Šifrovací standard AES

Bitva o trůn vrcholí

Výběr nového šifrovacího standardu AES pro třetí tisíciletí už je ve finále. V srpnu americký standardizační úřad NIST vybral z 15 kandidátů pět nejvhodnějších. Jeden z nich se stane standardem – který to bude, to závisí na průběhu druhého kola posuzování, jež právě začalo. V tomto a dalších číslech Chipu vás s finalisty postupně seznámíme.

V červencovém Chipu jsme vás v článku „Bitva o trůn“ (str. 52) informovali o časovém plánu NIST pro výběr AES. NIST slíbil, že uprostřed léta vybere několik finalistů, což také 9. srpna učinil. Kromě toho vydal „Zprávu o prvním kole vývoje AES“, v níž zcela otevřeně popsal svůj postup při výběru finalistů. Zpráva je, stejně jako vše kolem AES, veřejná a je k dispozici také na internetu (viz infotipy). Jména finalistů uvádíme v tabulce, kde najdete také některé vlastnosti, které NIST uvedl ve „Zprávě“, a pro porovnání připojujeme také některé rychlostní charakteristiky. Významnější poznámky NIST k jednotlivým kandidátům nejdete dále.

Rychlost a platformy

Výkon některých algoritmů podstatně závisí na architektuře procesoru. *Rijndael* a *Twofish* mají výborné výkony na všech platformách. *Serpent* je platformově nezávislý stejně jako oba uvedené, ale není tak rychlý. Naproti tomu *MARS* a *RC6* jsou platformově závislé – jsou rychlé jen tam, kde se rychle provádějí 32bitové operace násobení a proměnná cyklická rotace, ale ne jinde.

Výpočet klíčů

Všichni kandidáti používají inicializační fázi, v níž se ze šifrovacích klíčů (o podporovaných délkách 128, 192 a 256 bitů) vytvářejí pomocné klíčové proměnné (rundovní klíče, substituční tabulky ap.), které se už poté nemění, i když se šifruje velký objem dat. Se změnou šifrovacího klíče se ovšem musí vypočítat nově.
V situacích, kdy se šifrují malé objemy dat, ale rychle se mění šifrovací klíče, je pak čas na přípravu klíče významnější než čas potřebný k šifrování dat. Příkladem může být centrum platebního systému, které v jednom okamžiku odpovídá na množství klientských dotazů šifrovaných různými klíči. Z tohoto pohledu jsou *RC6* a *Rijndael* oproti ostatním rychlejší.
Jindy je výhodné, pokud šifra umožní výpočty klíčového materiálu „on-the-fly“, tj. souběžně se šifrováním dat (příkladem je tato možnost výpočtu rundovních klíčů u algoritmu DES). *MARS* a *RC6* výpočty nepodporují, zatímco ostatní ano.

infotipy

Zpráva o prvním kole vývoje AES:
http://www.nist.gov/aes
Zdrojové kódy kandidátů AES v C, ASM a další informace:
ftp://ftp.funet.fi/pub/crypt/cryptography/symmetric/

Čipové karty a paměť

Na čipových kartách, které disponují 256 bajty RAM a 2000 bajty ROM, jsou realizovatelné pouze algoritmy *Rijndael*, *Serpent* a *Twofish*. Pro *MARS* a *RC6* by vyhovovaly až karty s 512 bajty RAM a 6000 bajty ROM.

	MARS	RC6	Rijndael	Serpent	Twofish
Průměrná rychlost šifrování v Mb/s (NIST/ Gladman)	33/69	41/103	31/71	16/27	26/68
Příprava klíče v počtu hodinových cyklů (NIST/ Gladman)	5481/4316	2272/1632	6787(7467)/ 305(1389)	6953/2402	9724/8414
Autoři (stát)	IBM (USA)	RSA (USA)	Rijnmen a Daemen (Belgie)	Anderson, Biham, Knudsen (UK, Izrael, Norsko)	Schneier, Kelsey, Whiting, Wagner, Hall, Ferguson (USA)
Některé vlastnosti, které NIST u algoritmu zdůraznil	bezpečnostně orientovaný návrh, inovativní a heterogenní kryptografické jádro, použitý cyklický posun je závislý na datech i klíči, dodatečná malá modifikace popisu byla akceptována	vyvážená (nepřehnaná) bezpečnost, návrh je jednoduchý pro zapamatování i pro implementaci, nepoužívá substituční tabulky, užitá cyklická rotace je závislá na datech	bezpečnostně orientovaný návrh, výborný výkon na všech platformách, rychlá příprava klíče, malé paměťové nároky, je vhodný i pro paralelní procesory	ultrabezpečnostně orientovaný návrh, autoři dvakrát zvýšili počet iterací, o nichž si myslí, že jsou už bezpečné; proto je výkon šifry relativně nízký, velmi výhodný pro čipové karty	bezpečnostně orientovaný návrh, přizpůsobivý různým platformám, používá substituční tabulky závislé na klíči; různé možnosti předvypočítání těchto tabulek mohou zvýšit výkon