SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY
A INFORMATIKY

Ing. Viliam Hromada

Autoreferát dizertačnej práce

KRYPTOANALÝZA PRÚDOVÝCH ŠIFIER

na získanie: vedecko-akademickej hodnosti
philosophiae doctor, PhD.

v doktorandskom študijnom programe: Aplikovaná informatika
v študijnom odbore: 9.2.9 aplikovaná informatika

Miesto a dátum: Bratislava, 3. 7. 2014

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Ing. Viliam Hromada

Autoreferát dizertačnej práce

KRYPTOANALÝZA PRÚDOVÝCH ŠIFIER

na získanie: vedecko-akademickej hodnosti
philosophiae doctor, PhD.

v doktorandskom študijnom programe: Aplikovaná informatika

Miesto a dátum: Bratislava, 3. 7. 2014

Dizertačná práca bola vypracovaná: v dennej forme doktorandského štúdia na Ústave informatiky a matematiky FEI STU v Bratislave.

Predkladateľ: Ing. Viliam Hromada
ÚIM FEI STU
Ilkovičova 3
812 19 Bratislava

Školiteľ: doc. Ing. Milan Vojvoda, PhD.
FEI STU Bratislava

Konzultant: prof. RNDr. Peter Horák, DrSc.
University of Washington
Tacoma, WA, U.S.A.

Oponenti: Ing. Michal Varchola, PhD.
Technická univerzita v Košiciach
Letná 9
042 00 Košice

doc. RNDr. Ladislav Satko, PhD.
Púpavová 11
841 04 Bratislava

Autoreferát bol rozoslaný dňa: .....

Obhajoba dizertačnej práce sa koná: 25. 8. 2014 o 10:30 hod.

Na: Fakulte elektrotechniky a informatiky STU,
Ilkovičova 3, 812 19 Bratislava, v miestnosti C502.

prof. RNDr. Gabriel Juhás, PhD.
dekan FEI STU

Obsah

1 Úvod

Ľudská komunikácia je stará ako ľudstvo samo. Už z obdobia pred našim letopočtom sú známe prípady, keď si chceli dvaja korešpondenti vymeniť správu bez toho, aby ju dokázal čítať niekto iný, t.j. chceli túto komunikáciu nejakým spôsobom alebo utajiť, alebo správu previesť to takej formy, aby bola pre iného čitateľa nečitateľná.

Na zabezpečenie utajenia obsahu správy sa v dnešnej dobe používa šifrovanie, respektíve šifrovacie systémy - nazývané aj kryptosystémy. Zjednodušene sa dá povedať, že kryptosystém slúži na to, aby správu z jej čitateľnej podoby (takáto správa sa nazýva otvorený text - OT) transformoval do jej nečitateľnej podoby (takáto správa sa nazýva zašifrovaný text - ZT) pomocou tajného parametra - šifrovacieho kľúča. Takémuto procesu hovoríme šifrovanie. Samozrejme, kryptosystémy musia zabezpečiť aj proces opačný, t.j. transformáciu správy z jej nečitateľnej podoby späť na čitateľnú podobu, aby ju mohol legitímny príjemca, majiteľ dešifrovacieho kľúča, bez problémov prečítať. Tomuto procesu hovoríme dešifrovanie.

Dnešné kryptosystémy delíme podľa toho, ako šifrujú ten istý blok textu, na blokové šifry a prúdové šifry. Zatiaľ, čo blokové šifry zašifrujú vždy ten istý otvorený text, resp. jeho časť, pri použití rovnakého kľúča na ten istý zašifrovaný text (v základnom režime ECB - angl. Electronic Code-Book), pri prúdových šifrách to neplatí, t.j. rovnaké bloky otvoreného textu zašifruje prúdová šifra na iné bloky zašifrovaného textu.

