Eliptické křivky

15. a 16. přednáška z kryptografie

Obsah

Eliptické křivky nad $\mathbb{R}$

Důležitou roli v moderní kryptografii hrají grupy bodů na eliptických křivkách. Ukažme nejdříve eliptické křivky nad $\mathbb{R}$ ve zjednodušeném tvaru:

Definice

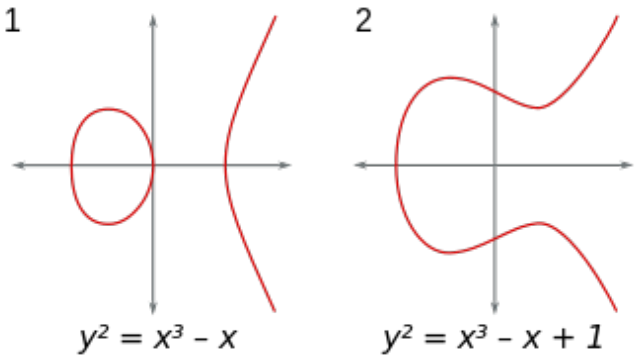
Eliptická křivka nad tělesem $\mathbb{R}$ je množina všech bodů (x, y) v rovině $\mathbb{R}^2$ splňujících rovnici:

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

A kubický polynom $x^3 + ax + b$ má pouze jednoduché kořeny v $\mathbb{C}$, což nastane, právě když diskriminant $D = 4a^3 + 27b^2 \neq 0$.

Eliptické křivky nad $\mathbb{R}$

Příklad



Eliptické křivky nad $\mathbb{R}$

Operace sčítání - geometricky

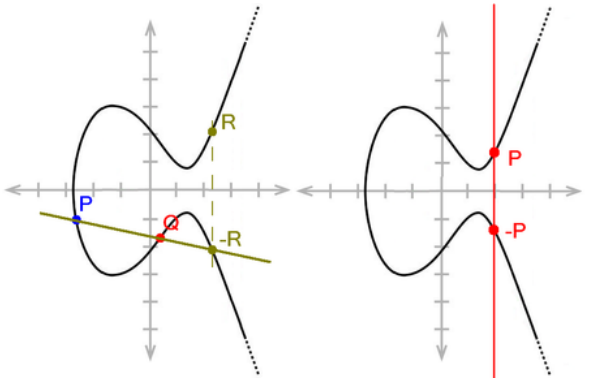
Na bodech ležících na eliptické křivce lze definovat sčítání. Geometrická definice využívá souměrnosti křivky podle osy x.

- Pokud $P \neq Q$, tak proložíme body P a Q přímku. Tato přímka ve většině případů protne křivku v jediném dalším bodě. Za součet $P + Q$ prohlásíme bod R, který je zrcadlovým obrazem tohoto průniku (podle osy x).
- Je-li přímka PQ tečnou ke grafu eliptické křivky v bodě P (resp. Q), definujeme součet $P + Q$ jako bod R, který je zrcadlovým obrazem bodu P (resp. Q).
- Je-li přímka PQ rovnoběžná s osou y definujeme součet $P + Q$ jako bod v nekonečnu (značí se O).

Eliptické křivky nad $\mathbb{R}$

Operace sčítání - geometricky

Pro $P = (p_1, p_2)$ značíme $-P = (p_1, -p_2)$ bod souměrný podle osy x.



$P + Q = R$ $\qquad$ $P + (-P) = O$

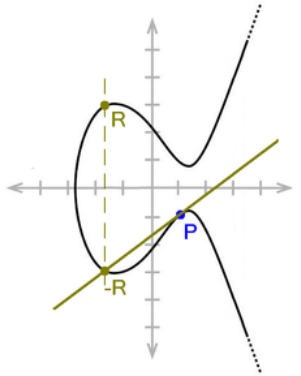
Eliptické křivky nad $\mathbb{R}$

Operace sčítání - geometricky

- Pokud $P = Q$, tak bodem P vedeme tečnu ke grafu eliptické křivky. Tato tečna většinou protne křivku v jediném dalším bodě. Za součet $P + P$ prohlásíme bod R, který je zrcadlovým obrazem tohoto průniku (podle osy x).
- Je-li tečna v bodě P rovnoběžná s osou y, definujeme součet $P + P$ jako bod v nekonečnu (značí se O).
- Dodefinujeme $O + P = P$, $P + O = P$, $O + O = O$.

