



EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání



Kryptologie

Moderní kryptologie: Asymetrické kryptografie - Eliptické křivky

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204

Obsah prezentace

- **Eliptické křivky - úvod**
- **Eliptické křivky - příklad**
- **Konstrukce eliptických křivek**
 - **Nevhodnost tělesa**
 - **Konečná tělesa**

1. Úvod do problematiky ECC

Eliptické křivky: Úvod

- Vznik v roce 1985 (Victor Miller a Neal Koblitz)
- Eliptická kryptografie poskytuje větší bezpečnost a efektivnější techniky systémů s veřejným klíčem, než poskytovala první generace (RSA a Diffie-Hellman)
- Jedná se o analogii kryptosystému s veřejným klíčem, ve kterých je modulární aritmetika nahrazena operacemi nad eliptickou křivkou (ECC)

Eliptické křivky: Úvod

- Kryptografie s veřejným klíčem potřebuje pro stejnou úroveň bezpečnosti delší klíče než kryptografie symetrická.
- **3072-bitový klíč** by měl u algoritmů založených na faktorizaci či diskrétním logaritmu postačovat na dosáhnutí bezpečnosti srovnatelné s tou pro 128-bitovou symetrickou šifru.
- Kryptografie založená na eliptických křivkách umožňuje používat kratší klíče.
- **Primární výhodou** krypto systémů na bázi eliptických křivek je jejich velká kryptografická bezpečnost vzhledem k dané velikosti klíče.

Eliptické křivky: Úvod

- Význačně **kratší délka klíčů** (např. oproti RSA) vede:
 - ke **kratším certifikátům** i menším parametrům systému a
 - tedy i k **větší výpočetní efektivnosti.**

Příklad výpočtů ECC systému na dalších slides dle: [1]

Rovnice eliptické křivky

Obecná forma Weierstrassovy rovnice:

$$E/K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$$a_1, a_2, a_3, a_4, a_6, x, y \in K$$

Zjednodušená forma Weierstrassovy rovnice:

$$y^2 = x^3 + a \cdot x + b$$

$$a, b \in K$$

Diskriminant D

- Koeficienty a, b musí splňovat podmíncu:

$$D = -16(4a^3 + 27b^2) \neq 0$$

Dvě řešení eliptické křivky

$$y^2 = x^3 + a \cdot x + b$$

$y^2 \Rightarrow$ pro každé x rovnice má 2 řešení:

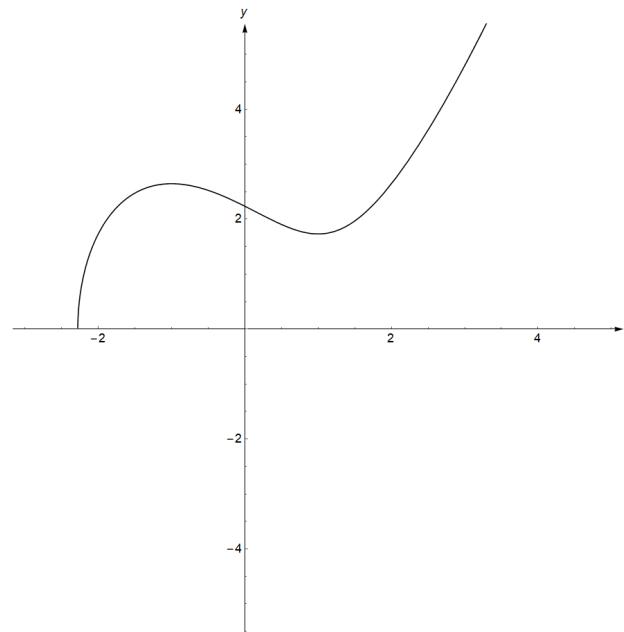
$$y = \sqrt{x^3 + a \cdot x + b}$$

$$-y = -\sqrt{x^3 + a \cdot x + b}$$

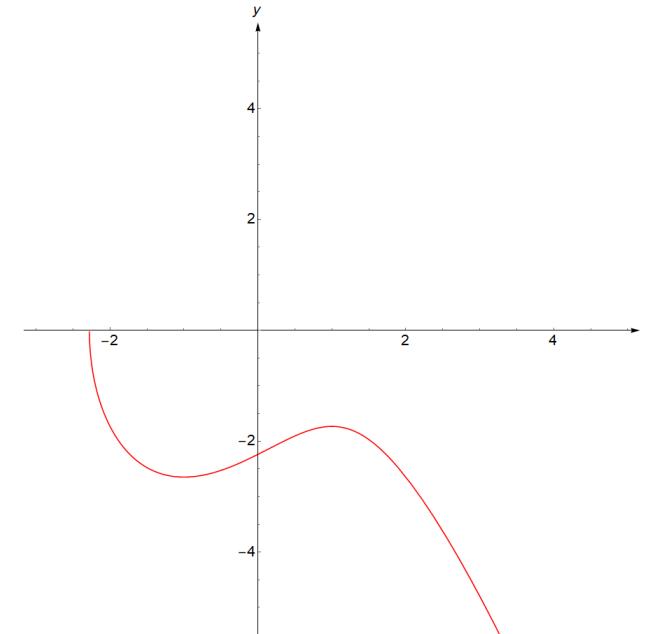
Konstrukce eliptické křivky

Ukažme si situaci: $a, b, x, y \in \mathbb{R}$

Pro y :

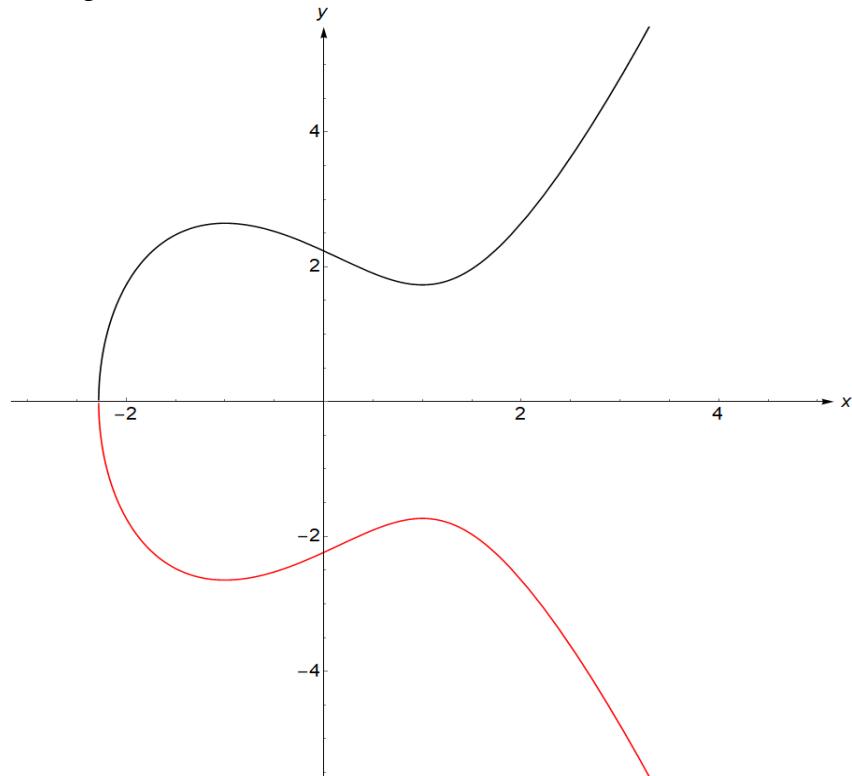


Pro $-y$:

