Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 14, číslo 2/2012 **15. únor**

2/2012

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info/
(1310 registrovaných odběratelů)

Obsah :

A. Československé šifry z obdobia 2. svetovej vojny Diel 10., Šifra „Utility“

Jozef Kollár, jmkollar@math.sk
KMaDG, SvF STU v Bratislave

Mnohé informácie o československých šifrách z obdobia 2. svetovej vojny mi stále chýbajú. Preto ak niekto viete doplniť, prípadne opraviť mnou uvádzané popisy šifier (TTS, Rímska 2, 8, 9, 10, 13, Eva, Marta, Růžena, Utility a Palacký), alebo máte akékoľvek informácie o ďalších československých šifrách z obdobia 2. svetovej vojny, poteší ma, ak mi o tom pošlete správu.

10 Šifra „Utility“

Šifra „Utility“, resp. v českej a slovenskej terminológii Zubatka, je typu ST. V prípade šifry Zubatka ide vlastne o nahradenie znakov dvojciferными číslami a následnú transpozíciu podľa obrazca. Túto šifru používal napríklad gen. Heliodor Píka počas svojho pôsobenia v Moskve, Chuste a Košiciach. Popis šifry Zubatka je uvedený v knihe [2] (str. 130–131) a v [5] (str. 314–332). V [5] je popísané predovšetkým lúštenie tejto šifry, ale z popisu je zrejmá napr. konštrukcia skupín služobných údajov, čo v [2] chýba.

10.1 Všeobecný popis a príklad šifrovania depeší

Pri šifrovaní sa text najskôr prepísal do číselnej podoby. Používala sa rovnaká 49 znaková česká abeceda ako pri niektorých iných šifrách, ale číselné kódy v nej boli neusporiadané. Podľa informácii z [2] bola ako substitučná tabuľka pre šifru „Zubatka“ použitá tabuľka 1, zobrazená na strane 3. Ako vidno z tabuľky, každý znak, okrem medzery, má jednoznačné vyjadrenie dvojciferným číslom. Medzera mala 5 rôznych vyjadrení, pričom týchto päť homofónov je zvolených veľmi priehľadným spôsobom. Vyjadrenie cifier 0 až 9 rovnako nebolo moc nápadité, pretože tie sa len zdvojovali. Našťastie táto šifra nebola určená na utajovanie matematických výpočtov.

Postup šifrovania predvedieme na príklade. Šifrovať budeme text:

> *Nic není ubohé, ledaže to za ubohé pokládáš, a naopak každý úděl je šťastný, snáší-li jej člověk s vyrovnanou myslí.*[1]

[1] Pôvodná verzia v latinčine: *Nihil est miserum, nisi cum putes, contraque beata sors omnis est aequanimitate tolerantis. Boethius (Cons.II,pros.4)*

A	B	C	Č	D	E	Ě	F	G	H
54	41	27	17	43	90	82	35	07	36

CH	I	J	K	L	M	N	O	P	Q
08	72	64	63	80	19	93	81	37	42

R	Ř	S	Š	T	U	V	W	X	Y
28	18	71	25	62	65	50	52	37	46

Z	Ž	.	?	:	!	,	-	/	0
73	59	47	74	38	83	29	92	56	00

1	2	3	4	5	6	7	8	9	
11	22	33	44	55	66	77	88	99	

Medzery:	01	23	45	67	89

Tabuľka 1: Česká 49 znaková abeceda pre šifru „Zubatka“

Tento text si obvyklým spôsobom prepíšeme tak, že použijeme len znaky obsiahnuté v substitučnej tabuľke. Špeciálne znaky, ktoré sa v substitučnej tabuľke nenachádzajú vynecháme. Slová sa oddeľujú buď medzerou, alebo špeciálnym znakom, t.j. za špeciálnymi znakmi sa medzera už nepíše. Dostaneme text:

```
NIC NENI UBOHE,LEDAŽE TO ZA UBOHE POKLADAŠ,A NAOPAK KAŽDY
UDĚL JE ŠTASTNY,SNAŠI-LI JEJ ČLOVĚK S VYROVNANOU MYSLI.
```

Pokiaľ ide o rozdeľovanie dlhších textov, tak v [2] sa o tom nič nepíše. Z príkladov depeší v [5] je ale zrejmé, že dlhšie texty sa rozdeľovali a posielali sa ako seriál. Vzhľadom na konštrukciu tejto šifry sa zdá byť rozumná dĺžka textu šifrovaného v jednej depeši 100–200 znakov. Znaky nadväznosti používali písmená abecedy, podobne ako sa to robilo aj pri väčšine iných československých šifier. Na koniec prvej časti sa teda písalo `/A`, na začiatok druhej časti `A/`, na koniec druhej časti `/B` atď. Náš text je krátky, takže ho nemusíme rozdeľovať a zašifrujeme ho do jednej depeše.

Okrem toho je z ukážok depeší v [5] zrejmé, že na začiatok prvej časti sa ako adresovacie znaky písalo kódové meno adresáta a na koniec poslednej

časti sa ako podpisové znaky písalo kódové meno odosieľateľa. Toto môže pomôcť lúštiteľom pri ich práci, pokiaľ sú im tieto mená už známe z iných zdrojov, alebo sa dajú predpokladať.

Text depeše už máme prepísaný len pomocou znakov zo substitučnej tabuľky. Následne sa volí heslo, ktoré použijeme pri transpozícii. Toto heslo sa vyberalo z vopred dohodnutej knihy podľa dátumu šifrovania. Heslo muselo mať najmenej 15 a najviac 20 písmen. Nepoznáme presný spôsob výberu hesla, takže pre náš príklad si zvolíme nasledovnú metódu. Na strane a riadku, ktoré zodpovedajú dňu šifrovania si vyberieme text, ktorý sa začína novým slovom a bude mať aspoň 15 písmen. Ak by 15. písmeno padlo doprostred slova, tak berieme celé toto slovo. Pokiaľ by potom heslo malo viac než 20 písmen, tak nadbytočné písmena vynecháme. Predpokladajme, že našu depešu šifrujeme 10. deň v mesiaci a ako dohodnutú knihu si zoberme: *Kryptologie, šifrováni a tajná písma* od pána P. Vondrušku (Albatros, 2006). Na strane 10 a na riadku 10 je text: *disciplínou, která*. To je 16 písmen, takže nemusíme pokračovať ďalej a tento text si zoberieme ako transpozičné heslo. Toto heslo obvyklým spôsobom vyčíslime, podľa použitej substitučnej tabuľky:

D	I	S	C	I	P	L	I	N	O	U	K	T	E	R	A
3	5	14	2	6	12	9	7	10	11	16	8	15	4	13	1

Podľa informácie z [2] sa pred šifrovaný text pridávali prvé tri znaky transpozičného hesla a bodka a na koniec textu zasa bodka a posledné tri znaky transpozičného hesla[2]. Náš text po úprave bude mať podobu:

```
DIS.NIC NENI UBOHE,LEDAŽE TO ZA UBOHE POKLADAŠ,A NAOPAK KAŽDY
UDĚL JE ŠTASTNY,SNAŠI-LI JEJ ČLOVĚK S VYROVNANOU MYSLI.ERA
```

Text na šifrovanie máme už pripravený a teraz znaky podľa substitučnej tabuľky 1 nahradíme číslami. Dostaneme depešu v tvare:

```
43727 14793 72270 19390 93722 36541 81369 02980 90435 45990
45628 16773 54896 54181 36900 13781 63805 44354 25295 42393
54813 75463 45635 45943 46676 54382 80896 49001 25625 47162
93462 97193 54257 29280 72236 49064 45178 08150 82636 77189
50462 88150 93549 38165 01194 67180 72479 02854
```

[2]Táto informácia je s najväčšou pravdepodobnosťou nesprávna, pretože takýto postup by mal opodstatnenie len ako kontrola vybraného hesla. Avšak túto kontrolu by sme mohli vykonať až po samotnej transpozícií, takže by bola zbytočná. V našom príklade to napriek tomu spravíme, ale prvé tri znaky hesla budeme považovať za kódové meno adresáta a posledné tri znaky hesla budeme považovať za kódové meno odosieľateľa.

Pokiaľ počet cifier depeše nebol násobok 5, tak sa, podľa [2], na jej koniec pridával potrebný počet núl. Tu pravdepodobne opäť dochádza ku svojskému pochopeniu pojmu nula pánom Hanákom. Vzhľadom na to, že pri zvolenej substitúcii sa na mieste desiatok a jednotiek môže vyskytnúť ľubovoľná cifra, doplníme chýbajúce cifry náhodne. Každá depeša totiž končí buď znakmi označujúcimi nadväznosť častí, alebo podpisom. Adresát teda bude vedieť náhodne pridané znaky na konci depeše rozpoznať. A naviac sa môže stať, že náhodne pridané cifry nebudú mať podľa substitučnej tabuľky vôbec žiaden význam a do textu depeše sa nepremietnu. Naša depeša má 240 cifier, takže ju dopĺňať nemusíme.

