Kryptologie pro praxi – schémata ElGamal

Ačkoliv byla *šifrovací a podpisová schémata ElGamal* ([1], [5]) prezentována kryptologem téhož jména až několik let po RSA ([5], [6]) a D-H [4], jsou dnes již na ústupu, a to zejména ve prospěch RSA, protokolu D-H a podpisového schématu DSA [3]. Posledně zmiňované schéma lze označit jako bezpečnostně podstatně vyspělejšího nástupce podpisového schématu ElGamal. Postavení protokolu D-H nebylo šifrovacím schématem ElGamal nijak otřeseno a jeho použití převládá. Přesto šifrovací schéma ElGamal nalezneme jako možnou volbu v mnoha světově rozšířených protokolech, programech a prostředcích. Jak jsme už naznačili, ElGamal představuje rodinu schémat, jejíž základní větve tvoří asymetrické *šifry a podpisová schémata*. Předesíláme, že narozdíl od podobně univerzálního systému RSA, kde jak šifrovací, tak i podpisové schéma vycházejí ze stejných základních transformací, v případě ElGamal tak dokonalou provázanost nenajdeme. V podstatě můžeme říci, že šifrovací a podpisové větve zde spojuje toliko společný problém pro jištění bezpečnosti (diskrétní logaritmus, viz [1], [5], [6]) a jméno autora.

Šifrovací schéma

Podívejme se nejprve na generování instance schématu, tj. veřejných parametrů, veřejného a privátního klíče. Veřejné parametry jsou tvořeny dvojicí (p, g), kde p je dnes alespoň 1024bitové prvočíslo a g je generátor multiplikativní grupy $\boldsymbol{Z}_p^*$. Privátní klíč x si uživatel volí jako celé číslo z intervalu $<1,p-2>$ a k němu příslušný veřejný klíč y počítá ze vztahu $y=g^x \bmod p$. Šifrování zformátované zprávy m (viz dále) probíhá následovně: Nejprve zvolíme náhodné číslo k z intervalu $<1,p-2>$ a vypočteme hodnoty $\gamma=g^k \bmod p$ a $K=y^k \bmod p$. Ne náhodou celý postup silně připomíná protokol D-H [4], neboť až sem se v podstatě nejedná o nic jiného, než o ustanovení sdíleného tajemství K v efemérní variantě D-H. To je mimochodem důvodem k tomu, proč některé aplikace nepřesně označují tuto variantu D-H jako *ElGamal key agreement* (tj. ElGamalovu dohodu na klíči). Tam, kde by v případě původního protokolu postup pokračoval odvozením symetrického klíče, kterým by se pak šifrovala vlastní zpráva, nyní následuje „multiplikativní šifrování" m jako $\delta=K*m \bmod p$. Kompletní šifrový text je pak tvořen dvojicí (γ,δ). Odšifrování kryptogramu $C=(\gamma,\delta)$ na straně příjemce technicky znamená nejprve rekonstrukci sdíleného tajemství K (proběhne na základě znalosti γ, jeho umocněním na privátní hodnotu x: $\gamma^x \bmod p=g^{kx} \bmod p=y^k \bmod p=K$), výpočet multiplikativní inverze K^{-1} ($K*K^{-1} \bmod p=1$) a nakonec odšifrování zprávy $m=\delta*K^{-1} \bmod p$. Matematicky to celé lze efektivně zapsat jedním výrazem jako $m=\delta*\gamma^{p-1-x} \bmod p$, kde x je příjemcův privátní klíč. Upozorněme, že s ohledem na algebraické vlastnosti použité „multiplikativní šifry" je nezbytné hodnotu k po použití nejen dobře utajit/zničit (viděno pohledem D-H, je to dočasný privátní klíč odesilatele, s jehož znalostí lze celé toto konkrétní spojení dešifrovat), ale také ji generovat skutečně náhodně a nezávisle pro každou zprávu.

Stejně jako v případě RSA, je zcela nezbytné výše popsaný postup doplnit ještě správným formátováním šifrované zprávy [2]. Pro ElGamal sice nemáme žádný obecně uznávaný standard, avšak můžeme využít robustní metody definované zejména pro RSA, například metodu OAEP ([2], [6]) a její následovníky.