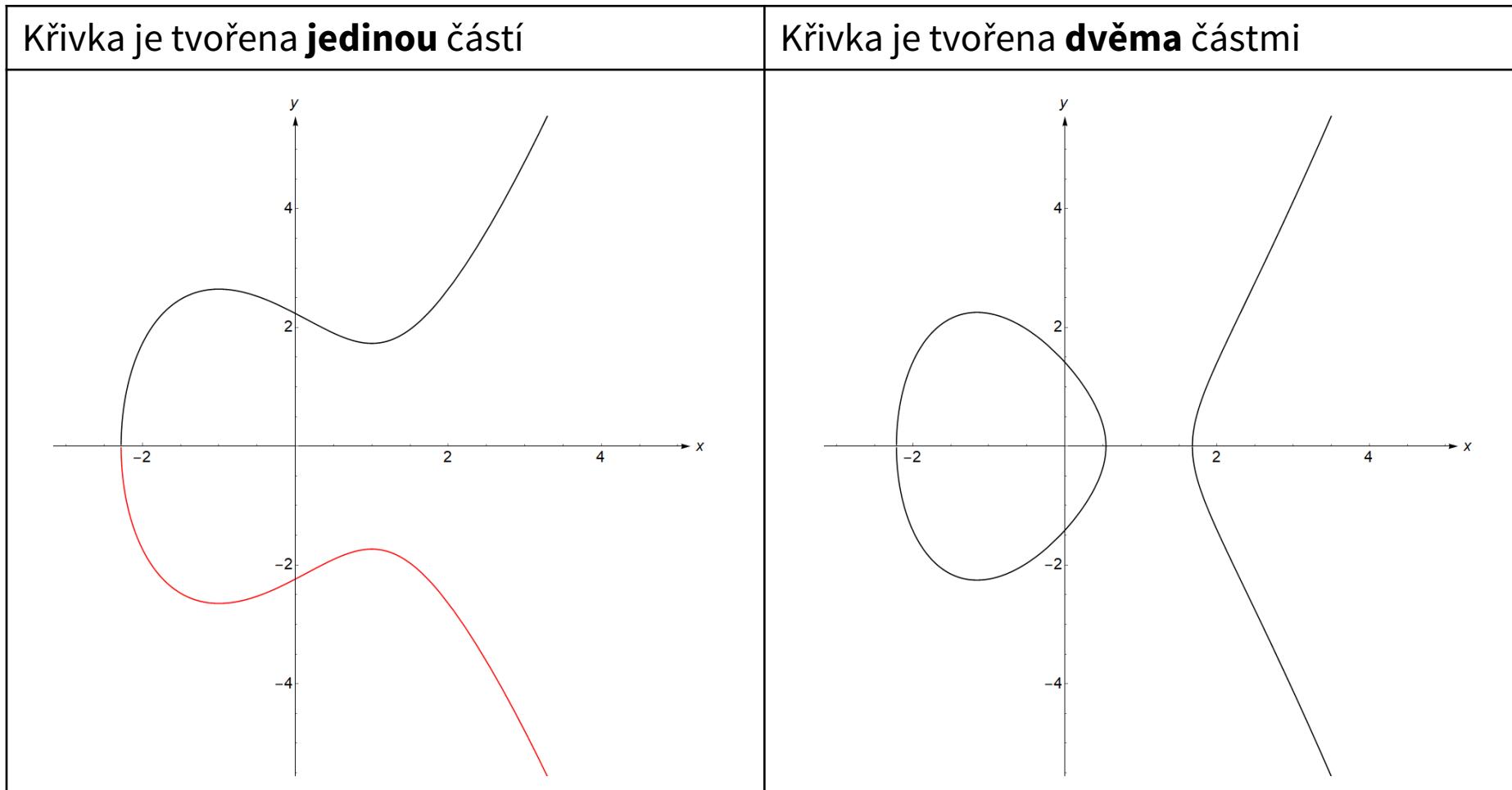


Konstrukce eliptické křivky

Spojením grafů pro y a $-y$ z obrázků na předchozím slajdu dostaneme výsledný graf eliptické křivky:



Eliptické křivky - mají dva tvary



Dvě části eliptické křivky

- Proč je jedna eliptická křivka z předchozího slajdu rozdělena na dvě samostatné části?

Dvě části eliptické křivky

Uvedená eliptická křivka odpovídající rovnici:

$$y^2 = x^3 - 4 \cdot x + 2$$

Pro výpočet y -ových souřadnic používáme vzorce s druhou odmocninou:

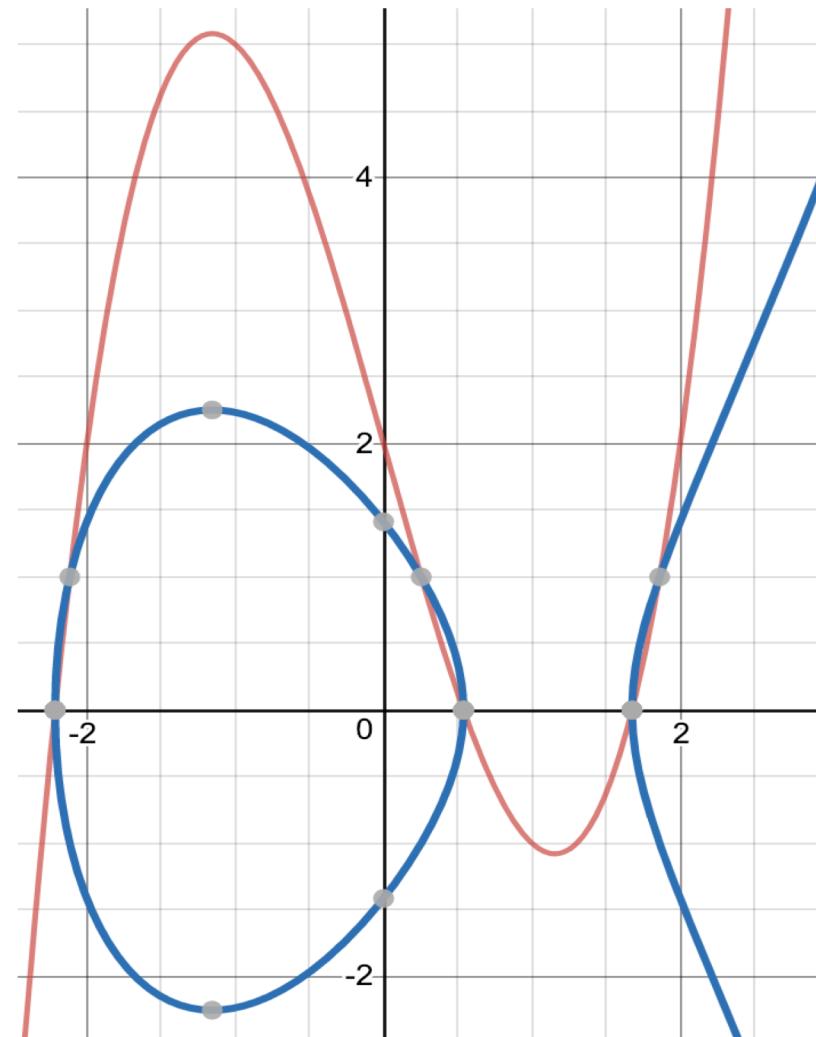
$$y = \sqrt{x^3 - 4 \cdot x + 2}$$

$$-y = -\sqrt{x^3 - 4 \cdot x + 2}$$

Dvě části eliptické křivky

Pokud nastane situace, že pro některá x bude výraz pod odmocninou nabývat záporných hodnot, pak řešení pro tato x nebudou v oboru reálných čísel.

Výraz je na obrázku označen
červeně $x^3 - 4 \cdot x + 2$



Zdroj obrázku: <https://www.desmos.com/calculator>

Nulový diskriminant

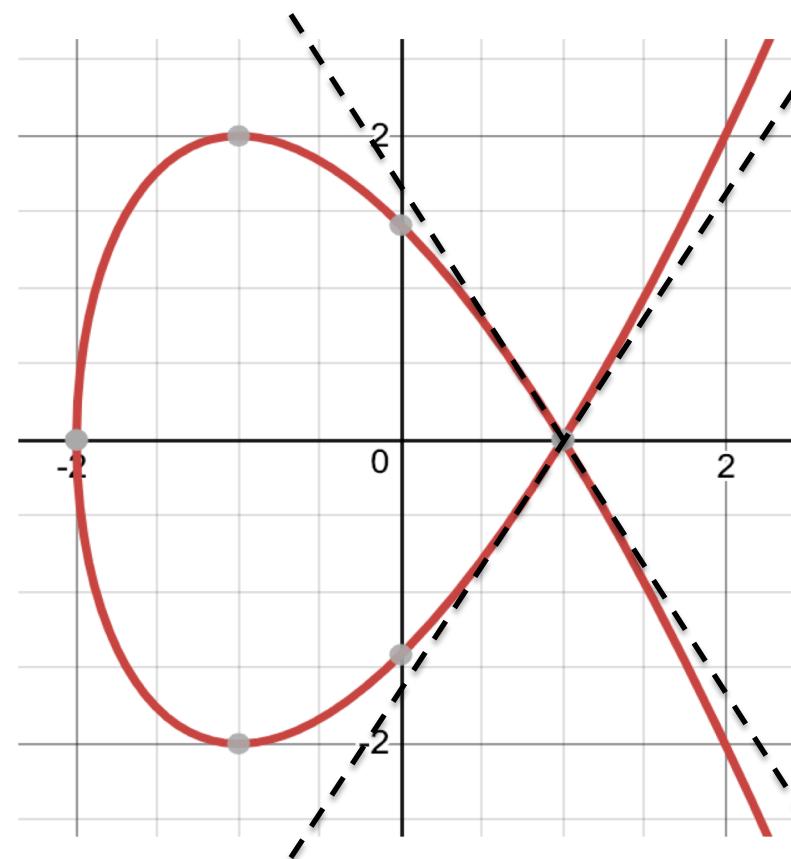
Výpočet diskriminantu pro rovnici:

$$y^2 = x^3 - 3 \cdot x + 2$$

$$a = -3, b = 2$$

$$\begin{aligned} D &= -16 \cdot (4 \cdot a^3 + 27 \cdot b^2) = \\ &= -16 \cdot (4 \cdot (-3)^3 + 27 \cdot 2^2) = \\ &= -16 \cdot (-108 + 108) = 0 \end{aligned}$$

Nulový diskriminant



Bod $[1, 0]$ je singulární,
protože v tomto bodě lze sestrojit dvě různé tečny.

Zdroj obrázku: <https://www.desmos.com/calculator>

Nulový diskriminant

- Křivky s nulovým diskriminantem nejsou eliptické!
- Nejsou hodné pro použití v kryptografii.
- Pokud jsou v šifrovacím algoritmu voleny koeficienty a a b , musí být vždy provedena kontrola, zda není diskriminant nulový!

Eliptická křivka

Množinu všech bodů $[x, y]$, které splňují rovnici
 $y^2 = x^3 + ax + b$ a bod O nazýváme $E(a, b)$.

Operace sčítání na eliptické křivce $P+Q=R$

- Sčítáme dvou různých bodů $P[x_P, y_P]$ a $Q[x_Q, y_Q]$, které nejsou opačné.
- Bod $R[x_R, y_R]$ je výsledek součtu bodů $P[x_P, y_P]$ a $Q[x_Q, y_Q]$
- Sčítání bodů na eliptické křivce je geometrická operace => není možné provést součet bodů tím, že sečteme jejich x -ové a y -ové složky:
$$P[x_P, y_P] + Q[x_Q, y_Q] \neq R[x_P+x_Q, y_P+y_Q]$$

Operace sčítání na eliptické křivce $P+Q=R$

- Sčítání dvou bodů $P[x_P, y_P]$ a $Q[x_Q, y_Q]$ se provede tak, že jsou oba body proloženy přímkou.
- Bod ve, kterém přímka znova protne eliptickou křivku, je označen jako bod $-R[x_R, \llbracket -y \rrbracket_R]$
- Poznámka: bod $-R[x_R, \llbracket -y \rrbracket_R]$ je negací bodu R .

Operace sčítání na eliptické křivce $P+Q=R$

- Výsledkem sčítání je bod $R[x_R, y_R]$ (nikoliv bod $-R$).
- Z bodu $-R[x_R, -y_R]$ je bod R vypočítám pomocí vzorce:
$$[x_R, (-1 \cdot y_R)]$$
- Tzn., že provedeme změnu znaménka y -ové souřadnice.

Operace sčítání na eliptické křivce $P+Q=R$

Provedení výpočtu

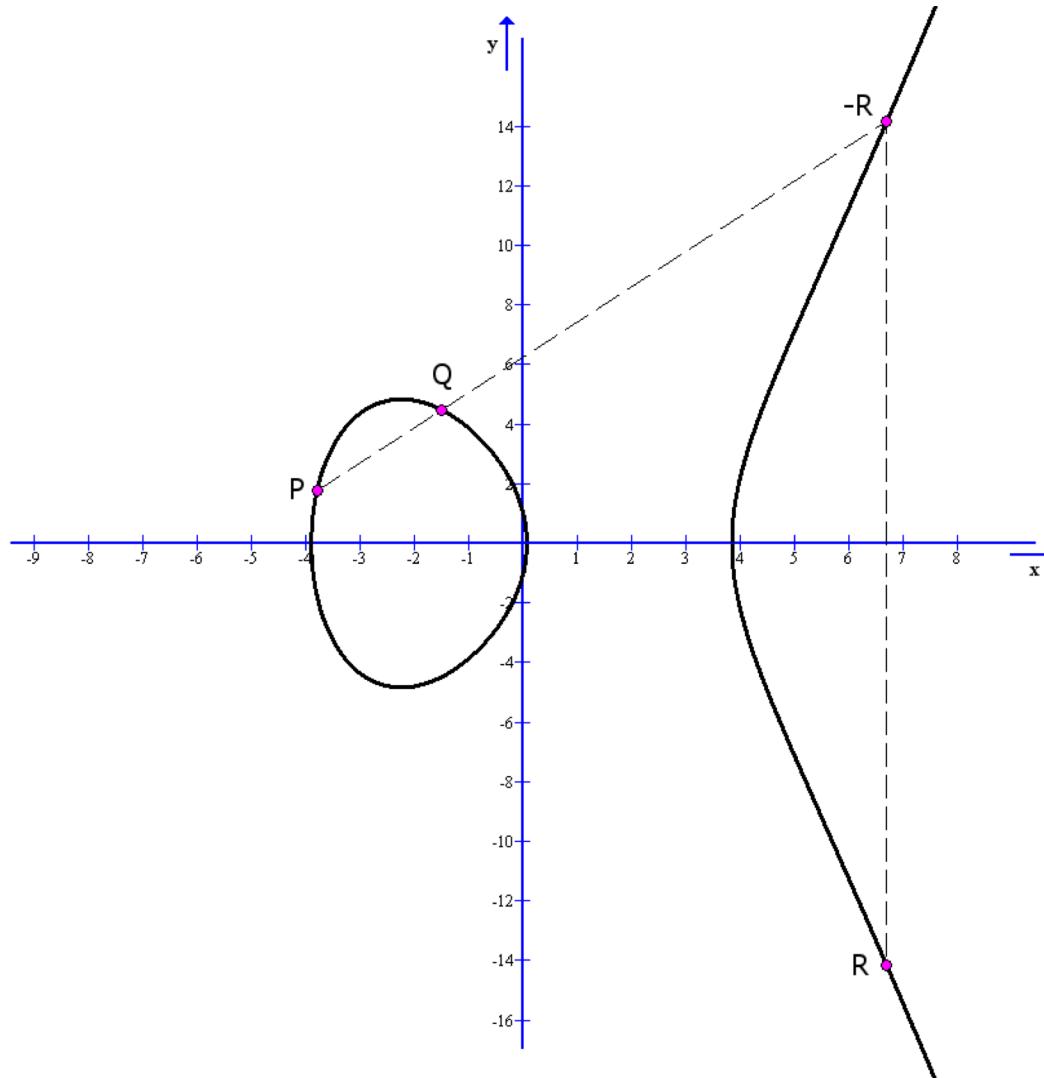
Směrnice, jež spojuje body P a Q se vypočítá pomocí vzorce:

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

Souřadnice bodu R jsou následně dopočítány pomocí:

$$\begin{aligned}x_R &= s^2 - x_P - x_Q \\y_R &= -y_P + s(x_P - x_R)\end{aligned}$$

Operace sčítání na eliptické křivce $P+Q=R$



Operace sčítání na eliptické křivce $P+Q=R$

- Sčítání dvou stejných bodů $\mathbf{P+P=2P}$
- Pokud jsou body $P[x_P, y_P]$ a $Q[x_Q, y_Q]$ stejné body na eliptické křivce, pak platí, že $Q=P$.
- Výsledný bod $2P$ je opět nazýván jako bod $R[x_R, y_R]$.

Operace sčítání na eliptické křivce $P+Q=R$

- Směrnice je definována jako:

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

- Poznámka: všimněte si, že, směrnice má jiný vzorec, než byl použit v případě součtu $P+Q=R$.

