Nesymetrická kryptografie s eliptickými křivkami

Základní principy

Ivo Rosol
ředitel vývojové divize

20. 5. 2010

OKsystem *Spojujeme software, technologie a služby*

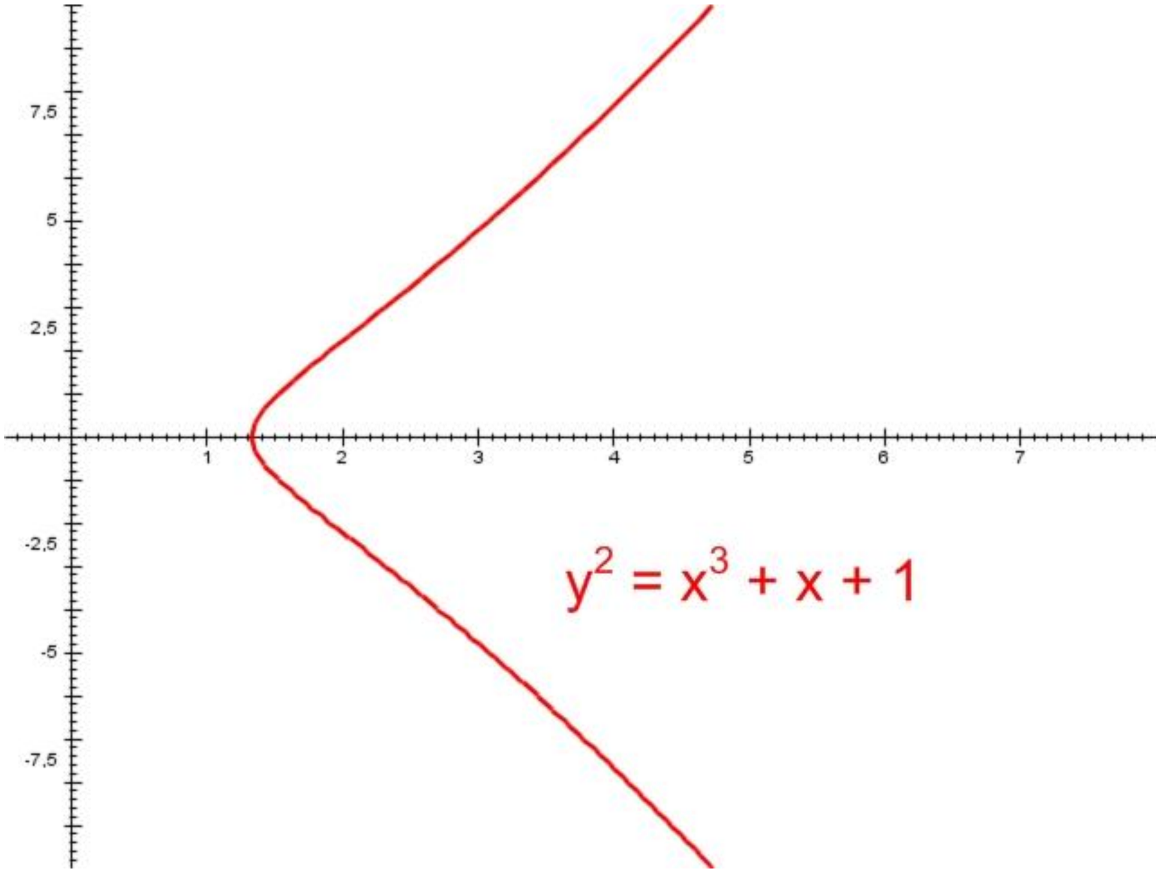
Eliptická křivka v rovině

Eliptická křivka je množina bodů (x,y), které vyhovují rovnici:

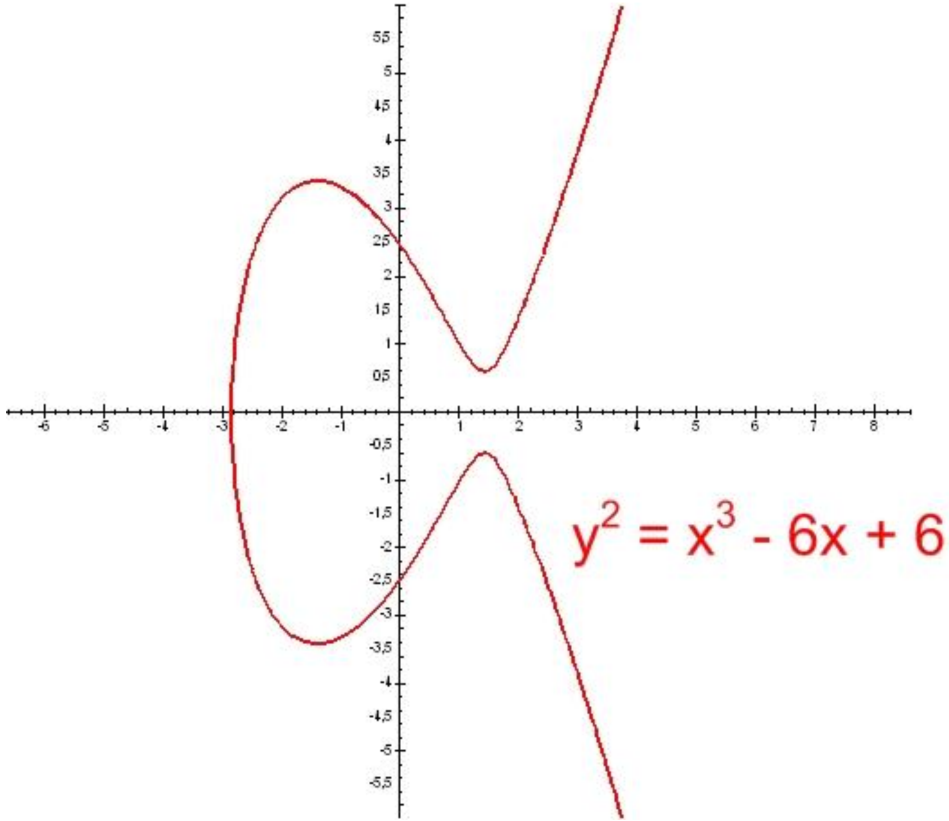
$$y^2 = x^3 + ax + b$$

x, y, a, b jsou reálná čísla

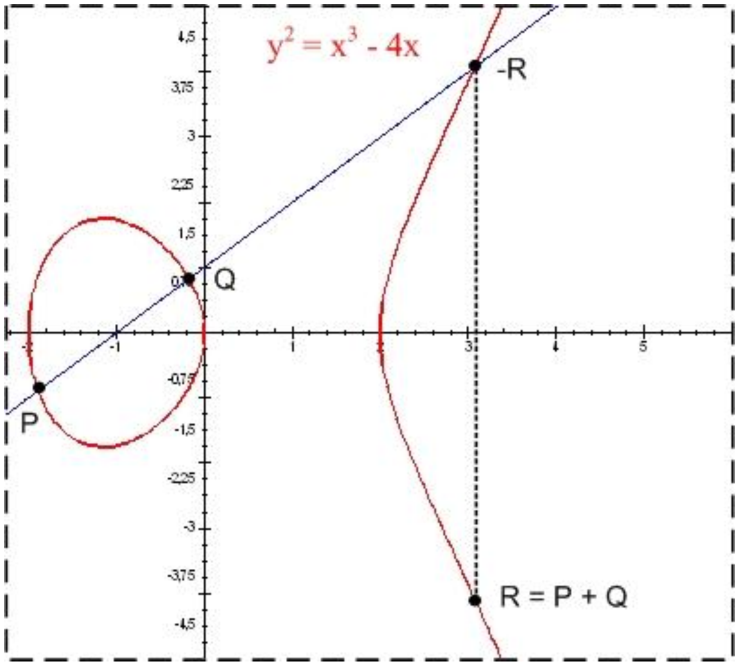
Eliptická křivka



Eliptická křivka



Sčítání bodů na eliptické křivce



OKsystem

Souřadnice bodu R = P + Q

Souřadnice součtu bodů R = P + Q získáme jako (třetí) průsečík přímky procházející body P a Q (ležícími na křivce) a eliptické křivky, s tím, že y souřadnici změníme znaménko.

$P = [x_1,y_1]$; $Q = [x_2,y_2]$; $R = [x_3,-y_3]$

Rovnice přímky, procházející body P, Q:

$\mathbf{y} - y_1 = (y_2 - y_1)/(x_2 - x_1) * (\mathbf{x} - x_1)$

Ve směrnicovém tvaru $\mathbf{y} = s*\mathbf{x} + q$,

je směrnice: $s = (y_2 - y_1)/(x_2 - x_1)$

a posunutí v ose y: $q = y_1 – s*x_1$

Souřadnice bodu R = P + Q

Bod přímky (x,y) = (x, s*x+q) leží na křivce, pokud: $(s*x+q)^2 = x^3+a*x+b$,

po úpravě: $\mathbf{x}^3-s^2*\mathbf{x}^2+(a-2*s*q)*\mathbf{x}+b-q^2 = 0$

Dva kořeny x_1 a x_2 (x-ové souřadnice bodů P a Q) této kubické rovnice jsou známy, hledáme třetí kořen x_3. Vyjádříme normovaný polynom 3. stupně ve tvaru rozkladu na kořenové činitele:

$$(\mathbf{x}-x_1)*(\mathbf{x}-x_2)(\mathbf{x}-x_3) = 0$$

$$\mathbf{x}^3 - (x_1+x_2+x_3)\mathbf{x}^2 + (x_1x_2 +x_1x_3 +x_2x_3)\mathbf{x} - x_1x_2\, x_3 =0$$

Porovnáním koeficientů u $\mathbf{x}^2$: $x_1+x_2+x_3 = s^2$,

tedy: $x_3 = s^2 - x_1-x_2$,

souřadnice y_3 se získá z rovnice přímky:

$$y_3 = s*x_3 + q$$

R = (x_3, $-y_3$)

Souřadnice bodu R = P + P

V případě kdy P=Q je R=P+P, což lze zapsat R = 2*P, je přímka tečnou eliptické křivky v bodě P, její směrnice je rovna derivaci (implicitní funkce) dy/dx:

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

$2*y*dy/dx = 3x^2 + a$

$dy/dx = (3x^2 + a)/2*y$,

v bodě $P = (x_1, y_1)$ je směrnice s: $(3x_1^2 + a)/2*y_1$

$x_3 = s^2 - 2*x_1$

$y_3 = s*x_3 + q$

$R = (x_3, -y_3)$

Těleso (pole)

V kryptografii nelze počítat s reálnými čísly, operace musí být přesné (bez zaokrouhlování a iracionálních čísel), prováděné s <u>celými čísly</u>. V počítači je navíc nutno pracovat s celými čísly s <u>omezenou velikostí</u>.

Při výpočtech **souřadnic bodů na eliptických křivkách** potřebujeme <u>sčítat, odečítat, násobit a dělit</u> (nenulovým prvkem). Algebraická struktura s těmito operacemi se nazývá těleso (pole).

Těleso reálných čísel s běžnými operacemi sčítání, odečítání, násobení a dělení nahradíme tělesem s konečným počtem prvků {0,1,2,...p-1}, kde p je prvočíslo a výpočetní operace se provádějí modulo p

Operace nad tělesem F(p)

Mějme číslo p, pak množina prvků F = (0;1;2;3; ... p-1) se dvěma operacemi sčítání + a násobení *, která pro všechna a;b;c z F splňuje následující podmínky:

1. a+(b+c) = (a+b)+c (asociativní pro +)
2. existuje 0 tak, že
   a + 0 = 0 + a = a (nulový prvek)
3. pro všechny a z F existuje (-a) tak, že
   a+(-a) = (-a)+a = 0 (opačný prvek)
4. a+b = b+a (komutativní)
5. (a*b)*c = a*(b*c) (asociativní pro *)
6. (a+b)*c = a*c+b*c ; c*(a+b) = c*a+c*b (distributivní)
7. Existuje 1 tak, že
   a * 1 = 1 * a = a (jednotkový prvek)
8. pro všechna a z F existuje a^{-1} tak, že
   $a*a^{-1} = a^{-1}*a = 1$ (inverzní prvek)

se nazývá (konečné) Galloisovo těleso GF(p)

OKsystem

Prvočíselné těleso F(23)

Těleso F(p), kde p je prvočíslo, má prvky F = { 0;1;2;3; ... p-1 }
Pokud by p nebylo prvočíslo, neexistoval by pro každé a inverzní prvek a^{-1}

Na rozdíl od běžných aritmetických operací se zde po každé operaci provede celočíselné dělení modulem p a výsledkem operace je zbytek po tomto dělení.