Tým je ukončená substitučná časť šifrovania a na rad prichádza transpozícia. Šírku transpozičnej tabuľky určuje počet písmen hesla. Stĺpce tabuľky budú očíslované vyčísleným heslom. Transpozičná tabuľka bude obdĺžniková a bude mať toľko stĺpcov ako má heslo písmen. Našu depešu v číselnej podobe si do transpozičnej tabuľky zapíšeme po riadkoch zľava doprava a zhora nadol:

3	5	14	2	6	12	9	7	10	11	16	8	15	4	13	1
4	3	7	2	7	1	4	7	9	3	7	2	2	7	0	1
9	3	9	0	9	3	7	2	2	3	6	5	4	1	8	1
3	6	9	0	2	9	8	0	9	0	4	3	5	4	5	9
9	0	4	5	6	2	8	1	6	7	7	3	5	4	8	9
6	5	4	1	8	1	3	6	9	0	0	1	3	7	8	1
6	3	8	0	5	4	4	3	5	4	2	5	2	9	5	4
2	3	9	3	5	4	8	1	3	7	5	4	6	3	4	5
6	3	5	4	5	9	4	3	4	6	6	7	6	5	4	3
8	2	8	0	8	9	6	4	9	0	0	1	2	5	6	2
5	4	7	1	6	2	9	3	4	6	2	9	7	1	9	3
5	4	2	5	7	2	9	2	8	0	7	2	2	3	6	4
9	0	6	4	4	5	1	7	8	0	8	1	5	0	8	2
6	3	6	7	7	1	8	9	5	0	4	6	2	8	8	1
5	0	9	3	5	4	9	3	8	1	6	5	0	1	1	9
4	6	7	1	8	0	7	2	4	7	9	0	2	8	5	4

Vyčíslenie hesla bude určovať rozdelenie stĺpcov tabuľky na hornú a dolnú časť, tak ako je to zobrazené aj v našej tabuľke. V hornej časti stĺpcov bude počet políčok zodpovedať hodnote vyčísleného hesla. Cifry budeme z tabuľky vypisovať po stĺpcoch zhora nadol tak, že najskôr vypíšeme horné časti všet-

kých stĺpcov a potom ich spodné časti.[3] Poradie stĺpcov je určené vyčísleným heslom. Cifry zapisujeme v päťmiestnych skupinách a týmto dostaneme zašifrovanú depešu:

```
12049 37144 33605 79268 57201 63125 33154 74788 34846 92969
53494 33070 47606 01392 14499 22508 58854 46968 87994 48958
72669 24553 26627 25202 76470 25602 78469 19914 53234 21940
51034 01547 31966 26855 96547 93551 30818 33324 40306 55867
47583 43279 32192 16509 91897 88584 00171 40157
```

Posledná vec, ktorú ešte musíme spraviť je pridať k depeši služobné údaje a záhlavie. Služobné údaje boli zakódované v prvých dvoch a v poslednej päťmiestnej skupine depeše. V prvej a poslednej skupine je zakódované číslo depeše a v druhej skupine je dvakrát zakódovaný dátum šifrovania. Ak prvé dve skupiny depeše budú `abcde fghij`, tak potom {`a+b b+c c+d`} je trojciferné číslo depeše a {`e+f f+g`} a {`h+i i+j`} je dvakrát zopakovaný deň šifrovania depeše. Všetky uvedené súčty sú modulo 10. Podobne, ak posledná skupina depeše má tvar `vwxyz`, tak {`v+w w+x x+y`} je číslo depeše. Toto číslo sa musí zhodovať s číslom depeše, ktoré je uvedené aj v prvej skupine a súčty sú opäť modulo 10.

Našu depešu sme šifrovali 10. deň v mesiaci a predpokladajme, že jej číslo je 056. Potom prvé dve a posledná skupina našej depeše môžu mať napríklad tvar: `82335 64473 ... 46978`. Ako záhlavie sa uvádzal len počet skupín depeše. Naša depeša bude mať výslednú podobu:

```
GR 51
82335 64473 12049 37144 33605 79268 57201 63125 33154 74788
34846 92969 53494 33070 47606 01392 14499 22508 58854 46968
87994 48958 72669 24553 26627 25202 76470 25602 78469 19914
53234 21940 51034 01547 31966 26855 96547 93551 30818 33324
40306 55867 47583 43279 32192 16509 91897 88584 00171 40157
46978
```

a tým je pripravená na odoslanie.

[3] Toto bolo neskôr (13. 12. 1944), podľa informácie z [5] (str. 332) prehodené. V neskorších variantách šifry „Zubatka“ sa najskôr vypisovali spodné a potom horné časti stĺpcov.

10.2 Postup pri šifrovaní

V tejto časti budeme vychádzať z nasledovných predpokladov:

a. Máme k dispozícii text na šifrovanie.

b. Je daný deň šifrovania.

c. Je dané 15–20 znakové heslo. V praxi sa toto heslo vyberalo z dohodnutej knihy na základe dátumu.

d. Máme dané číslo depeše. Budeme prepokladať, že depeše sa číslujú vzostupne, takže každá ďalšia depeša bude mať toto číslo o 1 väčšie než predchádzajúca.

Potom šifrovanie depeše bude prebiehať v nasledovných krokoch:

1. Text, ktorý ideme šifrovať, prepíšeme len pomocou znakov obsiahnutých v substitučnej tabuľke 1 (str. 3), čiže nahradíme písmená a vynecháme špeciálne znaky, ktoré sa v substitučnej tabuľke nevyskytujú.

2. Pokiaľ sa v texte nachádza niektorý zo špeciálnych znakov obsiahnutých v substitučnej tabuľke, tak sa za ním medzeru vynechávame.

3. Na začiatok textu ako adresovacie znaky pridáme kódové označenie adresáta a bodku a na koniec textu pridáme ako podpis kódové označenie odosieľateľa a bodku[4].

4. Text rozdeľujeme na časti dlhé 100–200 znakov. Dávame si pritom pozor, aby sme nedostali rovnako dlhé časti, pretože sa jedná o transpozičnú šifru a dala by sa pri lúštení použiť anagramová metóda.

5. Na koniec prvej časti pridáme, kvôli nadväznosti dielov `/A`. Na začiatok druhej časti pridáme `A/`, na koniec druhej časti pridáme `/B` atď. Každá časť textu (okrem prvej a poslednej) bude mať na začiatku písmeno identické s koncovým písmenom predošlej časti, znak `/` a na konci textu znak `/` a písmeno identické s písmenom označujúcim nasledovnú časť textu. Písmená na označovanie častí berieme podľa abecedy. Prvá časť má označenie len na konci a posledná časť len na začiatku.

6. Podľa tabuľky 1 nahradíme znaky depeše číslami.

[4]Toto nezodpovedá príkladu uvedenému v predošlom texte. Ten korešponduje s popisom z [2], ktorý je s najväčšou pravdepodobnosťou nesprávny. Tu uvádzaný popis je podľa príkladov depeší z [5] a je pravdepodobne správny.

7. Ak počet cifier depeše nie je násobkom 5, tak na jej koniec náhodne doplníme potrebný počet cifier.

8. Depešu zapíšeme po riadkoch do tabuľky s n stĺpcami, kde n je počet písmen hesla.

9. Obvyklým spôsobom si vyčíslime heslo podľa substitučnej abecedy a vyčísleným heslom očíslujeme stĺpce transpozičnej tabuľky.

10. Vyčíslenie hesla bude určovať rozdelenie stĺpcov tabuľky na hornú a dolnú časť. V hornej časti stĺpcov bude počet políčok zodpovedať hodnote vyčísleného hesla.

11. Cifry budeme z transpozičnej tabuľky vypisovať po stĺpcoch zhora nadol tak, že najskôr vypíšeme horné časti všetkých stĺpcov a potom ich spodné časti. Poradie stĺpcov je určené vyčísleným heslom. Cifry zapisujeme v päťmiestnych skupinách.

12. Zostrojíme tri päťmiestne skupiny služobných údajov. Prvá a tretia skupina bude obsahovať číslo depeše a druhá skupina bude dvakrat obsahovať deň šifrovania. Ak prvé dve skupiny depeše budú `abcde fghij`, tak potom {`a+b b+c c+d`} je trojciferné číslo depeše a {`e+f f+g`} a {`h+i i+j`} je dvakrát zopakovaný deň šifrovania depeše. Všetky uvedené súčty sú modulo 10. Podobne, ak tretia služobná skupina má tvar `vwxyz`, tak {`v+w w+x x+y`} je číslo depeše. Toto číslo sa musí zhodovať s číslom depeše, ktoré je uvedené v prvej služobnej skupine a súčty sú opäť modulo 10.

