Kryptologie pro praxi - principy ECC

V kryptografii označuje zkratka ECC schémata založená na eliptických křivkách (Elliptic Curve Cryptosystems). Zkráceně užíváme též pojmy eliptická kryptografie a eliptické kryptosystémy. ECC je alternativou například k systémům RSA, D-H či DSA (viz předchozí díly a [2]). V mnoha ohledech dosahuje ECC lepšího poměru cena/výkon. Umožňuje šifrování i digitální podpis s kratšími klíči a lze jej realizovat na omezeném hardwaru. Zejména z důvodu nižších nároků na kapacitu úložiště soukromého klíče se proto rozvíjí oblast eliptické kryptografie pro čipové karty včetně bezkontaktních, mobilní telefony, handheldy, a takzvané tenké klienty. Právě díky ECC lze i v těchto omezených prostředích realizovat velmi kvalitní kryptografické funkce. Příkladem budiž bezpečnostní protokol WTLS (Wireless Transport Layer Security) pro bezdrátová spojení, implementující eliptické kryptosystémy.

Proč nejsou ECC tolik rozšířené?

Důvodem je, že kryptosystémy RSA, DSA, Diffie-Hellman, ElGamal atd. jsou používány, studovány a známy déle a mají vybudovánu infrastrukturu. Zejména RSA bylo vyvinuto a nasazeno mnohem dříve a dříve pro něj byly vyvinuty standardy, programové moduly, knihovny, čipy apod. Alternativní systém má proto šanci jen někde, zejména v nových produktech na zelené louce. To může být příklad bezkontaktních čipových karet a mobilních zařízení, kde je mnohem výhodnější aplikovat eliptické kryptosystémy ze všech hledisek.

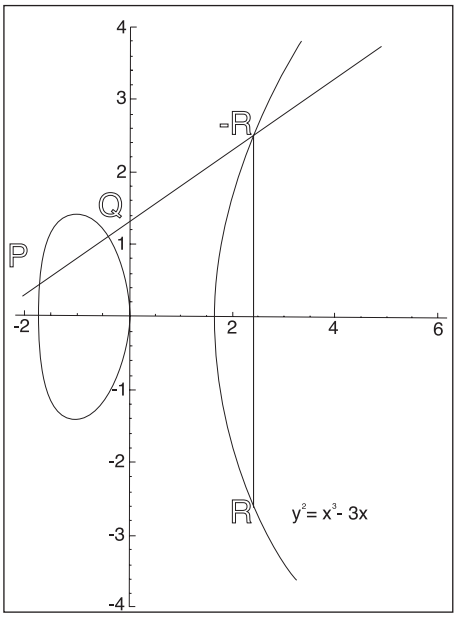
V současné době jsou eliptické kryptosystémy zařazeny v řadě celosvětově uznávaných standardů a z hlediska norem se už staly rovnocennou alternativou ke „klasickému“ RSA i DSA.

Bezpečnost

Srovnání bezpečnosti symetrických kryptosystémů (například AES) s RSA nebo ECC je orientačně možné, i když všechny tři systémy mají bezpečnostní záruky založené na jiných matematických základech (problémech). Přesto americký standardizační úřad NIST vydal orientační (to zdůrazněme) srovnávací tabulku bezpečnosti těchto systémů jako doporučení pro federální použití v USA. V *tabulce 1* například vidíte, že 160/224/512bitové klíče u ECC (později vysvětlíme, proč se jedná o sloupec s nápisem „řád generujícího bodu ECC“) odpovídají modulům RSA o 1024/2048/3072 bitech a klíčům symetrické šifry o délce 80/112/256 bitů.

Jak to začalo

Kryptosystémy s veřejným klíčem RSA i ECC pracují s různými matematickými strukturami. S eliptickými křivkami si matematici hráli přes 150 let, až z toho vyšlo něco praktického. V roce 1985 si