Příklad: Těleso F(23):
{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22}

Operace sčítání:	(a+b) mod p	15 + 9 = 24 = 1 (mod 23)
Operace odečítání:	(a + (-b)) mod p	6 – 11 = 6 + 12 = 18 (mod 23)
Operace násobení:	(a*b) mod p	5 * 12 = 60 = 14 (mod 23)
Operace dělení:	($a*b^{-1}$) mod p	8 / 14 = 8 * 5 = 40 = 17 (mod 23)

OKsystem

Sčítací tabulka pro F(23)

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	0
2	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	0	1
3	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	0	1	2
4	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	0	1	2	3
5	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	0	1	2	3	4
6	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	0	1	2	3	4	5
7	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	0	1	2	3	4	5	6
8	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	0	1	2	3	4	5	6	7
9	9	10	11	12	13	14	15	16	17	18	19	20	21	22	0	1	2	3	4	5	6	7	8
10	10	11	12	13	14	15	16	17	18	19	20	21	22	0	1	2	3	4	5	6	7	8	9
11	11	12	13	14	15	16	17	18	19	20	21	22	0	1	2	3	4	5	6	7	8	9	10
12	12	13	14	15	16	17	18	19	20	21	22	0	1	2	3	4	5	6	7	8	9	10	11
13	13	14	15	16	17	18	19	20	21	22	0	1	2	3	4	5	6	7	8	9	10	11	12
14	14	15	16	17	18	19	20	21	22	0	1	2	3	4	5	6	7	8	9	10	11	12	13
15	15	16	17	18	19	20	21	22	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
16	16	17	18	19	20	21	22	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
17	17	18	19	20	21	22	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
18	18	19	20	21	22	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
19	19	20	21	22	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
20	20	21	22	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
21	21	22	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
22	22	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

Odečítání

„Odečítání“ je zjednodušený zápis pro přičítání aditivního inverzního („záporného“) prvku.

$(a - b) \rightarrow (a + (-b)) \bmod p$,

Kde $b + (-b) \equiv 0 \bmod p$

Aditivní inverzní prvek

Snadné ověření:

(3 + 20) mod 23 ≡ 0

Příklad odečítání:

9 + (–15) mod 23 ≡
9 + 8 mod 23 ≡ 17

Zjednodušený zápis:

9 - 15 mod 23 ≡ 17

Prvek F(23)	Inverzní prvek (mod 23)
0	0
1	22 (-1)
2	21 (-2)
3	20 (-3)
4	19 (-4)
5	18 (-5)
6	17 (-6)
7	16 (-7)
8	15 (-8)
9	14 (-9)
10	13 (-10)
11	12 (-11)
12	11 (-12)
13	10(-13)
14	9(-14)
15	8 (-15)
16	7 (-16)
17	6 (-17)
18	5 (-18)
19	4 (-19)
20	3 (-20)
21	2 (-21)
22	1 (-22)

OKsystem

Násobící tabulka pro F(23)

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
2	0	2	4	6	8	10	12	14	16	18	20	22	1	3	5	7	9	11	13	15	17	19	21
3	0	3	6	9	12	15	18	21	1	4	7	10	13	16	19	22	2	5	8	11	14	17	20
4	0	4	8	12	16	20	1	5	9	13	17	21	2	6	10	14	18	22	3	7	11	15	19
5	0	5	10	15	20	2	7	12	17	22	4	9	14	19	1	6	11	16	21	3	8	13	18
6	0	6	12	18	1	7	13	19	2	8	14	20	3	9	15	21	4	10	16	22	5	11	17
7	0	7	14	21	5	12	19	3	10	17	1	8	15	22	6	13	20	4	11	18	2	9	16
8	0	8	16	1	9	17	2	10	18	3	11	19	4	12	20	5	13	21	6	14	22	7	15
9	0	9	18	4	13	22	8	17	3	12	21	7	16	2	11	20	6	15	1	10	19	5	14
10	0	10	20	7	17	4	14	1	11	21	8	18	5	15	2	12	22	9	19	6	16	3	13
11	0	11	22	10	21	9	20	8	19	7	18	6	17	5	16	4	15	3	14	2	13	1	12
12	0	12	1	13	2	14	3	15	4	16	5	17	6	18	7	19	8	20	9	21	10	22	11
13	0	13	3	16	6	19	9	22	12	2	15	5	18	8	21	11	1	14	4	17	7	20	10
14	0	14	5	19	10	1	15	6	20	11	2	16	7	21	12	3	17	8	22	13	4	18	9
15	0	15	7	22	14	6	21	13	5	20	12	4	19	11	3	18	10	2	17	9	1	16	8
16	0	16	9	2	18	11	4	20	13	6	22	15	8	1	17	10	3	19	12	5	21	14	7
17	0	17	11	5	22	16	10	4	21	15	9	3	20	14	8	2	19	13	7	1	18	12	6
18	0	18	13	8	3	21	16	11	6	1	19	14	9	4	22	17	12	7	2	20	15	10	5
19	0	19	15	11	7	3	22	18	14	10	6	2	21	17	13	9	5	1	20	16	12	8	4
20	0	20	17	14	11	8	5	2	22	19	16	13	10	7	4	1	21	18	15	12	9	6	3
21	0	21	19	17	15	13	11	9	7	5	3	1	22	20	18	16	14	12	10	8	6	4	2
22	0	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Dělení

„Dělení“ je zjednodušený zápis pro násobení multiplikativním inverzním prvkem:

$a/b \rightarrow (a * b^{-1}) \bmod p$

Kde $b * b^{-1} \equiv 1 \bmod p$

Opakování – v GF(p):

- Existuje 1 tak, že:
  $a * 1 = 1 * a = a$ (jednotkový prvek)
- pro všechna a z F existuje a^{-1} tak, že:
  $a*a^{-1} = a^{-1}*a = 1$ (inverzní prvek)

