NOVÉ SMĚRY V KRYPTOGRAFII S VEŘEJNÝM KLÍČEM

Ing.Jaroslav Pinkava, CSc.
AEC, spol. s r.o.
e-mail: jaroslav.pinkava@aec.cz

Systémy s veřejným klíčem se objevily v kryptografii teprve relativně nedávno. Svojí existencí však ovlivnily kryptografickou praxi zásadním způsobem. Jejich význačnou vlastností je existence dvou různých klíčů. Jeden klíč slouží k šifrování otevřeného textu, druhý klíč slouží k dešifraci. Pokud někdo zná pouze první klíč, může sice šifrovat, avšak pokud by chtěl dešifrovat zprávy tímto klíčem zašifrované, pak to může učinit pouze tehdy, zná-li navíc i dešifrovací klíč. Dešifrovací klíč přitom ze šifrovacího klíče nelze odvodit. Vzhledem k tomu jsou zašifrované zprávy chráněny proti třetím osobám a to i tehdy když tyto třetí osoby znají šifrovací klíč. Proto může být tento šifrovací klíč veřejně znám. Z těchto důvodů se také těmto kryptosystémům říká kryptosystémy **s veřejným klíčem** (asymetrické šifry). Dešifrovací klíč oproti tomu musí zůstat samozřejmě utajený. Tato základní vlastnost systémů s veřejným klíčem (šifrovací klíč není nutné chránit) se pak promítá do celé řady výhodných konstrukcí kryptografických protokolů.

Prvním významným konkrétním kryptosystém realizujícím tuto myšlenku bylo RSA (1978). V dalších létech se pak objevila celá řada schémat s veřejným klíčem.

Logicky vzniká následující otázka. Jestliže systémy s veřejným klíčem mají oproti klasickým symetrickým šifrovacím schématům (kdy existuje pouze jediný klíč sloužící jak k šifrování tak i k dešifraci) zásadní výhodu, proč je nevytlačily, proč se stále vedle nich používají blokové a proudové šifry? Ukázalo se totiž, že za tyto výhodné vlastnosti platí šifry s veřejným klíčem určitou daň. Tato daň spočívá především v tom, že jsou význačně pomalejší a bezpečná velikost klíče kryptosystémů s veřejným klíčem je podstatně větší než u klasických šifrovacích metod. Například pro blokové šifry (správně konstruované) je dnes za bezpečnou minimální velikost klíče považováno 90-100 bitů. Adekvátní bezpečnost např. pro RSA tvoří klíče o velikosti 900-1000 bitů. Pomalost systémů s veřejným klíčem na jedné straně a naopak jejich vhodnost pro konstrukci bezpečných kryptografických protokolů (např. pro výměnu klíče pro symetrickou šifru) vedla k dnešním modelům praktické každodenní kryptografie. Pro vlastní šifrování jsou používány rychlé symetrické šifry, zatímco systémy s veřejným klíčem tvoří jejich určitou nadstavbu. S jejich pomocí jsou konstruovány protokoly pro výměnu klíčů, slouží k autentizaci uživatelů, k vytváření digitálních podpisů atd.

Objevují se stále nové ideje, jak konstruovat systémy s veřejným klíčem. Z posledních let stojí za zmínku zejména systémy na bázi Lucasových funkcí a systém, který vyvíjí IBM (je založen na obtížnosti nalezení nejkratšího celočíselného vektoru v určité množině).

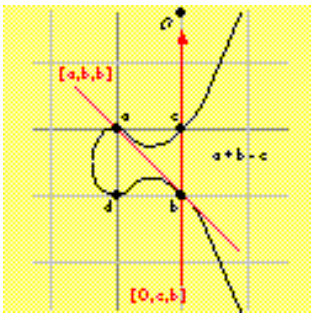
Uvedeme užívaná hodnotící kriteria pro vlastnosti systémů s veřejným klíčem:

- bezpečnost (obtížnost řešitelnosti příslušného matematického problému)
- velikost klíčů
- velikost podpisů
- rychlost
- vhodnost pro implementace v podobě hardwaru, softwaru resp. firmwaru
- náročnost implementace (objem potřebného kódu, počet cyklů, spotřeba proudu atd.),
- nároky na uložení
- průmyslové a vládní normy
- pokrytí patenty
- licenční politika