Útoky na kryptosystémy možno deliť na dve triedy: na priame útoky a na nepriame útoky. Priame útoky sú zamerané na algoritmickú podstatu kryptosystému, bez ohľadu na jeho implementáciu. Nepriame útoky využívajú fyzickú implementáciu kryptosystému a zahŕňajú širokú paletu techník, ktoré alebo poskytujú útočníkovi nejakú „vnútornú“ informáciu o procese šifrovania (ako napríklad časová analýza - angl. time analysis [6] alebo napäťová analýza - angl. power analysis [7]), alebo mu dovoľujú tento proces ovplyvniť (preklápanie bitov v pamäti zariadenia pomocou žiarenia, atď.). Chybová analýza študuje, aký efekt majú jednotlivé indukované chyby na zašifrovaný text, s cieľom získať aspoň čiastočnú informáciu alebo o kľúči, alebo o vnútornom stave šifrovacieho zariadenia.

2 Ciele dizertačnej práce

Táto dizertačná práca sa zaoberá prúdovými šiframi z dvoch hľadísk: návrhu nových prúdových šifier a vykonania chybovej analýzy vybraných prúdových šifier. Vedeckými cieľmi, resp. tézami, tejto dizertačnej práce boli nasledovné body:

1. Prispieť k chybovej analýze prúdových šifier analýzou niektorého z finalistov projektu eSTREAM pomocou techniky, ktorá ešte nebola na tohto finalistu aplikovaná.

2. Prispieť k oblasti návrhu prúdových šifier návrhom novej prúdovej šifry, resp. nového generátora náhodných čísiel.

Výsledky vedeckého bádania sú prezentované ako súbor 4 článkov v dizertačnej práci. Prvý článok sa zaoberá chybovou analýzou prúdovej šifry Trivium pomocou techniky útoku fázovým posunom (cieľ č. 1). Druhý článok sa zaoberá chybovou analýzou prúdovej šifry LILI-128. Tretí článok obsahuje návrh prúdovej šifry, ktorej konštrukcia je založená na sovietskom šifrátore Fialka M-125 (cieľ č. 2) a štvrtý článok popisuje kombináciu generátora náhodných čísiel MSTg a kryptosystému s verejným kľúčom Poly-Dragon (cieľ č. 2).

3 Dosiahnuté výsledky dizertačnej práce

Dosiahnuté výsledky sú zhrnuté do 4 častí podľa príslušných článkov, z ktorých sa skladá dizertačná práca.

3.1 Útok fázovým posunom na prúdovú šifru Trivium

V tomto výskume sme sa zaoberali chybovou analýzou prúdovej šifry Trivium [3], finalistu projektu eSTREAM pomocou tzv. „fázového posunu“ [5]. Jedná sa o techniku indukcie chyby, v ktorej dochádza k desynchronizácii registrov šifry. Šifra Trivium pozostáva z 3 nelineárnych registrov, ktoré sa spoločne posúvajú vždy o jeden takt a v každom takte generujú 1 bit výstupu. Pri útoku fázovým posunom sa ešte pred generovaním výstupu vynúti posun jedného z registrov o 1 takt, zatiaľ čo ostatné registre stoja. Tým dôjde k ich desynchronizácii. Následne sa spustí generovanie prúdového kľúča. Na základe pôvodného bezchybného prúdového kľúča a chybného prúdového kľúča sa potom snažíme zistiť vnútorné naplnenie registrov šifry IS_{t_0} v nejakom časovom momente t_0.

Na hľadanie vnútorného stavu IS_{t_0} sme použili metódu riešenia sústavy rovníc v premenných reprezentujúcich hľadaný stav. Na riešenie tejto sústavy sme použili

2 rôzne metódy z algebraickej kryptoanalýzy: SAT-solvery a algoritmus ElimLin [2].

Myšlienka spojenia indukcie chýb a algebraickej kryptoanalýzy v útoku na prúdovú šifru Trivium bola prvýkrát prezentovaná v práci [9]. Autori na útok použili indukciu jedno-bitových chýb a zistili, že na úspešný útok potrebujú indukovať 2 chyby a generovať 420 bitov prúdového kľúča, t.j. dokopy potrebujú vygenerovať cca. 1240 bitov. My sme sa teda rozhodli namiesto indukcie jedno-bitových chýb využiť fázový posun registrov.

