Co to je lehká kryptografie?

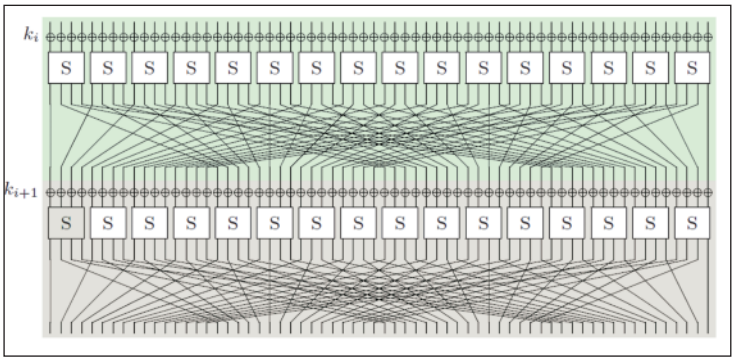
V tomto seriálu brojíme proti „pašákům“, tj. odborníkům na všechno, pro které není zatěžko semtam spíchnout nějakou tu šifru, rychle „nacpat někam AES“ nebo cokoliv nějak „zakódovat“. No a teď se najednou budeme věnovat tzv. lehké kryptografii, tj. něčemu, co pašáky silně připomíná.

Zeslabené šifry

Lehká kryptografie je opravdu zeslabená kryptografie, ale nikoli kvůli možnosti prolomení, nýbrž kvůli použitelnosti. Lehká kryptografie má poskytnout takový stupeň bezpečnosti, který je nejvyšší možný, ale zároveň proveditelný v čipech RFID. Je to něco jako taktické vojenské tajemství, které musí být chráněno velmi silně, ale jen krátce, například od naplánování útoku k jeho provedení. Musí být absolutní jistota, že toto tajemství zůstane skryto do doby útoku, ale jakmile útok začne, už je to veřejná informace. Informace, které mají být chráněny pomocí čipů RFID, musí být omezeny buď svojí důležitostí, cenou, nebo časem, který může útočník mít na prolomení, neboť pokud zeslabíme bezpečnost šifry, na něčem se to musí projevit. A současné silné šifry se do RFID prostě nevejdou. Například u blokových šifer se to projeví v tom, že lehká kryptografie bude požadovat pouze 80 bitů klíče. Nad tímto číslem je možné ohrnovat nos, ale vzhledem k chráněné informaci to může být více než dostatečné. Případný útočník by musel vynaložit velké úsilí nebo peníze na to, aby 80bitový klíč prolomil. Dosud se to nikomu veřejně nepodařilo. Připomeňme, že naposledy byl během několika let činnosti skupiny Distributed.net prolomen klíč o délce 64 bitů (pro RC5) s použitím Internetu a distribuovaných výpočtů a cca 70 tisíc převážně domácích počítačů.

Světová výzva pro kryptology

Tvrdé požadavky lehké kryptografie do čipů RFID již zahájily novou vlnu kryptografického výzkumu a velkou neoficiální světovou soutěž na nové standardy. Budou to blokové šifry, proudové šifry, hašovací funkce i asymetrická šifrovací a podepisovací schémata, integritní a autentizační kódy apod. Všechny tyto kryptografické funkce jsou sice již vyvinuty a standardizovány, ale víceméně pro oblast osobních počítačů, které se v RFID se nedají použít. RFID má omezený prostor a výkon, ale potřeba ochrany dat je neméně velká jako u světa PC. Například v oblasti proudových šifer se již na novém standardu pracuje v rámci evropského projektu eSTREAM. Během dvou let bude zahájen obdobný evropský projekt na hašovací funkce a blokové šifry. V oblasti blokových šifer dokonce už nastává dost těsno pro výzkumníky, neboť existují návrhy funkcí s téměř ideálními vlastnostmi jak pro bezpečnost, tak pro realizaci. Málo se ví o tom, že v oblasti asymetrických šifer byly již navrženy šifry, které jsou 10 000krát rychlejší než RSA!



Obr. 1 Dva cykly šifry PRESENT

Tabulka 1 Charakteristiky některých blokových a proudových šifer pro RFID

	Délka klíče [bit]	Délka bloku [bit]	Cyklů na blok	Plocha [počet GE]	Rychlost [kbit/s] @ 100 kHz	Zprac. logika [μm]
Blokové šifry						
XTEA	128	64		3490	57	0,13
HIGHT	128	64	1	6400	188	0,5
mCrypton	128	64		2500	492	0,3
mCrypton	96	64	13	2681	492	0,13
DES	56	64	144	2309	44	0,18
DESXL	184	64	144	2168	44	0,18
KATAN	80	64		1054	25	0,13
KTANTAN	80	64		688	25	0,13
PRESENT	80	64	32	1570	200	0,18
LBLOCK	80	64		1320	200	0,18
AES-128	128	128	1032	3400	12	0,35
Camelia	128	128	20	11350	640	0,35
Proudové šifry						
Trivium	80	1	1	2599	100	0,13
Grain	80	1	1	1294	100	0,13

