Eliptické křivky a jejich využití v kryptografii

13. května 2010

Motivace

Nalezení diskrétního logaritmu je výpočetně velmi obtížné. Existuje domněnka, že umocňování v cyklické grupě je jednosměrnou funkcí.

Motivace

Nalezení diskrétního logaritmu je výpočetně velmi obtížné. Existuje domněnka, že umocňování v cyklické grupě je jednosměrnou funkcí. Cílem je nalézt takovou grupu, v níž je výpočet diskrétního logaritmu stejně obtížný jako jeho výpočet v grupě $\mathbb{Z}_p^\times$ (ElGamal) a přitom má menší velikost. Podobně je žádoucí nalézt takovou grupu, v níž je výpočet d.l. stejně obtížný, jako rozložení čísla n (RSA) a přitom má mnohem méně prvků.

Projektivní prostor

Definice

Nechť K je těleso, n přirozené číslo. Na K^{n+1} definujme relaci ekvivalence $\sim$ předpisem

$$(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n) \Leftrightarrow \exists 0 \neq \lambda \in K : \lambda a_i = b_i$$

pro $1 \leq i \leq n$.
Pak $(K \setminus \{0\})/ \sim$ se nazývá projektivní prostor dimenze n nad K.

Definice eliptických křivek

Úvodem několik nutných definic

Definice

Nechť K je těleso, $P^n(K)$ n–rozměrný projektivní prostor nad K a $F(t_1, \ldots, t_{n+1}) \in K[t_1, \ldots, t_{n+1}]$ je homogenní polynom stupně k. Množina

$$\mathcal{C} = \{[x_1 : \ldots : x_{n+1}] \in P^n(K) | F(x_1, \ldots, x_{n+1}) = 0\}$$

se nazývá nadplocha (projektivní varieta) stupně k v $P^n(K)$. Pokud $n = 2$, hovoříme o křivce v $P^2(K)$. Pokud $k = 3$, řekneme že F je kubický polynom.

Po našich nadplochách budeme požadovat jistou hladkost. K tomu využijeme (stejně jako v analýze) derivaci.

Definice eliptických křivek

Definice

Nechť $F(t_1, \ldots, t_{n+1}) \in K[t_1, \ldots, t_{n+1}]$ je homogenní polynom stupně k nad tělesem K a $\mathcal{C}$ nadplocha příslušející k F. Bod $[x_1, \ldots, x_n] \in \mathcal{C}$ se nazývá **singulární**, jestliže pro každé $i \in \{1, \ldots, n+1\}$ platí

$$F_{x_i}(x_1, \ldots, x_{n+1}) = 0.$$

Nadplocha $\mathcal{C}$ se nazývá **singulární**, existuje-li na ní alespoň jeden singulární bod.

Definice eliptických křivek

Definice

Nechť $F(t_1, \ldots, t_{n+1}) \in K[t_1, \ldots, t_{n+1}]$ je homogenní polynom stupně k nad tělesem K a $\mathcal{C}$ nadplocha příslušející k F. Bod $[x_1, \ldots, x_n] \in \mathcal{C}$ se nazývá **singulární**, jestliže pro každé $i \in \{1, \ldots, n+1\}$ platí

$$F_{x_i}(x_1, \ldots, x_{n+1}) = 0.$$

Nadplocha $\mathcal{C}$ se nazývá **singulární**, existuje-li na ní alespoň jeden singulární bod.

Poznámka - Bod $[0, \ldots, 0] \notin P^n(K)$.

Definice eliptických křivek

Definice

Nechť $F(t_1, \ldots, t_{n+1}) \in K[t_1, \ldots, t_{n+1}]$ je homogenní polynom stupně k nad tělesem K a $\mathcal{C}$ nadplocha příslušející k F. Bod $[x_1, \ldots, x_n] \in \mathcal{C}$ se nazývá **singulární**, jestliže pro každé $i \in \{1, \ldots, n+1\}$ platí

$$F_{x_i}(x_1, \ldots, x_{n+1}) = 0.$$

Nadplocha $\mathcal{C}$ se nazývá **singulární**, existuje-li na ní alespoň jeden singulární bod.