Z našich experimentov vyplýva, že pre úspešné nájdenie vnútorného stavu je potrebné vykonať 2 rôzne fázové posuny, t.j. posunúť jeden register, vygenerovať výstup, zariadenie vrátiť do pôvodného stavu, posunúť iný register a znovu vygenerovať výstup. Na rozdiel od útoku [9] však tento útok potrebuje generovať len 120 bitov prúdového kľúča, t.j. dokopy je potrebné generovať cca. 420 bitov, čo predstavuje zníženie dátovej zložitosti útoku o 70 %.

Navyše sme zistili, že nie je dôležité, ktoré 2 registre budú fázovo-posunuté, keďže výsledky boli vo všetkých prípadoch rovnaké. Ďalším zaujímavým výsledkom bol fakt, že úspešnosť oboch metód algebraickej kryptoanalýzy, SAT-solverov a algoritmu ElimLin, bola približne rovnaká pre rovnaké sústavy rovníc, čo je pre relatívne nový algoritmus ElimLin sľubný výsledok v porovnaní so zaužívanou metódou SAT-solverov.

Výsledky tohto výskumu boli prezentované na konferencii *Central European Conference on Cryptology - CECC 2014* v Budapešti v máji 2014.

3.2 Chybová analýza prúdovej šifry LILI-128

V tomto výskume sme sa venovali chybovej analýze prúdovej šifry LILI-128, ktorá pozostáva z 2 registrov - 39-bitového časového registra, ktorý riadi taktovanie 89-bitového dátového registra, ktorý v každom takte generuje 1 bit prúdového kľúča. Pôvodný chybový útok na túto šifru [5] využíval indukciu jedno-bitových chýb na každej pozícii dátového registra v rôznych časových momentoch. Dokopy bolo potrebné na úspešné nájdenie počiatočného naplnenia oboch registrov indukovať cca. 1800 chýb.

My sme tento útok chybovou analýzou modifikovali nasledovným spôsobom. Na nájdenie naplnenia časového registra sa využívajú 4 rôzne fázové posuny dátového registra, pričom sa na základe príslušných chybových prúdových kľúčov dá zostro-

jiť sústava lineárnych rovníc nad pôvodným naplnením časového registra. Následne sme indukciou 89 jedno-bitových chýb v dátovom registri úspešne našli počiatočné naplnenie dátového registra.

Celkovo sa nám teda podarilo znížiť počet potrebných indukovaných chýb 20-násobne, avšak za použitia 4 fázových posunov, pričom počet bitov prúdového kľúča, ktorý bolo zakaždým potrebné vygenerovať, bol pri oboch útokoch rovnaký. Avšak celkový počet bitov potrebný pre náš útok bol zhruba 19-násobné menší ako počet bitov potrebných pre pôvodný chybový útok.

Výsledky tohto výskumu boli prezentované na konferencii *Mikulášská kryptobesídka 2011* v Prahe v decembri 2011.

3.3 Prúdová šifra založená na šifre Fialka M-125

Cieľom tohto výskumu bolo navrhnúť novú prúdovú šifru, ktorej dizajn by vychádzal zo sovietskeho šifrátora Fialka M-125 [10]. Inšpiráciou nám bola šifra Hummingbird [4], ktorá vychádza zo známeho nemeckého šifrovacieho stroja Enigma. Fialka M-125 nás zaujala aj tým, že dodnes nie sú známe účinné útoky na túto šifru.

Náš návrh v podstate kopíruje pôvodný dizajn Fialky. Fialka pre zašifrovanie vstupného znaku využívala 10 rotorov, pracujúcich v 2 nezávislých skupinách s opačným smerom otáčania. Vo všeobecnosti sa po každom zašifrovanom znaku otočili všetky rotory. Avšak otáčanie rotorov v jednej skupine bolo vzájomne ovplyvňované, keďže každý rotor mohol blokovať pohyb svojich nasledovníkov, čím sa docielilo ich nepravidelné krokovanie. Tieto konštrukčné princípy sme preniesli do nášho návrhu.