Multiplikativní inverzní prvek

Malý Fermatův teorém:

Pokud **p** je prvočíslo, **a** je celé číslo, pak platí

$$\mathbf{a^p \equiv a \bmod p}$$

pokud **a** není dělitelné **p** (například když $0 \leq a < p$)

$$\mathbf{a^{p-1} \equiv 1 \bmod p}$$

Inverzní prvek v F(p) lze nalézt pomocí:

$a^{p-1} = a * a^{p-2} \equiv 1 \bmod p$

tedy $\mathbf{a^{-1} \equiv a^{p-2} \bmod p}$

Multiplikativní inverzní prvek

Příklad:

$(3^{-1}) \bmod 23 = 8$, neboť

$(3 * 8) \bmod 23 = 24 \bmod 23 = 1$

1 je jednotkový prvek v F(23)

Prvek F(23)	* Inverzní prvek (mod 23)
0	neexistuje
1	1
2	12
3	8
4	6
5	14
6	4
7	10
8	3
9	18
10	7
11	21
12	2
13	16
14	5
15	20
16	13
17	19
18	9
19	17
20	15
21	11
22	22

Eliptická křivka nad GF(p)

Eliptická křivka E nad tělesem GF(p) je definována jako bod v nekonečnu (nulový bod) [BvN] společně s množinou bodů
P = (x, y),

kde x a y jsou z tělesa GF(p) a splňují rovnici:

$y^2 = x^3 + ax + b$ v GF(p), tj.

$y^2 \equiv x^3 + ax + b \pmod{p}$.

Řádem křivky #E rozumíme počet bodů křivky E

Příklad eliptické křivky nad GF(23)

Křivka E: $y^2 = x^3 + x + 1$ nad tělesem F(23) – 529 bodů

Řád křivky (počet bodů na křivce): 28

Body na křivce E:

[4,0] [0,1] [11,3] [17,3] [18,3] [5,4] [6,4] [12,4] [19,5] [1,7] [9,7] [13,7] [3,10] [7,11] [7,12] [3,13] [1,16] [9,16] [13,16] [19,18] [5,19] [6,19] [12,19] [11,20] [17,20] [18,20] [0,22] [BvN]

Ověření, že bod [11,3] leží na křivce E:

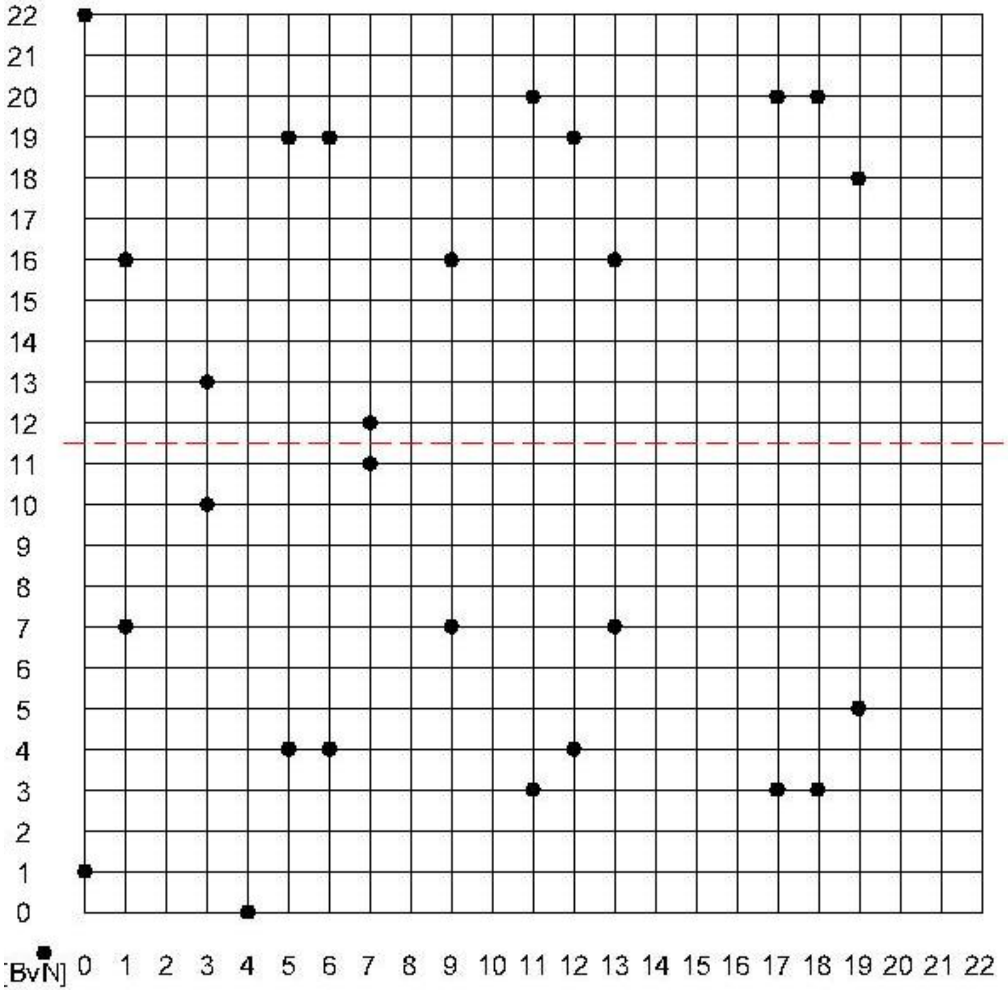
[11,3]: $3^2 \equiv 11^3 + 11 + 1 \pmod{23}$

$9 \equiv 1331 + 11 + 1 \pmod{23}$

$9 \equiv 20 + 11 + 1 \equiv 32 \equiv 9 \pmod{23}$

Graf všech bodů křivky

$y^2 = x^3 + x + 1$ nad $F(23)$



Sčítání bodů ležících na eliptické křivce

R = P + Q; $P = [x_1,y_1]$, $Q = [x_2,y_2]$, $R = [x_3,-y_3]$

$s \equiv (y_2 - y_1)*(x_2 - x_1)^{-1}$ (mod p) pro $P \neq Q$

$s \equiv (3x_1^2 + a)*(2y_1)^{-1}$ (mod p) pro $P = Q$

$q \equiv y_1 - s*x_1$ (mod p)