Poznámka - Bod $[0, \ldots, 0] \notin P^n(K)$. Odtud již můžeme definovat eliptickou křivku

Definice

Eliptická křivka nad K je uspořádaná dvojice $(\mathcal{E}, O)$, kde $\mathcal{E}$ je nesingulární kubická křivka v $P^2(K)$ a $O \in \mathcal{E}$.

Úprava tvaru eliptické křivky

Je třeba si nyní uvědomit, že obecný homogenní kubický polynom $F(x, y, z)$ je tvaru

$$F(x, y, z) = a_1x^3 + a_2x^2y + a_3x^2z + a_4y^3 \\ + a_5y^2x + a_6y^2z + a_7z^3 + a_8z^2y + a_9z^2x + a_{10}xyz,$$

se kterým se pracuje poměrně obtížně. Naštěstí je možné ukázat, že se stačí omezit na křivky "lepšího tvaru", což popisuje následující věta (uvádíme bez důkazu).

Věta

Úprava tvaru eliptické křivky

Je třeba si nyní uvědomit, že obecný homogenní kubický polynom $F(x, y, z)$ je tvaru

$$\begin{aligned} F(x, y, z) = {} & a_1x^3 + a_2x^2y + a_3x^2z + a_4y^3 \\ & + a_5y^2x + a_6y^2z + a_7z^3 + a_8z^2y + a_9z^2x + a_{10}xyz, \end{aligned}$$

se kterým se pracuje poměrně obtížně. Naštěstí je možné ukázat, že se stačí omezit na křivky "lepšího tvaru", což popisuje následující věta (uvádíme bez důkazu).

Věta

Libovolná eliptická křivka nad tělesem K je biracionálně ekvivalentní s nějakou eliptickou křivkou $(\mathcal{E}, O)$ zadanou polynomem $F(x, y, z)$ (naše transformace převádí vyznačený bod původní křivky na bod O), kde

$$F(x, y, z) = y^2z + a_1xyz + a_2yz^2 - x^3 - a_3x^2z - a_4xz^2 - a_5z^3, O = [0, 1, 0]$$

Úprava tvaru eliptické křivky

Eliptická křivka v uvedeném tvaru má jeden nevlastní bod (totiž O) a v afinní části je popsána vztahem

$$F(x, y, z) : y^2 + a_1 xy + a_2 y - x^3 - a_3 x^2 - a_4 x - a_5 = 0.$$

Tato rovnice se nazývá Weierstrassova rovnice. Pokud nyní navíc předpokládáme $char(K) \neq 2, 3$, snadno vidíme, že rovnici můžeme algebraickými úpravami dále zjednodušit:

Úprava tvaru eliptické křivky

Eliptická křivka v uvedeném tvaru má jeden nevlastní bod (totiž O) a v afinní části je popsána vztahem

$$F(x, y, z) : y^2 + a_1 xy + a_2 y - x^3 - a_3 x^2 - a_4 x - a_5 = 0.$$

Tato rovnice se nazývá Weierstrassova rovnice. Pokud nyní navíc předpokládáme $char(K) \neq 2, 3$, snadno vidíme, že rovnici můžeme algebraickými úpravami dále zjednodušit:nejdříve odstraníme členy s y převodem na čtverec: $(x, y) \to (x, \frac{1}{2}(y - a_1 x - a_3))$ a dostáváme rovnici

$$G(x, y, z) : y^2 = x^3 + b_1 x^2 + b_2 x + b_3.$$

Úprava tvaru eliptické křivky

Eliptická křivka v uvedeném tvaru má jeden nevlastní bod (totiž O) a v afinní části je popsána vztahem

$$F(x, y, z) : y^2 + a_1xy + a_2y - x^3 - a_3x^2 - a_4x - a_5 = 0.$$

Tato rovnice se nazývá Weierstrassova rovnice. Pokud nyní navíc předpokládáme $char(K) \neq 2, 3$, snadno vidíme, že rovnici můžeme algebraickými úpravami dále zjednodušit:nejdříve odstraníme členy s y převodem na čtverec: $(x, y) \to (x, \frac{1}{2}(y - a_1x - a_3))$ a dostáváme rovnici

$$G(x, y, z) : y^2 = x^3 + b_1x^2 + b_2x + b_3.$$

Nyní se zbavíme členu s x^2 tak, že položíme $(x, y) \to ((x - 3b_2)/36, (y/108))$. Odkud dostáváme často užívanou rovnici

$$H(x, y) : y^2 = x^3 + Ax + B,$$

kterou také někdy nazýváme Weierstrassova rovnice.

