Hash rychlejší než foton?

V článku v minulém dílu Kryptologie pro praxi jsme načali téma tzv. lehké kryptografie (lightweight cryptography). Není to výtvor „pašáků“, tj. odborníků na všechno, pro které není zatěžko semtam spíchnout nějakou tu šifru nebo hash, ale úmyslně zeslabená kryptografie proto, aby se vešla do RFID čipů. V současné době vzniká kromě blokových šifer, proudových šifer i neoficiální soutěž o hašovací funkci pro RFID. Nejžhavějšího kandidáta, představeného letos v srpnu na nejprestižnější konferenci v oboru, si ukážeme právě dnes.

Zeslabené hashe

Lehká hash má poskytnout takový stupeň bezpečnosti, který je nejvyšší možný, ale zároveň proveditelný v čipech RFID. U klasické hašovací funkce, poskytující n-bitový hašovací kód, se požaduje odolnost proti nalezení vzoru se složitostí 2^n a odolnost proti nalezení kolize se složitostí $2^{n/2}$. U lehkých hashí se ustupuje z takové bezpečnosti jak u kolize, tak u vzoru, neboť u specifického použití v RFID čipech hrozba nalezení kolize nebo vzoru (přepočtená na škodu, kterou to může způsobit) není tak kritická jako třeba u digitálních podpisů. Z toho důvodu se také lehká hash uvažuje kratší než u klasické kryptografie.

Vyhraje evropsko-singapurská hash?

Opravdu vynikající návrh se jménem PHOTON vzešel z evropsko-singapurského týmu při působení dvou evropských kryptologů v Singapuru. Výsledkem je velmi silná funkce na minimální křemíkové ploše pouhých 1120 GE (GE označuje ekvivalent hradla), současný absolutní rekord v ploše i v nabízené bezpečnosti. U RFID čipů máme na kryptografickou funkci k dispozici 200–2000 GE (z celkového počtu 1000–10 000 GE pro celý čip), přičemž například SHA-1 vyžaduje 5527 GE, SHA-2 10 868 GE a všichni finalisté SHA-3 jsou nad 12 000 GE, čili naprosto nepoužitelní.

PHOTON

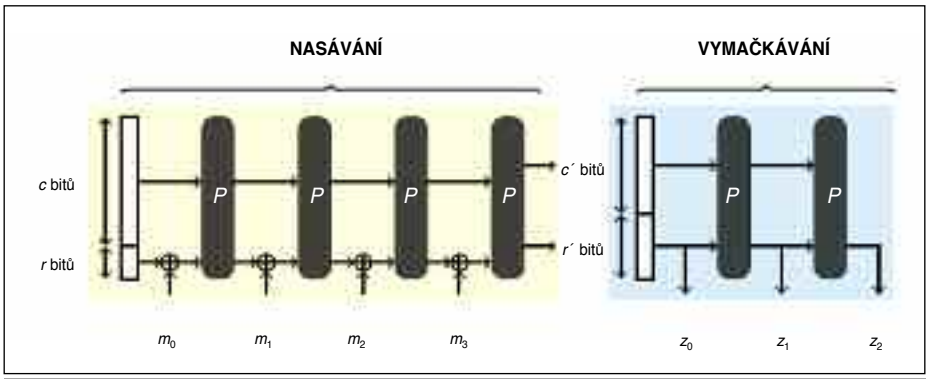
PHOTON nemá příliš velkou konkurenci, neboť dosavadní návrhy hašovacích funkcí pro RFID (ARMADILLO, QUARK, DM-PRESENT a H-PRESENT) zabírají větší plochu a ARMADILLO má i bezpečnostní problém. PHOTON vychází z AES, takže jeho bezpečnost je postavena na dobře prozkoumaných základech. Další výhodou je konstrukce typu houby („sponge“), která je momentálně velice módní, i když vznikla teprve nedávno (2007). Osobně ji nepovažuji za příliš šťastnou (právě z hlediska bezpečnosti), ale móda se projevuje i v kryptografii, a „kdo nenosí sponge, tak není in“. Konstrukci ukazuje *obr. 1*. Je na něm vidět fáze, kdy hash absorbuje po blocích (m_1, m_2, ...) zprávu m, a poté z výsledku postupně uvolňuje hašový kód. Permutace P na *obr. 1* pracuje na šířce $c + r$ bitů, kde c je tzv. kapacita a r je bitová rychlost (zpráva se zpracovává po r bitech). Na počátku se vstup naplní konstantou a zpráva postupně ovlivňuje vstupy do (pevné) permutace P. Při vyčítání hašového kódu je to podobné. Důležitý je poměr parametrů c, r, r' a n, kde n je celková délka hašového kódu. PHOTON – $n/r/r'$ je celá rodina funkcí, kde si můžeme vybrat délku hašového kódu n a podle toho jsou určeny ostatní parametry. Čím větší je n, tím větší je plocha pro tuto funkci. Volby parametrů, plochu a rychlost hašování ukazuje *tabulka 1*. Poznamenejme, že existují i varianty, kdy za cenu mírně větší plochy je možné při stejných parametrech docílit i řádově vyšší rychlost, blíže viz [1]. Pokud na hašovací funkci máme k dispozici prostředí PC, PHOTON spotřebuje na jeden bajt cca 100 taktů procesoru. V *tabulce 2* jsou měření, provedená na procesoru Intel Core i7 Q720 s 1,60 GHz, čili na PC s takovým procesorem dosahuje rychlosti cca 16 MB/s. Podobnou rychlost mají i varianty PRESENT, zatímco varianty QUARK jsou o řád pomalejší!