Operace sčítání na eliptické křivce $P+Q=R$

- Souřadnice x a y bodu R se počítají podle stejných vzorců, jako v případě součtu $P+Q=R$.
- Ale protože platí, že $Q=P$, lze vzorec pro výpočet souřadnice x_R upravit:

$$x_R = s^2 - x_P - x_Q = s^2 - x_P - x_P = s^2 - 2x_P$$

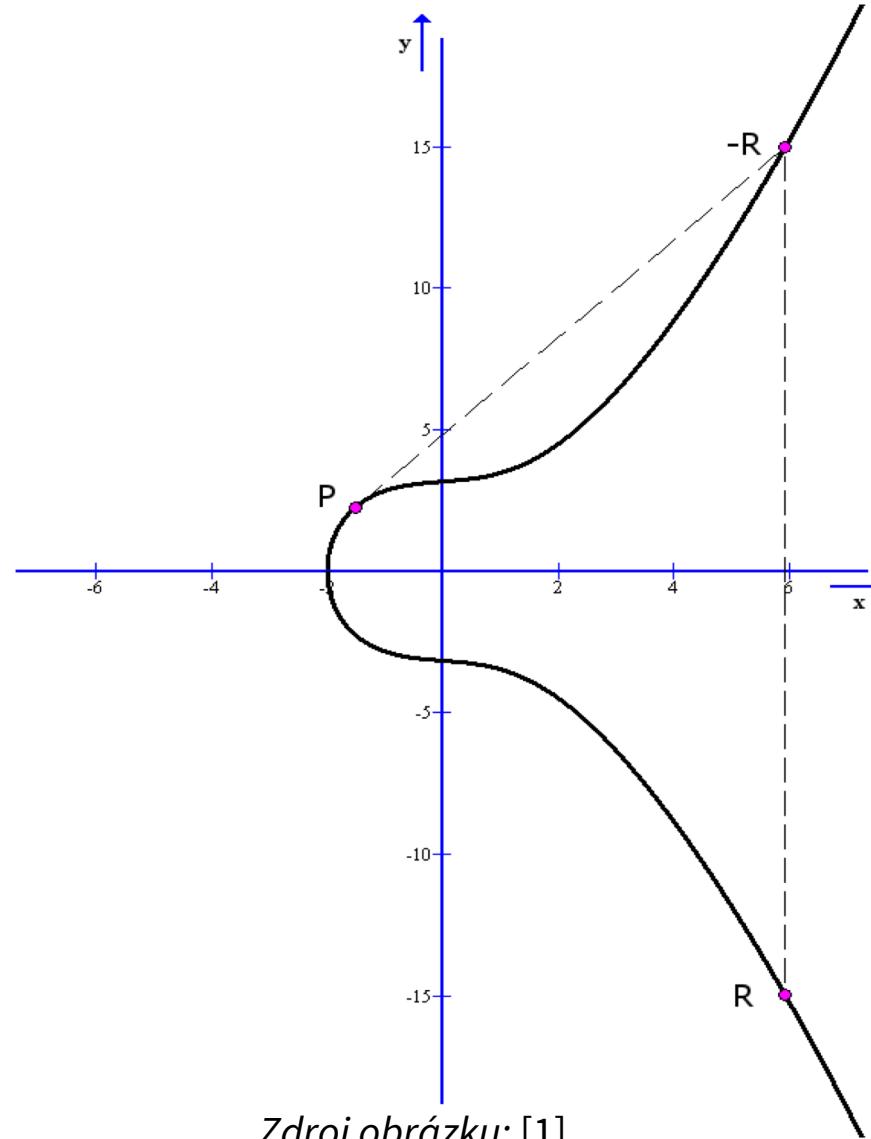
- Výsledný vzorec: $\mathbf{x}_R = s^2 - 2x_P$

Operace sčítání na eliptické křivce $P+Q=R$

- Vzorec pro výpočet souřadnice yR je beze změny:

$$y_R = -y_P + s(x_P - x_R)$$

Operace sčítání na eliptické křivce $P+Q=R$



2. Eliptické křivky: příklad

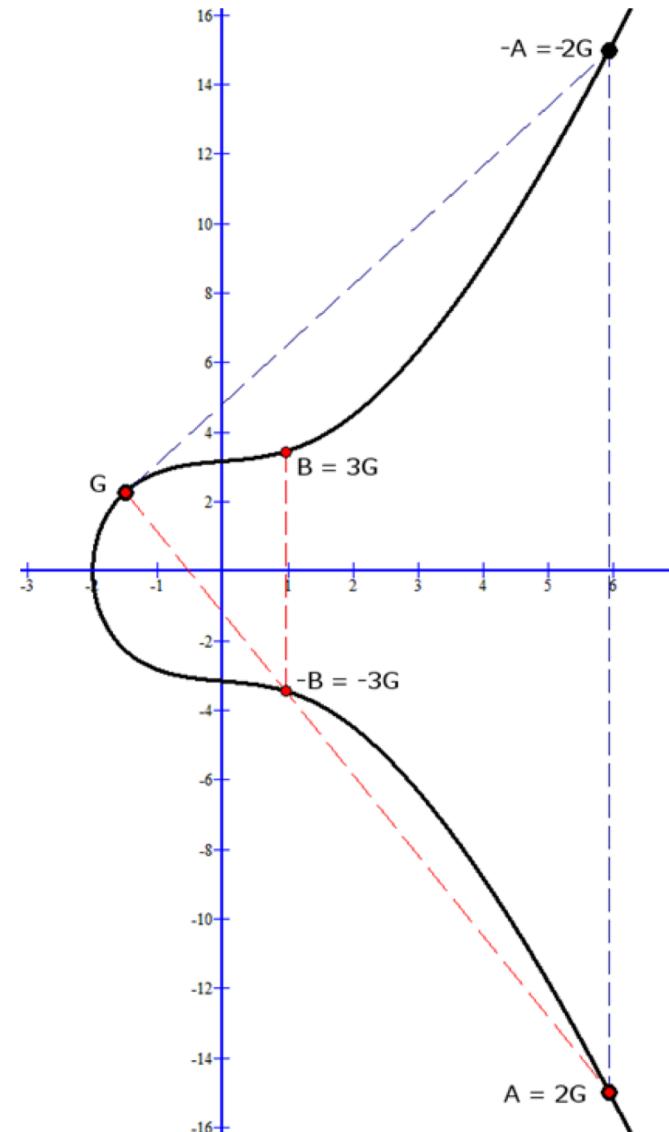
Eliptické křivky - příklad

Je dána rovnice eliptické křivky $y^2 = x^3 + a \cdot x + b$ a
bod G .

- Uživatel A si jako svůj soukromý klíč zvolí číslo 2, tedy $S_A = 2$.
- Následně spočítá bod A (veřejný klíč) jako: $A = S_A G = 2G$
- Násobení bodu skalárem realizujeme, jako opakované sčítání téhož bodu. Bod A spočítáme jako $G+G$.

Eliptické křivky - příklad

- Veřejný klíč A (2G):



Zdroj obrázku: [1]

Eliptické křivky - příklad

Je dána rovnice eliptické křivky $y^2 = x^3 + a \cdot x + b$ a
bod G .

- Uživatel B si jako svůj soukromý klíč zvolí číslo 3, tedy $S_B = 3$.
- Veřejný klíč, tedy bod B spočítá jako: $B = S_B G = 3G$.

Eliptické křivky - příklad

Bod B se počítá ve dvou krocích:

- v prvním kroku se vypočítá $G+G=2G$ (sčítání dvou stejných bodů);
- ve druhém kroku se provede výpočet $2G+G$ (sčítání různých bodů).