Diskriminant eliptické křivky

Dále předpokládáme $char(K) \neq 2, 3$. Užitečnou pomůckou pro určení, zda je křivka singulární, je její diskriminant:

Definice

Diskriminant eliptické křivky

Dále předpokládáme $char(K) \neq 2, 3$. Užitečnou pomůckou pro určení, zda je křivka singulární, je její diskriminant:

Definice

Buď $\mathcal{E}$ kubická křivka zadaná v afinní části $P^2(K)$ rovnicí $y^2 = x^3 + Ax + B, A, B \in K$. Pak její diskriminant $\Delta = 4A^3 + 27B^2$.

Diskriminant eliptické křivky

Dále předpokládáme $char(K) \neq 2, 3$. Užitečnou pomůckou pro určení, zda je křivka singulární, je její diskriminant:

Definice

Buď $\mathcal{E}$ kubická křivka zadaná v afinní části $P^2(K)$ rovnicí $y^2 = x^3 + Ax + B, A, B \in K$. Pak její diskriminant $\Delta = 4A^3 + 27B^2$.

Nenulovost diskrimantu funkce je pak znakem regularity křivky:

Věta

Rovnice $F(x, y, z) : x^3 + Axz^2 + Bz^3 - y^2z, (A, B \in K)$ *zadává nějakou eliptickou křivku, právě když platí* $4A^3 + 27B^2 \neq 0$.

Diskriminant eliptické křivky

Důkaz.

Platí

$F_x = -3x^2 - Az^2, F_y = 2yz, F_z = y^2 - 2Axz - 3Bz^2.$

Diskriminant eliptické křivky

Důkaz.

Platí
$F_x = -3x^2 - Az^2, F_y = 2yz, F_z = y^2 - 2Axz - 3Bz^2$.Předpokládejme, že $[x, y, z]$ je singulární bod F. Pak $z = 0 \Rightarrow x = y = 0$, spor. Tedy $z \neq 0$, čili $y = 0$. Pro $Q = \frac{x}{z}$ platí $3Q^2 = -A, 2AQ = -3B$. Pokud $A = 0$, pak $B = 0$ a bod $[0, 0, 1]$ je singulární a $\Delta = 0$.

Diskriminant eliptické křivky

Důkaz.

Platí
$F_x = -3x^2 - Az^2, F_y = 2yz, F_z = y^2 - 2Axz - 3Bz^2$.Předpokládejme, že $[x, y, z]$ je singulární bod F. Pak $z = 0 \Rightarrow x = y = 0$, spor. Tedy $z \neq 0$, čili $y = 0$. Pro $Q = \frac{x}{z}$ platí $3Q^2 = -A, 2AQ = -3B$. Pokud $A = 0$, pak $B = 0$ a bod $[0, 0, 1]$ je singulární a $\Delta = 0$.
Nechť $A \neq 0$. Pak nutně $Q = \frac{-3B}{2A}, Q^2 = \frac{-A}{3} = \frac{9B^2}{4A^2}$. Tedy $4A^2 + 27B^3 = 0$. Stačí pouze ověřit, že $[Q, 0, 1]$ leží na F :
$Q^3 + AQ + B = \frac{B}{2} - \frac{3B}{2} + B = 0$. $\square$

Binární operace $*$ na $\mathcal{E}$

Nyní bychom chtěli na eliptické křivce $\mathcal{E}$ zavést grupovou operaci $+$ tak, aby $(\mathcal{E}, +)$ byla komutativní grupou. Potřebujeme tedy každým dvěma bodům na křivce přiřadit bod třetí. Nabízí se následující způsob:

Binární operace $*$ na $\mathcal{E}$

Nyní bychom chtěli na eliptické křivce $\mathcal{E}$ zavést grupovou operaci $+$ tak, aby $(\mathcal{E}, +)$ byla komutativní grupou. Potřebujeme tedy každým dvěma bodům na křivce přiřadit bod třetí. Nabízí se následující způsob:vezmeme průsečík přímky zadané těmito dvěma body s křivkou $\mathcal{E}$. Průsečíky je ovšem potřeba počítat včetně jejich násobností, abychom měli vždy 3 body. V případě tečny ke křivce v některém jejím bodě tedy takový bod počítáme dvakrát.