$x_3 \equiv s^2 - x_1 - x_2$ (mod p) pro $P \neq Q$

$x_3 \equiv s^2 - 2x_1$ (mod p) pro $P = Q$

$y_3 \equiv s*x_3 + q$ (mod p)

Eliptická křivka je vzhledem k sčítání bodů komutativní (Abelova) grupa

Příklad sčítání bodů

$s \equiv (y_2 - y_1)/(x_2 - x_1) \pmod{p}$
$q \equiv y_1 - s*x_1 \pmod{p}$
$x_3 \equiv s^2 - x_1 - x_2 \pmod{p}$
$y_3 \equiv s*x_3 + q \pmod{p}$

R = P+Q,

$P[x_1,y_1] = [11,3]$, $Q[x_2,y_2] = [3,13]$

$s \equiv (13-3)/(3-11) \equiv (13+20)*(3+12)^{-1} \equiv 33*15^{-1} \equiv 10*20 \equiv 200 \equiv 16 \pmod{23}$

$q \equiv 3 - 16*11 \equiv 3-176 \equiv 3-15 \equiv 3+8 \equiv 11 \pmod{23}$

$x_3 \equiv 16^2-11-3 \equiv 256+12+20 \equiv 3+12+20 \equiv 35 \equiv 12 \pmod{23}$

$y_3 \equiv 16*12 + 11 \equiv 192+11 \equiv 8+11 \equiv 19 \pmod{23}$

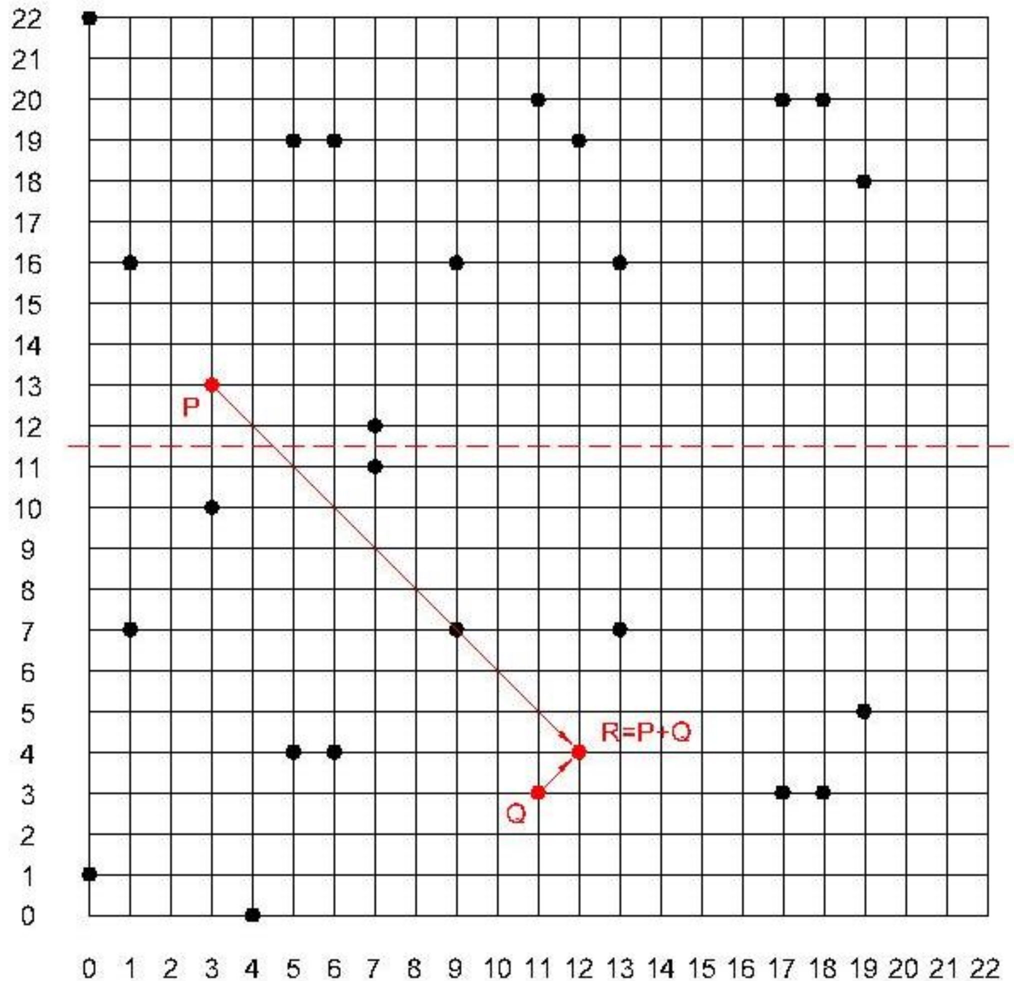
$-y_3 \equiv (-19) \equiv 4$

$R [x_3,-y_3] = [11,3] + [3,13] = [12,4]$

OKsystem

Příklad sčítání bodů – grafické znázornění

R = [11,3] + [3,13]
= [12,4]



OKsystem

Násobení bodu přirozeným číslem

Násobení bodu přirozeným číslem je zjednodušený zápis pro opakované sčítání bodů:

$$n*P = nP = P+P....+P \text{ (n krát).}$$

Důležitý je dvojnásobek bodu P+P, pomocí kterého se výhodně konstruují vyšší násobky, například:

200P = 2(2(2(P+2(2(2(P+2P)))))), tedy stačí pouze 9 operací sčítání.

Řádem bodu #P rozumíme nejmenší násobek bodu P, kdy platí nP=[BvN].

Po n sčítáních bodu se dostaneme do bodu [BvN]. Protože [BvN] +P=P, po n+1 sečteních bodu s vrátíme do původního bodu P a při dalším přičítání P se posloupnost bodů opakuje.

