Útoky

Z napadení, které šifrám hrozí, jsou dnes možná nejnebezpečnější útoky **na bázi fyzických metod**, které sledují čas provádění jednotlivých operací nebo jejich energetickou spotřebu. Tyto metody jsou poměrně nové a lze se jich obávat zejména u čipových karet. Nejvíce jsou z tohoto hlediska odolné *Rijndael* a *Serpent*, protože používají pouze booleovské operace, průchody přes tabulky a pevné bitové posuny či rotace. Chránit *Twofish* je už obtížnější a *MARS* i *RC6* jsou chráněny nejhůře, neboť se nevyhnuly operacím, jako je násobení, proměnné rotace a jiné. Další útoky jsou možné při přípravě pomocných klíčů na čipových kartách. Tam jsou na tom zase nejhůře *Rijndael*, *Serpent* a *Twofish*.

Závěr

Protože kompletní srovnání finalistů by bylo příliš dlouhé, zaměřili jsme se zde jen na jejich vybrané charakteristiky. Tipovat, který algoritmus má největší šanci vyhrát, by však i při mnohem podrobnějším přehledu asi bylo předčasné. Hledisek je totiž příliš mnoho a žádný z algoritmů nepřevyšuje ostatní ve všech kritériích. Výběr proto ještě nějakou dobu potrvá, aby se našlo co nejvíce argumentů pro vítěze.

Druhé kolo veřejného posuzování kandidátů AES začalo podle časového plánu 9. září a potrvá do 15. 5. 2000. V jeho závěru se bude v New Yorku 13. až 14. dubna příštího roku konat třetí konference AES, kde se očekává hlavní finálové klání. Do té doby vás se všemi pěti kandidáty seznámíme podrobněji. Dnes začínáme s *RC6*.

VLASTIMIL KLÍMA (*VKLIMA@DECROS.CZ*)

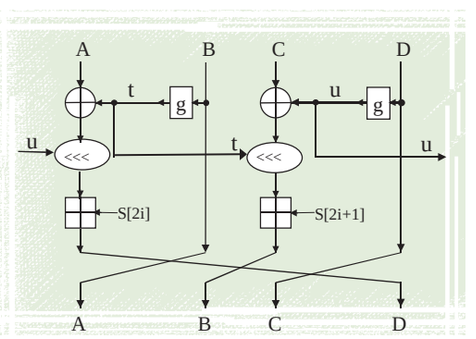
Šifrovací standard AES

Představujeme kandidáty na AES:

Šifra RC6

RC6 je jedním z pěti kandidátů na Advanced Encryption Standard (AES). O celém výběrovém řízení se podrobněji dozvíte v předcházejícím článku; zde se už věnujeme přímo technickému popisu šifry. Připomeňme jen, že AES se stane šifrovacím standardem pro příští století (nebo alespoň nějaká ta desetiletí) a bude mít dalekosáhlý vliv na počítačovou bezpečnost.

RC6 přihlásila do soutěže společnost **RSA** a její algoritmus navrhli Robshaw, Sidney a Yin (RSA) a Rivest (MIT). Myšlenkově vychází a značně těží z už dříve navržené a několika lety prověřené šifry *RC5*. Na rozdíl od jejího 64bitového bloku má ale RC6 šířku datového bloku dvojnásobnou – 128 bitů. Autoři proto postavili dvě „RC pětky“ paralelně vedle sebe a propojili je tak, aby každý bit 128bitového výstupního bloku závisel na každém bitu 128bitového vstupního bloku (viz obr. 1). K tomu mj. využili i datově závislé rotace, které RC5 zavedla jako svoji silnou kryptologickou zbraň. RC6 však do rotací navíc zanesla další nelinearitu (viz funkce **g** v obr. 1), kterou také ihned využila k posílení původních operací RC5.



Obr. 1. Jedna runda RC6.

Parametry a stavební prvky

RC6 má volitelné parametry **w** (počet bitů slova), **r** (počet rund) a **b** (počet bajtů klíče) a podle nich se také přesně označuje: *RC6-w/r/b*. Pro AES je stanoveno **w** = 32, **r** = 20, **b** volitelně 16, 24 nebo 32 – zde popíšeme právě tuto variantu. Vychází se z využití čtyř 32bitových registrů **A** až **D**, s nimiž se provádějí všechny základní operace, které umožňuje 32bitová architektura současných procesorů.

Označíme-li registry (slova) **A** a **B**, pak **A+B**, **A-B**, **A⊕B**, **A*B** znamenají běžné operace sčítání, odčítání, XOR a násobení slov (aritmetické přetečení se zanedbává). Symbolem **A<<<B** (resp. **A>>>B**) označujeme cyklickou rotaci bitů slova **A** doleva (resp. doprava) o určitý počet bitů **r**, který se rovná číslu v pěti nejnižších bitech registru **B** (**r** = **B** AND 0x1F). Zmíněná funkce **g** převádí slovo **B** na slovo g(B) = (B*(2B+1)) <<< 5. Je to neli-

neární, vzájemně jednoznačná funkce, zajišťující, že se při operaci A <<< g(B) uplatní všechny bity slova B.

