Lehká proudová šifra pro RFID Grain v1

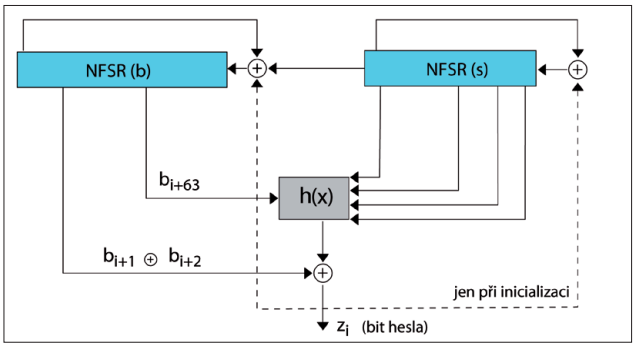
Vlastimil Klíma

V článku v čísle 12/2011 jsme se seznámili s proudovou šifrou Trivium, která má vynikající poměr plocha/výkon v oblasti čipů RFID (Trivium v Latině znamená trojcestí, nikoli triviální). Už z článku o Triviu bylo vidět, že jeho konkurent Grain v1 je natolik dobrý, že by bylo nefér ho vynechat. Navíc, nebyly prováděny komparativní testy pro SW realizaci, takže by mohl být lepší z tohoto hlediska.

Připomeneme ještě, že jsme načali téma tzv. lehké kryptografie (lightweight cryptography), což není výtvor „pašáků“, tj. odborníků na všechno, pro které není zatěžko semtam spíchnout nějakou tu šifru nebo hash. Je to úmyslně zeslabená kryptografie proto, aby se vešla do čipů RFID. Mimochodem, dost těžká věda, protože se posuzuje co nejmenší nárok na spotřebu hradel, paměti a energie a bezpečnost nesmí být menší než útok hrubou silou na klíč. Klíč se ustálil na 80 bitech, protože nejvíce hradel spotřebuje paměť právě na něco, kde se klíč „točí“, a „to“ musí mít nejméně tolik bitů jako klíč. Lehké proudové šifry by mohly mít použití nejen v RFID, ale díky HW nenáročnosti např. v Bluetooth nebo jako náhrada A5/1 v GSM apod. Grain v1 je lehký, ale silný! Než byl schválen do použití, trvalo to pět let v mezinárodní soutěži, pořádané EU. Byl to projekt eSTREAM, viz [1], probíhající v letech 2004 až 2008, kde také najdete další informace a podrobnosti o Grainu. Z původních 25 HW kandidátů zbyly a dnes patří do portfolia „schválených“ bezpečných proudových šifer 3 HW algoritmy (Grain v1, Trivium a MICKEY v2). Tyto tři algoritmy vydržely už několikátou každoroční revizi bezpečnosti, čili jsou to standardy, kterým je věnována dokonce větší pozornost, než například u standardů amerických.

Tabulka 1 Rychlost proudové šifry Grain v1

t	Počet hradel	Rychlost v hradlovém poli ALTERA		
		MAX 3000 A	MAX II	Cyclone
1	1450	49 Mbit/s	200 Mbit/s	282 Mbit/s
2	1637	98,4 Mbit/s	422 Mbit/s	576 Mbit/s
4	2010	196 Mbit/s	632 Mbit/s	872 Mbit/s
8	2756	–	1184 Mbit/s	1736 Mbit/s
16	4248	–	2128 Mbit/s	3136 Mbit/s



Obr. 1 Schéma Grain v1 – inicializace (čárkovaně) a produkce hesla (bez čárkované vazby)

$$b_{i+80} = s_i + b_{i+62} + b_{i+60} + b_{i+52} + b_{i+45} + b_{i+37} + b_{i+33} + b_{i+28} + b_{i+21} + b_{i+14} + b_{i+9} + b_i + b_{i+63}b_{i+60} + b_{i+37}b_{i+33} + b_{i+15}b_{i+9} + b_{i+60}b_{i+52}b_{i+45} + b_{i+33}b_{i+28}b_{i+21} + b_{i+63}b_{i+45}b_{i+28}b_{i+9} + b_{i+60}b_{i+52}b_{i+37}b_{i+33} + b_{i+63}b_{i+60}b_{i+21}b_{i+15} + b_{i+63}b_{i+60}b_{i+52}b_{i+45}b_{i+37} + b_{i+33}b_{i+28}b_{i+21}b_{i+15}b_{i+9} + b_{i+52}b_{i+45}b_{i+37}b_{i+33}b_{i+28}b_{i+21}.$$