Eliptické křivky nad $\mathbb{R}$

Operace sčítání - geometricky

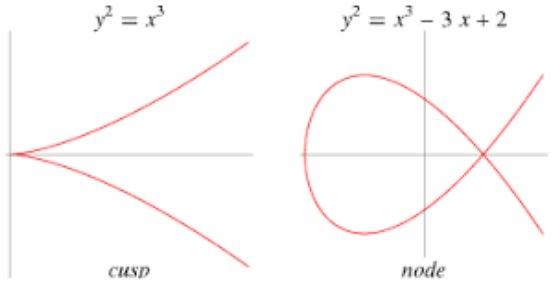


$2P = P + P = R$

Eliptické křivky nad $\mathbb{R}$

Poznámka

Podmínka na nenulový diskriminant zaručuje, že eliptická křivka se neprotne a že nemá ostrý zlom. Geometrickými konstrukcemi je jednoznačně definován součet pro všechny body křivky.



Eliptické křivky nad $\mathbb{R}$

Tvrzení

Označme $E(\mathbb{R})$ množinu všech bodů v rovině splňujících rovnici eliptické křivky spolu s bodem v nekonečnu O. Množina $E(\mathbb{R})$ s právě definovanou operaci sčítání tvoří Abelovu grupu. $(E(\mathbb{R}), +)$ se nazývá *grupa bodů na eliptické křivce*.

Důkaz: Komutativita je zřejmá, asociativita se ověřuje obtížněji. Neutrálním prvkem je přidaný bod O, opačným prvkem k bodu P je bod $-P$ souměrný s ním podle osy x.

Eliptické křivky nad $\mathbb{R}$

Operace sčítání - aritmetricky

Označme $P = (p_1, p_2)$, $Q = (q_1, q_2)$ body na eliptické křivce

$$y^2 = x^3 + ax + b, \text{ kde } D = 4a^3 + 27b^2 \neq 0.$$

Odvodíme výpočet souřadnic bodu $R = P + Q$ ze souřadnic bodu P a bodu Q. Označme neznámý bod $R = (r_1, r_2)$.

Eliptické křivky nad $\mathbb{R}$

Operace sčítání - aritmetricky

1) Nechť nejdříve $P \neq Q$ (ani $-P \neq Q$):

Přímka procházející body P, Q má rovnici $y = \lambda x + \kappa$, kde $\lambda = \frac{q_2 - p_2}{q_1 - p_1}$ (pro $p_1 \neq q_1$), $\kappa = p_2 - \lambda p_1$.

Dosazením do rovnice eliptické křivky najdeme $x-$ovou souřadnici průniku přímky s danou křivkou (což je r_1):

$$0 = x^3 - (\lambda x + \kappa)^2 + ax + b,$$

přičemž koeficient u x^2 je roven $-\lambda^2 = -(p_1 + q_1 + r_1)$ (Vietovy vzorce pro kořeny). Odtud $r_1 = \lambda^2 - p_1 - q_1$.

$y-$ová souřadnice průniku přímky s křivkou (což je $-r_2$) je $-r_2 = \lambda r_1 + \kappa$. Odtud $r_2 = \lambda(p_1 - r_1) - p_2$.

Pokud byla přímka PQ tečnou ke grafu křivky např. v bodě P, vyjde nám $R = -P$.

Eliptické křivky nad $\mathbb{R}$

Operace sčítání - aritmetricky

2) Nechť $P = Q$ (ale $p_2 \neq 0$):

Vztahem $F(x, y) = y^2 - x^3 - ax - b = 0$ je (za předpokladu nenulovosti parciální derivace funkce F podle y v bodě P) implicitně zadaná funkce $y(x)$ procházející bodem P. To nám umožní vypočítat směrnici tečny k eliptické křivce v bodě P jako hodnotu $y'(x) = \frac{3x^2+a}{2y}$ v bodě P.