- Platí, že řád bodu dělí řád křivky.
- Různé body na křivce mohou být různého řádu.
- „Nejzajímavější“ jsou body s vysokým řádem
- #E/#P se nazývá kofaktor

Příklad 2 násobku bodu

$s \equiv (3*x_1^2+a)/(2*y_1)$ (mod p)
$q \equiv y_1 - s*x_1$ (mod p)
$x_3 \equiv s^2 - 2*x_1$ (mod p)
$y_3 \equiv s*x_3 + q$ (mod p)

Bod na P = [5,4] na křivce $y^2 = x^3 + x + 1$

$s = (3*5*5+1)/(2*4) = 76/8 \equiv 7*3 = 21$

$q = 4 - 21*5 = 4 - 105 = 4 - 13 = 4 + 10 = 14$

$x_3 = 21*21-2*5 = 441-10 \equiv 4+13 = 17$

$y_3 = 21*17 + 14 = 357+14 = 12+14 = 3$

$-y_3 = (-3) = 20$

2P = [17,20]

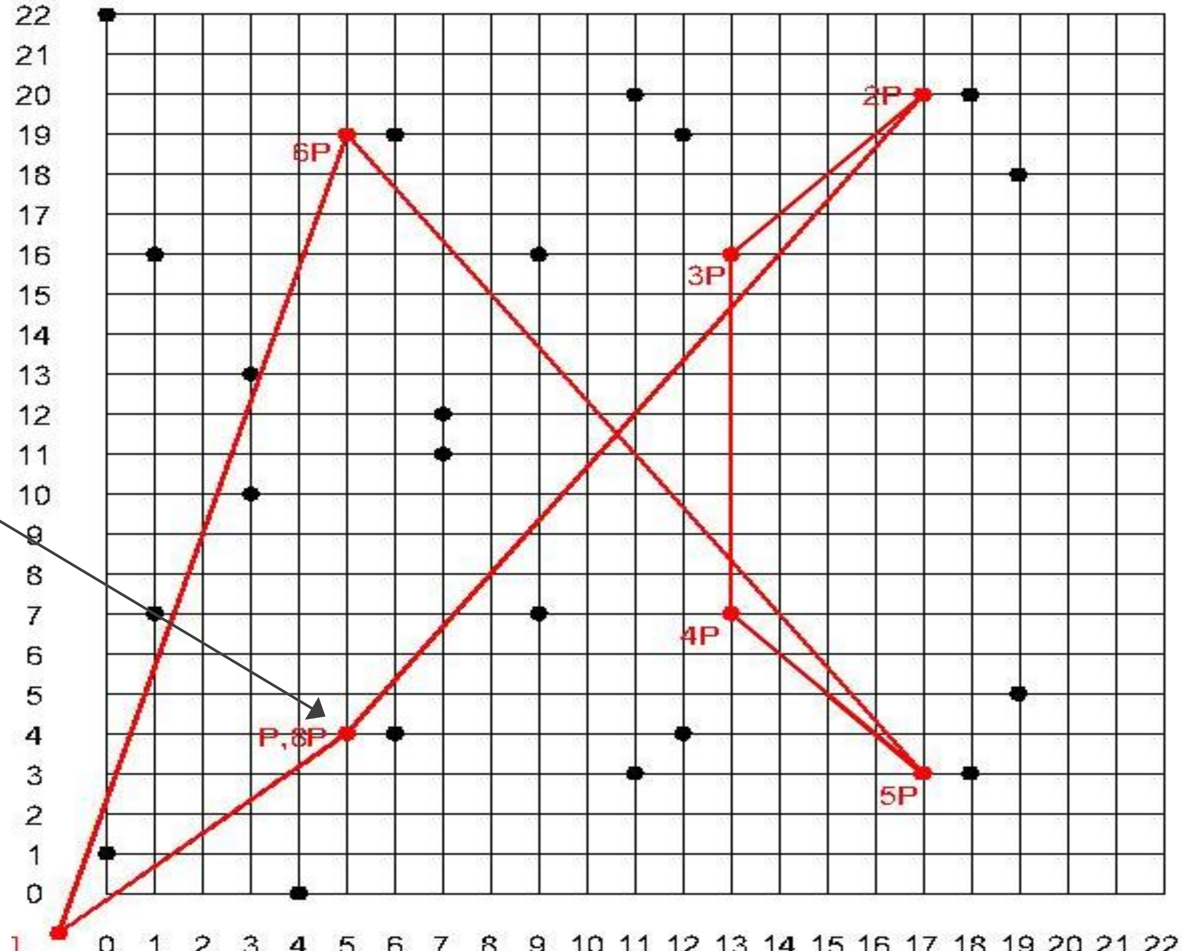
Příklad k-násobek bodu

Bod na P = [5,4] na křivce $y^2 = x^3 + x + 1$ má řád 7, jeho k násobky jsou:

2 * [5,4] = [5,4] + [5,4] = [17,20]
3 * [5,4] = 2 * [5,4] + [5,4] = [17,20] + [5,4] = [13,16]
4 * [5,4] = 3 * [5,4] + [5,4] = [13,16] + [5,4] = [13,7]
5 * [5,4] = [13,7] + [5,4] = [17,3]
6 * [5,4] = [17,3] + [5,4] = [5,19]
7 * [5,4] = [5,19] + [5,4] = [BvN] bod v nekonečnu
8 * [5,4] = [BvN] + [5,4] = [5,4]
9 * [5,4] = [5,4] + [5,4] = [17,20] ....

Příklad k-násobek bodu

Počáteční
bod



Problém diskrétního logaritmu nad E v F(p)

Pokud je řád bodu #P velký (například 2^{256}), je velká posloupnost různých bodů P,2P,3P,..., aniž dojde k zacyklení.

Lze zvolit <u>počáteční bod P, tajný násobitel k a vypočítat cílový bod Q=kP</u>. Oba body P i Q lze zveřejnit, nikdo není (v rozumné době) schopen z těchto bodů <u>určit násobitel k</u> (jeho určení tvoří tzv. problém diskrétního logaritmu).

Kryptografie s veřejným klíčem nad E v F(p)

Popis eliptické křivky $y^2 = x^3 + ax + b$ (tedy koeficienty a,b a modul tělesa p), počáteční bod B, řád křivky #E a kofaktor tvoří veřejné parametry kryptografie.

Tajný násobitel **k** tvoří privátní klíč subjektu.

Koncový bod **Q=kB** tvoří veřejný klíč subjektu.

