Kryptologie pro praxi – použití ECC

V minulém čísle *ST* jsme si uvedli principy konstrukce eliptických křivek nad tělesem GF(p). V tomto dílu si ukážeme, jak se používají k šifrování a digitálnímu podpisu. Příklad je uveden v *tabulce 1*.

Diskrétní logaritmus

Šifrování a podepisování na eliptické křivce se opírá o tzv. problém diskrétního logaritmu. Vezměme si třeba náš bod P=(13, 16) ∈ E a generujme posloupnost P, [2]P, [3]P, [4]P, [5]P, ..., čímž dostáváme postupně další body na křivce E. Bodů na křivce je ovšem jen konečný počet, který označujeme jako #E a nazýváme *řádem křivky*. Po určitém počtu kroků se nám proto musí uvedená posloupnost zacyklit. Označme bod zacyklení [m]P. Potom existuje nějaké n, 1≤n<m, pro které platí [m]P=[n]P, přičemž [n]P je nějaký předchozí bod naší posloupnosti. Označíme-li r=m–n, pak můžeme psát [r]P=[m–n]P=[m]P–[n]P=O, takže [r]P=O. Všimněme si, že 1≤r<m, takže bod [r]P je nutně sám v posloupnosti P, [2]P, [3]P, [4]P, [5]P, ..., [m]P také obsažen. Vidíme, že v každé posloupnosti P, [2]P, [3]P, [4]P, ... se vždy nakonec objeví bod O. Po něm přičtením P začíná cyklus znovu neboť O+P=P. Nejmenší takové r, pro něž je [r]P=O, nazýváme *řád bodu P*. V našem příkladu jsem viděli, že bod P=(13, 16) měl řád r=7. Lze dokázat, že řád bodu dělí řád křivky (v našem příkladu je #E=28=2^2.7=4.r). Různé body na křivce mohou mít různý řád. V kryptografických schématech ale obvykle používáme takový bod, jehož řád r je roven největšímu prvočíslu v rozkladu čísla #E. Hodnotu celočíselného podílu #E/r pak nazýváme kofaktor a snažíme se, aby byl co nejnižší. Například pro r=7 má naše křivka kofaktor 4. U bodu prvočíselného řádu r máme zaručeno, že v posloupnosti P, [2]P, [3]P, ... dojde k zacyklení až po $r$tém kroku (P=[r+1]P), kde r je obvykle voleno velmi velké, například řádově 2^{256}.

Nyní zvolíme tajné číslo k (byl by to náš privátní klíč) a vypočteme bod Q=[k]P. Body P a Q a popis křivky můžeme nyní zveřejnit – budou součástí našeho veřejného klíče. *Problém diskrétního logaritmu* (DLP – Discrete Logarithm Problem) je úloha požadující ze znalosti bodů P, Q určit číslo k tak, aby Q=[k]P. Pro malý řád bodu P je tato úloha triviální, neboť vyzkoušíme všechny hodnoty 1≤k<r tím, že procházíme postupně celou posloupnost [2]P, [3]P, [4]P, [5]P a sledujeme, zda a kdy se dostaneme do bodu Q. Pro velká r je to však úloha, kterou matematici už nedovedou efektivně (v polynomiálním čase) řešit. Proto body P a Q můžeme zveřejnit, neboť z nich nikdo neumí tajné číslo k v dohledné době určit. Dosud nejúčinnější obecná metoda na řešení této úlohy je tzv. Pollardova ρmetoda, jejíž složitost je řádově $(\pi.r/2)^{1/2}$ kroků. Pokud je r=2^{256}, dostáváme asi 2^{128} kroků, což je z výpočetního hlediska dnes dostatečně bezpečná bariéra. Proto říkáme, že kryptosystém založený na tomto problému diskrétního logaritmu je *výpočetně bezpečný*. Úloha DLP na naší eliptické křivce by mohla být tato: zveřejníme body P=(13, 16) a Q=(17, 20). Jaké je k? Odpověď je, jak snadno zjistíme, k=3. Podobně jako s tělesem GF(p) můžeme pracovat i s křivkou nad tělesem GF(2^m), je zde jen jiná rovnice křivky a jiný předpis pro sčítání bodů. Pro předvedení vlastností křivek zůstaneme proto u našeho GF(p).

Tabulka 1 Výběr křivky (křivka P-192 z FIPS PUB 182-2)

ECDSA

E: $y^2 \equiv x^3 - 3x + b \pmod p$
prvočíselný modul
p=6277101735386680763835789423207666416083908700390324961279
prvočíselný řád křivky
#E = r = 6277101735386680763835789423176059013767194773182842284081
kofaktor = 1
parametr b křivky E:
b = 64210519 e59c80e7 0fa7e9ab 72243049 feb8deec c146b9b1 (hex.)
bod P = (x_P, y_P):
x_P = 188da80e b03090f6 7cbf20eb 43a18800 f4ff0afd 82ff1012 (hex.)
y_P = 07192b95 ffc8da78 631011ed 6b24cdd5 73f977a1 1e794811 (hex.)