Navrhli sme modernú prúdovú šifru, kde sme permutáciu danú rotorom reprezentovali pomocou S-boxu a operácie XOR, prípadne modulárnym sčítaním a odčítaním. Nepravidelné otáčanie rotorov riadené blokovacími pinmi sme implementovali pomocou rotačných posuvných registrov. Celkovo sme navrhli 3 verzie šifrátora s rôznymi veľkosťami vstupov/výstupov: 4 bity, 5 bitov a 8 bitov. Následne sme každú verziu podrobili rýchlostným testom a štatistickým testom inštitútu NIST [11]. Testy sme vykonávali na počítači s parametrami CPU 2.8 GHz Intel Core i7, RAM 4GB 1333 MHz DDR3, Mac OS X 10.7.5.

V tabuľke 1 uvádzame výsledky testovania 8-bitovej verzie šifry. Testovali sme jej rôzne varianty, v závislosti na počte použitých S-boxov (t.j. „rotorov“) a na použitej operácii (t.j. XOR vs. modulárne sčítanie a odčítanie).

Rotory / operácia	10/mod	10/xor	8/mod	8/xor	6/mod	6/xor
Rýchlosť *Mbit/sec*	124	134	155	159	200	208
NIST testy	ÁNO	ÁNO	ÁNO	ÁNO	ÁNO	ÁNO

Tabuľka 1: Výsledky 8-bitovej verzie

Z tabuľky vidno, že najrýchlejšou verziou šifry je 8-bitová verzia so 6 S-boxami s použitou operáciou XOR, ktorá dosahuje rýchlosť 208 Mbps. Verzie s menším počtom rotorov neuvádzame, keďže neprechádzali štatistickým testovaním. Pre porovnanie, rýchlosť hardvérovej implementácie šifry Hummingbird je 165 Mbps.

Tieto výsledky boli prezentované na konferencii *Central European Conference on Cryptology - CECC 2013* v máji 2013 a príslušný článok [1] vyšiel v časopise *Tatra Mountains Mathematical Publications*.

3.4 Použitie kryptosystému Poly-Dragon v generátore náhodných čísiel MSTg

Tento výskum bol zameraný na použitie kryptosystému s verejným kľúčom Poly-Dragon [12] na generovanie prvkov náhodných pokrytí grúp, ktoré sa využívajú v generátore náhodných čísiel MSTg [8].

MSTg je generátor náhodných čísiel, ktorý využíva tzv. náhodné pokrytia grúp, t.j. náhodne vygenerované množiny prvkov grupy, z ktorých sa grupovou operáciou dá zložiť každý prvok grupy. Spätná faktorizácia prvku je vo všeobecnosti považovaná za ťažký problém, na základe čoho sa definuje jednocestná funkcia, ktorá tvorí základ generátora.

Na generovanie prvkov náhodného pokrytia sme zvolili post-kvantový kryptosystém s verejným kľúčom Poly-Dragon, ktorého bezpečnosť je založená na NP-úplnom probléme riešenia sústavy nelineárnych booleovských rovníc viacerých premenných a ktorého dizajn vychádza z permutačných polynómov konečných polí. Šifru sme v zapojení v CTR-móde použili na generovanie prvkov náhodného pokrytia, pričom jeden výstup šifrovania tvoril jeden prvok pokrytia. V takom prípade, ak aj útočník pozná 2 po sebe idúce prvky pokrytia, nedokáže generovať ďalšie prvky, keďže to by znamenalo zlomenie šifry Poly-Dragon. Tým sme zabezpečili

náhodné pokrytia použité v generátore.

Výslednú konštrukciu sme podrobili sade štatistických testov NIST [11] a porovnali sme dosiahnuté výsledky s pôvodnou verziou generátora MSTg. Naša verzia dosiahla porovnateľné štatistické výsledky ako pôvodná verzia. Taktiež sme zistili, že štruktúra použitých náhodných pokrytí zohráva v generátore MSTg väčšiu úlohu, ako počet týchto pokrytí, čo naznačili aj autori pôvodnej práce [8].

Výsledky tohto výskumu boli prezentované na konferencii *International Student Conference on Applied Mathematics and Infomatics - ISCAMI 2012* v máji 2012 a príslušný článok bol prijatý na publikovanie v časopise *Tatra Mountains Mathematical Publications*.