Algoritmus ECDH pro nalezení shody na klíči

B: základní bod

k_A: privátní klíč Alice; $Q_A = k_A B$: veřejný bod (klíč) Alice

k_B: privátní klíč Boba; $Q_B = k_B B$: veřejný bod (klíč) Boba

Společný bod Z spočtou obě strany následovně:

Alice: $Z = k_A Q_B = k_A k_B B$

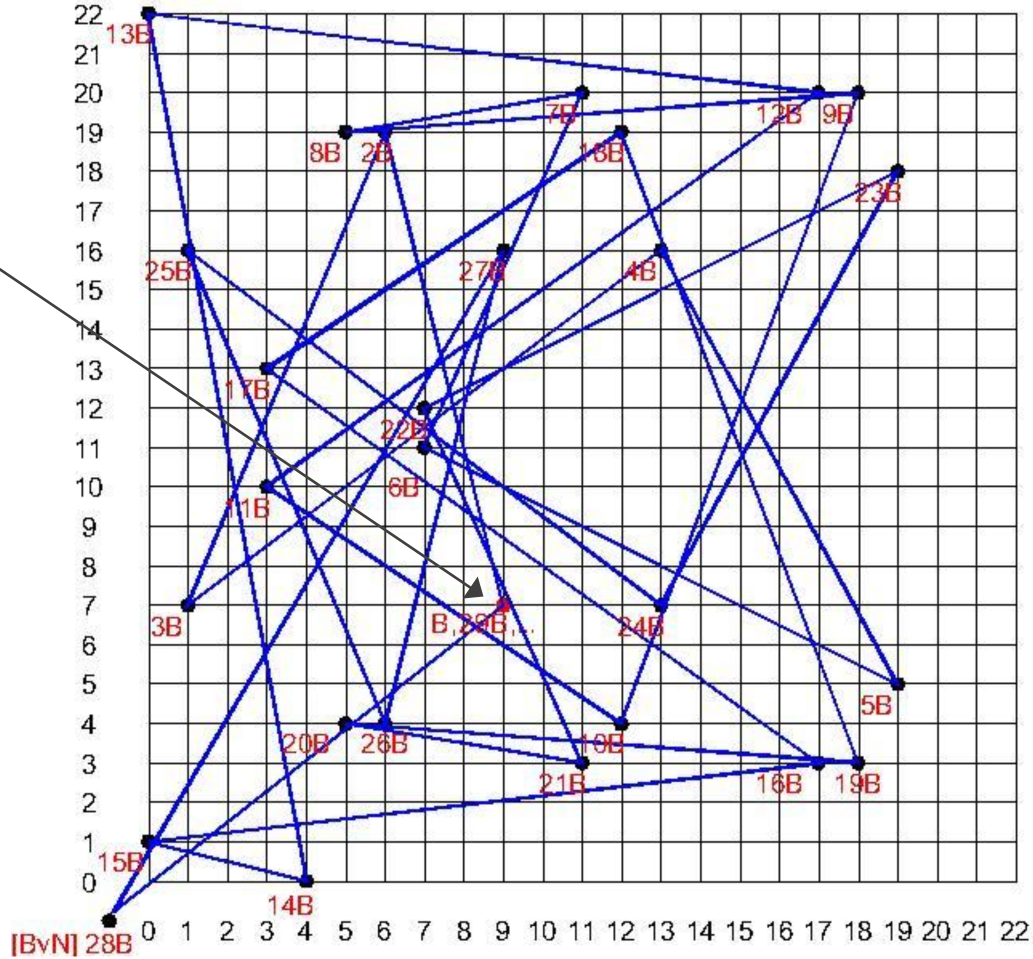
Bob: $Z = k_B Q_A = k_B k_A B$

Společný bod Z slouží k odvození klíčů relace (například z X souřadnice bodu Z se odvodí sdílený symetrický klíč relace mezi Alicí a Bobem)

Příklad ECDH

Eliptická křivka $y^2 = x^3 + x + 1$ nad F(23)
Počáteční bod B:[9,7] , řád bodu je 28

Počáteční bod B



Násobky bodu [9,7]
B=[9,7]
2B=[6,19]
3B=[1,7]
4B=[13,16]
5B=[19,5]
6B=[7,11]
7B=[11,20]
8B=[5,19]
9B=[18,20]
10B=[12,4]
11B=[3,10]
12B=[17,20]
13B=[0,22]
14B=[4,0]
15B=[0,1]
16B=[17,3]
17B=[3,13]
18B=[12,19]
19B=[18,3]
20B=[5,4]
21B=[11,3]
22B=[7,12]
23B=[19,18]
24B=[13,7]
25B=[1,16]
26B=[6,4]
27B=[9,16]
28B=[BvN]
29B=[9,7]

Příklad ECDH

Eliptická křivka $y^2 = x^3 + x + 1$ nad F(23)
Počáteční bod B:[9,7] , řád bodu je 28

k_A: privátní klíč Alice = 3
k_B: privátní klíč Boba = 7
$Q_A=k_AB$: veřejný bod (klíč) Alice = 3B = [1,7]
$Q_B=k_BB$: veřejný bod (klíč) Boba = 7B = [11,20]

Bob spočte $Z = k_BQ_A$ = 7* [1,7] = [11,3]
Alice spočte $Z = k_AQ_B$ = 3* [11,20] = [11,3]

Souřadnice bodu Z mohou sloužit jako sdílené tajemství Alice a Boba

B=[9,7]	Q_A=[1,7]	Q_B=[11,20]
2B=[6,19]	$2Q_A$=[7,11]	$2Q_B$=[4,0]
3B=[1,7]	$3Q_A$=[18,20]	$3Q_B$=[11,3]
4B=[13,16]	$4Q_A$=[17,20]	$4Q_B$=[BvN]
5B=[19,5]	$5Q_A$=[0,1]	
6B=[7,11]	$6Q_A$=[12,19]	
7B=[11,20]	$7Q_A$=[11,3]	
8B=[5,19]	$8Q_A$=[13,7]	
9B=[18,20]	$9Q_A$=[9,16]	
10B=[12,4]	$10Q_A$=[6,19]	
11B=[3,10]	$11Q_A$=[19,5]	
12B=[17,20]	$12Q_A$=[5,19]	
13B=[0,22]	$13Q_A$=[3,10]	
14B=[4,0]	$14Q_A$=[4,0]	
15B=[0,1]	$15Q_A$=[3,13]	
16B=[17,3]	$16Q_A$=[5,4]	
17B=[3,13]	$17Q_A$=[19,18]	
18B=[12,19]	$18Q_A$=[6,4]	
19B=[18,3]	$19Q_A$=[9,7]	
20B=[5,4]	$20Q_A$=[13,16]	
21B=[11,3]	$21Q_A$=[11,20]	
22B=[7,12]	$22Q_A$=[12,4]	
23B=[19,18]	$23Q_A$=[0,22]	
24B=[13,7]	$24Q_A$=[17,3]	
25B=[1,16]	$25Q_A$=[18,3]	
26B=[6,4]	$26Q_A$=[7,12]	
27B=[9,16]	$27Q_A$=[1,16]	
28B=[BvN]	$28Q_A$=[BvN]	

