Y36BEZ – Bezpečnost přenosu a zpracování dat

Róbert Lórencz

14. přednáška

Kryptografie eliptických křivek

http://service.felk.cvut.cz/courses/Y36BEZ
lorencz@fel.cvut.cz

Obsah přednášky

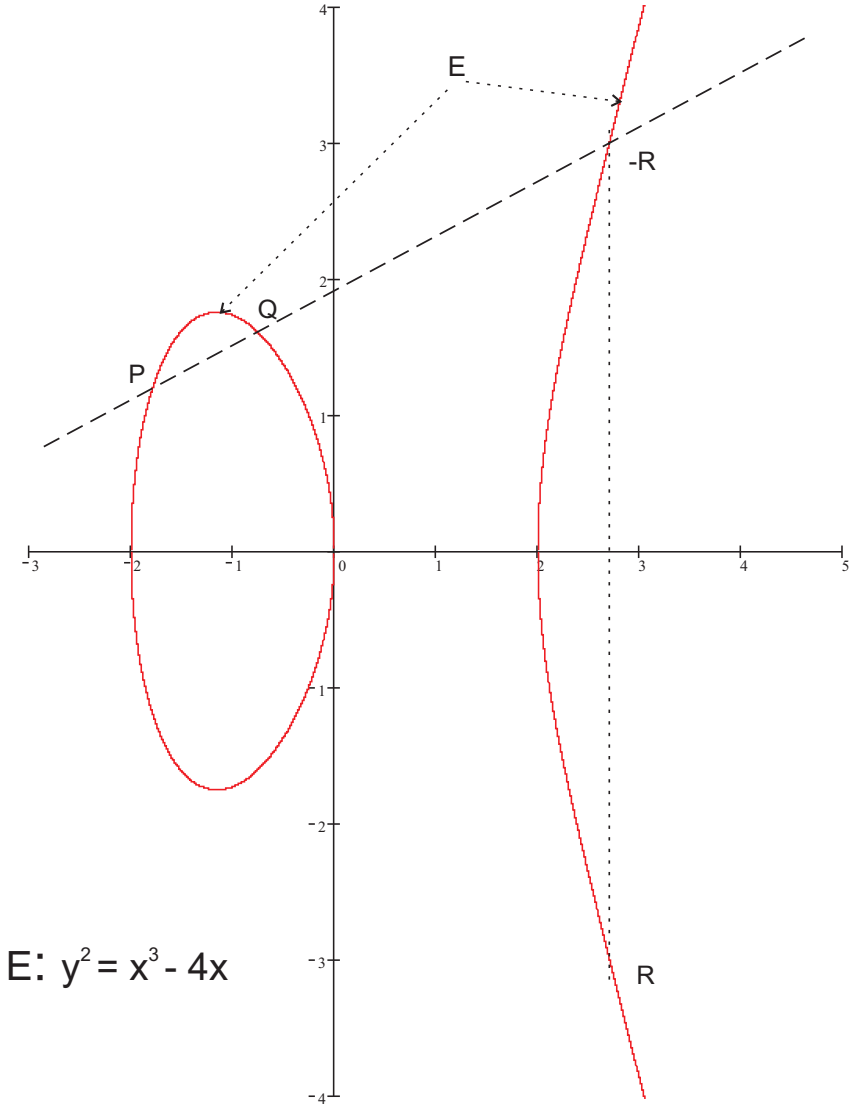
- Historie
- Matematický základ
- Eliptická křivka nad tělesem GF(p)
- ECC a problém diskrétního logaritmu
- Šifrování s ECC

Historie

- Kryptografie eliptických křivek (ECC) je moderním a slibným směrem současné kryptografie.
- ECC je další možností pro realizaci elektronického podpisu.
- ECC v některých ukazatelích dává lepší výsledky než současné běžně používané kryptosystémy.
- V současnosti jsou eliptické kryptosystémy v řadě světových standardů a staly se alternativou k RSA.
- ECC má výhodu v rychlosti a menší náročnosti na hardware.
- Eliptické křivky jsou speciální podtřídou kubických křivek.
- Název eliptické vznikl proto, že kubické rovinné funkce se v minulosti používaly k výpočtu obvodu elipsy.
- Zkoumáním vlastností eliptických křivek se nejvíce zabýval německý matematik K. T. W. Weierstrass (1815 — 1897).
- V. Miller a N. Koblitz přišli nezávisle na sobě na možnost použití eliptických křivek v rámci kryptosystému veřejného klíče (1985).