13. Prvé dve služobné skupiny pridáme na začiatok a tretiu služobnú skupinu na koniec zašifrovanej depeše.

14. Na začiatok depeše pridáme ešte návestie v tvare `GR xx`, kde `xx` je počet päťmiestnych skupín depeše. Týmto je šifrovanie depeše ukončené a depeša je pripravená na odoslanie.

10.3 Postup pri dešifrovaní

V tejto časti budeme vychádzať z nasledovných predpokladov:

a. Máme k dispozícii kompletný text zašifrovanej depeše.

b. Je dané 15–20 znakové heslo. V praxi sa toto heslo vyberalo z dohodnutej knihy na základe dňa šifrovania, ktorý je zakódovaný v služobných údajoch priamo v depeši.

Potom dešifrovanie depeše bude prebiehať v nasledovných krokoch:

1. Na základe návestia overíme kompletnosť depeše (počet cifier) a vynecháme návestie, pretože ho už nebudeme potrebovať.

2. Služobné skupiny depeše sú prvé dve a posledná. V prvej a poslednej skupine je zakódované číslo depeše a v druhej skupine je dvakrát zakódovaný deň šifrovanie depeše. Popis kódovania služobných skupín je v bode 12 postupu šifrovania. Po získaní čísla depeše a dňa šifrovania, všetky tri skupiny služobných údajov môžme vynechať, pretože ich už nebudeme potrebovať.

3. Transpozičná tabuľka bude mať toľko stĺpcov, koľko má dané heslo znakov. Obvyklým spôsobom vyčíslime heslo podľa substitučnej abecedy a označíme ním stĺpce transpozičnej tabuľky.

4. Podľa hodnôt vyčísleného hesla stĺpce transpozičnej tabuľky rozdelíme na hornú a dolnú časť. V hornej časti stĺpcov bude počet políčok zodpovedať hodnote vyčísleného hesla.

5. Cifry depeše vpisujeme do transpozičnej tabuľky po stĺpcoch zhora nadol. Poradie stĺpcov je určené vyčísleným heslom a najskôr vyplníme všetky horné a až potom spodné časti stĺpcov.

6. Z transpozičnej tabuľky cifry vypisujeme po riadkoch zľava doprava a zhora nadol. Potom podľa tabuľky 1 nahradíme čísla znakmi.

7. Na začiatku prvej časti depeše je kódové označenie adresáta a bodka a na konci poslednej časti depeše je kódové označenie odosieľateľa a bodka. Okrem toho tam môžu byť najviac dva náhodné znaky, ktoré boli doplnené preto, aby počet cifier depeše bol násobok 5. Adresovacie, podpisové a náhodné znaky môžme vynechať.

8. Okrem prvej a poslednej časti majú všetky ostatné časti na začiatku a na konci znaky určujúce nadväznosť častí. Prvá časť má tieto znaky len na konci a posledná len na začiatku.

9. Doplníme medzery za špeciálne znaky v texte, čím dostávame pôvodný text depeše.

10. Pokiaľ sa jedná o seriál, tak text zostavíme v správnom poradí podľa označenia na začiatku a konci jednotlivých častí seriálu.

10.4 Lúštenie

Lúštenie tejto šifry podrobne popísal pán Janeček v [5] (str. 314–332) a predvádza ho tam na príklade autentických depeší z 2. svetovej vojny.

Napriek zdanlivej komplikovanosti transpozície použitej pri šifre Zubatka je jej lúštenie jednoduchšie než pri iných, nám známych, československých šifrách využívajúcich transpozície. V tomto prípade použitá transpozícia má hneď niekoľko slabín, čo vidno aj z príkladu lúštenia v [5]. Takže na tejto šifre sa opäť raz potvrdilo, že komplikovanie postupu šifrovania nemusí viesť nutne k bezpečnejšej šifre. V praxi to platí skôr naopak, t.j. komplikovaním šifry jej bezpečnosť väčšinou oslabujeme. Keď už nie priamo, ako v prípade Zubatky, tak minimálne tým, že zvyšujeme pravdepodobnosť chyby šifrantov a dešifrantov, čo následne vyžaduje opakovaný prenos depeší, poskytuje záchytné body lúštiteľom a pod.

Okrem toho nemeckí lúštitelia boli o tejto šifre, vopred informovaní aj v depeši, ktorú z Londýna posielali do Moskvy generálovi Píkovi 13. 12. 1944 zašifrovanú už prelomenou šifrou[5]. V nej im spravodajci z Londýna popísali postup šifrovania, ako aj výber hesiel, takže na samotné lúštenie toho už veľa nezostalo.

Literatúra

[1] Grošek Otokar, Vojvoda Milan, Zajac Pavol: Klasické šifry
STU v Bratislave, 2007

[2] Hanák Vítězslav: Muži a radiostanice tajné války
Elli Print, 2002

[3] Janeček Jiří: Gentlemani (ne)čtou cizí dopisy
Books Bonus A, 1998

[4] Janeček Jiří: Odhalená tajemství šifrovacích klíčů minulosti
Naše vojsko, 1994

[5] Janeček Jiří: Válka šifer – výhry a prohry československé vojenské rozvědky (1939–1945)
Votobia, 2001

[5] Zdroj: [5], strana 332.

B. Lehká kryptografie a pár slov k hackingu

Vlastimil Klíma, kryptolog,
KNZ, s.r.o., Crypto-World.info
http://cryptography.hyperlink.cz,
vlastimil.klima@knzsro.cz

Příspěvek na konferenci SOOM.CZ Hacking & Security Konference 2012, SOOM.CZ[1], 2. února 2012, Hotel Michael, Praha.

Abstrakt. V tomto příspěvku seznamujeme s výsledky v oblasti tzv. lehké kryptografie. Představujeme blokové a proudové šifry a hašovací funkce pro oblast RFID čipů. Zamýšlíme se také nad současným a budoucím hackingem. Zmiňujeme se o oblasti postranních kanálů, opomíjeném hackingu hardwéru a vznikajícím státním hackingu.

1 Lehká kryptografie – příležitost pro hacking?

Téma lehké kryptografie vychází ze seriálu „Kryptologie pro praxi“ ve Sdělovací technice, čísla 10-12/2011 a 02/2012.

Co to je lehká kryptografie?
Lehká kryptografie (lightweight cryptography), je zeslabená kryptografie, ne kvůli zadním vrátkům a možnosti prolomení, nýbrž kvůli použitelnosti. Má poskytnout nástroje, použitelné v miniaturních čipech RFID, a současně zajistit dostatečný stupeň bezpečnosti. Omezený prostor[2] a omezená energie, dostupné v nejmenších čipech RFID, neumožňují implementovat klasickou silnou kryptografii s 256bitovou bezpečností, jako je například AES-256 nebo SHA-512. Také se sem nevejdou klasická asymetrická kryptoschémata, jako RSA apod. Avšak informace, které mají být chráněny pomocí čipů RFID, jsou často omezeny buď svojí cenou nebo časem utajení nebo časem, který mohou systémy poskytnout útočníkům na provedení útoku. A právě toho takticky využívá lehká kryptografie, která stanovila požadovanou bezpečnost na 80 bitů. Nad tímto číslem je možné ohrnovat nos, ale vzhledem k chráněné informaci to může být více než dostatečné. Případný útočník by musel vynaložit příliš velké prostředky nebo úsilí, aby 80bitový klíč prolomil, a to i dnes, přičemž zisk z tohoto útoku by nebyl adekvátní. Proto byly vyvinuty blokové a proudové šifry a hašovací funkce pro RFID s 80bitovou bezpečností. A snad budou pro RFID vyvinuta i asymetrická schémata, což je těžký problém.

[1] http://www.soom.cz/index.php?name=conference/prednasky

[2] Omezeným prostorem se rozumí velikost a požadavky na napájení. Čipy RFID mohou být různě velké, zde máme na mysli především ty nejmenší možné, mající maximálně 10 000 GE (GE - prvek, ekvivalentní hradlu). Například největší verze Spartan-3 mají 1 000 000 GE, příkon 92mW a frekvence do 500MHz. V tuto chvíli nejmenší chip má rozměr křemíkového plátku 0,05mm x 0,05mm.

Kryptografie do 2000 hradel
Tvrdé požadavky na lehkou kryptografii do čipů RFID již zahájily novou vlnu kryptografického výzkumu a neoficiální světovou soutěž na nové standardy. RFID na kryptografii poskytují pouze 1000 - 2000 hradel (se skřípěním zubů i trošičku více) z celkového počtu 1000 - 10000 hradel pro celý čip. Místo hradel se často používá pojem Gate Equivalent (GE), tj. prvek, ekvivalentní jednomu hradlu. Pro blokovou a proudovou šifru a hašovací funkci jsou už hlavní hráči představeni a jsou hlavně použitelní. V následujícím se s nimi seznámíme.

Výsledky dosavadního výzkumu
V tomto odstavci předbíháme a souhrnně uvádíme dosažené výsledky.