Požadavky na blokové šifry pro RFID

Zastavíme se u blokových šifer, protože se domníváme, že jeden z následujících kandidátů bude zvolen, eventuelně s nějakou mírnou modifikací. Pokud se nenajde jiný princip než ten, který se použil kolem roku 1970 (DES) a kolem roku 2000 (AES), je počet stupňů volnosti již víceméně vyčerpán. Především je to dáno tím, že na blokovou šifru je možné spotřebovat pouze 1300–2600 hradel, přesněji prvků, ekvivalentních hradlům, což označujeme zkratkou GE (Gate Equivalent). Spotřebu hradel u známých a navrhovaných blokových a proudových šifer ukazuje *tabulka 1*. Je vidět, že i na tak malém prostoru, který poskytuje RFID, blokovou šifru zrealizovat lze. Nebude to sice AES, protože zabírá příliš velkou plochu, ani DES, protože ten má zase krátký klíč, ale máme nadějné kandidáty PRESENT a LBLOCK, na které se podíváme.

Evropská a čínská šifra – kdo vyhraje?

Asi nebude překvapením, že PRESENT vychází z AES a LBLOCK z DES. Je jasné, že bloková šifra musí být nelineární binární funkcí, jinak bychom ji hravě prolomili. Přitom jediným nelineárním prvkem u AES a DES jsou nelineární funkce, realizující tzv. substituční boxy (S-boxy). U AES jsou typu 8×8 bitů, u DES 6×4 bity (sestavené z S-boxů typu 4×4). Právě složitost S-boxů AES typu 8×8 vede k tomu, že se do RFID nevejdou (viz *tabulka 1*). PRESENT i LBLOCK proto používají S-boxy typu 4×4, jejichž nelineární funkce lze realizovat rychlou a nepříliš náročnou logikou. Tato snaha však musí být velmi dobře promyšlena, protože nelinearitu zase nelze příliš šidit z důvodu bezpečnosti. Celkovou složitost šifry tak musí dohánět počet cyklů těchto šifer, přičemž výstupní bity jdou opět na vstup S-boxů v novém cyklu. Aby čtyři bity na vstupu jednoho S-boxu nevystupovaly to téhož boxu, zařazuje se permutace z výstupních bitů tak, aby každý bit výstupu odcházel na vstup do jiného S-boxu (viz *obr. 1*). No, a pak je tu ještě klíč, který se také musí nějak účastnit této transformace, a to jednoduše. U AES i DES, u PRESENT a LBLOCK to probíhá stejně, prostě se na výsledek permutace klíč načte operací xor. Potom se už výsledek vede na vstup nového cyklu. Jak vidíme, v hradlovém poli se realizuje celkem jednoduchá struktura, a to substituce, permutace a xor s klíčem, viz *obr. 1* (jeden cyklus PRESENT).

Minimalizace

Z *obr. 1* je vidět, že 64bitový vstup musí u PRESENTu procházet 16 S-boxy typu 4×4. LBLOCK jde dále v optimalizaci a tuto strukturu aplikuje pouze na polovinu vstupu. Poté obě poloviny mixuje stejným způsobem jako DES. Tímto trikem (tzv. Feistelova struktura) ušetří polovinu nelineárních funkcí, ale složitost musí dohnat cca dvojnásobným počtem cyklů, neboli máme zde klasickou výměnu paměti za čas. Celkově tak LBLOCK spotřebovává méně hradel než PRESENT a v porovnání s ostatními algoritmy je současně i rychlý. Stává se tak horkým kandidátem na standard. Poznamenejme ještě, že obě dvě šifry mají část, která se nazývá příprava rundovních klíčů. To je proto, že vlastní klíč se musí pro každý z cyklů z kryptografických důvodů nějak upravit. Jak to udělat s co nejmenšími náklady, je podobná věda jako s vlastní „datovou mlečkou". Pokud máte zájem o podrobnosti nebo chcete navrhnout vlastní šifru, v literatuře naleznete odkazy na příslušné dokumenty.

Závěr

Minimální nároky na paměť a maximální výkon, to jsou nové výzvy, kterými čelí tzv. lehká kryptografie. Jejími výstupy budou všechny tradiční kryptografické nástroje, které však budou použitelné v čipech RFID. Horkým kandidátem na hledaný standard blokové šifry pro RFID je nyní čínská šifra LBLOCK a evropská PRESENT, resp. jejich principy.

Vlastimil Klíma,
vlastimil.klima@knzsro.cz

LITERATURA

[1] Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw M. J. B., Seurin, Y. and Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. CHES 2007, Springer, LNCS Vol. 4727, pp. 450-466.

[2] Wenling Wu, Lei Zhang: LBlock: A Lightweight Block Cipher, IACR eprint Archive, http://eprint.iacr.org/2011/345.pdf.