Obr. 2 Nelineární zpětná vazba v NFSR

HW nároky a rychlost Grainu

Jak vidíme v *tabulce 1*, nejmenší nároky na počet hradel (měří se v jednotkách GE, tj. Gate Equivalent) potřebuje základní nezrychlená verze Grainu 1450 hradel ve všech třech typech hradlových polí, uvedených v tabulce. Jaké je taktování hradlového pole, taková je dosažená rychlost Grainu, neboť na jeden takt produkuje jeden bit hesla. V tabulce vidíme také možnosti urychlení (parametr *t*), které zabere určitý počet hradel navíc. Nárůst hradel oproti nárůstu rychlosti je však mnohem menší. V extrémním případě požadavku desetinásobného zrychlení (na cca 2 nebo 3 Gb/s) vzroste počet hradel pouze cca trojnásobně. Zrychlení se dosahuje trikem, který využívá (podobně jako u Trivia) toho, že víme dopředu, kam se posunou buňky lineárních posuvných registrů během, řekněmě, 5 taktů, a produkci hesla tak můžete predikovat najednou po pěti bitech. Je potřeba jen správně vyřešit zpětnou vazbu pro pět kroků najednou, neboť v daném schématu nejsou jen lineární posuvné registry. Počet kroků dopředu v *tabulce 1* ukazuje parametr *t*. Pro $t = 16$ tak na jeden takt dostáváme 16 bitů hesla, což při taktování 196 MHz dává pěknou rychlost přes 3 Gbit/s. Pro RFID je přesto nejdůležitější nejmenší počet hradel, což je zde vynikajících 1450 hradel.

Jak pracuje Grain v1

Grain v1 je synchronní proudová šifra, založená na tradiční kryptografické technice – lineárních posuvných zpětnovazebních registrech (LSFR) a nelineárních filtrech. Zde ve funkci filtru vystupuje, i když se to nezdá, nelineární zpětnovazebný registr (NFSR), který nelinearizuje a zároveň kumuluje zpětnou vazbu z lineárního registru přes nelineární funkci, viz *obr. 2*. Nelineární filtr pro LSFR tak tvoří *h*(x) a NFSR, přičemž NFSR zde hraje roli interní paměti tohoto filtru. Klasické proudové šifry z minulého století se konstruovaly pouze s funkcí *h*(x) bez paměti. Jako ostatní lehké nástroje, Grain v1 používá 80bitový klíč, kromě toho se na každé použití inicializuje vektorem IV o délce 64 bitů. Po fázi inicializace těmito proměnnými začíná produkovat heslo jako bitový proud, který se načítá operací xor na proud bitů otevřeného textu.

Konstrukce

Grain v1 má dva registry o délce 80 bitů, viz *obr. 1*. Buňky registru NFSR označujeme proměnnou *b*, buňky LSFR proměn-

nou *s*. Zpětné vazby registrů jsou dány vzorci z *obr. 2* a *3*. Při inicializaci se NFSR naplní bity klíče a LSFR bity IV doplněnými 16jedničkovými bity. Poté se zapojí čárkovaná zpětná vazba z *obr. 1* a schéma udělá 160 kroků, při nichž dojde v registru NFSR k promíchání klíče s IV. Poté se čárkovaná vazba vypojí a začíná se na každý takt odvádět bit hesla z_i, viz *obr. 4*. Vidíme, že do něj z NFSR vstupuje 7 bitů lineárně a jeden bit nelineárně do *h*(x). Funkce *h*(x) navíc zpracovává 4 bity z LSFR. Je to nelineární funkce 3. řádu, viz *obr. 5*.

$$s_{i+80} = s_{i+62} + s_{i+51} + s_{i+38} + s_{i+23} + s_{i+13} + s_i.$$

Obr. 3 Lineární zpětná vazba v LFSR

$$z_i = \sum_{k \in \mathcal{A}} b_{i+k} + h(s_{i+3}, s_{i+25}, s_{i+46}, s_{i+64}, b_{i+63})$$
$$\mathcal{A} = \{1, 2, 4, 10, 31, 43, 56\}.$$

Obr. 4 Výstupní bit hesla

$$h(x) = x_1 + x_4 + x_0x_3 + x_2x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4 + x_2x_3x_4$$

Obr. 5 Nelineární filtr

Závěr

Po řadě let bezpečnostního posuzování byla schválena bezpečná synchronní proudová šifra Grain v1, vhodná pro použití v čipech RFID. Je zrealizovatelná pouze pomocí 1450 hradel, a přitom za jeden takt produkuje jeden bit hesla. Zvýšíme-li počet hradel na trojnásobek, lze jednoduchým trikem zvýšit rychlost až na desetinásobek. Například v hradlovém poli ALTERA Cyclone EP1C3T100C6 při taktování 196 MHz s využitím 4248 hradel lze docílit rychlosti šifrování 3,136 Gbit/s.

LITERATURA

[1] Projekt eSTREAM, http://www.ecrypt.eu.org/stream/.