Funkce	Kandidát	Popis	Plocha (počet hradel, GE)	Rychlost (v jakém prostředí viz text)
Hašovací funkce	PHOTON-160/36/36	Délka hašovacího kódu 160 bitů	1396	1 kbit/s
Bloková šifra	PHOTON	Délka klíče 80 bitů	1570	200 kbit/s
Bloková šifra	LBLOCK	Délka klíče 80 bitů	1320	200 kbit/s
Proudová šifra	Trivium	Délka klíče 80 bitů	2580	240 Mbit/s
Proudová šifra	Grain v1	Délka klíče 80 bitů	1450	282 Mbit/s

Tab. 1: Stručné výsledky

Z tabulky vidíme, že se podařilo vyhovět neuvěřitelným podmínkám malé plochy a energie a vtěsnat nejpotřebnější tři kryptografické nástroje do prostoru cca 1500 hradel. Přitom dosažená rychlost těchto nástrojů je nad očekávání příznivá.

Následující kapitola se zabývá podrobnostmi těchto nástrojů.

----- pozn. pod čarou ------

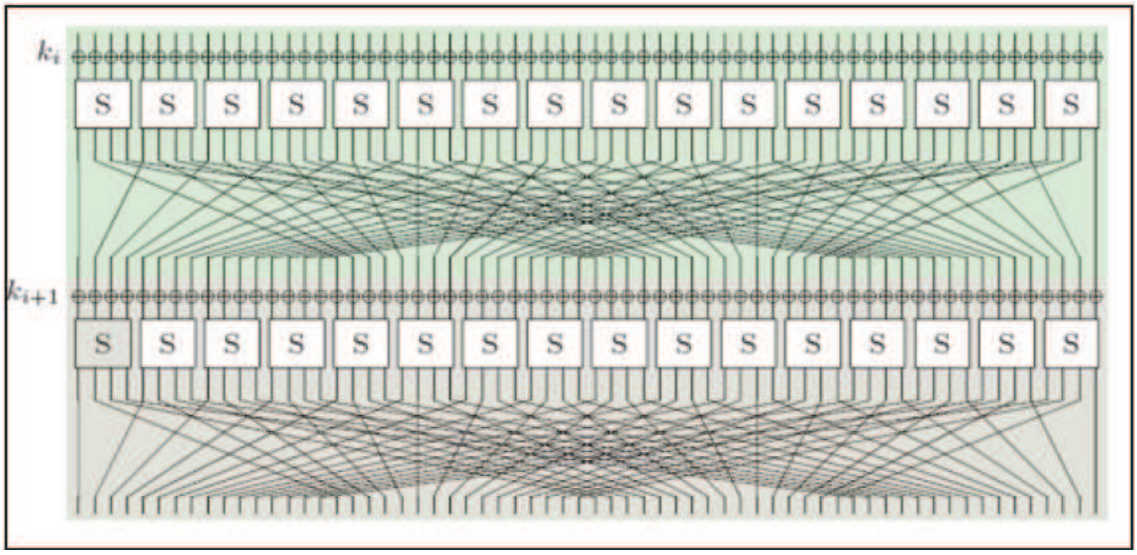
Zdroje infomací

1 Hitachi RFID powder freaks us the heck out (rekord v miniaturizaci dosahujici 0,05mm x 0,05mm) http://www.engadget.com/2007/02/14/hitachis-rfid-powder-freaks-us-the-heck-out
2 A Field Programmable RFID Tag and Associated Design Flow http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.129.9016&rep=rep1&type=pdf
3Xilinx Product and Support Documentation http://www.xilinx.com/support/index.htm
4 Altera Low-Cost Cyclone FPGA http://www.altera.com/devices/fpga/cyclone/cyc-index.jsp
5 Chinese Telecom Company Pushing For US Inroads Suspected As Spy For Chinese Military Aktivity (možnost využít i jako Moonlinght Maze, Titan Rain, Operation Aurora ...)

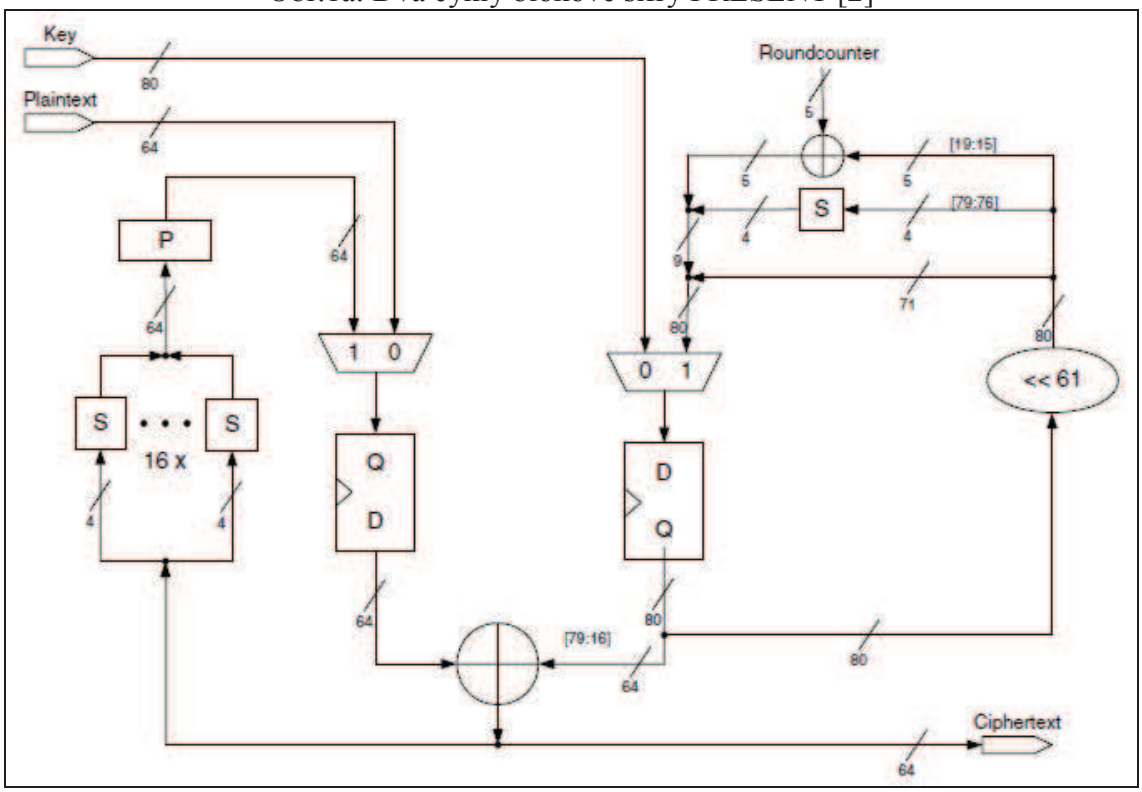
2 Existující nástroje

2.1 Blokové šifry pro RFID - PRESENT a LBLOCK

Pokud shrneme 60 let vývoje blokových šifer do několika vět, máme tady dva hlavní principy, z kterých se neustále těží – Feistelovu strukturu (vyvinuta kolem r. 1970), jejímž představitelem je DES, a substitučně permutační strukturu, jejímž představitelem je AES (2000). Pro RFID máme dnes dva kandidáty, evropský PRESENT, vycházející z AES, a čínský LBLOCK, vycházející z DES. PRESENT se připravuje jako norma ISO, zatímco LBLOCK je o 200 hradel menší.



Obr.1a: Dva cykly blokové šifry PRESENT [2]



Obr.1b: HW schéma blokové šifry PRESENT [2]

Principy
AES, DES, PRESENT i LBLOCK mají společné prvky. Všechna pracují v cyklech (10 - 32), přičemž výstup z jednoho cyklu je vstupem do dalšího. V každém z cyklů se pak na vstup přičítá klíčový materiál a výsledek vstupuje do nelineárních booleovských funkcí, tzv. substitučních boxů. Aby bity na výstupu daného S-boxu nevstupovaly v dalším cyklu do téhož S-boxu, zařazuje se za S-boxy permutace bitů tak, že každý bit výstupu odchází na vstup do jiného S-boxu. Všechny tyto šifry také používají jednoduchou úpravu šifrovacího klíče tak, aby do každé rundy vstupoval jiný klíčový materiál (tzv. rundovní klíč). Toto opatření má teoretické důvody a způsobuje, že každé schéma blokové šifry má dvě části - jednu pro přípravu rundovních klíčů a druhé pro vlastní zpracování dat, viz obrázky.