Matematický základ (1)

- Eliptická křivka E je množina bodů v rovině, která vyhovuje rovnici
$$y^2 = x^3 + ax + b. \qquad (1)$$
- Součtem 2 různých bodů P a Q z E bude opět bod ležící na E, a tedy také vyhovující rovnici (1).
- Geometrické interpretace součtu: Spojíme body P = [x_P, y_P] a Q = [x_Q, y_Q] přímkou, ta protne křivku E v bodě –R.
- Výsledkem sčítání je potom bod R, který je symetrický k –R podle osy x. Body symetrické podle osy x nazýváme *opačné*.



Matematický základ (2)

- Směrnice přímky, která spojuje dva různé body P a Q je rovná

$$s = \frac{y_Q - y_P}{x_Q - x_P}. \tag{2}$$

- Pro souřadnice bodu R = $[x_R, y_R]$ platí

$$x_R = s^2 - x_P - x_Q \quad \text{a} \quad y_R = s(x_P - x_R) - y_P. \tag{3}$$

- Když P = Q $\Rightarrow$ jejich spojnice je tečna k E a její směrnice je rovná

$$s = \frac{3{x_P}^2 + a}{2y_P}. \tag{4}$$

- Sčítáním 2 opačných bodů (P = – Q) měli bychom dostat "0 bod".
- Taková přímka nám E už neprotne, resp. ji protne v ∞. $\Rightarrow$ definitoricky k E "bod v ∞" O přidáme $\Rightarrow$ sčítání 2 opačných bodů definujeme: P + (–P) = O. *Bod v* ∞ je název "0 bodu" křivky E.
- Dodefinujeme sčítání pro O: P + O = P, O + O = O a O = –O.
- Takto je definováno sčítání pro $\forall$ dvojice bodů na E včetně O.

Eliptická křivka nad tělesem GF(p)(1)

Využití eliptických křivek pro šifrování

Při využití eliptických křivek pro šifrování pracujeme v oblasti diskrétních hodnot (celých čísel, bitových řetězců, m-tice bitů) $\Rightarrow$

- Uvažujeme těleso GF(2^m) a těleso GF(p), kde p je prvočíslo.
- Obě tělesa jsou v praxi využívaná – každé z nich má své přednosti.
- Pro jednoduchost výkladu dále jen operace nad tělesem GF(p).
- Eliptická křivka nad tělesem GF(p) je definována jako bod O v ∞ společně s množinou bodů P = [x, y], kde x a y jsou z tělesa GF(p) a vyhovují rovnici $y^2 = x^3 + ax + b$ v GF(p), tj.

$$y^2 \equiv x^3 + ax + b \pmod{p} . \tag{5}$$

Eliptická křivka nad tělesem GF(p)(2)

- Koeficienty a a b jsou také prvky tělesa GF(p) a musí splňovat podmínku
$$|4a^3 + 27b^2|_p \neq 0. \tag{6}$$
- Takto definovaná množina bodů tvoří grupu, koeficienty a a b volíme libovolně (veřejné parametry příslušného kryptosystému).
- V této grupě definujeme opačný bod k O jako O = –O a pro ostatní nenulové body P = $[x_P, y_P] \in$ E definujeme –P = $[x_P, |-y_P|_p]$, dále pro všechny body P $\in$ E definujeme P + –P = O a P + O = P.
- Bod O nazýváme také nulovým bodem, vzhledem k jeho roli při sčítání v grupě E. Sčítání stejných nenulových bodů P + P definujme jako R = P + P = $[x_R, y_R]$, kde směrnice s je rovná
$$s = \left|\frac{3x_P{}^2 + a}{2y_P}\right|_p \tag{7}$$