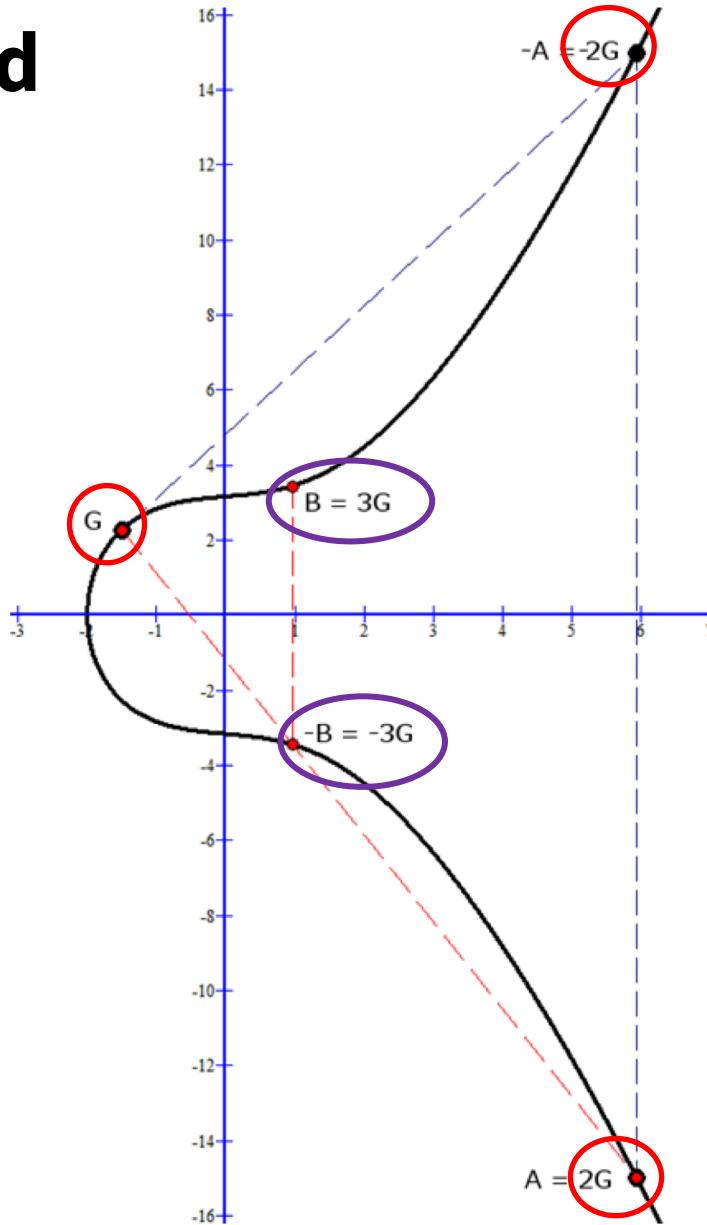
Tzn.: $(G+G)+G=3G$.

Eliptické křivky - příklad

- Veřejný klíč B ($3G$):

$$G + G = 2G$$

$$2G + G = 3G$$



Zdroj obrázku: [1]

Eliptické křivky - příklad

Výměna veřejných klíčů:

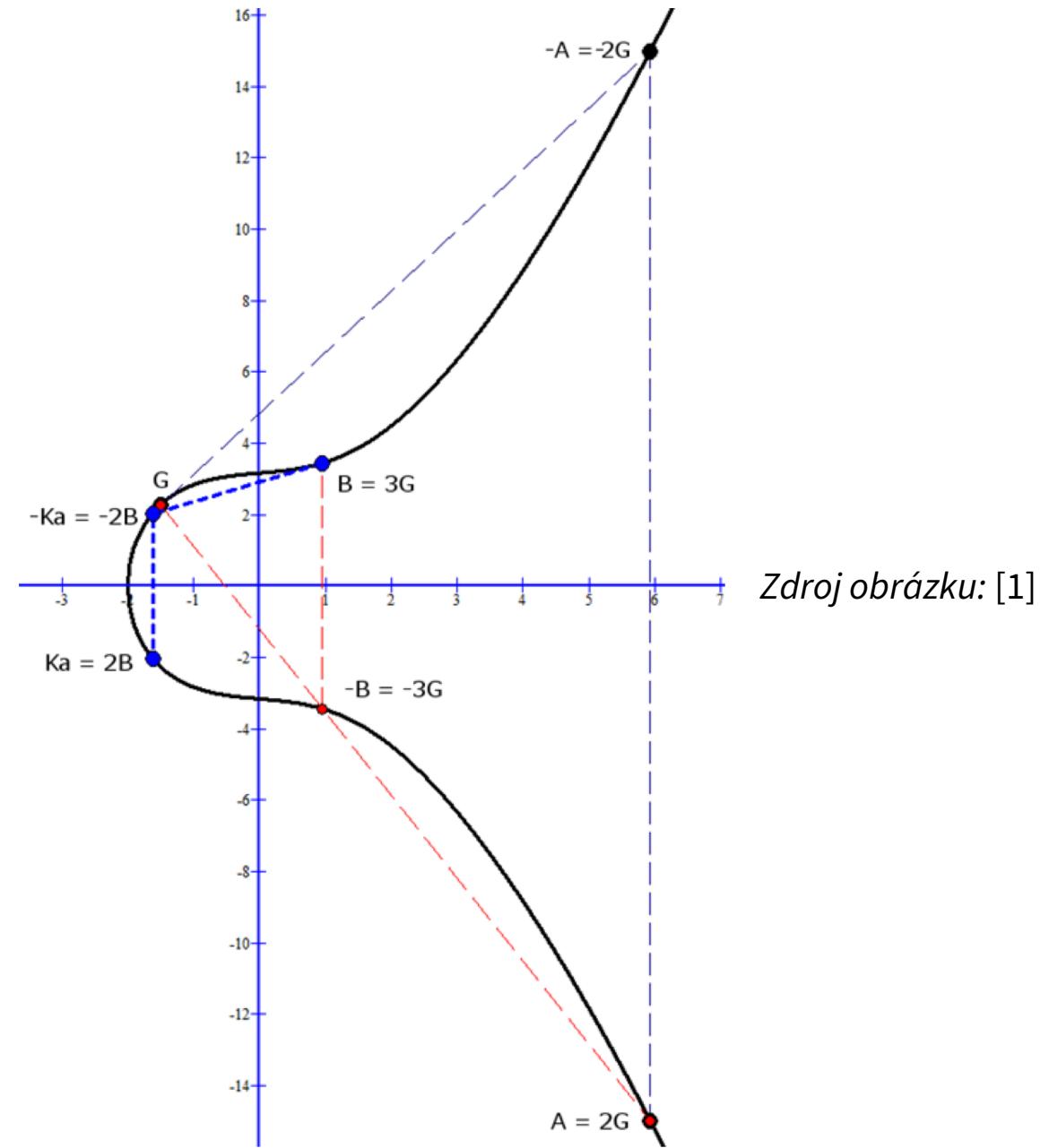
- Uživatel A pošle bod A ($2G$) uživateli B.
- Uživatel B pošle bod B ($3G$) uživateli A.

Eliptické křivky - příklad

- Uživatel A vypočítá pomocí:
 - svého soukromého klíče $S_A = 2$ a
 - přeneseného veřejného klíče B

bod K_A :

$$K_A = S_A \cdot B = 2B.$$



Zdroj obrázku: [1]