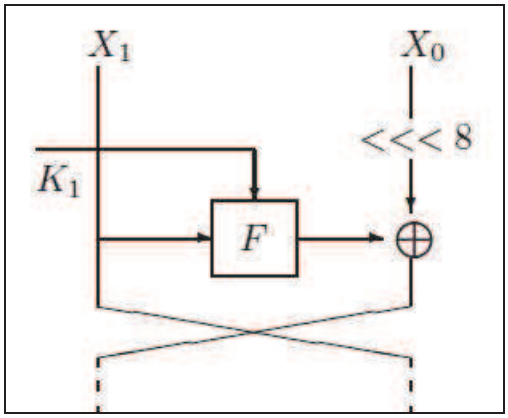
Nelineární S-boxy v RFID
S-boxy jsou jediným nelineárním prvkem u všech zmíněných blokových šifer. V SW na osobních počítačích jsou realizovány konstatními tabulkami, u RFID je však paměť drahá. S-boxy u AES jsou typu 8x8 bitů, u DES 6x4 bity (sestavené z S-boxů typu 4x4). Právě složitost S-boxů AES typu 8x8 vede k tomu, že se do miniaturních RFID nevejdou (viz tabulka 2). PRESENT i LBLOCK proto používají S-boxy typu 4x4, jejichž nelineární funkce lze realizovat nepříliš náročnou logikou. Tato snaha však musí být velmi dobře promyšlena, protože nelinearitu zase nelze příliš šidit z důvodu bezpečnosti. Celkovou složitost šifry tak může dohánět už jen počet cyklů těchto šifer (PRESENT i LBLOCK má 32 rund, AES-128 10 rund, DES 16 rund).

	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

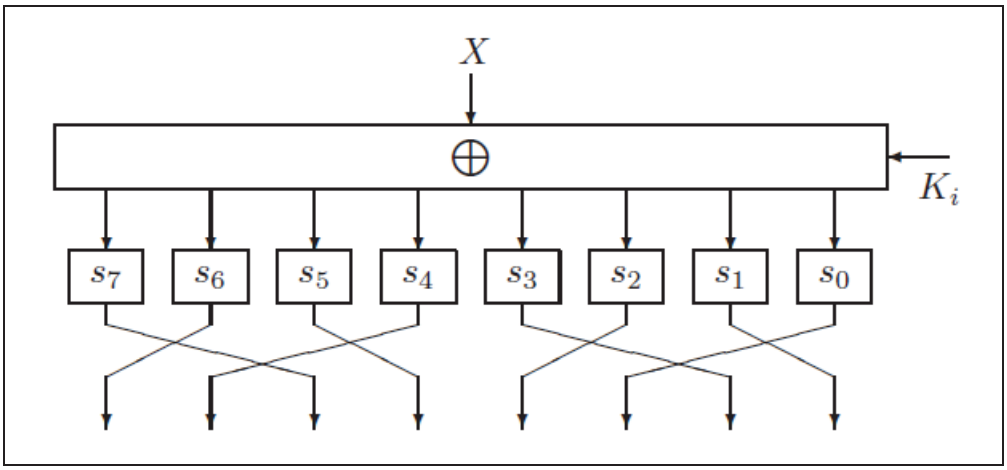
Tab.2: Charakteristiky některých blokových šifer pro RFID [2]

Minimalizace
Z obrázku 1a je vidět, že 64bitový vstup musí u PRESENT procházet 16 S-boxy typu 4x4. LBLOCK to optimalizuje a S-boxy aplikuje pouze na polovinu vstupu, což je právě prvek

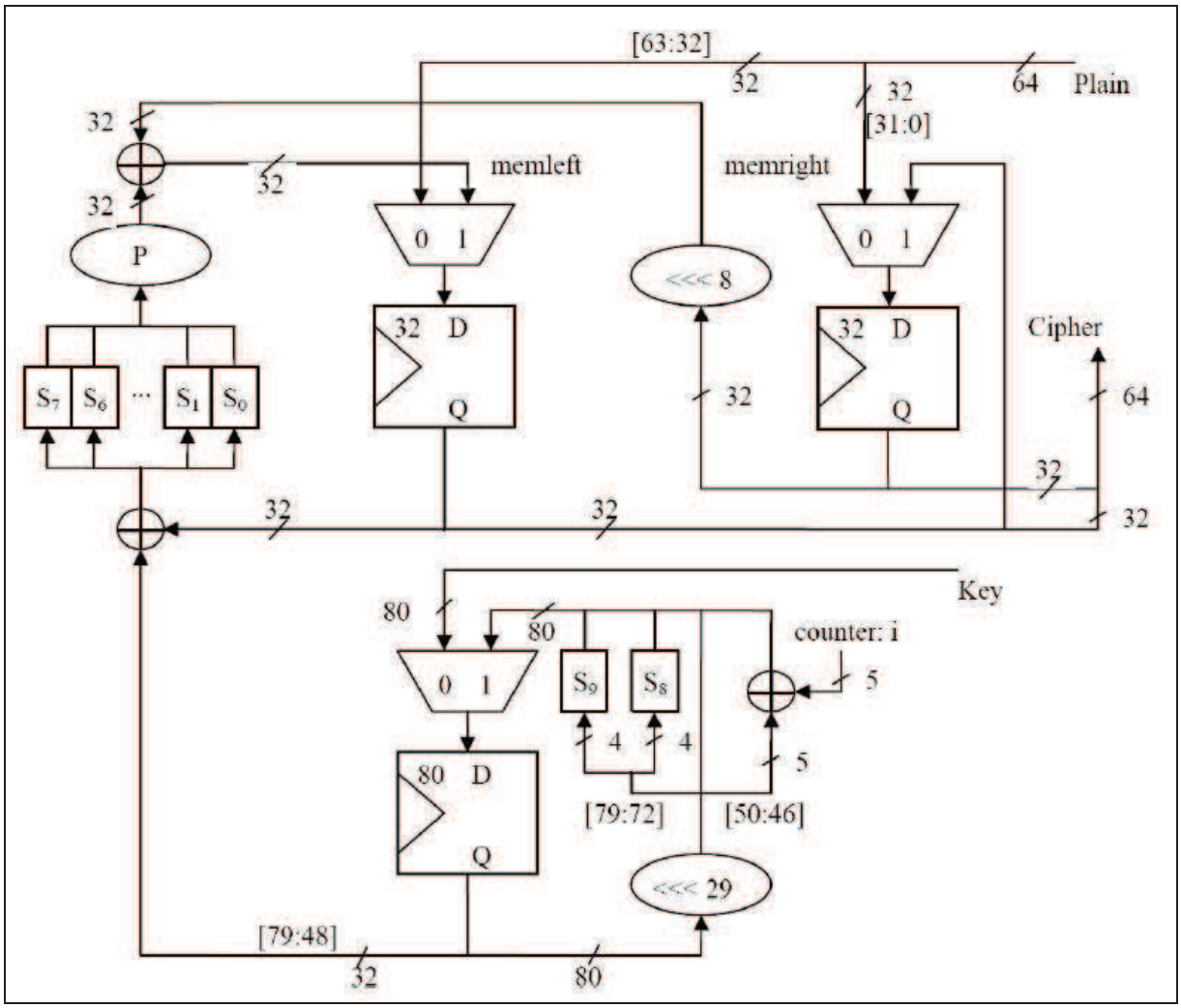
Feistelovy struktury, viz obr. 2a a 2b. Poté obě poloviny mixuje stejným způsobem jako DES. Tím LBLOCK ušetří polovinu hradel nelineárních S-boxů. Celé HW schéma LBLOCK ukazuje obrázek 2c. V tabulce 3 jsou pak ukázány možnosti výměny času za paměť. Když nebudeme lpět na vysoké rychlosti, mohli bychom LBLOCK realizovat na neuvěřitelně malé ploše 866 hradel. Z tabulky také vidíme, že možnosti, kde šetřit, jsou sice dost vyčerpány, ale že zde jsou ještě rezervy.



Obr. 2a: Feistelova struktura blokové šifry LBLOCK [3]



Obr. 2b: Funkce F blokové šifry LBLOCK [3]



Obr. 2c: Schéma blokové šifry LBLOCK [3]