Teorie hledá především další cesty jak zlepšit vlastnosti systémů s veřejným klíčem. Jestliže v dosažené rychlosti šifrování se zatím žádné význačně změny nerýsují, je tomu jinak z hlediska velikosti použitých klíčů. V tomto směru význačná zlepšení přináší implementace nových systémů s veřejným klíčem na bázi tzv. **eliptických křivek.**

Řada současných systémů s veřejným klíčem je založena na využití operace umocňování ve velkých konečných matematických grupách. Kryptografická síla těchto systémů je odvozována ze složitosti řešení úlohy diskrétního logaritmu v těchto grupách, resp. z obtížnosti úlohy faktorizace velkých čísel na prvočísla. Obvykle jsou využívány grupy Z_p (celá čísla modulo nějaké prvočíslo p; v případě, kdy bezpečnost systému stojí jako pro RSA na obtížnosti úlohy faktorizace, je p = r.s, kde r a s jsou velká prvočísla). Nejsou to však jediné možné grupy, které lze využít pro

konstruování kryptografických systémů. V roce 1985 přišli nezávisle na sobě pánové Neil Koblitz (University of Washington) a Victor Miller (tehdy IBM, Yorktown Heights) s návrhem využívat pro kryptografické účely grupy na eliptických křivkách. Bezpečnost těchto systémů opět závisí na obtížnosti řešitelnosti úlohy diskrétního logaritmu v těchto grupách. Dokonce nejsou pro tyto logaritmy známy žádné subexponenciální algoritmy (jako pro klasický diskrétní logaritmus, resp. úlohu faktorizace), nejlepší algoritmy mají plně exponenciální charakter (platí pro obecné křivky, nikoliv však pro některé speciální podtřídy eliptických křivek).



Primární výhodou kryptosystémů na bázi eliptických křivek je jejich velká kryptografická bezpečnost vzhledem k dané velikosti klíče. Význačně kratší délka klíčů (např. oproti RSA) vede ke kratším certifikátům i menším parametrům systému a tedy i k větší výpočetní efektivnosti algoritmů. Druhá výhoda je v tom, že fakticky všechna již známá použití v systémech na bazi diskrétního logaritmu (kryptografické protokoly, ElGamalův podpis atd.) lze převést do systémů na bázi eliptických křivek. To se podařilo zejména při převodu normy DSA na ECDSA.
V praxi jsou používány algoritmy pro eliptické křivky v polích F_p , kde p je rovno buď prvočíslu nebo číslu 2^m pro nějaké přirozené číslo m. V polích, kde je $p = 2^m$ existují v zásadě dva typy eliptických křivek. Prvním typem jsou tzv. supersingulární křivky, které mají rovnici:

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

Supersingulární křivky mají tu výhodu, že pro ně snadným výpočtem lze stanovit řád křivky. Jak ukázali A. J. Menezes, T. Okamoto a S. Vanstone (MOV attack) lze vhodnou konstrukcí úlohu diskrétního logaritmu pro tyto eliptické křivky převést na úlohu klasického diskrétního logaritmu (s určitým koeficientem B). Proto také tyto křivky v současnosti nejsou navrhovány pro konstrukci kryptosystémů.

Druhým typem jsou tzv. nonsupersingulární křivky s rovnicí:

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

Obecně platí, že pro tyto křivky je matematicky dosti obtížnou úlohou stanovení jejich řádu.