Generování klíče:
– zvolíme bod P ∈ E řádu r
– zvolíme náhodně privátní klíč – celé číslo d ∈ [1, r–1]
– vypočteme veřejný klíč (bod) Q = [d]P
– veřejný klíč spolu s veřejnými parametry je čtveřice (E, P, r, Q)

Vytvoření podpisu zprávy m:
– zvolíme náhodně číslo k ∈ [1, r–1]
– vypočteme bod [k]P = (x_1, y_1) a číslo a = x_1 mod r
– je-li a = 0, pak generujeme jiné číslo k
– vypočteme k^{-1} mod r, b = k^{-1} {h(m) + da} mod r, kde h je hašovací funkce
– je-li b = 0, pak se vrátíme ke generování nového k
– podpisem zprávy m je dvojice čísel (a, b)

Ověření podpisu:
– obdržíme zprávu m a její podpis (a, b)
– získáme veřejný klíč podepisujícího (E, P, r, Q)
– ověříme, že a, b jsou z intervalu [1, r–1]
– vypočteme w = b^{-1} mod r a h(m)
– vypočteme u_1 = h(m)w mod r a u_2 = aw mod r
– vypočteme $[u_1]P + [u_2]Q = (x_0, y_0)$ a v = x_0 mod r
– podpis prohlásíme za platný, právě když v=a

Šifrování

Podobně jako u jiných schémat asymetrické kryptografie nešifrujeme s eliptickou křivkou většinou přímo data, ale dohadujeme si s protistranou klíč pro jejich symetrické šifrování. Ukážeme si to na algoritmu, který se nazývá Diffieho-Hellmanův algoritmus na eliptické křivce (ECDH), a to proto, že postup je stejný jako u klasického Diffieho-Hellmanova protokolu dohody na klíči (viz *ST* 5/2004). Mění se jen algebraická struktura, s níž pracujeme. Pomocí ECDH si strany A a B ustavují tajný sdílený klíč na nechráněném komunikačním kanálu. Předpokládejme, že každá ze stran má k dispozici veřejný klíč protistrany a navíc, že obě strany sdílejí stejnou křivku E a stejný bod P ∈ E. Označme si d_A privátní klíč strany A (je to celé číslo) a Q_A(=[d_A]P) její veřejný klíč (bod křivky) a analogicky zaveďme i d_B a Q_B(=[d_B]P) pro stranu B. Potom si obě dvě strany mohou ustavit společný tajný klíč – bod Z na křivce E. Dokonce spolu nemusí ani komunikovat, takže tento systém je vhodný i pro off-line spojení, například posílání šifrovaných e-mailů. Strana A vypočte bod Z jako [d_A]Q_B a strana B jako [d_B]Q_A. Snadno nahlédneme, že tyto body jsou stejné, neboť Z=[d_A]Q_B=[d_A] ([d_B]P)=[$d_A d_B$]P a současně Z=[d_B]Q_A=[d_B]([d_A]P)=[$d_B d_A$]P. Bod Z ovšem nezná nikdo jiný, než strany A a B, neboť veřejně je k dispozici pouze P spolu s Q_A(= [d_A]P) a Q_B(= [d_B]P), což

jsou přesně vstupní hodnoty pro DLP. Z xové souřadnice bodu Z pak obě strany odvodí tajný symetrický klíč například pro chráněné spojení nebo e-mail, a to pomocí různých technik podle konkrétního systému, kde je ECDH použit.

Šifrování off-line

Pokud jedna z komunikujících stran nemá veřejný klíč založený na stejné křivce a bodu jako protistrana, vůbec to nevadí. Například odesílatel šifrovaného e-mailu si z veřejného klíče adresáta vezme jeho bod *P* a křivku *E* a „ad hoc“ si vytvoří svůj klíčový pár pro tuto křivku. Svůj veřejný klíč (bod *Q*) pak společně se zašifrovanou zprávou pošle protistraně a vše funguje jako v předchozím případě.

Digitální podpis

U digitálního podpisu je situace analogická. Opět se mění jen algebraická struktura, postup zůstává obdobný. Například k algoritmu DSA existuje jeho eliptické dvojče ECDSA (Elliptic Curve Digital Signature Algorithm), oba jsou definovány ve standardu FIPS 186-2, který zmiňuje i česká vyhláška k zákonu o elektronickém podpisu. Standard definuje více křivek, zde si vybereme tu nad tělesem GF(*p*) se 192bitovým prvočíslem *p*. Parametry křivky vidíte v rámečku, společně s algoritmem vytvoření podpisu a jeho ověření.