Tečna k eliptické křivce v bodě P má rovnici $y = \lambda x + \kappa$, kde $\lambda = \frac{3p_1^2+a}{2p_2}$ (pro $p_2 \neq 0$), $\kappa = p_2 - \lambda p_1$.

Dosazením do rovnice eliptické křivky najdeme $x-$ovou souřadnici průniku tečny s danou křivkou, $r_1 = \lambda^2 - 2p_1$.
Pak $y-$ová souřadnice zrcadlového obrazu průniku je $r_2 = \lambda(p_1 - r_1) - p_2$.

Eliptické křivky nad $\mathbb{R}$

Operace sčítání - aritmetricky

Pro $P = (p_1, p_2)$, $Q = (q_1, q_2)$ body na eliptické křivce $E : y^2 = x^3 + ax + b$, kde $D = 4a^3 + 27b^2 \neq 0$ je definován součet $R = P + Q$ takto:

- Je-li $p_1 = q_1$, $p_2 = -q_2$, pak $P + Q = O$, kde O je přidaný bod v nekonečnu.
- $P + O = P$, $O + P = P$, $O + O = O$.
- V ostatních případech je $P + Q = R = (r_1, r_2)$, kde $r_1 = \lambda^2 - p_1 - q_1$, $r_2 = \lambda(p_1 - r_1) - p_2$,
  $\lambda = \frac{q_2-p_2}{q_1-p_1}$, pokud $P \neq Q$,
  $\lambda = \frac{3p_1^2+a}{2p_2}$, pokud $P = Q$.

Eliptické křivky nad $\mathbb{Z}_p$

V aritmetice pro sčítání bodů na eliptických křivkách potřebujeme sčítání a odčítání, násobení a dělení nenulovými čísly v tělese $\mathbb{R}$. To vše ale umíme v libovolném tělese!

Odvození souřadnic průniku přímky $y = \lambda x + \kappa$ s křivkou $y^2 = x^3 + ax + b$ lze udělat nad libovolným tělesem (včetně formální derivace polynomů). Přitom $x-$ová souřadnice průniku r_1 byla třetím kořenem jistého kubického polynomu, ale v každém tělese má kubický polynom nejvýše tři kořeny a platí Vietovy vzorce.

Můžeme zcela analogicky zavést grupu bodů na eliptické křivce nad konečným tělesem, kde sčítání bude definovávo stejnými vztahy jako nad $\mathbb{R}$ (pouze místo dělení budeme násobit inverzními prvky).

Eliptické křivky nad $\mathbb{Z}_p$

Každé konečné těleso je isomorfní s Galoisovým tělesem a má p^k prvků, kde p je prvočíslo. Budeme ho značit $GF(p^k)$. Číslo p se nazývá charakteristika tělesa.

V praxi se nejčastěji používají tělesa $\mathbb{Z}_p$ nebo $GF(2^k)$.

Budeme se věnovat grupám bodů na eliptické křivce nad $\mathbb{Z}_p$, ale vše lze analogicky definovat pro libovolné těleso $GF(p^k)$.

Eliptické křivky nad $\mathbb{Z}_p$

Definice

Eliptická křivka nad tělesem $\mathbb{Z}_p$, kde $p > 3$ je prvočíslo, je množina všech bodů (x, y) v $\mathbb{Z}_p^2$ splňujících rovnici:

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

kde $a, b \in \mathbb{Z}_p$ a $D = 4a^3 + 27b^2 \neq 0$ v $\mathbb{Z}_p$.

Označme $E(\mathbb{Z}_p)$ množinu všech těchto bodů spolu s přidaným bodem O.

Tvrzení

Množina $E(\mathbb{Z}_p)$ spolu se sčítáním zavedeným aritmetickými vztahy jako v $E(\mathbb{R})$ tvoří Abelovu grupu.

Eliptické křivky nad $\mathbb{Z}_p$

Příklad

Eliptická křivka nad $\mathbb{Z}_{17}$ je dána rovnicí $y^2 = x^3 + 7x + 13$.
Určíme body na této křivce.