Zpracování klíče

Šifrovací klíč, který má **b** (16, 24 nebo 32) bajtů, se nejprve uloží do **c** (4, 6 nebo 8) čtyřbajtových slov **L[0]** až **L[c-1]** a případně se do plné délky slov doplní nulami. Pole **L** se pak postupně stává složitějším a rozšiřuje se na pole slov **S[0]** až **S[43]**. **S** je na počátku naplněno konstantou, ale krok za krokem se „zesložiťuje“ pomocí pole **L** a naopak pole **L** se „zesložiťuje“ pomocí nově vytvořeného obsahu **S**. To vše se na polích **S** a **L** opakuje ve smyčce třikrát za sebou (viz obr. 3). Pole **L** se po konci procesu nemusí zachovat, což může být někdy bezpečnostní výhoda – jeho obsah (šifrovací klíč) totiž nelze určit jen z obsahu pole **S** (rundovní klíče). Pole **S** se využije jako rundovní klíče, přičemž první a poslední dva slouží k maskování (tzv. *whitening*) vstupů a výstupů a zbylé se po dvou postupně využijí ve 20 rundách schématu (viz obr. 2).

```
B = B + S[0], D = D + S[1]
for i = 1 to 20 do
{
    t = g(B), u = g(D)
    A = ( (A ⊕ t) <<< u ) + S[2i]
    C = ( (C ⊕ u) <<< t ) + S[2i + 1]
    (A, B, C, D) = (B, C, D, A)
}
A = A + S[42], C = C + S[43]
```

Obr. 2. Schéma zašifrování.

Rychlost a implementace

Při zašifrování se nejprve ze šifrovacího klíče vytvoří pole **S**. Otevřený text se naplní do registrů **A** až **D** a pak proběhnou operace zašifrování podle pseudokódu na obr. 2. Odšifrování probíhá trochu jinak (snadno jej odvodíte reverzí operací zašifrování), ale využívá stejné pole rundovních klíčů označené **S**. Pokud se RC6 realizuje v 32bitovém assembleru, pak se projeví výhoda zvolených operací s 32bitovými slovy: při šifrování 128bitového bloku se použije pouze 254 instrukcí a při přípravě klíče 1108 instrukcí. To na 200MHz PC znamená rychlost šifrování (v paměti) cca 12,6 MB/s. Na osmibitovém procesoru Intel MCS51 (1 MHz) se dosáhne rychlosti šifrování kolem 1,1 KB/s a příprava klíče zabere 27 milisekund. Výhodou je, že celé schéma lze realizovat na čipových kartách s méně než 256 bajty RAM (povšimněte si zejména „pouhých“ 176 bajtů pole **S**).

```
S[0] = 0xB7E15163
for i = 1 to 43
do S[i] = 0xB7E15163 + i*0x9E3779B9
A = B = i = j = 0
for s = 1 to 132 do
{
   A = S[i] = (S[i] + A + B) <<< 3
   B = L[j] = (L[j] + A + B) <<< (A + B)
   i = (i + 1) mod 44
   j = (j + 1) mod c
}
```

Obr. 3. Příprava klíče.

infotipy

Zdrojové kódy v C, ASM:
ftp://ftp.funet.fi/pub/crypt/cryptography/symmetric/rc6/
Domovská stránka AES:
http://csrc.nist.gov/encryption/aes/aes_home.htm

Bezpečnost

Návrháři tvrdí, že analyzovali celé i zjednodušené schéma a nalezli pouze lineární aproximace pro osmnáctirundovní schéma. Účinnost diferenciální analýzy (s definicí diference pomocí tradiční operace XOR i s novou definicí pomocí operace odčítání) se zastavila ještě před 18 rundami. Přípravu klíče autoři použili z RC5, kde dosud nebyly zjištěny žádné slabiny. Nejsou také známy žádné slabé klíče ani útoky pomocí příbuzných klíčů a rundovní klíče mají všechny znaky náhodnosti. NIST autorům (ve srovnání s ostatními kandidáty) vyčítá pouze malou bezpečnostní rezervu, čímž má na mysli přidání pouze dvou rund nad 18, tj. nad schéma, kde už teoreticky existují určité slabiny.

Závěr

RC6 je na první pohled elegantním a vysoce kvalitním algoritmem. Kdybych si ale mohl vybrat, pro AES bych tuto šifru volil raději s 32 rundami...

Vlastimil Klíma
(*vklima@decros.cz*)