4 Literatúra

[1] ANTAL, E. - HROMADA, V. A New Stream Cipher Based on Fialka M-125. In *Tatra Mountains Mathematical Publications*, Bratislava. 2013, s. 101 - 118.

[2] COURTOIS, N., et al. ElimLin Algorithm Revisited. In *Fast Software Encryption.* Springer Berlin Heidelberg, 2012, p. 306-325.

[3] DE CANNIERE, C. Trivium: A Stream Cipher Construction Inspired by Block Cipher Design Principles. In *Information Security.* Springer Berlin Heidelberg, 2006, p. 171-186.

[4] ENGELS, D., et al. Hummingbird: Ultra-lightweight Cryptography for Resource-constrained Devices. In *Financial Cryptography and Data Security.* Springer Berlin Heidelberg, 2010. p. 3-18.

[5] HOCH, J. - SHAMIR, A. Fault Analysis of Stream Ciphers. In *Chryptographic Hardware and Embedded Systems – CHES 2004, Lecture Notes in Computer Science*, Springer-Verlag, 2004, s. 240 - 253.

[6] KOCHER, P. Timing Attacks on Implementation of Diffie-Hellman, RSA, DSS and Other Systems. In *Advances in Cryptology: Proceedings of CRYPTO '96*, Springer-Verlag, 1996, s. 104 - 113.

[7] KOCHER, P. - JAFFE, J. - JUN, B. Differential Power Analysis. In *Lecture Notes in Computer Science*, 1999, s. 388 – 397.

[8] MARQUARDT, P. - SVABA, P. - van TRUNG, T. Pseudorandom Number Generators Based on Random Covers for Finite Groups. In *Designs, Codes and Cryptography*, 2011, s. 1 - 12.

[9] MOHAMED, S. E. M., et. al. Using Sat Solving to Improve Differential Fault Analysis of Trivium. In *Information Security and Assurance*, Springer Berlin Heidelberg, 2011, p. 62-71.

[10] REUVERS, P. - SIMONS, M. *Fialka M-125: Detailed Description of the Russian Fialka Cipher Machines*. PAHJ Reuvers & MJH Simons, 2009.

[11] RUKHIN, A., et. al. *Statistical test suite for random and pseudorandom number generators for cryptographic applications*. Dostupné na internete: `http://csrc.nist.gov/rng`.

[12] SINGH, R.P. - SAIKIA, A. - SARMA, B.K. Poly-Dragon: an efficient multivariate public key cryptosystem. In *Journal of Mathematical Cryptology*, 2010, s. 365 - 373.

5 Zoznam prác dizertanta

5.1 Publikované výsledky dizertačnej práce

ANTAL, E. - HROMADA, V. A New Stream Cipher Based on Fialka M-125. In *Tatra Mountains Mathematical Publications*, Bratislava. 2013, s. 101 - 118.

HROMADA, V. - VOJVODA, M. Fault Analysis of Stream Ciphers. In *Mikulášská kryptobesídka 2011 : Sborník příspěvků: Praha, 1. - 2. decembra 2011*. Praha: Trusted Network Solutions, 2011, s. 69 - 70.

HROMADA, V. - VOJVODA, M. Using Poly-Dragon Cryptosystem in a Pseudorandom Number Generator MSTg. *Prijaté na publikovane v Tatra Mountains Mathematical Publications*.

5.2 Publikované vedecké články

HORAK, P. - HROMADA, V. Tiling R^5 by Crosses. In *Discrete & Computational Geometry*, Volume 51 Issue 2, Springer-Verlag, 2014, s. 269 - 284.

HORAK, P. - HROMADA, V. On a Tiling Paradox. *Prijaté na publikovanie v Journal of Combinatorial Mathematics and Combinatorial Computing*.

5.3 Príspevky na konferenciách

HROMADA, V. - VOJVODA, M. Using Public-Key Cryptosystem Poly Dragon to Create a PRNG Based on Random Covers for Finite Groups. In *ISCAMI 2012 : Book of abstracts. Malenovice, Czech Republic, 10. - 13.5.2012*, Ostrava: University of Ostrava, 2012, s. 44.