Podpisové schéma

Jsme toho názoru, že zatímco výše popsané šifrovací schéma má ještě v současné praxi určité uplatnění (jako „konkurence" RSA, založená na jiném matematickém problému), tak původní podpisové schéma [1] již dnes s ohledem na existenci a snadnou dostupnost jeho podstatně vyspělejšího následníka DSA [3] není v praktických aplikacích už příliš vidět. Nejde o to, že by u DSA bylo něco provedeno výrazně elegantněji, ostatně tato schémata jsou si stále velmi podobná, avšak v případě DSA bylo ošetřeno několik zásadních slabin, které byly u schémat [1] a jim příbuzných v průběhu času objeveny. To je důvod, proč zde podrobnější popis vynecháme s odkazem na [5], kde je možné přehledně sledovat i samotný vývoj od ElGamal až po DSA. Připomínáme, že tímto krokem rozhodně nijak nesnižujeme teoretickou hodnotu, kterou existence podpisového schématu ElGamal pro kryptologii měla a má, avšak naším cílem je soustředit se zde na ryze praktické aspekty této oblasti.

Bezpečnost

Jak jsme už naznačili, opírá se bezpečnost ElGamalových schémat o problém diskrétního logaritmu. I zde je možné stejně jako u [3] a [4] volit, zda budeme používat multiplikativní grupu $\boldsymbol{Z}_p^*$ (odpovídá popisu výše), nebo nějakou vhodnou aditivní grupu bodů rovinné eliptické křivky. Opět i zde přitom zatím neexistuje pro přechod na eliptické křivky s ohledem na bezpečnost výraznější praktická motivace. V případě šifrovacího schématu lze také snadno dokázat ekvivalenci problému jeho luštění s problémem prolomení protokolu D-H se stejnými veřejnými parametry a klíči (tj. buď lze v dané instanci prolomit obě schémata nebo žádné z nich). Některé prameny pak poukazují na to, že věříme-li protokolu D-H, není důvod nevěřit šifrovacímu schématu ElGamal. Argumentace této hypotézy vychází z předpokladu, že pokud by někdo uměl rutinně luštit ElGamal, tak by to podle uvedeného tvrzení znamenalo, že umí rutinně luštit i protokol D-H, což se zatím nikomu nepovedlo. S ohledem na současné poznání je však nutné takové interpretace brát s určitou rezervou. Například tímto způsobem nejsou nijak vyloučeny implementační slabiny v podobě postranních kanálů, nevhodně zvoleného formátování zpráv, slabých veřejných parametrů atp., stejně jako je nikdo nevylučuje u protokolu D-H. Právě tyto aspekty mají pak v praxi nejčastěji na svědomí fatální prolomení celého systému. V tomto směru jsou schémata ElGamal v určité nevýhodě, neboť jejich definice není narozdíl od RSA, D-H či DSA ukotvena žádným široce akceptovaným a hlavně udržovaným standardem, který by transparentně reflektoval aktuální poznatky kryptoanalýzy. Bezstarostné naprogramování ElGamal podle nějaké příručky může být proto dost nebezpečné. S ohledem na to doporučujeme pečlivě zvážit jeho použití v nových aplikacích. Starší implementace by pak určitě měly být revidovány, a to zejména s ohledem na formátování zpráv, které se dříve běžně nepoužívalo, a slabé instance, což se týká zejména podpisových schémat (základní přehled viz [5]). Ta by pokud možno měla být nahrazena DSA.

Vlastimil Klíma, Tomáš Rosa,
klima@lec.cz, trosa@ebanka.cz

LITERATURA

[1] ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms, In Proc. of CRYPTO 84, pp. 10–18, 1985

[2] Kryptologie pro praxi – formátování a bezpečnost, ST č. 10/2003

[3] Kryptologie pro praxi – DSA, ECDSA, ST č. 4/2004

[4] Kryptologie pro praxi – protokol D-H, ST č. 5/2004

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

[6] Archivy: http://cryptography.hyperlink.cz a http://crypto.hyperlink.cz