Pro $x = 0$ vyjde $y^2 = 13$, přičemž $13^{\frac{p-1}{2}} = 13^8 = 1$ v $\mathbb{Z}_{17}$,
tedy 13 je čtverec a hrubou silou určíme $y = \pm 8$.
Body $(0, 8)$, $(0, 9)$ jsou na křivce.

Pro $x = 3$ vyjde $y^2 = 10$, přičemž $10^{\frac{p-1}{2}} = 10^8 = -1$ v $\mathbb{Z}_{17}$,
tedy 10 není čtverec. Na křivce není žádný bod $(3, y)$.

Grupa $E(\mathbb{Z}_{17}) = \{(0,8), (0,9), (1,2), (1,15), (2,1), (2,16), (6,4), (6,13), (14,4), (14,13), (15,5), (15,12), O\}$ má 13 prvků.

$P + Q = (1,2) + (6,4) = ((-3)^2 - 1 - 6, -3(1 - r_1) - 2) = (2,1)$,
neboť $\lambda = 2 \cdot 5^{-1} = -3$ v $\mathbb{Z}_{17}$.

Eliptické křivky nad $\mathbb{Z}_p$

Odhad řádu grupy $E(\mathbb{Z}_p)$

- $|E(\mathbb{Z}_p)| \leq 2p + 1$, neboť pro každé $x \in \mathbb{Z}_p$ má $x^3 + ax + b$ nejvýše dvě druhé odmocniny.
- $|E(\mathbb{Z}_p)| \doteq p$, neboť pouze polovina prvků v $\mathbb{Z}_p$ jsou čtverce a výsledky $x^3 + ax + b$ jsou zhruba rovnoměrně rozdělené v $\mathbb{Z}_p$.
- Hasseho věta: Pro každou eliptickou křivku nad $\mathbb{Z}_p$ platí: $p + 1 - 2\sqrt{p} \leq |E(\mathbb{Z}_p)| \leq p + 1 + 2\sqrt{p}$
- Hasseho věta platí i pro eliptické křivky nad $GF(p^k)$, když p nahradíme v odhadu p^k.

Eliptické křivky nad $\mathbb{Z}_p$

Struktura grupy $E(\mathbb{Z}_p)$

- $E(\mathbb{Z}_p) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, kde $n_2 \mid \gcd(n_1, p - 1)$.
  Aneb grupa je vnitřním direktním součtem dvou cyklických podgrup řádů n_1, resp. n_2, tudíž $|E(\mathbb{Z}_p)| = n_1 \cdot n_2$.
- Je-li $n_2 = 1$, pak je $E(\mathbb{Z}_p)$ cyklická.
- Je-li n_2 malé (cca $2, 3, 4$), pak říkáme, že $E(\mathbb{Z}_p)$ je téměř cyklická.
- Stejnou strukturu mají grupy bodů eliptických křivek nad $GF(p^k)$ s tím, že zde $n_2 \mid \gcd(n_1, p^k - 1)$.

Eliptické křivky nad $\mathbb{Z}_p$

Obecná definice

Obecný tvar rovnice pro eliptickou křivku nad tělesem:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Pokud charakteristika tělesa $\neq 2$, lze rovnici transformovat do tvaru $y^2 = x^3 + ax^2 + bx + c$.
Pokud charakteristika $\neq 2, 3$, lze dosáhnout tvaru $y^2 = x^3 + ax + b$.

Pro tělesa $GF(2^k)$ lze rovnici upravit na $y^2 + xy = x^3 + ax^2 + b$, anebo na $y^2 + cy = x^3 + ax + b$.

Každý tvar má jiný diskriminant a pro každý tvar se odvodí jiné vzorce na sčítání bodů eliptické křivky.

Eliptické křivky v kryptografii

Diffieho-Hellmanova domluva klíče

Alice zvolí grupu bodů na eliptické křivce $E(\mathbb{Z}_p)$ a v ní bod A velkého řádu n. Má tedy cyklickou podgrupu $G = \langle A \rangle$ řádu n.

Dále zvolí $x \in \mathbb{Z}_n$ a spočte prvek $B = xA$ v grupě $E(\mathbb{Z}_p)$.
Alice pošle Bobovi prvek B a informace o grupě $(E(\mathbb{Z}_p), n, A)$.