Binární operace $*$ na $\mathcal{E}$

Nyní bychom chtěli na eliptické křivce $\mathcal{E}$ zavést grupovou operaci $+$ tak, aby $(\mathcal{E}, +)$ byla komutativní grupou. Potřebujeme tedy každým dvěma bodům na křivce přiřadit bod třetí. Nabízí se následující způsob:vezmeme průsečík přímky zadané těmito dvěma body s křivkou $\mathcal{E}$. Průsečíky je ovšem potřeba počítat včetně jejich násobností, abychom měli vždy 3 body. V případě tečny ke křivce v některém jejím bodě tedy takový bod počítáme dvakrát. Další nejasnost se týká přímek kolmých na osu x. Intuitivně se zdá, že takové přímky mohou mít s eliptickou křivkou nejvýše 2 průsečíky. Třetím průsečíkem je ovšem bod v nekonečnu $O = [0, 1, 0]$.

Binární operace $*$ na $\mathcal{E}$

Definice

Nechť $A, B \in \mathcal{E}$, kde $A = [x_A, y_A, 1]$, $B = [x_B, y_B, 1]$. Přímku určenou body A a B označme p. Definujme binární operaci $*$ následovně:

$$A * B = \begin{cases} \text{třetí průsečík přímky } p \text{ a křivky } \mathcal{E} & \text{pro } x_A \neq x_B \\ O = [0, 1, 0] & \text{pro } x_A = x_B \end{cases}$$

Binární operace $*$ na $\mathcal{E}$

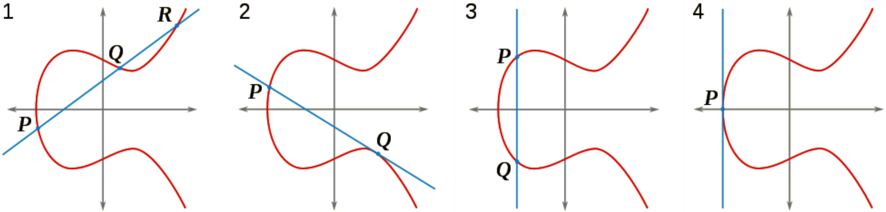
Definice

Nechť $A, B \in \mathcal{E}$, kde $A = [x_A, y_A, 1], B = [x_B, y_B, 1]$. Přímku určenou body A a B označme p. Definujme binární operaci $*$ následovně:

$$A * B = \begin{cases} \text{třetí průsečík přímky } p \text{ a křivky } \mathcal{E} & \text{pro } x_A \neq x_B \\ O = [0, 1, 0] & \text{pro } x_A = x_B \end{cases}$$

Bohužel, takto definovaná operace nemá neutrální prvek N. Aby totiž platilo $A * N = A$ pro libolvolné $A \in \mathcal{E}$, musela by přímka určená body A a N mít s křivkou $\mathcal{E}$ dvojnásobný bod dotyku A, čili by se muselo jednat o tečnu v bodě A. Bod N by proto musel ležet na všech tečnách vedených libovolným bodem $\mathcal{E}$, což nelze.
Je vhodné si uvědomit, že se jedná o komutativní operaci. Rovněž z definice vidíme, že eliptická křivka $\mathcal{E}$ je na tuto operaci uzavřená.

Přímka určená dvěma body z $\mathcal{E}$



Zde vidíme, že
1)$P * Q = R$ (tři různé body),
2)$P * Q = Q$ (tečna v bodě Q),
3)$P * Q = O$ a
4)$P * P = O$ (tečna v bodě P).