Tabulka 1 Charakteristiky některých hašovacích funkcí pro RFID

Hash	Délka hashe [bit]	Bezpečnost – vzor	Bezpečnost – kolize	Plocha (počet hradel, GE)	Rychlost pro krátké zprávy 96 bitů [kbit/s]
PHOTON-80/20/16	80	2^{64}	2^{40}	865	1,51
DM-PRESENT-80	64	2^{64}	2^{32}	1600	5,85
PHOTON-128/16/16	128	2^{112}	2^{64}	1122	0,69
U-QUARK	136	2^{128}	2^{64}	1379	0,61
PHOTON-160/36/36	160	2^{124}	2^{80}	1396	1,03
S-QUARK	256	2^{224}	2^{112}	2296	0,85
PHOTON-256/32/32	256	2^{224}	2^{128}	2177	0,88

Tabulka 2 Rychlosti PHOTONu v SW na procesoru Intel Core i7 Q720 s 1,60 GHz

PHOTON-80/20/16 [cyklů/B]	95
PHOTON-128/16/16 [cyklů/B]	156
PHOTON-160/36/36 [cyklů/B]	116
PHOTON-224/32/32 [cyklů/B]	227
PHOTON-256/32/32 [cyklů/B]	157



Obr. 1 PHOTON a princip houby („sponge“)

Triky

PHOTON používá dva triky, jak docílit malé plochy. Permutace P je tvořena jakoby čtyřmi rundami blokové šifry AES (v dané délce bloku $c + r$), přičemž tu nejsložitější část – matici MDS, realizuje nikoli paralelně, ale sériově. Autoři vybrali velmi jednoduchou matici, kterou realizují v jednom taktu, ale čtyřikrát za sebou. Tím dostanou matici dostatečně složitou, avšak zabírající čtvrtinovou plochu! Druhým trikem je použití S-boxů nikoli 8×8, ale 4×4 bity, které se nerealizují tabulkově, nýbrž logikou. No, a to je celé!

Závěr

Minimální nároky na paměť a maximální výkon, to jsou nové výzvy, kterým čelí tzv. lehká kryptografie. U hašovací funkce se povedl velmi dobrý návrh [1], který v minimální verzi spotřebuje pouhých 865 hradel. Neuvěřitelné!

Vlastimil Klíma,
vlastimil.klima@knzsro.cz

LITERATURA

[1] Guo, J., Peyrin, T., Poschmann, A.: The PHOTON Family of Lightweight Hash Functions. CRYPTO 2011, Springer, 2011, LNCS Vol. 6841, pp. 222–239.