Eliptická křivka nad tělesem GF(p)(3)

- a souřadnice bodu R

$$x_R = \left| s^2 - x_P - x_Q \right|_p \quad \text{a} \quad y_R = \left| s(x_P - x_R) - y_P \right|_p . \tag{8}$$

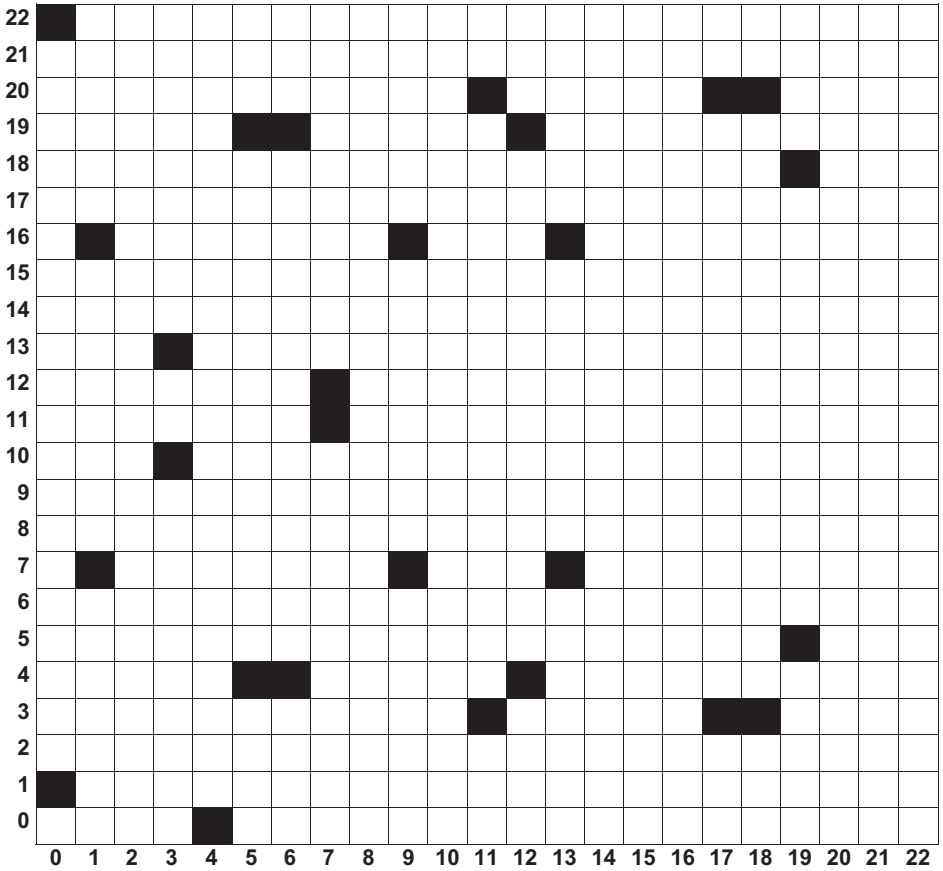
- Sčítáním různých nenulových a vzájemně neinverzních bodů P = [x_P, y_P] a Q = [x_Q, y_Q] křivky E definujeme jako P + Q = R = [x_R, y_R], kde směrnice s je rovná

$$s = \left| \frac{y_Q - y_P}{x_Q - x_P} \right|_p \tag{9}$$

- a souřadnice bodu R

$$x_R = \left| s^2 - x_P - x_Q \right|_p \quad \text{a} \quad y_R = \left| s(x_P - x_R) - y_P \right|_p . \tag{10}$$

Eliptická křivka nad tělesem GF(p)(4)



(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)	O

28 bodů eliptické křivky $y^2 = x^3 + x + 1$ nad $GF(23)$

ECC a problém diskrétního logaritmu (1)