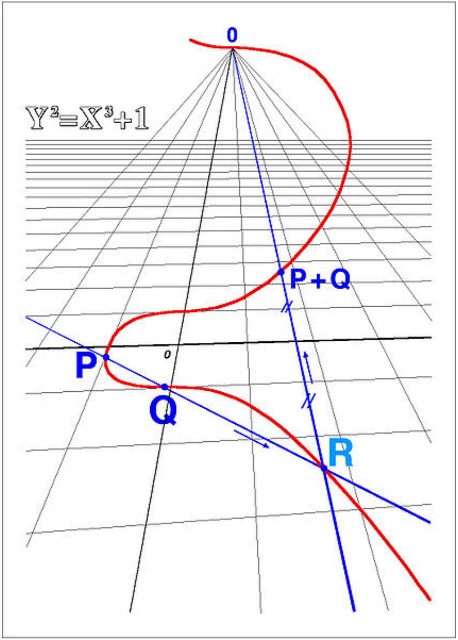
Binární operace $+$ na $\mathcal{E}$

Uvedená operace $*$ tedy nemá neutrální prvek, ale lze ji použít. Pro dva body P a Q vezměme onen třetí bod $P * Q$, bod O a jimi vedenou přímkou získáme opět bod na křivce. S pomocí operace $*$ nyní zaveďme konečně požadovanou operaci $+$.

Definice

Nechť $A, B \in \mathcal{E}$, kde $A = [x_A, y_A, 1]$, $B = [x_B, y_B, 1]$. Definujme binární operaci $+$ následovně:

$$A + B = (A * B) * O$$


0
$Y^2=X^3+1$
P+Q
0
P
Q
R

Komutativní grupa

Věta

Eliptická křivka $(\mathcal{E}, O)$ nad tělesem K s výše definovanou operací $+$ tvoří komutativní grupu.

Idea důkazu.

Z vlastností operace $*$ plyne komutativita $+$ a uzavřenost křivky na tuto operaci. Pro lib. bod $A \in \mathcal{E}$, kde $A = [x_A, y_A, 1]$ označme $-A := [x_A, -y_A, 1]$. Takový bod dostaneme jako průsečík, vedeme-li přímku body A a O, tj. $A * O = -A$. Mějme $A \in \mathcal{E}$ libovolný, pak platí: $A + O = (A * O) * O = -A * O = -(-A) = A$, tedy bod O je neutrálním prvkem grupy. Opačným prvkem k prvku $A \in \mathcal{E}$ je již zmiňovaný bod $-A$, neboť $A + (-A) = O$. Zbývá dokázat asociativitu: to je již značně netriviální. $\square$

Věty platné pro eliptické křivky $(\mathcal{E}, O)$

Věta

Nechť $(\mathcal{E}, O)$ *je eliptická křivka nad konečným tělesem* $(\mathbb{Z}/p\mathbb{Z}, +)$*, kde* p *je kladná mocnina prvočísla. Pak* $(\mathcal{E}, +)$ *je cyklická grupa nebo součin dvou cyklických grup. Navíc, je-li* $(\mathcal{E}', +)$ *izomorfní se součinem cyklických grup o* d_1 *a* d_2 *prvcích a* $d_1 | d_2$*, potom platí* $d_1 | p - 1$*.*

Věty platné pro eliptické křivky $(\mathcal{E}, O)$

Věta

Nechť $(\mathcal{E}, O)$ *je eliptická křivka nad konečným tělesem* $(\mathbb{Z}/p\mathbb{Z}, +)$*, kde* p *je kladná mocnina prvočísla. Pak* $(\mathcal{E}, +)$ *je cyklická grupa nebo součin dvou cyklických grup. Navíc, je-li* $(\mathcal{E}', +)$ *izomorfní se součinem cyklických grup o* d_1 *a* d_2 *prvcích a* $d_1|d_2$*, potom platí* $d_1|p-1$.

V následujících dvou větách budeme potřebovat pro snazší formulaci pojem torzní podgrupy.

Definice

Podgrupa $(\mathcal{E}', +)$ grupy $(\mathcal{E}, +)$ se nazývá torzní podgrupa, jestliže obsahuje právě prvky konečného řádu z grupy $(\mathcal{E}, +)$.

