Základy kryptografie VI.

Šifrovat?…..Rozhodně Ano!

Kryptosystémy s veřejným klíčem na bázi eliptických křivek. 2 část

Jaroslav Pinkava

1. Úvod

V první části byly popsány základní vlastnosti eliptických křivek a některé metody výpočtu řádu eliptických křivek. Dále bylo hovořeno o konstrukci eliptických kryptosystémů a posouzena bezpečnost těchto kryptosystémů. Tato část bude obsahovat stručnou charakteristiku existujících norem (draftů norem) pro problematiku kryptografických systémů s veřejným klíčem na bázi eliptických křivek a některé příklady aplikace těchto kryptosystémů (digitální podpisy, dohoda na klíči).

2. Existující normy pro eliptické křivky

Poměrně kompletní seznam norem pro eliptické kryptosystémy je obsažen na webovské stránce Certicomu (http://www.certicom.ca/stand/index.htm). V tomto přehledu se budeme orientovat zejména na normy zabývající se popisem vlastního kryptosystému na bázi eliptických křivek.

2.1. IEEE P1363

Od ledna roku 1994 fungující pracovní skupina P1363 připravila zatím nejobsažnější materiál v oblasti norem pro kryptografii s veřejným klíčem. Hlavní dokument (Standard Specifications for Public-Key Cryptography) „specifikuje obecné techniky kryptografie s veřejným klíčem, včetně definice matematických primitivů pro odvozování sdílené tajné hodnoty, šifrování veřejným klíčem a pro digitální podpisy. Rovněž specifikuje příslušné kryptografické parametry, veřejné a soukromé klíče.“ Materiál definuje tři rodiny kryptografických technik: techniky založené na úloze diskrétního logaritmu (DL), techniky založené na úloze diskrétního logaritmu pro eliptické křivky (EL) a konečně techniky založené na úloze celočíselné faktorizace. Poslední techniky přitom obsahují jak klasické RSA, tak i Rabin-Williamsův systém s veřejným klíčem. Eliptické křivky, které draft navrhuje pro používání, jsou dvojího typu. Jednak to jsou křivky definované v prvočíselném tělese a jednak to jsou křivky definované v binárním tělese. Pro generování samotných eliptických křivek a výpočet jejich řádu (pomocí Schoofova algoritmu či speciálních algoritmů např. pro tzv. Koblitzovy křivky) nechává materiál možnost využití celé škály různých postupů.

Tyto postupy umožňují vyhovět např. následujícím požadavkům:

- prokazatelná náhodnost vygenerovaných parametrů (takto mohu ubezpečit druhou stranu, že použitý kryptosystém neobsahuje žádná zadní vrátka)
- možnost efektivní implementace
- snadnost výpočtu řádu příslušné křivky.

Tyto tři požadavky si však v zásadě protiřečí a při výběru konkrétní eliptické křivky je nutné zvážit, jaký z těchto požadavků je momentálně pro nás nejdůležitější.

Základní materiál je doplněn řadou příloh. Nejvýznamnější z nich je Annex A (Number-Theoretic Background) obsahující důležité podrobnosti k implementačním technikám jednotlivých algoritmů.

V současné době jsou zmíněné materiály již v etapě schvalovacího procesu a předpokládá se, že v roce 1999 by tento proces měl být ukončen.

Práce skupiny dále pokračuje pod hlavičkou P1363a (addendum). Výsledkem této další činnosti by měla být navazující rozpracování celé řady kryptografických protokolů a souvisejících technik. Týká se to např. :

- dohoda na klíči a přenos klíčů (pro všechny tři výše zmíněné rodiny),
- šifrování dlouhých bloků
- podpisy s rozkrytím zprávy pro rodiny DL a EC
- podpisy s částečným rozkrytím zprávy
- dokazatelně bezpečné podpisy
- dodatečné kódovací a podobné techniky (např. maskovací funkce)
- další teoreticko-číselné algoritmy

2.2. ANSI X9.62, ANSI X9.63

Tyto materiály (normy pro finanční a bankovní sektor) bezprostředně navazují na práce skupiny P1363. Jsou přitom v některých směrech konkrétnější.

