O Weilově párování na eliptických křivkách

Miroslav Kureš

Aplikovaná matematika Ostravice 2012
2. workshop
A-Math-Net Síť pro transfer znalostí v aplikované matematice

Abstrakt. Pracovní seminární text, jehož účelem je poskytnout jen tu nejzákladnější představu, s jakými algebraickými problémy se lze setkat v eliptické kryptografii a v kryptografii založené na identitě.

1. Kryptosystémy s veřejným klíčem ve srovnání s kryptosystémy založenými na identitě. *Kryptosystém s veřejným klíčem*: veřejný klíč K_U, soukromý klíč K_R. Klíč K_U je generován jednosměrnou funkcí z K_R. Pokud je Bob offline, nelze komunikovat. Pokud Eva (*man-in-the-middle*) přesvědčí Alici, že K_U je jiný, snadno pak dešifruje zprávy určené Bobovi. Tento *autentikační problém* (ověření identity) je řešen *certifikáty* poskytovanými *důvěryhodnou autoritou*.

Kryptosystém založený na identitě: veřejným klíčem K_U je jednoznačná identifikace Boba (např. telefonní číslo nebo e-mailová adresa). Certifikáty nejsou třeba. Je-li Bob offline, lze komunikovat (např. zpráva může čekat v *Short Message Service Center* a být odeslána později).

2. Eliptické křivky. *Eliptickou křivkou* $\mathcal{E}$ nad polem $\mathbb{F}$ rozumíme algebraickou křivku třetího stupně s rovnicí

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

kde $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$ a kde tzv. *diskriminant* Δ eliptické křivky $\mathcal{E}$ je nenulový. Přitom

$$\begin{aligned}
\Delta &= -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6 \\
d_2 &= a_1^2 + 4a_2 \\
d_4 &= 2a_4 + a_1 a_3 \\
d_6 &= a_3^2 + 4a_6 \\
d_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 + a_4^2.
\end{aligned}$$

Je-li $\mathbb{F}_q = \mathbb{F}_{p^n}$ (p prvočíslo, $n \in \mathbb{N}$ konečné pole s charakteristikou různou od 2 a 3, pak vhodnou změnou souřadnic lze Weierstrassovu rovnici transformovat na rovnici

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

Je-li $\mathbb{F}_q$ konečné pole s charakteristikou 2, pak vhodnou změnou souřadnic lze Weierstrassovu rovnici transformovat na rovnici

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

(tzv. *nesupersingulární* eliptická křivka) nebo na rovnici

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

(tzv. *supersingulární* eliptická křivka). Obdobná věta platí i pro pole charakteristiky 3.

Bodem eliptické křivky $\mathcal{E}$ rozumíme každý bod $[x, y]$ se souřadnicemi $x, y \in \mathbb{F}$ splňujícími její rovnici a dále bod ∞. Nad body eliptické křivky (nadále již bereme $\infty \in \mathcal{E}$) lze zavést binární operaci značenou $+$ a nazvanou *sečno-tečnové sčítání* takto: jsou-li dva body $P = [x_1, y_1]$, $Q = [x_2, y_2]$ eliptické křivky $\mathcal{E}$ různé, vedeme skrze ně přímku; ta protne $\mathcal{E}$ ještě v dalším bodě a $R = P + Q$ vezmeme jako bod osově souměrný s tímto třetím bodem podle osy x. (Je-li přímka rovnoběžná s osou y, třetí bod $\mathcal{E}$ na ní již neexistuje, pak klademe $P + Q = \infty$.) Dále, pro součet $P + P$ vedeme bodem bodem P tečnu; ta protne $\mathcal{E}$ ještě v dalším bodě a $R = P + P$ vezmeme jako bod osově souměrný s tímto bodem podle osy x. (Opět, je-li přímka rovnoběžná s osou y, klademe $P + P = \infty$.) Součet libovolného bodu P eliptické křivky $\mathcal{E}$ s bodem ∞ položíme roven P.

Vzorce pro sečno-tečnové sčítání (pro pole s p různým od 2 i od 3):
(případ $R = P + Q; R = [r_1, r_2], P = [p_1, p_2], Q = [q_1, q_2]$)

$$r_1 = \left(\frac{q_2 - p_2}{q_1 - p_1}\right)^2 - p_1 - q_1 \qquad r_2 = \left(\frac{q_2 - p_2}{q_1 - p_1}\right)(p_1 - r_1) - p_2$$

(případ $R = 2P = P + P; R = [r_1, r_2], P = [p_1, p_2]$)

$$r_1 = \left(\frac{3p_1^2 + a}{2p_2}\right)^2 - 2p_1 \qquad r_2 = \left(\frac{3p_1^2 + a}{2p_2}\right)(p_1 - r_1) - p_2$$