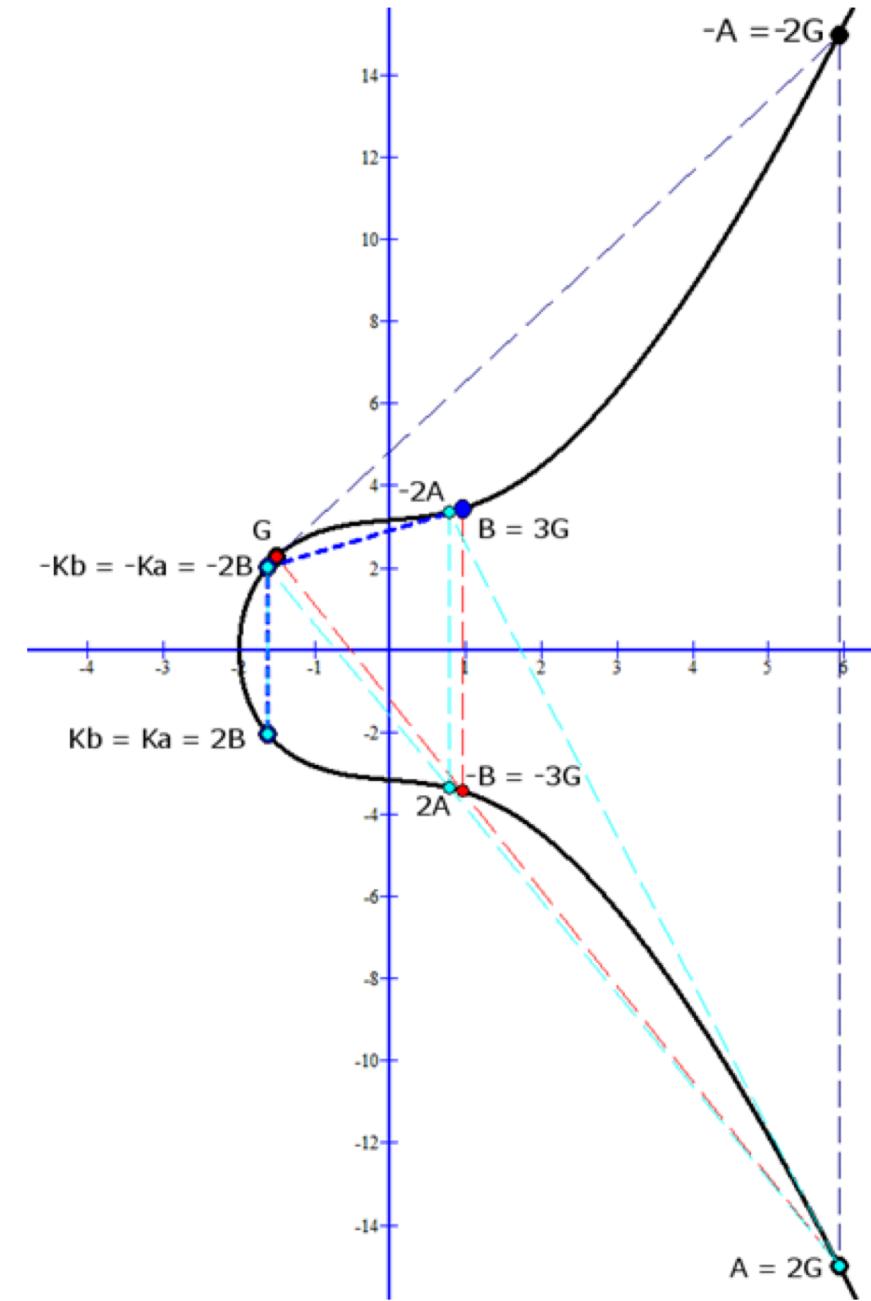
Eliptické křivky - příklad

- Uživatel B vypočítá pomocí svého soukromého klíče $S_B = 3$ a přeneseného veřejného klíče A

bod $K_B = S_B \cdot A = 3A = (\textcolor{green}{A + A}) + \textcolor{red}{A} = \textcolor{green}{2A} + A$

$$K_B = K_A$$

- Oba body se rovnají
=> mají je k dispozici obě strany komunikace:



Zdroj obrázku: [1]

Eliptické křivky - příklad

Příklad použití: $K_B = K_A = [16, 25]$

Enter your text below:

1625

Treat each line as a separate string

SHA256 Hash of your string:

2B8AE4541022864D57E65A7DB4C70B75FEA47C9101EDEBF0325DA25EA84DEF02

Zdroj obrázku: Vlastní výukový SW Autorů [1]

Nevhodnost tělesa \mathbb{R}

Výpočty v příkladu byly provedeny pomocí kapesního kalkulátoru.

Jako výsledky jsme dostali: $K_A[-1,61788, -2,03646]$
 $K_B[-1,61761, -2,03698]$

Tedy přísně vzato platí, že $K_A \neq K_B$. Odchylky Δ_x a Δ_y :

$$\Delta_x = |x_{K_A} - x_{K_B}| = |-1,61788 - (-1,61761)| = 0,00027;$$
$$\Delta_y = |y_{K_A} - y_{K_B}| = |-2,03646 - (-2,03698)| = 0,00052;$$

Nevhodnost tělesa \mathbb{R}

Nyní provedeme výpočty pomocí jednoduchého programu:

The application window has two main sections for calculating points on an elliptic curve defined by $y^2 = x^3 + 1$.

Top Section (R = 2P):

X _p	0,957466761632603
Y _p	3,44020461161142
a	1

$s = 0,545058829674819$
 $X_r = -1,61784439545872$
 $Y_r = -2,03650852627872$

Bottom Section (R = P + Q):

X _p	-1,5
Y _p	2,2638
X _q	5,92999785567817
Y _q	-14,9819030527224

$s = -2,32109125570512$
 $X_r = 0,957466761632603$
 $Y_r = 3,44020461161142$

Right Column (R = 2P):

X _p	5,92999785567817
Y _p	-14,9819030527224
a	1

$s = -3,55410869134184$
 $X_r = 0,771692878515276$
 $Y_r = -3,35127349920412$

Right Column (R = P + Q):

X _p	5,92999785567817
Y _p	-14,9819030527224
X _q	0,771692878515276
Y _q	-3,35127349920412

$s = -2,25473864089269$
 $X_r = -1,61784439545882$
 $Y_r = -2,03650852627865$

Nevhodnost tělesa \mathbb{R}

Jako výsledek jsme dostali:

$$\begin{aligned} K_A &[-1,61784439545872, & -2,03650852627872] \\ K_B &[-1,61784439545882, & -2,03650852627865] \end{aligned}$$

Odchylky Δ_x a Δ_y :

$$\Delta_x = |x_{K_A} - x_{K_B}| = |-1,61784439545872 - (-1,61784439545882)| = 0,000000000001;$$

$$\Delta_y = |y_{K_A} - y_{K_B}| = |-2,03650852627872 - (-2,03650852627865)| = 0,000000000007;$$

Odchylky jsou menší, ale jsou stále přítomné.

Nevhodnost tělesa \mathbb{R}

- Důvodem vzniku odchylek je omezená reprezentace reálných čísel ve výpočetní technice!
- Výsledky výpočtů jsou zaokrouhlovány, tak aby vešly do příslušných datových typů.
- V závislosti na velikosti odchylek Δ_x a Δ_y dochází při šifrování a dešifrování ke zkreslení či dokonce poškození celé zprávy.

Nevhodnost tělesa \mathbb{R}

- Z tohoto důvodu není možné tvořit eliptické křivky pro kryptografické účely nad \mathbb{R} !
- Pro ECC algoritmy je křivky tvoří nad konečnými tělesy!

Eliptické křivky nad konečnými tělesy $GF(p)$

- Prvočíselná eliptická křivka E nad konečným tělesem $GF(p)$ je opět definována zjednodušenou formou Weierstrassovy rovnice.
- Nicméně tato rovnice byla upravena tak, aby odpovídala pravidlům modulární aritmetiky:

$$E/GF(p) : y^2 \bmod p = (x^3 + a \cdot x + b) \bmod p$$

kde $a, b, x, y \in GF(p)$,

p je prvočíslo, pro něž platí $p > 3$

Eliptické křivky nad konečnými tělesy $GF(p)$

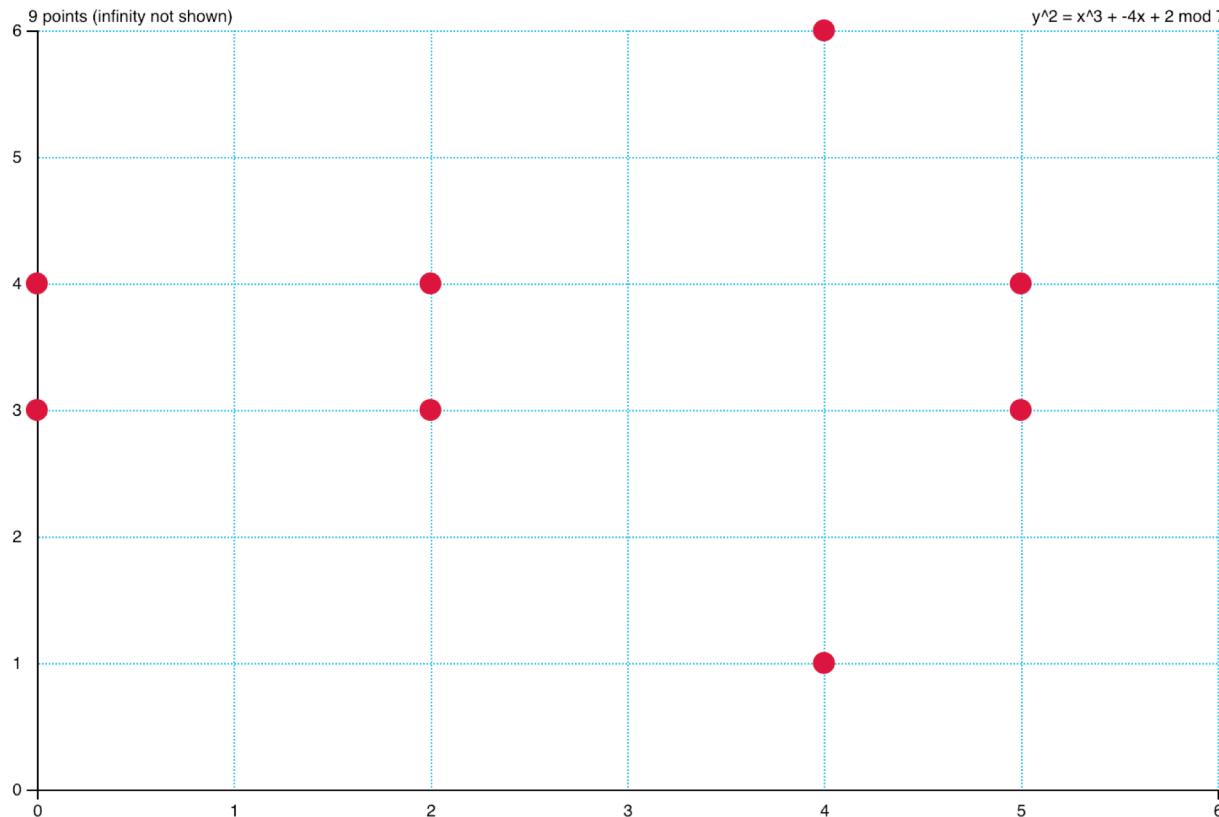
- Diskrétní eliptická křivka nad $GF(p)$ je nyní tvořena konečnou množinou bodů $P[x, y]$, jejichž souřadnice $x, y \in GF(p)$ vyhovují rovnici:

$$y^2 \bmod p = (x^3 + ax + b) \bmod p.$$

- Do množiny bodů eliptické křivky, je (stejně jako v případě \mathbb{R}) zahrnut i bod \mathcal{O} , což je bod v nekonečnu.

Eliptické křivky nad konečnými tělesy $GF(p)$

Draw the elliptic curve $y^2 = x^3 + ax + b \pmod{r}$, where $a: -4$ $b: 2$ $r: 7$ **DRAW!**



Zdroj obrázku: [2]

Sčítání dvou různých bodů $P+Q=R$ nad konečnými tělesy $GF(p)$

- Směrnice přímky se počítá pomocí vzorce:

$$s = \left(\frac{y_Q - y_P}{x_Q - x_P} \right) \bmod p$$

- Souřadnice x_R a y_R bodu R , který je výsledkem součtu, se počítají pomocí:

$$x_R = (s^2 - x_P - x_Q) \bmod p$$

$$y_R = (-y_P + s(x_P - x_R)) \bmod p$$

Sčítání dvou různých bodů $P+Q=R$ nad konečnými tělesy $GF(p)$

- Příklad:
 - Sečteme dva různé body $P[3, 18]$ a $Q[7, 17]$, které leží na prvočíselné eliptické křivce :

$$y^2 \bmod 71 = (x^3 + x + 10) \bmod 71.$$

Sčítání dvou různých bodů $P+Q=R$ nad konečnými tělesy $GF(p)$

Nejprve vypočítáme směrnici s :

$$\begin{aligned}s &= \left(\frac{y_Q - y_P}{x_Q - x_P} \right) \bmod p = \left(\frac{17 - 18}{7 - 3} \right) \bmod 71 = \\&= \left(\frac{-1}{4} \right) \bmod 71 = (-1 \cdot \textcolor{red}{4^{-1}}) \bmod 71 = \\&= (-1 \cdot \textcolor{red}{18}) \bmod 71 = 53;\end{aligned}$$

Sčítání dvou různých bodů $P+Q=R$ nad konečnými tělesy $GF(p)$

Číslo **18** je multiplikativní inverzí čísla 4 modulo 71. Správnost výpočtu multiplikativní inverze snadno ověříme, neboť platí, že:

$$(a \cdot \textcolor{red}{a^{-1}}) \bmod p = 1$$

Dosadíme: $(4 \cdot \textcolor{red}{18}) \bmod 71 = 72 \bmod 71 = 1$.

Sčítání dvou různých bodů $P+Q=R$ nad konečnými tělesy $GF(p)$

- Výpočet x -ové souřadnice výsledného bodu R :

$$\begin{aligned}x_R &= (s^2 - x_P - x_Q) \bmod p = \\&= (53^2 - 3 - 7) \bmod 71 = \\&= (2809 - 10) \bmod 71 = 2799 \bmod 71 = 30.\end{aligned}$$

Sčítání dvou různých bodů $P+Q=R$ nad konečnými tělesy $GF(p)$

- Výpočet y -ové souřadnice výsledného bodu R :

$$\begin{aligned}y_R &= (-y_P + s(x_P - x_R)) \bmod p = \\&= (-18 + 53 \cdot (3 - 30)) \bmod 71 = \\&= (-18 - 1431) \bmod 71 = -1449 \bmod 71 = 42.\end{aligned}$$

- Výsledkem součtu bodů $P[3, 18]$ a $Q[7, 17]$ je bod $R[30, 42]$.

Sčítání dvou různých bodů $P+Q=R$ nad konečnými tělesy $GF(p)$

- Výsledkem součtu bodů $P[3, 18]$ a $Q[7, 17]$ je bod $R[30, 42]$

mod p	71
A	1
B	10
point P	x: 3 y: 18
point Q	x: 7 y: 17
number n	1
Calculate nP	
Calculate P + Q	
Result:	x: 30 y: 42

Sčítání dvou stejných bodů (zdvojení bodu)

$P+P=R$ nad konečnými tělesy $GF(p)$

- Bod $P [x_P, y_P]$ leží na eliptické křivce.
- Výsledkem součtu $P+P$ (tedy součtu bodu se sebou samým) je bod $R[x_R, y_R]$.
- Směrnice je počítána podle modulárního vzorce:

$$s = \left(\frac{3x_P^2 + a}{2y_P} \right) \bmod p$$

Sčítání dvou stejných bodů (zdvojení bodu)

$P+P=R$ nad konečnými tělesy $GF(p)$

- Souřadnice x_R a y_R bodu R , který je výsledkem součtu, se počítají pomocí:

$$x_R = (s^2 - 2x_P) \bmod p$$

$$y_R = (-y_P + s(x_P - x_R)) \bmod p$$

Sčítání dvou stejných bodů (zdvojení bodu)

$P+P=R$ nad konečnými tělesy $GF(p)$



Příklad:

- je dána prvočíselná eliptická křivka $y^2 \text{mod } 71 = (x^3 + x + 10) \text{ mod } 71$ a bod $P[3, 18]$, ležící na dané křivce. Provedeme součet $P+P=R$.
- Nejprve vypočítáme směrnici s:

$$\begin{aligned}s &= \left(\frac{3x_P^2 + a}{2y_P} \right) \text{ mod } p = \left(\frac{3 \cdot 3^2 + 1}{2 \cdot 18} \right) \text{ mod } 71 = \left(\frac{28}{36} \right) \text{ mod } 71 = \\ &= (28 \cdot 36^{-1}) \text{ mod } 71 = (28 \cdot 2) \text{ mod } 71 = 56;\end{aligned}$$



Sčítání dvou stejných bodů (zdvojení bodu)

$P+P=R$ nad konečnými tělesy $GF(p)$

- Správnost výpočtu multiplikativní inverze ověříme:
 $(36 \cdot 2) \bmod 71 = 72 \bmod 71 = 1$.
- Pomocí směrnice spočítáme souřadnice bodu $R[x_R, y_R]$:

$$\begin{aligned}x_R &= (s^2 - 2x_P) \bmod p = (56^2 - 2 \cdot 3) \bmod 71 = \\&= (3136 - 6) \bmod 71 = 6;\end{aligned}$$

$$\begin{aligned}y_R &= (-y_P + s(x_P - x_R)) \bmod p = \\&= (-18 + 56 \cdot (3 - 6)) \bmod 71 = \\&= (-18 - 168) \bmod 71 = -186 \bmod 71 = 27;\end{aligned}$$

Sčítání dvou stejných bodů (zdvojení bodu)

$P+P=R$ nad konečnými tělesy $GF(p)$

- Pohledem na obrázek, ověříme, že $R[6, 27] \in E_{71}(1, 10)$. Provedený výpočet je správný.

mod p	71
A	1
B	10
point P	x : 3 y : 18
point Q	x : 3 y : 18
number n	
Calculate nP	
Calculate P + Q	
Result:	x : 6 y : 27

Bod v nekonečnu \mathcal{O}

- Bod v nekonečnu \mathcal{O} je neutrálním prvkem v množině bodů eliptické křivky $E/GF(p)$.
- **Pro každý bod eliptické křivky platí, že pokud je k němu přičten bod v nekonečnu \mathcal{O} , je výsledkem součtu původní bod P .**
- => výsledek součtu je stejný jako by operace vůbec neproběhla.