Draft ANSI X9.62 (oproti materiálům skupiny P1363) obsahuje definici ECDSA jako kompletního analogu americké vládní normy pro podpis DSA a dále obsahuje celou řadu konkrétních příkladů již vygenerovaných eliptických křivek (ukázány jsou parametry eliptické křivky, řád této křivky, zvolený bod na křivce, kofaktor a pro binární křivky i příslušný irreducibilní polynom). Jsou zde rovněž obsaženy i některé číselné příklady – např. pro vytváření a verifikaci digitálního podpisu – jsou vhodné zejména pro verifikaci jednotlivých implementací.

Draft ANSI X9.63 obsahuje popisy schémat pro dohodu na klíči a pro přenos klíčů. Popsané techniky pro dohodu na klíči jsou dvojího typu. Jsou to jednak techniky symetrické, kda obě strany podnikají akce zcela shodného typu a jednak techniky asymetrické, kdy je nezbytné popsat oba různé algoritmické postupy. Je přitom ukázána celá řada různých postupů vhodných pro různé praktické situace.

Schéma pro přenos klíče je používano entitou, která potřebuje přenést data popisující klíč jiné entitě. Použité techniky jsou vždy asymetrické.

2.3. SECG

V prosinci roku 1998 vznikla z iniciativy firmy Certicom a Centra pro aplikovaný kryptografický výzkum (CACR) při universitě ve Waterloo pracovní skupina Standards for Efficient Cryptography Group. Jejím prvním počinem bylo vydání dvou draftů:

SEC1: Elliptic Curve Cryptography,
GEC1: Recommended Elliptic Curve Domain Parameters.

První z těchto materiálů vychází z draftů P1363 a draftů ANSI X9.62 a X9.63. Navíc obsahuje některé testovací data vhodná pro verifikaci konkrétních implementací (např.

softwareových). Také je zde obsažena ASN.1 syntaxe algoritmických typů potřebných pro práci s eliptickými křivkami.

Materiál GEC 1 obsahuje celkem dvacet devět konkrétních vygenerovaných parametrů kryptosystémů na bázi eliptických křivek. Jsou to kryptosystémy pro čtrnáct následujích délek těles:

v prvočíselném tělese (délky prvočísel jsou pro doporučované křivky 112, 160, 256, pro doplňkové křivky 128, 192, 224 bitů),

v binárním tělese (jeho velikost je pro doporučované křivky 113, 163, 239, pro doplňkové křivky 131, 163, 193, 233, 277 bitů).

Jsou použity buď Koblitzovy křivky nebo křivky generované náhodně. V příloze materiálu je obsažena ASN.1 syntaxe pro parametry eliptických křivek a OID (object identifiers) pro tyto parametry.

2.4. NIST

V květnu 1999 vydalo NIST materiál Recommended Elliptic Curves for Federal Government Use. Materiál obsahuje numerická data celkem pro patnáct různých eliptických kryptosystémů.

V prvočíselných tělesech jsou dány data pro eliptické křivky s rovnicí:

$$y^2 = x^3 - 3x + b \qquad \text{mod } p,$$

tyto křivky mají kofaktor rovný jedné a jsou generovány náhodně. Délky příslušných pěti prvočísel jsou 192, 224, 256, 384 a 521.

V binárních tělesech jsou dány data pro eliptické křivky dvou typů. Jednak to jsou náhodně generované eliptické křivky s rovnicí

$$y^2 + xy = x^3 + x + b \qquad \text{mod } 2^m$$

Kofaktor pro tyto křivky je roven 2.

Jednak to jsou Koblitzovy křivky s rovnicí

$$y^2 + xy = x^3 + ax + 1 \qquad \text{mod } 2^m$$

kde kofaktor je roven 2, pokud a = 1 a kofaktor je roven 4, pokud a = 0.

Oboje křivky mají vygenerované parametry v tělesech o délce 163, 233, 283, 409 a 571 bitů. Pro náhodné křivky je dána jak jejich polynomiální reprezentace tak i reprezentace pomocí normální báze. Pro Koblitzovy křivky je dána reprezentace pouze pomocí normální báze.

Součástí materiálu je popis postupů pro efektivní implementaci eliptických křivek, jejichž parametry materiál obsahuje.

3. Dohoda na klíči při využití systému s veřejným klíčem na bázi eliptických křivek.

Následující příklad je obsažen rovněž v materiálu „Úvod od kryptologie“ na webovské stránce AEC (http://www.aec.cz).

Cílem celého postupu dvou zúčastněných stran (strana A a strana B) je dohodnout se na klíči pro symetrickou šifru, pomocí něhož pak bude probíhat vlastní utajené spojení.