- Pro pochopení podstaty šifrování a podepisování v ECC je důležité využití tzv. problému diskrétního logaritmu.
- Pro určitý bod P na křivce E postupně vypočítáme body 2P, 3P, 4P, 5P, 6P atd., čímž dostaneme obecně různé body xP na E.
- Protože křivka má konečný počet bodů, označíme ho #P, po určitém kroku m se nám musí tato posloupnost opakovat.
- V bodě opakování mP tak platí mP = nP, kde nP je některý z předešlých bodů. Odtud dostáváme mP – nP = O $\Rightarrow$
- existuje nějaké $r = m - n, r < m$ takové, že rP = O, z toho plyne, že v posloupnosti P, 2P, 3P, 4P, 5P,... se vždy dostaneme k bodu O, a poté cyklus začína znovu od bodu P, protože $(r + 1)$P = rP +P = O + P = P.
- Nejmenší takové r, pro které je rP = O, nazýváme *řád bodu* P.

ECC a problém diskrétního logaritmu (2)

- Lze dále dokázat, že řád bodu dělí řád křivky, přičemž *řádem křivky* nazýváme počet bodů na křivce #E.
- Různé body na křivce E mají různý řád. V kryptografické praxi vybíráme takové body, jejichž řád je roven největšímu prvočíslu v rozkladu čísla #E nebo jeho násobku, který nazýváme *kofaktor*.
- U bodu řádu r máme zaručeno, že dojde k opakování v posloupnosti P, 2P, 3P,... až po r-tém kroku.
- V případě, že r je velké číslo, např. 2^{256}, je to skutečně dlouhá posloupnost.
- Právě při šifrování a elektronickém podepisování se využívá tak velké posloupnosti a to právě v souvislosti s tzv. problémem diskrétního logaritmu.
- V případě, že si zvolíme jako náš privátní klíč číslo k a vypočteme $Q = kP$, potom body P a Q můžeme zveřejnit jako součást veřejného klíče.

ECC a problém diskrétního logaritmu (3)

- Problém diskrétního logaritmu je úloha, jak z bodů P a Q získat tajné číslo k tak, aby platilo Q = kP.
- Je zřejmé, že pro malý řád bodu P je úloha triviální. Pro velká r je to úloha, která se nedá řešit efektivně, tj. v polynomiálním čase. Z tohoto důvodu mohou být body P a Q zveřejněné.
- Dosud nejúčinnější metodou pro řešení takto definovaného problému diskrétního logaritmu je tzv. Pollardova ρ metoda, jejíž složitost je řádově $(\pi r/2)^{1/2}$ kroků.
- Pokud máme $r = 2^{256}$, dostáváme $\approx 2^{128}$ kroků, což je zhruba na úrovní luštitelnosti symetrické blokové šifry se 128 bitovým klíčem.
- Pro nás je to z výpočetního hlediska neřešitelné, a tedy příslušná šifra je výpočetně bezpečná.

Šifrování s ECC

- Podstatu šifrování pomocí ECC si ukážeme na analogii Diffie-Hellmanova schématu výměny klíče.
- Strana *i* a *j*, si chtějí vyměnit tajnou informaci přes veřejný kanál.
- Každá strana má důvěryhodnou cestou získaný veřejný klíč protistrany. V případě ECC ještě navíc předpokládáme, že oba sdílejí stejnou křivku E a její bod P.
- Označme po řadě d_i a Q_i privátní a veřejný klíč strany *i*, a obdobně d_j a Q_j pro stranu *j*, potom si obě strany mohou ustanovit společný klíč — bod Z na křivce E, aniž spolu komunikují.
- Strana *i* vypočte bod Z jako $d_i Q_j$ a strana *j* jako $d_j Q_i$. Tyto body jsou ve skutečnosti stejné, protože $Z = d_i Q_j = d_i(d_j P) = (d_i d_j)P$ a současně $Z = d_j Q_i = d_j(d_i P) = (d_j d_i)P$.
- Tedy každá strana vezme bod veřejný klíč — bod protistrany a sečte ho *n*-krát, kde *n* je privátní klíč. Protože obě strany vycházejí ze stejného bodu P, dospějí do stejného bodu Z.