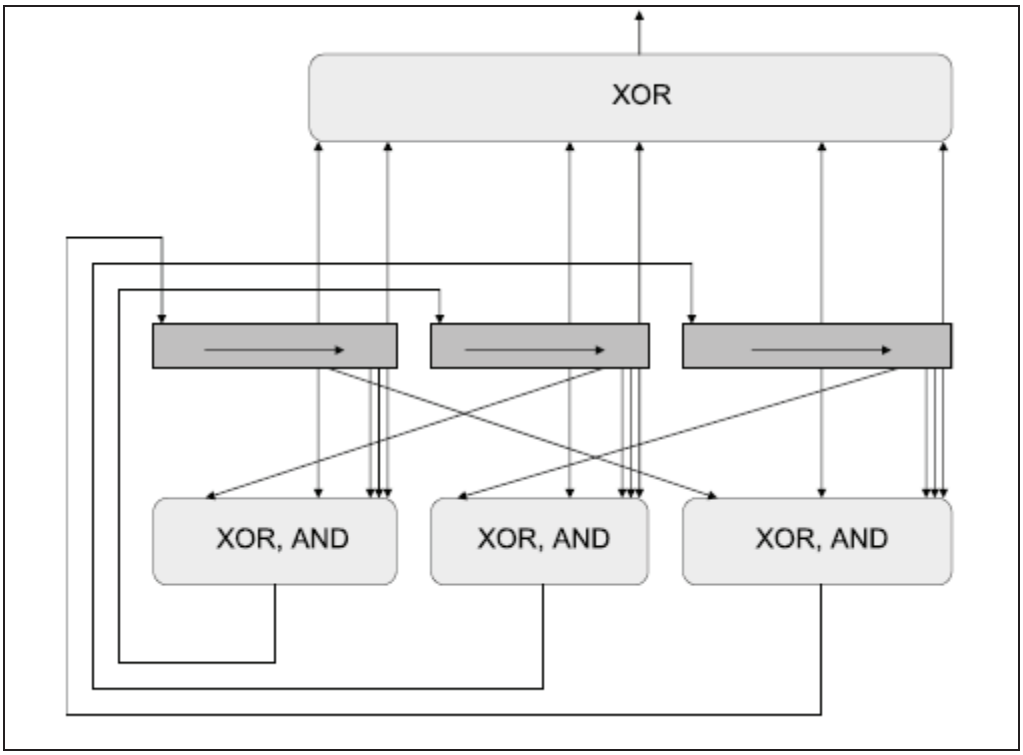
Module	Speed Optimized	Area Optimized
64-bit Data Register	384	192
Key Addition	87	87
S-box Layer	174.8	174.8
P Layer	0	0
32-bit XOR	87	87
80-bit Key Register	480	212
S-boxes (Key Scheule)	43.7	30
5-bit Constant XOR	13.5	13.5
Control Logic	50	70
Sum	1320 GE	866.3 GE (with RAM)

Tab.3: Možnosti optimalizace u blokové šifry LBLOCK [3]

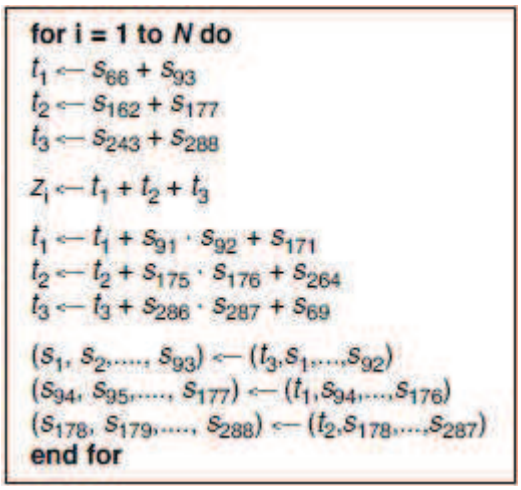
2.2 Proudové šifry pro RFID - Trivium a Grain v1

Trivium

Z kandidátů na proudovou šifru pro RFID je nejperspektivnější Trivium. V hradlovém poli Spartan 3 (Xilinx) zabírá 2580 GE a při taktování 240 MHz dává rychlost šifrování 240 Mbit/s. Má však neuvěřitelnou možnost paralelizace, kdy na ploše pouze 6,5 krát větší dosahuje rychlosti šifrování 13 Gbit/s. Trivium je provokativní šifra, posuďte sami z obrázku. Obsahuje pouze tři registry, které se vzájemně nelineárně plní a společně přispívají do výstupního bitu hesla. Celý popis Trivia je uveden na obrázcích 3a, b, c. V celé funkci jsou použity pouze tři operace AND ! Největší spotřeba hradel zde padne na paměť pro 288 buněk tří registrů.



Obr.3a: Tvorba hesla algoritmem Trivium provokuje průzračností a jednoduchostí [7]



Obr.3b: Pseudokód tvorby hesla Trivia

(*s* jsou buňky registrů, *t* meziproměnné, *z* je bit hesla) [7]

$(s_1, s_2, \ldots, s_{93}) \leftarrow (K_{80}, \ldots, K_1, 0, \ldots, 0)$
$(s_{94}, s_{95}, \ldots, s_{177}) \leftarrow (IV_{80}, \ldots, IV_1, 0, \ldots, 0)$
$(s_{178}, s_{179}, \ldots, s_{288}) \leftarrow (0, \ldots, 0, 1, 1, 1)$

for i = 1 to 4 · 288 do

$t_1 \leftarrow s_{66} + s_{91} \cdot s_{92} + s_{93} + s_{171}$
$t_2 \leftarrow s_{162} + s_{175} \cdot s_{176} + s_{177} + s_{264}$
$t_3 \leftarrow s_{243} + s_{286} \cdot s_{287} + s_{288} + s_{69}$

$(s_1, s_2, \ldots, s_{93}) \leftarrow (t_3, s_1, \ldots, s_{92})$
$(s_{94}, s_{95}, \ldots, s_{177}) \leftarrow (t_1, s_{94}, \ldots, s_{176})$
$(s_{178}, s_{179}, \ldots, s_{288}) \leftarrow (t_2, s_{178}, \ldots, s_{287})$

end for

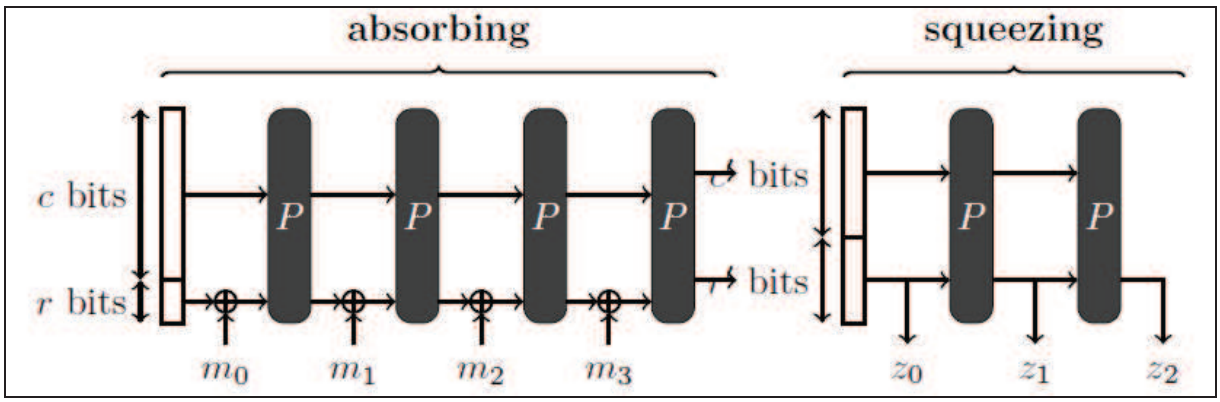
Obr.3c: Pseudokód inicializace Trivia
(*s* jsou buňky registrů, *K* je klíč, *IV* inic. vektor) [7]

Grain v1
Další kandidát Grain v1 ([8]) je ještě méně náročný na HW a ještě rychlejší než Trivium, ale nemá takovou možnost paralelizace ([1], ST 02/2012). V hradlovém poli Altera Cyclone s taktováním 282 MHz zabírá 1450 hradel a dosahuje rychlosti 282 Mbit/s. Přestože se zdá Grain v1 výhodnější, Trivium získalo zřejmě více sympatií.

2.3 Hašovací funkce pro RFID – PHOTON

Nejperspektivnější je evropsko-singapurský návrh se jménem PHOTON ([6]). Pro 80bitový výstup potřebuje 865 hradel s rychlostí hašování 1,5 kbit/s. Pro 160bitový výstup potřebuje 1396 hradel s rychlostí hašování 1 kbit/s.

PHOTON, evropsko-singapurská hash
Tento opravdu vynikající návrh vzešel z evropsko-singapurského týmu při působení dvou evropských kryptologů v Singapuru. Výsledkem je velmi silná funkce na minimální ploše pouhých 1396 GE. Pro srovnání, SHA-1 vyžaduje 5527 GE, SHA-2 10868 GE a všichni finalisté SHA-3 jsou nad 12000 GE.



Obr. 4: PHOTON a princip houby („sponge“) – má fázi nasávání a fázi vymačkávání

Konstrukce typu houby – nasát a vymačkat
PHOTON nemá příliš velkou konkurenci, navíc vychází z AES, takže jeho bezpečnost je postavena na prozkoumaných základech. Další výhodou je konstrukce typu houby („sponge“), která je momentálně velice módní (2007), viz obr. 4. Vidíme na něm fázi, kdy haš absorbuje

zprávu *m* po blocích o *r* bitech (m_0, m_1, m_2,...) a poté z výsledku postupně uvolňuje hašový kód o *r´* bitech (z_0, z_1, z_2,...). Nelineární transformace P na obrázku 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 nelineární transformace 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. Připomeňme, že 80bitové bezpečnosti odpovídá 160bitový hašový kód, čili základní verze PHOTONu je PHOTON – 160/36/36. Pokud stačí, aby nalezení kolize mělo složitost 2^40, můžeme použít menší PHOTON – 80/20/16 s 80bitovým hašovacím kódem. Volby parametrů, plochu a rychlost hašování ukazuje tabulka. Poznamenejme, že existují i varianty, kdy za cenu mírně větší plochy lze při stejných parametrech docílit i řádově vyšší rychlost [6]. Pokud na hašovací funkci máme k dispozici prostředí PC, PHOTON spotřebuje na jeden bajt cca 100 taktů procesoru. V tabulce 4 jsou měření, provedená na procesoru Intel Core i7 Q720 s 1.60GHz, což dává rychlost hašování cca 16 MByte/s. V tabulce také vidíme hašovací funkci DM-PRESENT-80, založenou na blokové šifře PRESENT, která ale není tak dobrá jako PHOTON.