1) Strany A a B se dohodli na užívaní kryptosystému s eliptickou křivkou s parametry **(q, a, b, r, G)**. Zde:
   q je velikost tělesa ve kterém je křivka definována,
   a, b jsou paramery v rovnici křivky,
   G je zvolený bod na eliptické křivce,
   r je prvočíselný dělitel řádu křivky.
   Tyto parametry jsou veřejné.
2) Dále strana A zvolí svůj soukromý klíč s a spočte svůj veřejný klíč **U = sG**.
   Obdobně strana B zvolí svůj soukromý klíč t a spočte svůj veřejný klíč **V = tG**.
3) Strana A spočte sdílenou tajnou hodnotu z následovně:
   Nejprve spočte bod **P = sV**, potom **z =x_p** (**x**-tá souřadnice bodu **P**).
4) Stran B si obdobně spočte sdílenou tajnou hodnotu z takto:
   Spočte bod **Q = tU** a pak **z = x_Q** (**x**-tá souřadnice bodu **Q**) - neboť platí **Q = tU = tsG = s(tG) = sV = P**.
5) Strany A a B jsou dohodnuty na hodnotách parametrů $\mathbf{h_i}$ (lze i veřejnou cestou).
6) K výpočtu hodnot jednotlivých klíčů je použita funkce pro odvození klíčů:

$$\mathbf{K_i = hash\ (z \mid\mid h_i)}$$

   Jako hashovací funkce je použita např. SHA-1.

Poznámka: V popisu protokolu jsou vynechány některé detaily - formáty a délky jednotlivých veličin.

Celý postup má (např. oproti obdobným postupům využívajícím algoritmus RSA) následující velice užitečnou vlastnost. Pokud obě strany získaly bezpečnou cestou (např. prostřednictvím digitálního certifikátu od certifikační autority) veřejné klíče opačných stran, pak v průběhu výše uvedeného postupu již spolu nemusí nijak komunikovat a přesto výsledkem postupu je dohodnutý tajný klíč pro symetrickou šifru.

4. Závěr.

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.

Normy pro kryptosystémy na bázi eliptických křivek se ještě stále vyvíjí (materiál NIST pochází z května 1999). Současné úsilí směřuje jednak do oblasti návrhu konkrétních parametrů eliptických kryptosystémů – to je důležité zejména z hlediska interoperability (kompatibility) různých implementací. Jednak jsou rozpracovávany metody pro efektivní implementace těchto kryptosystémů a rovněž tak se tvůrci norem zabývají navazujícími problematikami (dohoda na klíči, přenos klíče, různé varianty digitálních podpisů atd.).

Slovník kryptologických pojmů:

ECDSA: The Elliptic Curve Digital Signature Algorithm – název použitý v normě ANSI X9.62-1998, Public Key Cryptography For The Financial Services Industry (analog normy DSA)

Terminologie použitá v draftu normy IEEE P 1363:

ECKAS-DH1 : Schéma pro dohodu na klíč s využitím eliptického kryptosystému, Diffie-Hellmanova verze, každá strana má k dispozici jednu dvojici klíčů (veřejný a soukromý)

ECKAS-DH2 : Schéma pro dohodu na klíč s využitím eliptického kryptosystému, Diffie-Hellmanova verze, každá strana má k dispozici dvě dvojice klíčů (veřejný a soukromý)

ECKAS-MQV: Schéma pro dohodu na klíč s využitím eliptického kryptosystému, Menezes-Qu-Vanstone verze, každá strana má k dispozici dvě dvojice klíčů (veřejný a soukromý)

ECSSA : Podpisové schéma s přívěškem na bázi eliptických křivek. Může využívat dva typy kryptografických primitivů:

ECSP-DSA: DSA podpisová varianta (resp. ECVP-DSA pro verifikaci)

ECSP-NR: Nyberg-Rueppelova podpisová varianta (resp. ECVP-NR pro verifikaci podpisu)

Některé zajímavé WWW stránky:

http://www.secg.org/
Standards for Efficient Cryptography Group

http://www.certicom.com
přední světová firma v oblasti eliptických křivek

http://www.ietf.org/html.charters/pkix-charter.html
přehled draftů skupiny pkix, obsahuje i metodiku práce s ECDSA

http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-13.html
příprava draftu PKCS pro práci s eliptickými křivkami