Bob zvolí $y \in \mathbb{Z}_n$ a spočte prvek $C = yA$ v grupě $E(\mathbb{Z}_p)$.
Bob pošle Alici prvek C.

Alice spočte $S_A = xC$ a Bob spočte $S_B = yB$ v grupě $E(\mathbb{Z}_p)$.
Tím oba získají stejný tajný klíč $S = S_A = S_B = xyA$.

Analogicky můžeme podgrupu $G = \langle A \rangle$ grupy $E(\mathbb{Z}_p)$ použít pro ElGamalovo šifrování.

Eliptické křivky v kryptografii

Diffieho-Hellmanova domluva klíče

Časová náročnost výpočtu:

- Celočíselný násobek xP bodu P na eliptické křivce $E(\mathbb{Z}_p)$ spočteme algoritmem opakovaných dvojnásobků. To bude vyžadovat $O(len(n))$ sčítání pro $x \in \mathbb{Z}_n$.
  ("Repeat doubling" algoritmus je aditivní analogií k "repeat squaring" algoritmu).
- Součet dvou bodů $P + Q$ vyžaduje 6 sčítání, 3 násobení a 1 výpočet inverze v $\mathbb{Z}_p$. Dublování bodu $2P = P + P$ vyžaduje o jedno násobení více.
  To znamená, že jedno sčítání bodů v $E(\mathbb{Z}_p)$ je zhruba pětkrát pomalejší než jedno násobení v $\mathbb{Z}_p$.

Eliptické křivky nad $\mathbb{Z}_p$

Příklad

Eliptická křivka nad $\mathbb{Z}_{17}$ je dána rovnicí $y^2 = x^3 + 7x + 13$.

Grupa $E(\mathbb{Z}_{17}) = \{(0,8), (0,9), (1,2), (1,15), (2,1), (2,16), (6,4), (6,13), (14,4), (14,13), (15,5), (15,12), O\}$ má 13 prvků, je tedy cyklická a libovolný prvek kromě O je jejím generátorem.

Alice a Bobem použijí $E(\mathbb{Z}_{17}) = \langle A = (1,2) \rangle$ řádu $n = 13$.

Alice volí $x = 5$ a spočte $B = 5 \cdot (1,2) = (2,16)$.
Bob volí $y = 2$ a spočte $C = 2 \cdot (1,2) = (0,9)$.
Domluvený tajný klíč bude $S = 2 \cdot B = (14,13)$.

Eliptické křivky v kryptografii

Problém diskrétního logaritmu

Nechť $G = \langle A \rangle$ řádu n je podgrupa grupy $E(\mathbb{Z}_p)$.
Pro bod $B \in G$ hledáme $x \in \mathbb{Z}_n$ tak, aby $B = xA$ v grupě $E(\mathbb{Z}_p)$.

- Ve většině grup $E(\mathbb{Z}_p)$ je problém diskrétního logaritmu exponenciální problém se složitostí $O(\sqrt{n})$, resp. $O(\sqrt{q})$, kde q je největší prvočíslo ve faktorizaci čísla n.
- V grupě $E(\mathbb{Z}_p)$ funguje "Baby step-giant step" algoritmus i Pohlingův-Hellmanův algoritmus na výpočet diskrétního logaritmu (stejně tak jako Pollardova $\rho-$metoda). Subexponenciální algoritmus "index calculus" zde nefunguje.

Eliptické křivky

Literatura

- Hankerson, Menezes, Vanstone: Guide to Eliptic Curve Cryptography. Kapitoly 1. a 3.1 a 4.1.
- Koblitz: A Course in Number Theory and Cryptography. Kapitola 6,1-2.

Eliptické křivky v kryptografii

Problém diskrétního logaritmu

- Je znám jiný subexponenciální algoritmus pro grupy tzv. supersingulárních křivek, což jsou křivky:
  $y^2 = x^3 + ax$ nad tělesem $GF(p^k)$, kde $p \equiv -1\,(mod\,4)$,
  $y^2 = x^3 + b$ nad tělesem $GF(p^k)$, kde $p \equiv -1\,(mod\,3)$.

Poznámka

Musíme také vyřešit problém jak převést zprávy na body na eliptické křivce (kódování zpráv).