Triky PHOTONu

PHOTON používá dva triky jak docílit malé plochy. Transformace 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 8x8, ale 4x4 bity, které se nerealizují tabulkově, nýbrž logikou.

Hash	Délka hashe (bitů)	Bezpečnost - vzor	Bezpečnost - kolize	Plocha (počet hradel, GE)	Rychlost v kbit/s pro krátké zprávy 96 bitů
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
PHOTON-160/36/36	160	2^124	2^80	1396	1.03
PHOTON-256/32/32	256	2^224	2^128	2177	0.88

Tab. 4: Charakteristiky některých hashovacích funkcí pro RFID

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

Tab.5: Rychlosti PHOTONu v SW na procesoru Intel Core i7 Q720 s 1.60GHz

2.4 Zajímavá míra bezpečnosti

Když u jakéhokoliv kryptografického nástroje projdou všechny analýzy bezpečnosti, můžeme se na něj čistě ze zajímavosti podívat téměř "absolutně" nezaujatě, a to pomocí soustavy rovnic. Dokonce tím můžeme porovnávat složitost stejných nástrojů (!) mezi sebou, například složitost DES a AES. Můžeme porovnat i složitost různých nástrojů (!) mezi sebou, například AES a SHA-2. Mírou složitosti je počet operací AND, které jsou použity. Velice rychle je spočítáme u funkce Trivium, ale i u dalších uvedených nástrojů. Tam, kde jsou použity S-boxy, vyjádříme jejich výstupní bity booleovskými polynomy vstupních bitů a hned vidíme, kolik operací AND je zde použito (podrobnosti viz [4]). Jak srovnávat různé blokové šifry? Pokud mají například blokové šifry jiný počet bitů klíče, vypočteme složitost a podělíme ji počtem bitů klíče. U hašovacích funkcí je to zase složitost určení vzoru k danému otisku (dělená počtem bitů vzoru) nebo složitost určení dvou zpráv dané délky, vedoucích ke kolizi, apod. Pokud bychom srovnávali PRESENT a LBLOCK z tohoto hlediska, zjistíme, proč je LBLOCK rychlejší a menší. Ušetřil polovinu nelineárních S-boxů a nenahradil je dvojnásobným počtem rund. Tím snížil počet operací AND oproti šifře PRESENT na polovic. V tom je ale právě podstata jak ušetřit - návrháři LBLOCK usoudili, že taková bezpečnost (složitost) postačuje, zatímco návrháři PRESENT trochu přidali na bezpečnostní rezervě. Výpočet složitosti na jeden bit spolehlivě ukáže míru této opovážlivosti. U algoritmu Trivium se bojíme ji vůbec spočítat. V tabulce 6 čistě pro zajímavost vidíme v druhém sloupci srovnání složitosti některých kandidátů na SHA-3. Je docela záhadné, jak se tito různorodí kandidáti od různých týmů, mající různé vnitřní konstrukce, shodnou na míře složitosti kolem čísla 20. Přitom jejich algoritmy vznikaly v utajení před ostatními.

Algoritmus	Rychlost (cyklů/bajt)	Počet operací AND na jeden bit zprávy	Koeficient rych-lost/složitost
SHA-1	9	17	1,89
BMW	7	24	3,43
BLAKE	9	29	3,22
Shabal	10	13	1,30
SIMD	12	23	1,92
Skein	21	26	1,24
SHA-2	20	40	2,00

Tab.6: Různorodí kandidáti hašovací funkce SHA-3 (vznikaly v utajení před konkurenty) a jejich zatím záhadná inklinace k témuž číslu složitosti (kolem 20, viz druhý sloupec)

2.5 Omezení obvodů RFID

(Tento odstavec připravil Jan Dušátko, jan@dusatko.org)
Omezení daná rozměry a napájecími charakteristikami RFID čipů vyprodukovala některá zajímavá řešení z pohledu hardware. Jak pasivní (pro svoji práci využívají energii vysílače shromážděnou v kondenzátorech) tak aktivní (mají vlastní baterie) mohou obsahovat jednodušší či složitější procesory. Fyzikální limity jsou:

1) rozměr zařízení limituje množství přijaté a vysílané energie (kondenzátory, antény)
2) rozměr čipu a použitá technologie omezuje množství hradel (je nutné, aby se zde podařilo vtěsnat nejenom "procesor", ale i paměť a další komponenty)
3) velikost použitelné energie u pasivních RFID omezuje využitelnost pro výpočty

Samozřejmě, ne každé RFID zařízení lze miniaturizovat tímto způsobem. Je otázkou také jeho praktické nasazení. Proto například výrobky schopné výpočtů jsou větší. Porovnat jednotlivé typy podle velikosti, odběru, použité technologie a dalších ukazatelů je časově náročná práce, ale zhruba lze tvrdit následující:

1) FPGA procesory pro RFID mají plochu od 5x5 mm do 30x30 mm
2) Frekvence se pohybuje dle použití od 33MHz po téměř 733MHz
3) Napájecí napětí od 1V do 3,3V, celkový příkon se pohybuje většinou v řádu desetin Wattu (jedná se doopravdy o šetřílky)
4) Limitujícím faktorem, na který se zapomíná, je i cena

Zdroj informací: XILINX (48% trhu) a Altera (45% trhu).

2.6 RFID a příležitost pro hacking

Kryptografické funkce pro RFID samy o sobě neposkytují útočníkovi žádnou radost, neboť složitost útoku daná číslem 2^80 operací, tvoří příliš silnou obrannou bariéru. V praxi to bývá tak, že bariéru je možné obejít. To však už není v moci kryptologie, nýbrž lidí, kteří obranné prvky staví. Bohužel lze očekávat, že při použití tohoto typu kryptografie bude v příslušných systémech (jako ve všem novém) spousta "pašáckých" vylepšení, implementačních chyb a postranních kanálů. To vytvoří značný prostor pro hacking.

2.7 Postranní kanály

Postranní kanály jsou na rozdíl od postranních úmyslů mladou vědeckou disciplinou v kryptologii. Pomocí ní byly "prolomeny" věci jinak „neprolomitelné“. Postranní kanály mají k hackingu docela blízko, neboť využívají drobnosti, které vypadají neškodně, jako jsou chybové hlášky systémů, zpoždění při čtení z paměti, doba trvání nějaké operace, průběh spotřeby energie, měření a vyhodnocování změn napětí na čipu, elektromagnetické vyzařování apod. Tyto postranní informace se matematicky vyhodnocují, čímž získávají nový - kryptografický - význam. Častým výsledkem útoků postranními kanály je získání šifrovacích klíčů. Jedná se o rozsáhlou a mimořádně zajímavou oblast (např. [9-13], úvodní přednáška v [11]).

2.8 Závěr

Minimální nároky na paměť a maximální výkon, to jsou nové výzvy, kterým čelí tzv. lehká kryptografie. Jejími výstupy jsou všechny tradiční kryptografické nástroje, které budou použitelné v čipech RFID. Zatím jsou k dispozici výborní kandidáti na blokovou a proudovou šifru a hašovací funkci. Pro hacking tu není žádná nová možnost oproti silné kryptografii neboť zeslabení bezpečnosti je stále nad hranicí praktických útoků. Zůstává však ohromné pole možností, které je naprosto shodné se silnou kryptografií, a to jsou útoky na praktické implementace. Pole velice široké, chtělo by se přímo říci **".....velké žírné rodné lány..."**.

3 Pár slov k hackingu

Na téma hacking si dovolím hovořit pouze z pohledu kryptologa, nezabývajícího se hackingem.

Dnešní ICT – snadná příležitost pro hackery

Současné informační a komunikační technologie jsou celkem snadnou kořistí pro hacking. Důvod je jednoduchý - počítače ani internet nebyly konstruovány s cílem, aby byly bezpečné. A proto také nejsou a nebudou. Z toho důvodu existuje spousta příležitostí pro hacking čehokoliv z této oblasti. Připočteme-li k tomu lidský faktor, omylný a lenivý, občas i neznalý, současné ICT jsou a mohou být kořistí hackerů.