Příklad ECDH – grafické znázornění

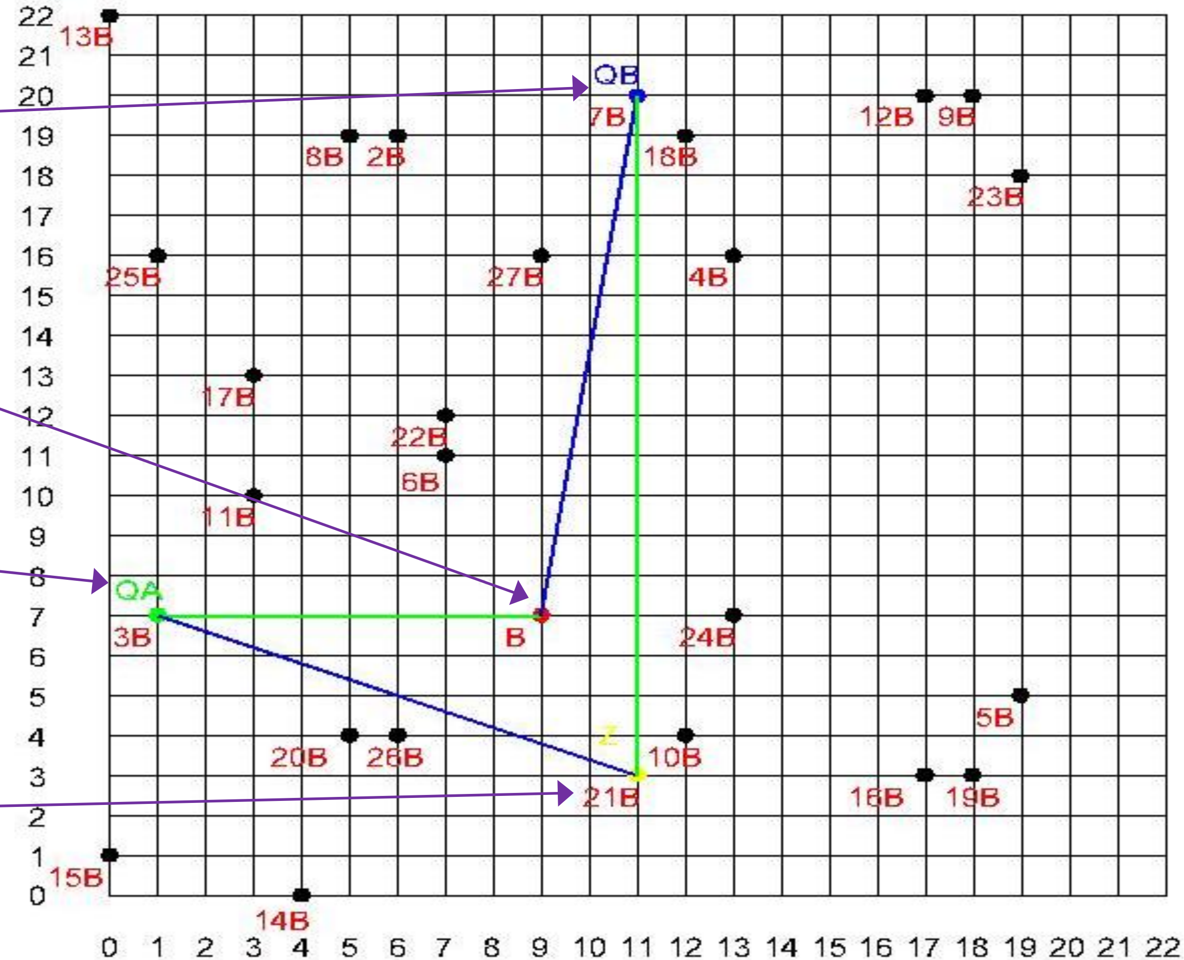
Veřejný bod Boba Q_B= 7*B

Společný počáteční bod B

Veřejný bod Alice Q_A= 3*B

Společný koncový bod 21*B = 3*7*B

= 7*3*B



Šifrování s veřejným klíčem

Algoritmus ElGamal:

Zprávu m, která se má zašifrovat, je nutno nejprve vhodně zobrazit (mapovat) na bod na křivce E

B: základní bod

k_A: privátní klíč Alice; $Q_A = k_A B$: veřejný bod (klíč) Alice

k_B: privátní klíč Boba; $Q_B = k_B B$: veřejný bod (klíč) Boba

m: zpráva k zašifrování; P_m: bod, na který je zobrazena zpráva m

Alice pošle Bobovi bod S, spočtený jako součet bodu zprávy s veřejným bodem Boba vynásobeným privátním klíčem Alice:

$$S = P_m + k_A Q_B = P_m + k_A k_B B$$

Bob vynásobí svým privátním klíčem veřejný bod Alice:

$$R = k_B Q_A = k_B k_A B$$

a výsledný bod R odečte od bodu S, který obdržel od Alice:

$S – R = P_m + k_A k_B B – k_B k_A B = P_m$

Tímto způsobem Bob rozšifroval bod zprávy P_m od Alice

Elektronický podpis ECDSA

Necháme na příště....

Smart Card Forum 2011

Dotazy, kontakt

Ing. Ivo Rosol, CSc.

ředitel vývojové divize

OKsystem s.r.o.

www.oksystem.cz

rosol@oksystem.cz