Další informace k ECC

ECC mají velkou budoucnost, neboť jsou už ukotveny v mnoha mezinárodních normách. „Domovskou firmou“ ECC je společnost Certicom, kde pracují uznávaní tvůrci eliptické kryptografie, na jejímž webu (http://www.certicom.com) naleznete všechny potřebné informace a odkazy. Podobně jako RSA vydává standardy PKCS, standardy k ECC vydává a prosazuje komerční uskupení SECG (http://www.secg.org/). Dalším důležitým hráčem je zde pracovní skupina P1363 organizace IEEE, která definuje řadu asymetrických algoritmů, včetně těch na bázi eliptických křivek (http://grouper.ieee.org/groups/1363/index.html). Konečně nejznámější normou pro ECC je FIPS 186-2 od NIST (http://csrc.nist.gov/).

Eliptické křivky předčily RSA

V době psaní článku učinily USA rozhodnutí, že pomocí ECC je možné chránit státní tajemství až stupně SECRET a TOP SECRET. Takové cti se například RSA nedostalo. Pro ochranu utajovaných informací do stupně SECRET včetně je konkrétně možné používat tyto algoritmy (o všech jsme psali v tomto seriálu, viz [1]): pro šifrování dat AES-128 a AES-256 (FIPS 197), pro digitální podpis ECDSA (FIPS 186-2 s 256- a 384bitovými prvočíselnými řády), pro dohodu na klíčích algoritmy ECDH nebo ECMQV (návrh NIST Special Publication 800-56 s 256- a 384bitovými prvočíselnými řády), pro hašování SHA-256 a SHA-384 (FIPS 180-2). Pro ochranu utajovaných informací do stupně TOP SECRET včetně jsou to z uvedených tyto vybrané: AES-256, SHA-384 a ECC s 384bitovým prvočíselným řádem.

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

LITERATURA

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

Biometrické čipy, právo a bezpečnost

Hranice mezi právně zaručenou ochranou osobních údajů a svobod občana na straně jedné, a shromažďováním a kontrolou informací v databázích bezpečnostních složek na straně druhé, jsou trvalým ohniskem sporů odborníků – politologů, humanitních filozofů – i politických a občanských sdružení. Některé polemiky patří, pravda, spíše do kategorie žabomyších, jiné však mohou nést zárodky růstu moderního modelu totality s vážnou hrozbou pro lidstvo. Kontrola biometrických údajů má, podle rozhodnutí vlády, i v ČR snížit růst zločinnosti, zabránit šíření terorismu a přispět k celkovému zlepšení bezpečnostní situace. Návrh na zavedení biometrických prvků do cestovních dokladů byl zpracován odborníky z Ministerstva vnitra tak, aby v souladu s „Nařízením Rady EU č. 2252/2004 o normách pro bezpečnostní a biometrické prvky v cestovních dokladech vydávaných členskými státy“ garantoval bezpečnostní principy schválené poslanci Evropského parlamentu. Státy sdružující se v EU mají zavést cestovní doklady, jejichž součástí bude bezkontaktní čip obsahující biometrická data s popisem obličeje a otisků prstů. Zavedení cestovních dokladů s biometrickými prvky je podmínkou stanovenou USA pro zachování – v případě ČR zavedení – bezvízového styku s dotčenými zeměmi.

Členské státy EU jsou povinny zavést digitální fotografii do pasu do 28. 8. 2006 a otisky prstů by měly přijít na řadu někdy v polovině roku 2008. Nařízení se vztahuje pouze na nově vydávané cestovní doklady. Vláda ČR dále rozhodla, že správní poplatky za vydání cestovních dokladů s biometrickými údaji zůstanou stejné jako dosud (200 Kč). Digitální fotografie a digitalizace otisků prstů budou pořizovat přímo pracovníci úřadů pověřených vedením evidence cestovních dokladů (obecní úřady s rozšířenou působností). Otisky prstů nebudou evidovány a po uplynutí 60 dnů od vydání dokladu budou komisionálně zničeny.

Zhruba 400 zaměstnanců společnosti Lufthansa začalo na letišti ve Frankfurtu nad Mohanem testovat nový způsob odbavování a nastupování cestujících do letadel, který je založen na snímání otisků prstů. Německé aerolinie se rozhodly vyzkoušet připravovaná opatření týkající se kontroly biometrických údajů v praxi. Potřebná technologie byla vyvinuta a dodavatelsky instalována firmou Siemens Business Services za podpory dceřiné softwarové společnosti Siemens PSE. V další fázi (asi v polovině roku 2006) bude projekt Trusted Traveller převeden do reálného provozu na hlavním letišti ve Frankfurtu. Systém funguje tak, že při odbavení na terminálu jsou pasažérům sejmuty otisky prstů, které jsou následně uloženy do databáze. Otisky prstů jsou společně s informací z odbavení vytištěny v zašifrované podobě jako čárový kód na palubní lístek. Při nastupování do letadla je pak kód lístku porovnán s vlastním otiskem prstu a pokud se údaje shodují, je cestujícímu umožněn vstup do letadla.

Noh