HROMADA, V. - VARGA, J. Accelometers as Sources of Randomness in Mobile Device. In *ISCAMI 2013 : Book of abstracts. Malenovice, Czech Republic, 2. - 5.5.2013*, Ostrava: University of Ostrava, 2013, s. 34.

HROMADA, V. - VARGA, J. Phase-shift Fault Analysis of Trivium. In *Central European Conference on Cryptology 2014 : conference pre-proceedings. Budapest, Hungary, May 21-23, 2014*, Budapest: Alfréd Rényi Institute of Mathematics, 2014. - s. 54 - 55

HROMADA, V. - VOJVODA, M. A Note on Poly-Dragon Cryptosystem. In *ELITECH'12 : 14th Conference of Doctoral Students. Bratislava, Slovak Republic, 22 May 2012*, Bratislava: Nakladateľstvo STU, 2012, s. 5.

HROMADA, V. - VOJVODA, M. Statistical Testing of MSTg/Poly-Dragon Generator. In *ELITECH'13 : 15th Conference of Doctoral Students. Bratislava, Slovak Republic, 5 June 2013*, Bratislava: Nakladateľstvo STU, 2013, s. 6.

HROMADA, V. - VARGA, J. Extracting Randomness from Mobile Devices. In *EE časopis pre elektrotechniku, elektroenergetiku, informačné a komunikačné technológie, Roč. 19, mimoriadne č.: konferencia ELOSYS, Trenčín, 15.-18.10.2013.* 2013, s. 20 - 22.

6 Summary

This dissertation deals with stream ciphers, namely with the fault analysis of stream ciphers and with the propositions of new stream ciphers. It consists of four articles, two articles deal with a fault analysis of two stream ciphers Trivium and LILI-128, the other two contain propositions of two new stream ciphers.

In the first article, we investigated the phase-shift fault analysis of the stream cipher Trivium. In phase-shift fault attack, we induce a desynchronization fault into the cipher. In the case of Trivium, which consists of three non-linear feedback shift

registers, before the generation of the keystream, we shifted one of the registers by one clock while the other two registers were not clocked and proceeded to generate the faulted keystream. By observing the faulted keystream and the unfaulted one we tried to find the inner state of the cipher at some time moment. It stems from our experiments that it is sufficient to perform two different phase-shifts with 120 generated bits per each keystream for a successful attack, which improves the data complexity (the number of keystream bits) of the best known fault attack by 70 %.

Second article describes the fault analysis of the stream cipher LILI-128. In the original fault attack against the cipher the authors used the bit-flipping fault attack and needed to induce approx. 1800 one-bit faults to successfully find the initial loadings of the registers of the cipher. We combined the bit-flipping and the phase-shift fault analysis and were able to find the initial loadings of the registers with 4 different phase-shifts and 89 one-bit faults, which significantly reduces the overall number of induced faults.

In the third article, we proposed a new stream cipher based on an old Soviet encryption machine Fialka M-125 used during the Cold War, both in the USSR and in the CSSR. We used Fialka's design principle - irregularly clocked rotors working in two independent groups, where one rotor could block the movement of all the following rotors in the corresponding group - to design a modern stream cipher by using S-boxes representing the rotors and rotational shift registers representing the blocking pins controlling the movement of subsequent rotors. We carried out performance and statistical tests on a notebook to test our design and compared it with a stream cipher Hummingbird inspired by a German encryption device Enigma. An 8-bit version of our construction with 6 rotors passed the NIST statistical test suite and had an output speed 208 Mbps, which is faster than Hummingbird, having an output speed of 165 Mbps on the same testing computer.

Fourth article deals with a new design of a random number generator. We combined a random number generator MSTg based on random covers for finite groups with a public-key cryptosystem Poly-Dragon. We used the output of Poly-Dragon to generate random covers (the elements of the covers) used in the MSTg generator. We used Poly-Dragon in a regular counter mode with the succeeding output ciphertexts forming the random covers. This implies that even if an attacker is able to find out some elements of the covers, he is still unable to calculate the other ones, because he would have to break the post-quantum cryptosystem Poly-Dragon in order to do so. We carried out statistical tests of this construction. The results were similar to the original results of MSTg without Poly-Dragon - the construction passed all NIST statistical tests.