Nyní je $(\mathcal{E}, +)$ grupa. *Řádem eliptické křivky* $\mathcal{E}$ pak rozumíme řád této grupy čili počet bodů $\mathcal{E}$; značíme ho $\#\mathcal{E}$. Je-li $\mathcal{E}$ eliptická křivka nad konečným polem $\mathbb{F}_q$, pro její řád $\#\mathcal{E}(\mathbb{F}_q)$ platí odhad

$$q + 1 - 2\sqrt{q} \leq \#\mathcal{E}(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$$

(*Hasseho interval*). Existuje tedy $t \in \mathbb{Z}$ takové, že

$$\#\mathcal{E}(\mathbb{F}_q) = q + 1 - t, \quad \text{kde } |t| \leq 2\sqrt{q}.$$

Řád eliptické křivky lze pomocí t a Legendrova symbolu určit takto:

$$t = -\sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p}\right)$$

Přímé užití tohoto vztahu se nazývá *naivní algoritmus* pro určení řádu eliptické křivky.

3. Torzní podgrupy.

Pro $m \in \mathbb{N}$ bod P křivky $\mathcal{E}$ splňující $mP = \infty$ nazveme *m-tý torzní bod*. Množina všech m-tých torzních bodů se značí $\mathcal{E}[m]$, se zavedeným sčítáním bodů je $\mathcal{E}[m]$ podgrupou grupy $\mathcal{E}$, nazýváme ji *m-tá torzní grupa*.

Je-li m libovolným násobkem řádu bodu P, pak $P \in \mathcal{E}[m]$. První torzní podgrupa je evidenentě triviální (obsahuje pouze bod ∞), zatímco $\#\mathcal{E}$-tá torzní podgrupa už je rovna $\mathcal{E}$. (Nic nového nepřináší, uvažujeme-li $m > \#\mathcal{E}$.) Bod ∞ je prvkem všech m-tých torzních grup a dále je zřejmé, že v případě nesoudělného m a $\#\mathcal{E}$ je také m-tá torzní podgrupa vždy triviální.

Jak vypadá druhá torzní grupa eliptických křivek? Pro její body platí $P + P = \infty$, což je možné jen pro nulovou y-ovou souřadnici bodu P. Tedy jde o to, zda existuje kořen rovnice $x^3 + ax + b = 0$ (v $\mathbb{F}_p$). Pokud ano, je řád $\#\mathcal{E}(\mathbb{F}_p)$ sudý a tedy t je sudé, neexistuje-li kořen $x^3 + ax + b = 0$ (v $\mathbb{F}_p$), je t je liché.

Obecně nejsou torzní podgrupy grupy G cyklické, neboť sama grupa G nemusí být cyklická; nejsou cyklické ani pro případ m, které je menší než řád grupy G: například druhá torzní grupa grupy $G = \mathbb{Z}_4 \oplus \mathbb{Z}_6$ je tvořena body $(0,0)$, $(2,0)$, $(0,3)$, $(2,3)$ a evidentně není generovaná jediným prvkem.

Pokud jde o grupu $\mathcal{E}$ nad polem $\mathbb{F}_q$, pak ta je vždy **izomorfní grupě** $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$**, přičemž** n_2 **dělí jak** n_1**, tak** $q-1$ (Teorém 3.12, [**2**]). Pak ovšem $\#\mathcal{E} = n_1 n_2$. Je-li $n_2 = 1$, je grupa $\mathcal{E}$ cyklická. Je-li $n_2 > 1$ malé přirozené číslo $(2, 3, 4, \dots)$, říkáme, že grupa $\mathcal{E}$ je *téměř cyklická*. V cyklické grupě existuje bod, jehož řád je roven již přímo $\#\mathcal{E}$. Pro určení řádu eliptické křivky je ale také výhodné, je-li téměř cyklická, neboť v ní existují body dostatečně vysokého řádu, jejichž násobek patří do Hasseho intervalu.

4. Eliptická kryptografie. Uvedeme nyní, v čem spočívá podstata eliptické kryptografie s veřejným klíčem (ECC). Pro jednoduchost vezmeme prvočíselné polem $\mathbb{F}_p$, nad kterým uvažujeme eliptickou křivku $\mathcal{E}$ a její bod $P \in \mathcal{E}$. *Řádem bodu* P rozumíme nejmenší $n \in \mathbb{N}$ takové, že $nP = \infty$. Řád každého bodu P eliptické křivky $\mathcal{E}$ dělí řád této křivky. (To je známý Lagrangeův teorém z teorie grup.) Bod P vyberme tak, aby jeho řádem bylo prvočíslo n. Dále vyberme nějaké $k \in [1, n-1]$ a spočtěme $Q = kP$. Údaje o poli a eliptické křivce jsou tzv. *definiční parametry* a pokládají se za známé. Veřejným klíčem jsou body P a Q a soukromým klíčem číslo k.