Věty platné pro eliptické křivky $(\mathcal{E}, O)$

Věta (Mordell)

Nechť $(\mathcal{E}, O)$ *je eliptická křivka nad* $\mathbb{Q}$. *Pak* $(\mathcal{E}, O)$ *je konečně generovaná grupa. Pro každou torzní podgrupu* $(\mathcal{E}', +)$ *rovněž existuje jednoznačně určené* $r \in \mathbb{N}_0$ *takové, že*

$$(\mathcal{E}, +) \cong (\mathcal{E}', +) \times (\mathbb{Z}, +)^r$$

Věta (Mazur)

Nechť $(\mathcal{E}, O)$ *je eliptická křivka nad* $\mathbb{Q}$. *Pak je její torzní podgrupa izomorfní s některou z následujících 15 grup:*

$(\mathbb{Z}/m\mathbb{Z}, +)$ *pro* $1 \leq m \leq 10$ *nebo* $m = 12$

$(\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/2m\mathbb{Z}, +)$ *pro* $1 \leq m \leq 4$

Domain parameters

- definují eliptickou křivku,

Domain parameters

- definují eliptickou křivku,
- pokud je křivka nad $\mathbb{F}_p$ jsou tvaru (p, a, b, G, n, h),

Domain parameters

- definují eliptickou křivku,
- pokud je křivka nad $\mathbb{F}_p$ jsou tvaru (p, a, b, G, n, h),
- pokud je křivka nad $\mathbb{F}_{2^m}$ jsou tvaru (m, f, a, b, G, n, h),

Domain parameters

- definují eliptickou křivku,
- pokud je křivka nad $\mathbb{F}_p$ jsou tvaru (p, a, b, G, n, h),
- pokud je křivka nad $\mathbb{F}_{2^m}$ jsou tvaru (m, f, a, b, G, n, h),
- kde

p	prvočíslo, modul se kterým pracujeme,
m	mocnina čísla 2 v binárním případě,
f	ireducibilní polynom stupně m nad $\mathbb{Z}_2$ $(\mathbb{F}_{2^m} \cong \mathbb{Z}_2[x]/(f))$,
a	koeficient u x v rovnici křivky,
b	absolutní člen v rovnici křivky,
G	bod křivky, generátor cyklické podgrupy,
n	řád bodu G,
h	$h = \lvert\mathcal{E}\rvert/n$.

- Mějme křivku $y^2 = x^3 + 1$ nad $\mathbb{Z}_{13}$.

- Mějme křivku $y^2 = x^3 + 1$ nad $\mathbb{Z}_{13}$.

bod	řád	bod	řád
$[[0]_{13}, [1]_{13}]$	3	$[[5]_{13}, [10]_{13}]$	6
$[[0]_{13}, [12]_{13}]$	3	$[[6]_{13}, [3]]_{13}$	6
$[[2]_{13}, [3]_{13}]$	6	$[[6]_{13}, [10]_{13}]$	6
$[[2]_{13}, [10]_{13}]$	6	$[[10]_{13}, [0]_{13}]$	2
$[[4]_{13}, [0]_{13}]$	2	$[[12]_{13}, [0]_{13}]$	2
$[[5]_{13}, [3]_{13}]$	6		

-

- Mějme křivku $y^2 = x^3 + 1$ nad $\mathbb{Z}_{13}$.
-

bod	řád	bod	řád
$[[0]_{13}, [1]_{13}]$	3	$[[5]_{13}, [10]_{13}]$	6
$[[0]_{13}, [12]_{13}]$	3	$[[6]_{13}, [3]]_{13}$	6
$[[2]_{13}, [3]_{13}]$	6	$[[6]_{13}, [10]_{13}]$	6
$[[2]_{13}, [10]_{13}]$	6	$[[10]_{13}, [0]_{13}]$	2
$[[4]_{13}, [0]_{13}]$	2	$[[12]_{13}, [0]_{13}]$	2
$[[5]_{13}, [3]_{13}]$	6		

- Domain parameters mohou vypadat následovně

$$(13, 0, 1, [2, 10], 6, 2).$$

Vytvoření klíče

- Alice

  soukromý klíč $d_A = 3$,
  veřejný klíč $Q_A = d_A \cdot G = 3 \cdot [2, 10] = [12, 0]$.