Opačný/inverzní prvek: bod $-P$

- Pro všechny body P , ležící na křivce $E/GF(p)$, existuje jejich negace, tj. $-P$.
- Bod $-P$ je v grupě inverzním prvkem.
- Nad \mathbb{R} se provádí negace bodu otočením znaménka y -ové souřadnice.
- Princip vytváření negací bodů je stejný, jen je upraven tak, aby byl v souladu s modulární aritmetikou

Opačný/inverzní prvek: bod $-P$

- Bod $P[x, y]$ leží na eliptické křivce nad $GF(p)$.
- První část negace, je stejná jako nad \mathbb{R} : $-P[x, -y]$
- Uvedený bod neleží na eliptické křivce, protože x -ové a y -ové souřadnice bodů musí být z množiny $GF(p)$, (tzn.: $0, 1, \dots, p-1$).

Opačný/inverzní prvek: bod $-P$

- Proto musí být záporná y -ová souřadnice převedena na nezápornou:
 - Pro souřadnice všech bodů ležících na křivce $E/GF(p)$ platí, že jsou menší než p , takže můžeme použít korekci záporného modula, kterou známe ze cvičení:
 - tzn., že p sečteme se souřadnicí $-y$:

$$\bar{y} = p + (-y)$$

Opačný/inverzní prvek: bod $-P$

- Ještě odstraníme závorku (optimalizace výpočtu: jedna operace místo dvou), tím dostaneme výsledný vzorec pro výpočet y -ové souřadnice bodu $-P$:

$$\bar{y} = p - y$$

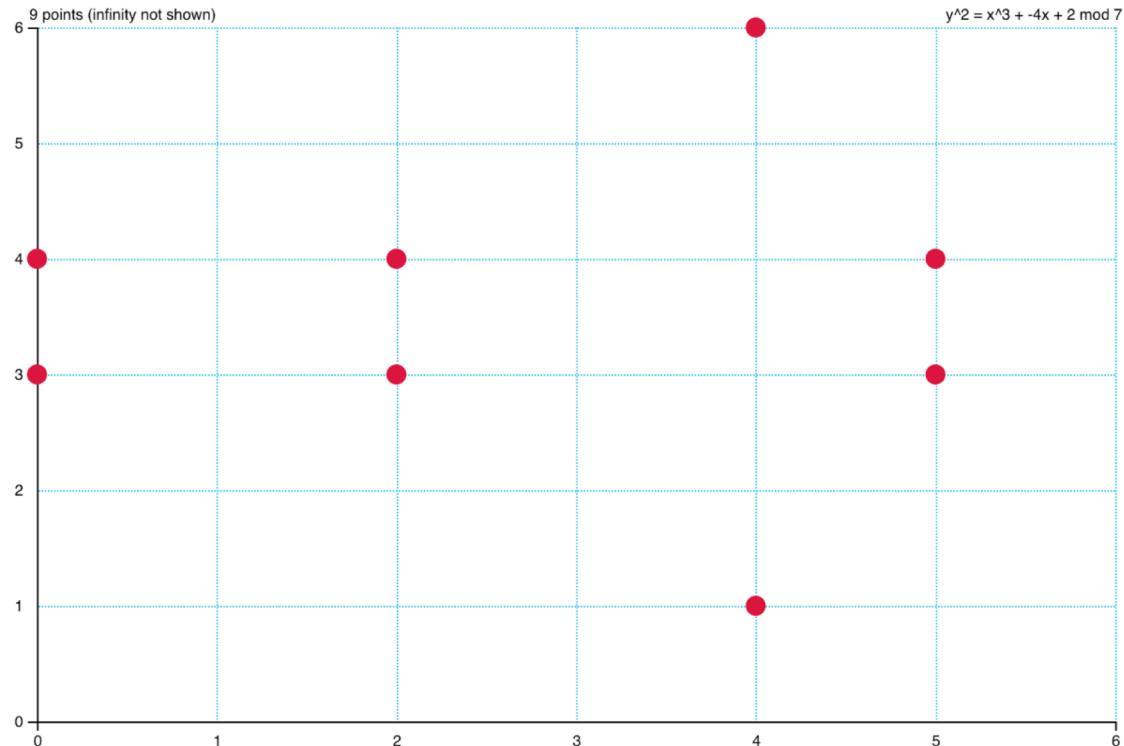
3. Konstrukce eliptických křivek

Konstrukce eliptických křivek nad $GF(p)$ pomocí rovnice

Jestli bod $P[x, y]$ leží na křivce, je možné zjistit, pomocí dvojice výpočtů:

- nejprve je dosazena y -ová souřadnice bodu P do levé strany rovnice: $y^2 \bmod p$.
- pak je dosazena x -ová souřadnice bodu P do pravé strany rovnice: $(x^3 + a \cdot x + b) \bmod p$.
 - **Pokud se obě strany rovnice rovnají, znamená to, že bod P leží na dané křivce.**

Konstrukce eliptických křivek nad $GF(p)$ pomocí rovnice



Zdroj obrázku: [2]

Body eliptické křivky $y^2 \pmod{7} = (x^3 - 4 \cdot x + 2) \pmod{7}$:

$[0, 3], [0, 4], [2, 3], [2, 4], [4, 1], [4, 6], [5, 3], [5, 4]$, bod \mathcal{O}

Konstrukce eliptický křivek nad $GF(p)$ pomocí generátoru

- Postup vychází ze skutečnosti, že body diskrétních křivek $GF(p)$ tvoří cyklické grupy.
- Pro výpočet je použit jediný bod, který leží na eliptické křivce, a s jehož pomocí lze vypočítat všechny ostatní body dané křivky.
- O tomto bodu říkáme, že je **generátorem** eliptické křivky.

Konstrukce eliptický křivek nad $GF(p)$ pomocí generátoru

- Je vybrán jakýkoliv bod P , ležící na dané křivce.
- Grupa bodů eliptické křivky je uzavřena vzhledem k operaci sčítání bodů. Tzn., že pokud bod P sečteme se sebou samým, dostaneme bod $2P$, který také leží na dané křivce.

Konstrukce eliptický křivek nad $GF(p)$ pomocí generátoru

- $2P = P + P$
- $3P = 2P + P$
- $4P = 3P + P$
- $5P = 4P + P$
- $6P = 5P + P$
- $7P:$

$$s = \left(\frac{y_{6P} - y_P}{x_{6P} - x_P} \right) \bmod p = (A \cdot 0^{-1}) \bmod p$$

Konstrukce eliptický křivek nad $GF(p)$ pomocí generátoru

- Nelze vytvořit multiplikativní inverzi 0^{-1} .
- Z toho vyplývá, že bod $7P$ je posledním bodem na dané křivce. Jedná se o bod v nekonečnu \mathcal{O} (abstraktní konstrukt => nemá souřadnice).

Konstrukce eliptický křivek nad $GF(p)$ pomocí generátoru

- $7P = \mathcal{O}$
- $8P = 7P + P = \mathcal{O} + P = P$
- $9P = 8P + P = P + P = 2P$
- $10P = 9P + P = 2P + P = 3P$
- ...

Chcete vědět více?

- Uceleným zdrojem příkladů a matematických základů je publikace autorů Milana Oulehly a Romana Jaška: Moderní Kryptografie [1].

Seznam odkazů

- [1] OULEHLA, Milan a Roman JAŠEK. Moderní kryptografie. Praha: IFP Publishing, 2017. ISBN 978-80-87383-67-4.
- [2] Elliptic Curves over Finite Fields. [online]. Dostupné z: <http://www.graui.de/code/elliptic2/>
- [3] Elliptic Curve Calculator. [online]. Dostupné z: <http://www.christelbach.com/ECCalculator.aspx>



EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání



Děkuji za pozornost

Strategický projekt UTB ve Zlíně, reg. č. CZ.02.2.69/0.0/0.0/16_015/0002204