Speciální podtřídou jsou tzv. Koblitzovy křivky. To jsou křivky E_0 a E_1 definované rovnicí:

$$E_a : \quad y^2 + xy = x^3 + ax^2 + 1.$$

Pro tuto třídu existuje jednoduchá metoda výpočtu počtu bodů křivky (řád křivky). Co činí Koblitzovy křivky atraktivními je kromě snadnosti výpočtu řádu křivky také fakt, že pro tyto křivky jejich kardinalita může být pro určitá m jednoduše rozložitelná (kromě velkého prvočísla rozklad řádu obsahuje již jen velmi malé číslo). V praxi kromě určitého zobecnění Koblitzových křivek (tzv. CM křivky, křivky s komplexním násobením) jsou ještě využívány křivky jejichž kardinalita (počet bodů na křivce) je počítána užitím tzv. Weilovy věty.
Problematika bezpečnosti kryptologických systémů na bázi eliptických křivek je dnes stále ještě poněkud méně prozkoumanou oblastí kryptologie. Pro RSA např. lze na základě již dlouhodobě vyvíjených algoritmů (prioritní je nyní number field sieve) poměrně exaktně zhodnotit současnou i perspektivní odolnost tohoto systému. Existující algoritmy mají subexponenciální charakter a (samozřejmě pokud nedojde k nějakému revolučnímu objevu např. pokud se nepodaří zrealizovat kvantový počítač) vylepšování jejich možností jde v zásadě ruku v ruce se zvětšující se výpočetní silou, kterou má lidstvo k dispozici. Ve stejné situaci je i řešení úlohy diskrétního logaritmu v konečných polích.

Oproti tomu vývoj algoritmů pro řešení diskrétního algoritmu pro eliptické křivky má zatím poměrně krátkou historii. Především je třeba poukázat na skutečnost, že pro úlohu není znám žádný subexponenciální logaritmus (jako je tomu v případě obvyklého diskrétního logaritmu). Pro úlohu v obecné podobě je nejlepším známým algoritmem Pollardova ρ-metoda, jejíž složitost je $\sqrt{(\pi n/2)}$, každým jednotlivým krokem je součet na eliptické křivce. Číslo n je

zde největší prvočíselný dělitel velikosti grupy eliptické křivky. Při paralelizaci na w procesorech je očekávaný počet kroků (než získáme jeden diskrétní logaritmus) roven $\sqrt{(\pi n/2)}/w$.
Předpokládejme, že počítač provádějící jeden milion instrukcí za vteřinu může provést zhruba 4×10^4 součtů na eliptické křivce za vteřinu. Pokud použijeme 10 000 takových počítačů s rychlostí 1 000 MIPS (Million Instructions Per Second) pak například pro křivku s $n \approx 2^{160}$ může být eliptický logaritmus spočten za 96 000 roků, viz následující tabulka:

Velikost pole (v bitech)	Velikost n (v bitech)	$\sqrt{(\pi n/2)}$	MIPS roků
163	160	2^{80}	$9{,}6 \times 10^{11}$
191	186	2^{93}	$7{,}9 \times 10^{15}$
239	234	2^{117}	$1{,}3 \times 10^{23}$
359	354	2^{177}	$1{,}5 \times 10^{41}$
431	426	2^{213}	$1{,}0 \times 10^{52}$

Pokud budeme pro možný útok na systémy na bázi eliptických křivek používat speciální hardware pro paralelizaci výpočtů, je situace (pro útočníka) ještě výhodnější. Např. v [2] autoři odhadují, že pokud $n \approx 2^{120}$, pak zařízení s w = 325 000 procesory v ceně zhruba 10 000 000 dolarů spočte jeden eliptický diskrétní logaritmus asi za 35 dní. Existují ale speciální situace, kdy se úloha stává výpočetně jednodušší. Jedná se o situace, kdy je použitelný MOV attack (pro supersingulární eliptické křivky) anebo jestliže platí tzv. Anomalous condition (počet bodů křivky je roven počtu bodů pole, ve které je křivka definována).