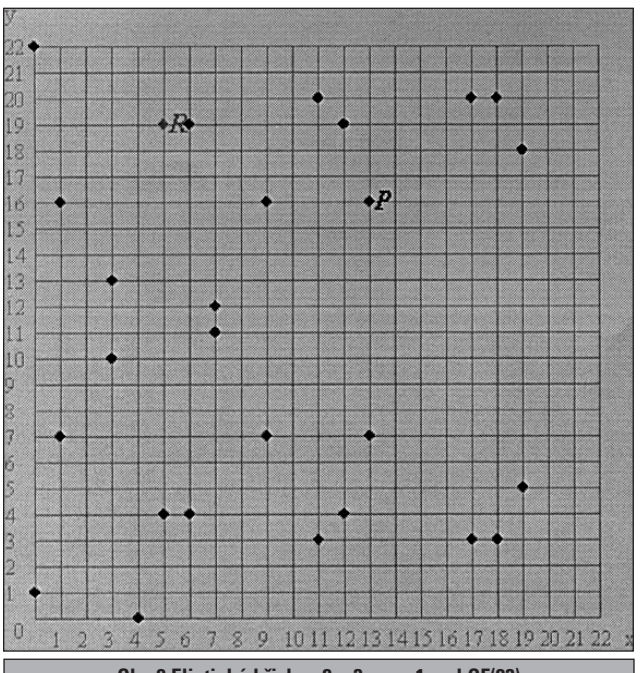
Obr. 1 Grafická interpretace principu sčítání dvou bodů v rovině

V. Miller a N. Koblitz povšimli, že by výsledky čisté algebry mohli přenést do kryptografie a vytvořit nový kryptosystém s veřejným klíčem. Během následujících 20 let se tato oblast rozvinula a doplnila praktickými výsledky tak, že dnes na eliptické kryptosystémy máme k dispozici „kuchařky“ i standardy na jejich implementaci.

Hruška + hruškA = HrušKa...

Při povídání o ECC si musíme zvyknout, že v algebře lze v zásadě sečíst cokoliv – třeba dva body na rovinné křivce. Výsledkem pak je opět bod na křivce. Na *obr. 1* máme konkrétní eliptickou křivku v rovině danou rovnicí E: $y^2=x^3 - 3x$ (dále uvažujeme obecnější rovnici $y^2=x^3 + ax+ b$). Je to množina bodů (x, y) v rovině, jejichž souřadnice vyhovují uvedenému vztahu. Nyní vezmeme dva různé body P, Q z křivky a definujeme jejich součet $P + Q$, bod R. Graficky spojíme body $P=(x_P, y_P)$ a $Q=(x_Q, y_Q)$ přímkou. Ta protne křivku v dalším bodě, který označíme $-R$ a výsledkem je bod R, symetrický k $-R$ podle osy x. Body R a $-R$ nazýváme opačné či inverzní vzhledem k právě definované operaci součtu dvou bodů. Směrnice s přímky PQ je tedy $s=(y_Q - y_P)/(x_Q - x_P)$. Souřadnice bodu $R=(x_R, y_R)$ lze odvodit jako společné řešení rovnic křivky E a přímky PQ jako $x_R=s^2 - x_P - x_Q$ a $y_R = s.(x_P - x_R) - y_P$. V případě $P=Q$ je jejich spojnice tečnou se směrnicí $s=(3x_P^2 + a)/(2y_P)$. Sčítáme-li opačné body, máme dostat něco jako „nulový bod“. Spojnice dvou opačných bodů je ale rovnoběžná s osou y a křivku E už v nějakém třetím bodě o konečných souřadnicích neprotíná. My však nulový bod potřebujeme, abychom mohli zavedenou operaci sčítání využít k sestavení algebraické struktury zvané grupa (té se budeme věnovat příště). Proto ke křivce E definitoricky přidáme „bod v nekonečnu O“. Definujeme $P + (-P)=O$, $P + O=P$, odkud dále plyne $O + O=O$, $-O=O$.

Právě jsme si ukázali eliptickou křivku nad tělesem reálných čísel společně se zavedením operace součtu bodů této křivky. V kryptografii je ovšem jednoznačně vhodné místo reálných čísel pracovat s čísly celými. Proto kandidátem na strukturu, která nahradí těleso reálných čísel, je takzvané Galoisovo těleso $GF(p)$, kde p je obvykle velmi velké prvočíslo. ECC často využívají i $GF(2^m)$, což zde pro jednoduchost vynecháme. Jako prvky tělesa $GF(p)$ můžeme uvažovat čísla {0,1, ..., p–1}, při-



Obr. 2 Eliptická křivka y2=x3 + x + 1 nad GF(23)

čemž výpočty v něm se provádějí *modulo p*. Připomeňme si, že pod aditivní inverzí čísla $x \in GF(p)$ rozumíme $y \in GF(p)$ splňující $(x + y) \bmod p=0$. Píšeme $y=-x$ (případně $y=-x \bmod p$, hrozí-li záměna s operacemi na tělese reálných čísel). Obdobně za multiplikativní inverzi čísla x považujeme y splňující $(x*y) \bmod p=1$. Píšeme $y=x^{-1}$ (případně $y=x^{-1} \bmod p$, hrozí-li záměna s operacemi na tělese reálných čísel). Jak jsme viděli z předchozích vzorců pro sčítání bodů, budeme v našem tělese potřebovat operaci dělení. S využitím zavedených inverzí ji definujeme jako násobení inverzním číslem. Například $x/y=x*(y^{-1})$, kde $y*(y^{-1}) \bmod p=1$. Například v GF(23) máme $5^{-1}=14$, protože $14*5 \bmod 23=70 \bmod 23=(23*3 + 1) \bmod 23=1$. Analogicky budeme s využitím aditivní inverze pracovat se „zápornými čísly“. Více se o těchto operacích dozvíte například v [1].

