC

Voľba verejných prvkov

- $E_q(a, b)$- eliptická krivka s parametrami a, b a q,kde q je prvočíslo
- P- bod na eliptickej krivke s veľkým rádom n

Generovanie kľúča účastníkom A

- Voľba súkromného kľúča n_A, kde $n_A < n$
- Výpočet verejného kľúča Q_A, kde $Q_A = n_A \times P$

Generovanie kľúča účastníkom B

- Voľba súkromného kľúča n_B, kde $n_B < n$
- Výpočet verejného kľúča Q_B, kde $Q_B = n_B \times P$

Výmena tajného kľúča na báze ECC

Generovanie tajného kľúča K účastníkom A

- $K = n_A \times Q_B$

Generovanie tajného kľúča K účastníkom B

- $K = n_B \times Q_A$

Na získanie kľúča je potrebné zo známych hodnôt Q_A, resp. Q_B určiť n_A a n_B, čo je pre veľké hodnoty n_A a n_B obťažné.

Tajný kľúč je dvojica čísel (x, y). Ak sa má tento kľúč použiť ako kľúč relácie pre bežné šifrovanie, potom je potrebné iba jedno číslo. Na tento účel možno použiť jednoducho súradnicu x alebo jednoduchú funkciu súradnice x.

Šifrovanie na báze ECC

- otvorený text m je postupnosť symbolov, ktorá sa interpretuje ako postupnosť súradníc x, y bodov P_m na zvolenej eliptickej krivke
- tieto body P_m sa šifrujú, čím sa získa zašifrovaný text
- dešifrovaním sa opäť získa postupnosť bodov P_m a tým aj postupnosť symbolov otvoreného textu

Vo zvolenom postupe šifrovania sa predpokladá, že prebehla výmena verejných kľúčov, ktorá vyžaduje voľbu eliptickej krivky $E_q(a, b)$ a bodu P, teda Q_A, resp. Q_B, v ktorých boli zvolené hodnoty n_A resp. n_B.

Šifrovanie na báze ECC

- účastník A zvolí náhodné kladné číslo k a generuje symbol zašifrovaného textu C_m, ktorý je reprezentovaný dvojicou bodov na eliptickej krivke v tvare

$$C_m = \{k \cdot P, P_m + k \cdot Q_B\},$$

  t.j. účastník A zašifruje správu vo forme P_m pričítaním hodnoty $k \cdot Q_B$.
- POZN.: účastník A pozná verejný kľúč účastníka Q_B
- pri dešifrovaní prijatého symbolu C_m účastník B realizuje $P_m + k \cdot Q_B - n_B(k \cdot P) = P_m + k \cdot (n_B \cdot P) - n_B \cdot (k \cdot P) = P_m$

Pretože iba A pozná hodnotu k, aj pri známej hodnote Q_B (verejný kľúč B) je dešifrovanie, teda získanie P_m, obťažné.

Bezpečnosť kryptografických algoritmov na báze ECC

- je založená na obťažnosti určenia k pre známe $k.P$ a P, teda na probléme diskrétneho logaritmu v eliptických krivkách ECDLP
- zložitosť riešenia ECDLP je exponenciálna
- aj keď je pomerne obťažné presne určiť bezpečnosť algoritmov na báze ECC, ukazuje sa, že dĺžka kľúča minimálne 160 bitov v ECC je ekvivalentná s dĺžkou kľúča 1024 bitov v RSA
- veľkou výhodou ECC je teda podstatne menšia dĺžka kľúča v porovnaní s RSA pri rovnakom stupni bezpečnosti

Ďakujem za pozornosť

OTÁZKY?