Řada kryptologů je zatím skeptická k zavádění eliptických křivek do praxe. Poukazují zejména na malý stupeň poznání problematiky. Samotná praxe však předbíhá tuto skepsi. Bez řešení konkrétních úloh souvisejících jak s konkrétními implementacemi ECC (hledání vhodných křivek, určování jejich mohutnosti, posuzování bezpečnosti konkrétního ECC atd.) nelze předpokládat ani rozvoj příslušné teoretické baze. Určitou roli zde může hrát i setrvačné trvání na RSA (i když právě RSA comp. je jednou ze společností, která rozvíjí kryptosystémy na bazi eliptických křivek). Naopak pozitivní roli zde sehrává zejména snaha zavést obecnou normu na bazi ECC – ECDSA.
Při určování bezpečnosti (konkrétních) kryptosystémů na bázi eliptických křivek je nutné vycházet ze současného stupně poznání problematiky, resp. z některých možných extrapolací pro nejbližší budoucnost. Draft X9.62 obsahuje určité konkrétní matematické podmínky:

1. Řád použité křivky (nikoliv pole v kterém je křivka definována) by měl být dělitelný velkým prvočíslem n $>2^{160}$;
2. Měly by být splněny podmínky MOV a Anomalous (tj. ověřit, že daná křivka není supersingulární ani anomální)

Eliptické křivky navrhované pro praktické použití jsou dnes především dvojího druhu. Jednak křivky s náhodně vygenerovanými parametry a jednak jsou pro praktické použití zvažovány Koblitzovy křivky (viz také Certicom Chalenge, http://www.certicom.ca/chal/index.htm).

Pro oblasti, kde je otázka utajení zvláště citlivá (vojenství, bezpečnost státu) požadovaná velikost mohutnosti n (největšího prvočísla dělícího řád křivky) eliptické křivky vzrůstá ze 160 bitů na 180.
Uvedeme dva standartní příklady užití kryptosystému na bázi eliptických křivek.

Digitální signatura

Značení

M otevřená zpráva (kterou vysílající strana podepisuje)
d tajný klíč (dekadické číslo, $2 \le d \le n - 2$),
Q veřejný klíč (bod na eliptické křivce, $Q = (Q_x, Q_y)$)
k náhodně vygenerované číslo ($2 \le k \le n - 2$)

Průběh protokolu

I. Generování signatury:

Vysílající (podepisující) strana

1. spočte pomocí algoritmu SHA-1 hash zprávy M:

e = hash(M)

2. vygeneruje náhodné číslo k ($2 \leq k \leq n - 2$)
3. spočte bod S = kP
4. spočte $r = S_x + e \pmod q$
5. použije tajný klíč d k výpočtu $s = k - d.r \pmod n$
6. zašle přijímající straně zprávu M a podpis (r,s)

II. Verifikace signatury:

Přijímající (ověřující) strana

1. Vyhledá veřejný klíč Q vysílající strany
2. spočte bod S
   S = sP + rQ
3. spočte hash e = hash(M)
4. spočte $r' = S_x + e \pmod q$
5. přijem podpis vysílající strany tehdy a jen tehdy když r = r´

Dohoda na tajném klíči

Eliptická křivka s parametry: q,a,b,P,n
Strana U: tajný klíč d, veřejný klíč Q
Strana V: tajný klíč d´, veřejný klíč Q´

1. Strana U spočte bod R=dQ´.
2. Položí $z = x_R$ (x-ová souřadnice bodu R).
3. Konvertuje z na bitový řetězec Z.
4. Ověří délky dat.
5. Spočte výsledný klíč K ze sdílené tajné hodnoty Z pomocí určité speciální funkce („key derivation function“).

Poznámka: Totéž provádí strana V pro d´a Q (Platí R=dQ´ = dd´P = d´dP = d´Q)

Dnes řada předních světových firem implementuje do svých produktů kryptosystémy na bázi eliptických křivek. Vládní organizace v USA jako ANSI, IEEE, ISO, IETF, ATM Forum a NIST připravují normy k podpoře širokého používání eliptických kryptosystémů. Obdobně specifikace SET (Secure Electronic Transactions) ve verzi 2.0 budou obsahovat tato kryptosystémy.

Literatura:

[1] Menezes, A.J.: *Elliptic Curve Public-Key Cryptosystems*, Kluwer Academic Publishers, 1993
[2] ANSI X9.62-199x, Public Key Cryptography For The Finacial Services Industry: *The Elliptic Curve Digital Signature Algorithm (ECDSA)*, Working Draft, Novenber 1997
[3] *Standard Specifications for Public Key Cryptography* (IEEE P1363, Draft 1998)