Eliptická křivka *E* nad tělesem GF(*p*)

Budiž pro naše účely definována jako bod v nekonečnu O společně s množinou bodů $P=(x, y)$, kde x a y jsou z tělesa GF(p) a splňují rovnici $y^2=x^3 + ax + b$ nad GF(p). Koeficienty a, b v rovnici jsou také prvky tělesa GF(p) a musí splňovat podmínku (pro jednoduchost ji uvádíme bez odvození): $(4a^3 + 27b^2) \bmod p \neq 0$, která zaručuje, že takto definovaná množina bodů tvoří společně s výše definovanou operací sčítání grupu (viz příště). Jinak koeficienty a a b můžeme volit libovolně – v tom případě to budou veřejné parametry příslušného kryptosystému.

Příklad

Mějme eliptickou křivku $y^2=x^3 + x + 1$ nad GF(23). Její body jsou graficky znázorněny na *obr. 2*, včetně bodu $P=(13, 16)$. Vypočítáme $P + P$, což značíme jednoduše jako $[2]P$. Pozor – zde operátor plus znamená součet bodů na křivce, nikoliv operaci v GF(p). Máme $R=P + P=(x_R, y_R)$, kde s využitím operací na GF(23) $s=(3*13^2 + 1)/(2*16) \bmod 23=508/32 \bmod 23=508*18 \bmod 23=9144 \bmod 23=13$, $x_R=(13^2 - 13 - 13) \bmod 23=143 \bmod 23=5$, $y_R=(13*(13 - 5) - 16) \bmod 23=88 \bmod 23=19$, takže $[2]P=(5, 19)$. Nyní již hravě vypočteme $[3]P=P + P + P=(P + P) + P=[2]P + P$, sčítáme tedy body (5, 19) a (13, 16). Dostaneme $s=(16 - 19)/(13 - 5) \bmod 23=-3/8 \bmod 23=-3*3 \bmod 23=14$, $x_R=(142 - 5 - 13) \bmod 23=178 \bmod 23=17$, $y_R=(14*(5 - 17) - 19) \bmod 23=20$, takže $[3]P=(17, 20)$. Podobně bychom vypočítali $[4]P=(17, 3)$, $[5]P=(5, 4)$, $[6]P=(13, 7)$ a $[7]P=O$. Při výpočtu $[7]P=[6]P + P=(13, 7) + (13, 16)=(13, 7) + (13, -7)$ také vidíme, že nepotřebujeme souřadnice nulového bodu, neboť během operace zjistíme, že sčítáme opačné body. Při výpočtu $[8]P$ se pochopitelně dostaneme zpět k bodu P, neboť $[8]P=[7]P + P=O + P=P$.

Příště bude…

V tomto dílu jsme se seznámili s pojmem eliptické křivka a ukázali jsme si, jak ji konstruovat nad tělesem reálných čísel a konečným tělesem GF(p). Dále nás bude zajímat hlavně konstrukce nad GF(p), neboť z ní vychází řada kryptografických schémat založených na eliptických křivkách. To, jak se tato vytvářejí, si ukážeme v příštím dílu.

Tabulka 1 Srovnání délek klíčů podle NIST

Symetrická šifra – délka klíče	Příklad	RSA– velikost modulu [b]	Řád generujícího bodu ECC [b]	ECC nad GF(p) – velikost p [b]	ECC nad GF(2^m) – číslo m [b]
80	Skipjack	1024	160	192	163
112	Triple DES se dvěma různými klíči	2048	224	224	233
128	AES – nejkratší klíč		256	256	283
192	AES – středně dlouhý klíč		384	384	409
256	AES – dlouhý klíč	3072	512	521	571

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, trosa@ebanka.cz

LITERATURA

[1] Menezes, A. J., van Oorschot, P. C., and Vanstone, S. A.: Handbook of Applied Cryptography, CRC Press, 1996

[2] E-archivy http://cryptography.hyperlink.cz, http://crypto.hyperlink.cz