Algoritmus. Základní ElGamal šifrování pomocí eliptických křivek.

Vstup: Definiční parametry, veřejný klíč P, Q, zpráva m.

Výstup: Šifrovaná zpráva (C_1, C_2).

1. Vyjádři m jako bod M eliptické křivky.
2. Vyber $a \in [1, n-1]$.
3. Spočti $C_1 = aP$.
4. Spočti $C_2 = M + aQ$.
5. Vrať (C_1, C_2).

ALGORITMUS. ZÁKLADNÍ ELGAMAL DEŠIFROVÁNÍ POMOCÍ ELIPTICKÝCH KŘIVEK.

VSTUP: DEFINIČNÍ PARAMETRY, VEŘEJNÝ KLÍČ P, Q, SOUKROMÝ KLÍČ k, ŠIFROVANÁ ZPRÁVA (C_1, C_2).

VÝSTUP: ZPRÁVA m.

1. Spočti $M = C_2 - kC_1$.
2. Převeď M na m.
3. Vrať m.

5. Bilineární zobrazení grup a Weilovo párování. Uvažujme dvě grupy $G = (G, +)$, $H = (H, \cdot H)$, $k \in \mathbb{Z}$ a zobrazení $\phi\colon G \times G \to H$ splňující

$$\begin{aligned} \phi(g_1 + g_2, g_3) &= \phi(g_1, g_3) \cdot \phi(g_2, g_3) \\ \phi(kg_1, g_2) &= (\phi(g_1, g_2))^k \\ \phi(g_1, g_2 + g_3) &= \phi(g_1, g_2) \cdot \phi(g_1, g_3) \\ \phi(g_1, kg_2) &= (\phi(g_1, g_2))^k . \end{aligned}$$

Takové zobrazení nazveme *bilineární zobrazení*. (Užíváme zde aditivní notaci pro G a multiplikativní notaci pro H.)

V případě eliptických křivek můžeme uvažovat např. $G = (\mathcal{E}, +)$ a $H = (\mathbb{F}_q - \{0\}, \cdot)$, pro dále uvedené Weilova párování je volba grup speciálnější.

Weilovo párování je zobrazení

$$e\colon \mathcal{E}[m] \times \mathcal{E}[m] \to U_m,$$

kde $U_m = (U_m, \cdot)$ je grupa m-tých odmocnin jedničky v $\bar{\mathbb{F}}_p$ ($\bar{\mathbb{F}}_p$ je algebraický uzávěr $\mathbb{F}_q = \mathbb{F}_{p^n}$).

6. Weilovo párování v kryptografii založené na identitě. Důvěryhodná autorita je označována jako PKG (*private key generator*). Ta zvolí univerzální tajný klíč s. Poté zveřejní: rovnici eliptické křivky, její základní bod P, veřejný klíč systému sP a hašovací funkci h. Každý uživatel má veřejný klíč $K_U = Q_{ID}$ (bod eliptické křivky vycházející z identity) a soukromý klíč $K_R = sQ_{ID}$, který

obdrží od PKG. Odesílatel zprávy M vybere náhodně číslo r a posílá

$$(U, V) = (rP, M + \mathsf{h}(e(Q_{\mathrm{ID}}, sP)^r)) .$$

Adresát pak za použití svého soukromého klíče sQ_{ID} z (U, V) spočte

$$M = V + \mathsf{h}(e(sQ_{\mathrm{ID}}, U)).$$

7. Závěrečné poznámky. Kryptografie založená na identitě je vhodná zejména pro šifrování mobilními telefony. Mezi eliptické křivky doporučené standardy patří

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

nad binárními poli $\mathbb{F}_{2^{163}}$, $\mathbb{F}_{2^{233}}$, $\mathbb{F}_{2^{409}}$ (síla šifrování roste).

Např. pro $q = 2^{409}$ musí n_2 dělit jak n_1, tak některé z čísel

4480666067023,

76025626689833,

388119657591324467371942577087124648789568693795169094445383858676407269513158661795581193694512 9,

tzn. pro drtivou většinu křivek (pro všechny?) nad tímto polem je grupa eliptické křivky cyklická.

Bezpečnost kryptosystému založeného na identitě pak plyne z obtížnosti tzv. *Diffieho-Hellmanova problému pro cyklické grupy.*

Reference

1. J.-S. Hwu, R.J. Chen a Y.-B. Lin, An efficient identity-based cryptosystem for end-to-end mobile security, *IEEE Transactions* **5**, 2586–2593 (2006)
2. D. Hankerson, A. Menezes a S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer 2004
3. R. Sakai a M. Kasahara, ID based cryptosystems with pairing on elliptic curve, *Cryptology ePrint Archive*, Report 2003/054

E-mail address: kures@fme.vutbr.cz