Vytvoření klíče

- Alice

  soukromý klíč $d_A = 3$,
  veřejný klíč $Q_A = d_A \cdot G = 3 \cdot [2, 10] = [12, 0]$.

- Bob

  soukromý klíč $d_B = 5$,
  veřejný klíč $Q_B = d_B \cdot G = 5 \cdot [2, 10] = [2, 3]$.

Vytvoření klíče

- Alice

  soukromý klíč $d_A = 3$,
  veřejný klíč $Q_A = d_A \cdot G = 3 \cdot [2, 10] = [12, 0]$.
- Bob

  soukromý klíč $d_B = 5$,
  veřejný klíč $Q_B = d_B \cdot G = 5 \cdot [2, 10] = [2, 3]$.
- Potom

$$d_A \cdot Q_B = 3 \cdot [2, 3] = [12, 0],$$

$$d_B \cdot Q_A = 5 \cdot [12, 0] = [12, 0].$$

Doporučené křivky (NIST)

- prvočísla, která mají v binárním zápise délku: $192, 224, 256, 384, 521,$

Doporučené křivky (NIST)

- prvočísla, která mají v binárním zápise délku: $192, 224, 256, 384, 521$,
- binární případ: $2^{163}, 2^{233}, 2^{283}, 2^{409}, 2^{571}$,

Doporučené křivky (NIST)

- prvočísla, která mají v binárním zápise délku: $192, 224, 256, 384, 521$,
- binární případ: $2^{163}, 2^{233}, 2^{283}, 2^{409}, 2^{571}$,
- n (řád bodu G) je prvočíslo,

Doporučené křivky (NIST)

- prvočísla, která mají v binárním zápise délku: $192, 224, 256, 384, 521$,
- binární případ: $2^{163}, 2^{233}, 2^{283}, 2^{409}, 2^{571}$,
- n (řád bodu G) je prvočíslo,
- h není dělitelné n, co nejmenší: 1, 2, nebo 4,

Doporučené křivky (NIST)

- prvočísla, která mají v binárním zápise délku: $192, 224, 256, 384, 521$,
- binární případ: $2^{163}, 2^{233}, 2^{283}, 2^{409}, 2^{571}$,
- n (řád bodu G) je prvočíslo,
- h není dělitelné n, co nejmenší: 1, 2, nebo 4,
- doporučené prvočíslo je například

$$6277101735386680763835789423207666416083908700390324961279,$$

které má v binárním zápise délku 192. Řád bodu G na křivce

$$y^2 \equiv x^3 - 3x + b \bmod p$$

je

$$6277101735386680763835789423176059013767194773182842284081.$$

Bezpečnost klíčů

Porovnání:

- RSA: aktuálním rekordem je prolomení RSA-768 (prosinec 2009, cca. 2,5 roku, subexponenciální metoda síta v číselném tělese)

Bezpečnost klíčů

Porovnání:

- RSA: aktuálním rekordem je prolomení RSA-768 (prosinec 2009, cca. 2,5 roku, subexponenciální metoda síta v číselném tělese)
- ECDLP:
  - Pro binární případ je rekordem prolomení 109-bitového klíče (2004, využití 2600 strojů po dobu 17 měsíců).
  - Pro prvočíselný případ je rekordem prolomení 112-bitového klíče (duben 2009, výpočetní cluster 200 konzolí Playstation 3, cca. 3,5 měsíce).

Bezpečnost klíčů

Porovnání:

- RSA: aktuálním rekordem je prolomení RSA-768 (prosinec 2009, cca. 2,5 roku, subexponenciální metoda síta v číselném tělese)
- ECDLP:
  - Pro binární případ je rekordem prolomení 109-bitového klíče (2004, využití 2600 strojů po dobu 17 měsíců).
  - Pro prvočíselný případ je rekordem prolomení 112-bitového klíče (duben 2009, výpočetní cluster 200 konzolí Playstation 3, cca. 3,5 měsíce).
  - Všechny známé algoritmy pro výpočet diskrétního logaritmu mají exponenciální složitost.