Tuto realitu může skutečně změnit jen nová koncepce osobních počítačů a nová koncepce internetu nebo chcete-li používání paralelní bezpečné verze internetu a paralelní svět bezpečných počítačů. Toto není utopie. Existují paralelní světy sítí a počítačů, kde se pracuje s utajovanými informacemi. Každý, kdo takový systém provozuje, ví, že to je sice možné, ale není to přirozené. Naše myšlení a svět okolo nás nás nutí být on-line a v otevřené síti. Zároveň to ukazuje, jak je složité a nepohodlné provozovat bezpečný počítač a bezpečnou síť.

Ve světě normálním, otevřeném, bezpečnostní průniky a obavy z virů nastolily zajímavou situaci. Uživatel osobního počítače si již zvykl, že jeho počítač se někam automaticky spojuje a automaticky opravuje nebo aktualizuje své vybavení, operační systém, antivirovou ochranu i jiné programy. Do tohoto procesu nezasahuje a nechává ho plně pod kontrolou výrobce příslušného program. Stamiliony uživatelů tím svěřují svoji bezpečnost do rukou výrobců programů, aniž by věděli, co v jejich počítači tyto programy provádí. Je to správné? Je to nějaké východisko ze situace, kdy operační systém a internet jsou zranitelné a jsou každý den vystavovány neznámým hrozbám. Dostali jsme se do situace, kdy správu bezpečnosti nemohou zajišťovat sami uživatelé, ale specializované skupiny lidí (zde výrobci programů, operačních systémů apod.). A ukázalo se, že z důvodu rychlosti a ceny je nutné, aby tuto správu výrobci programů prováděli on-line. To je paradox dnešní počítačové bezpečnosti: abyste počítač uchránili od hrozeb z internetu, musíte svěřit bezpečnost někomu neznámému na internetu a prostřednictvím internetu. Správa bezpečnosti počítačů stamilionů uživatelů je navíc centralizovaná a dána do ruky relativně malému okruhu lidí. I tito lidé jsou však chybující, což opět vytváří a bude vytvářet značné příležitosti pro hacking.

Podobnou situaci zažívá i hardware. Množina výrobců elementárních součástek a čipů se zmenšuje a zmenšuje se skupina lidí, kteří mohou ovlivňovat funkce tohoto hardware. Může se jednat o neúmyslné i úmyslné chyby, stejně jako u výrobců SW. Zde také přechází bezpečnost HW do rukou specializovaných skupin lidí, přičemž pojem národní bezpečnost se pomalu vytrácí. Ani mocnosti nejsou schopny zajistit, aby jejich komunikační infrastruktura, civilní letadla, automobily, vlaky, mobilní telefony nebo jiná elektronika, používaly bezpečné

součástky, čipy a komponenty. A přitom se to týká bezpečnosti jejich uživatelů v širokém smyslu, tj. od fyzické až po informační bezpečnost. Jako špička ledovce jsou chápány odhalené dodávky čínských čipů, přepínačů, USB zařízení apod., které obsahovaly špionážní funkce a dostaly se až do obranné infrastruktury některých mocností. Ohromný potenciál proniknout do obranné i civilní infrastruktury mají mobilní telefony, špionující jak z komerčních, tak z vojenských důvodů.

Hacking se dnes chápe zejména v softwérové oblasti, stejné šance má i v oblasti hardwérové.

Budoucí ICT – hackerský ráj ?!

Zdá se, že současná módní vlna k chytrým přístrojům není jen dočasná. Ona vlastně začala už dávno, u praček a automobilů, kde část nebo celé řízení převzal minipočítač. Vlna pak přeskočila na mobilní telefony, kde klasický displej nahradily obrázkové symboly a dotykové ovládání. Zdá se, že v brzké budoucnosti toto přejde do operačních systémů osobních počítačů, viz připravovaný styl "Windows Metro". Poměrně neznámé je, že v EU se z důvodu úspor připravuje výměna starých elektroměrů za chytré přístroje. Testují se chytré ulice, kde se pouliční osvětlení v noci rozsvěcuje jen lokálně, pokud po ulici jde chodec nebo jede auto apod.

Chytré přístroje přináší a přinesou vpád do soukromí. Chytrý elektroměr může prozradit i že jste přepnuli televizi na jiný kanál. Chytrý mobil může prozradit Vaši pozici a kamsi ji pravidelně hlásit (toto se skutečně děje). Chytrý počítač prozradí, že jste v práci, cloudové řešení prozradí na čem právě pracujete, chytré osvětlení ve firmě rozsvítí světlo nad Vámi a lokalizuje Vaši pozici apod. Když pojedete z práce domů autem, město bude vědět, kdo jede, odkud a kam. Když zaparkujete, chytré auto to nahlásí pojišťovně. Když rozsvítíte v domě, elektroměr to ve formě malé vlnky zaznamená a předá elektrárenskému koncentrátoru, a když jdete spát, tak to "práskne" také, protože zhasnete lampičku u postele. Ráno Vás prozradí lednička, když doobjedná vyjmutý jogurt a RFID snímač na odpadkovém koši zaznamená vyhozenou krabici od čokoládových lupínků a doobjedná ji.

Trend k chytrým přístrojům, propojenost všeho do kyberprostoru a malé zabezpečení poskytne ráj příležitostí pro hacking neboť bezpečnost opět není a nebude kategorickým imperativem pro tyto systémy. A jaké příležitosti to budou? Nechme se překvapit. A nebo raději: nenechme se překvapit.

4 Místo závěru

Kryptologie a hacking se liší materií, s kterou pracují. Kryptologové více pracují s čísly, hackeři se softwarem a hardwérem. Myšlenkově si však jsou velmi blízko. Dobrý kryptograf musí myslet jako hacker, aby předešel všem útokům a dobrý kryptoanalytik musí být teprve skvělý hacker, aby odhalil slabiny, které nikdo jiný nenašel. Moderní kryptoanalýza se pak hackingu velice přibližuje i materiálně, a to v oblasti postranních kanálů, kdy se kryptoanalytické útoky spojují s fyzickou realizací a implementací kryptoschémat.

LITERATURA

[1] Vlastimil Klíma: Seriál „Kryptologie pro praxi“, Sdělovací technika, čísla 10-12/2011 a 02/2012, on-line na http://www.stech.cz/ nebo http://cryptography.hyperlink.cz

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

[3] Wenling Wu, Lei Zhang: "LBlock: A Lightweight Block Cipher", IACR eprint Archive, http://eprint.iacr.org/2011/345.pdf
[4] Vlastimil Klíma: Utajená míra složitosti, Crypto-World 06/2010, str. 2 - 6, ISSN 1801-2140, červen 2010, http://cryptography.hyperlink.cz/2010/crypto06_10_str_02_06.pdf

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

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

[7] Christophe De Canniere, Bart Preneel: Trivium Specifications, http://www.ecrypt.eu.org/stream/p3ciphers/trivium/trivium_p3.pdf

[8] Martin Hell, Thomas Johansson, Willi Meier: Grain - A Stream Cipher for Constrained Environments, http://www.ecrypt.eu.org/stream/p3ciphers/grain/Grain_p3.pdf

[9] Vlastimil Klima, Ondrej Pokorny, Tomas Rosa: Attacking RSA-based Sessions in SSL/TLS, presented at CHES 2003, pp. 426 - 440, Springer-Verlag, 2003, Preliminary version: IACR ePrint archive Report 2003/052

[10] Vlastimil Klima, Tomas Rosa: Attack on Private Signature Keys of the OpenPGP format, PGP (TM) Programs and Other Applications Compatible with OpenPGP, IACR ePrint archive Report 2002/076, March 2001

[11] Vlastimil Klima, Tomas Rosa: Side Channel Attacks - Highly Promising Directions in Modern Cryptanalysis, TATRACRYPT '03, The 3rd Central European Conference on Cryptology, June 26-28, 2003, Bratislava, Slovakia

[12] Vlastimil Klima, Tomas Rosa: Side Channel Attacks on CBC Encrypted Messages in the PKCS#7 Format, NATO PfP/PWP - 2nd International Scientific Conference Security and Protection of Information, Brno, Czech Republic, 28. - 30.4.2003, IACR ePrint archive Report 2003/098

[13] Vlastimil Klima, Tomas Rosa: Further Results and Considerations on Side Channel Attacks on RSA, CHES 2002 , pp. 245-260, Springer-Verlag, 2002, IACR ePrint archive Report 2002/071

C. Pozvánka na SCIENCE Cafe v Hradci Králové

D. O čem jsme psali v únoru 2000 – 2011

E. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí e-ziny, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály: http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška Vlastimil Klíma Tomáš Rosa Dušan Drábik
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Jaroslav Pinkava
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	jaroslav.pinkava@gmail.com ,	http://crypto-world.info/pinkava/
Tomáš Rosa	tomas.rosa@rb.cz ,	http://crypto.hyperlink.cz/
Dušan Drábik	Dusan.Drabik@o2bs.com ,	
Pavel Vondruška	pavel.vondruska@crypto-world.info	http://crypto-world.info/vondruska/index.php
Pavel Vondruška, jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info