VEDECKÁ RADA FAKULTY ELEKTROTECHNIKY
A INFORMATIKY SLOVENSKEJ TECHNICKEJ
UNIVERZITY V BRATISLAVE

Ing. Michal Šrámka

Autoreferát dizertačnej práce

CRYPTANALYSIS OF SELECTED PUBLIC-KEY AND PRIVATE-KEY CRYPTOSYSTEMS

Na získanie vedecko-akademickej hodnosti philosophiae doctor
v odbore doktorandského štúdia:

11-14-9 Aplikovaná matematika

Bratislava, február 2006

Dizertačná práca bola vypracovaná v externej forme doktorandského štúdia na Katedre aplikovanej informatiky a výpočtovej techniky Fakulty elektrotechniky a informatiky Slovenskej technickej univerzity v Bratislave

Predkladateľ: Ing. Michal Šrámka
Mirka Nešpora 853/11
962 32 Sliač

Školiteľ: Prof. RNDr. Otokar Grošek, PhD.
Katedra aplikovanej informatiky FEI STU
Ilkovičova 3, 812 19 Bratislava 1

Oponenti: Prof. RNDr. Štefan Porubský, DrSc.
Ústav informatiky, Akademie věd České republiky
Pod Vodárenskou věží 2
182 07 Praha 8 - Libeň, Česká republika

RNDr. Karol Nemoga, PhD.
Matematický ústav SAV
Štefánikova 49, 814 73 Bratislava

Doc. RNDr. Karol Macák, PhD.
Národný bezpečnostný úrad SR
Budatínska 30, 850 07 Bratislava 57

Autoreferát bol rozoslaný dňa .....
Obhajoba dizertačnej práce sa koná dňa 4. mája 2006 (štvrtok) o 10:00
pred komisiou pre obhajobu dizertačnej práce v odbore doktorandského štúdia,
vymenovanou predsedom spoločnej odborovej komisie
11-14-9 Aplikovaná matematika
v zasadačke dekana FEI STU, Ilkovičova 3, 812 19 Bratislava

Predseda spoločnej odborovej komisie
Prof. RNDr. Zdenka Riečanová, PhD.
Katedra matematiky FEI STU
Ilkovičova 3, 812 19 Bratislava

1 Úvod

Kryptológia, veda o skrývaní a utajovaní informácií, sa za posledné tri desaťročia stala hlavným nástrojom bezpečnej komunikácie, súkromia, kontroly prístupu, elektronických platieb, elektoronických volieb a mnohých ďalších oblastí.

Kryptológia sa zaoberá tromi dominantnými oblasťami. *Kryptografia* je veda o vytváraní bezpečných systémov a schém; *kryptoanalýza* je naopak veda o hľadaní slabín v takýchto schémach; a *steganografia* je veda zaoberajúca sa všeobecným skrývaním informácií.

Úlohu kryptoanalýzy je nachádzanie slabých článkov daných kryptografických schém za účelom oslabenia schémy, zníženia jej bezpečnosti. Kryptoanalýzu vykonávajú cudzí oponenti, ktorí sa snažia získané poznatky využiť vo svoj prospech alebo zničiť danú kryptografickú schému. Obyčajne kryptoanalýzu vykonávajú aj navrhovatelia nových kryptosystémov, aby overili či daný návrh spĺňa všetky bezpečnostné kritériá.

Moderná kryptoanalýza sa nezaoberá len lámaním šifrovacích metód - pokrýva všetko od bezpečnostnej analýzy, cez hľadanie slabých článkov až po úplné zlomenie množstva kryptografických schém ako napríklad: schém pre digitálne podpisy, kryptografické hašovacie funkcie, kryptografické protokoly, atď. Okrem toho sa moderná kryptoanalýza zaoberá aj analýzou útokov na implementácie jednotlivých kryptografických schém - útoky postrannými kanálmi a útoky na (úmyselne vyvolanú) chybovosť implementácií schém.

2 Ciele dizertácie

Úlohou predkladanej práce je rozšírenie šúčasných znalostí v kryptológii, hlavne v kryptoanalýze. Táto dizertačná práca skúma oba typy šifrovacích systémov - jednak symetrické šifrovacie systémy so spoločným kľúčom ako aj asymetrické šifrovacie systémy s pármi verejných a utajovaných kľúčov.

Dizertačná práca pozostáva zo súboru štyroch článkov, ktoré skúmajú rôzne šifrovacie schémy založené na rozdielnych matematických problémoch. Napriek tomu, výsledkom bádania je ukážka, aké informácie je možné kryptoanalýzou získať a kam až siaha kryptoanalýza.

Ďalšie ciele dizertačnej práce sú:

- Prezentovať kryptoanalýzu asymetrického šifrovacieho systému založeného na probléme rozpoznávania slov vo voľnej grupe. V tejto časti kryptoanalýza viedla k priamemu uplatneniu získaných poznatkov na návrh nového, podobného šifrovacieho systému.
- Objasniť symetriu grupy mrežových bodov použitých pri kryptoanalýze šifrovacieho systému NTRU a využiť túto symetriu pri návrhu efektívneho (navyše vysoko paralelizovateľného) algoritmu na hľadanie najmenších báz takýchto grúp mrežových bodov.
- Ukázať, na príklade kryptoanalýzy symetrického šifrovacieho systému založeného na báze Hopfieldových neurónových sietí, že kryptoanalýza šifrovacích systémov založených na jednom probléme môže viesť k riešeniu známych problémov z iných oblastí matematiky.
- Zdôrazniť potrebu kryptoanalýzy pri návrhu nových kryptografických schém. Zlým príkladom je nedávny návrh troch symetrických šifrovacích systémov určených na utajenie multimediálnych údajov, ktoré akoby ignorovali bežné poznatky z kryptografie a kryptoanalýzy, a aj preto nespĺňajú základné bezpečnostné požiadavky.

V neposlednom rade, cieľom dizertačnej práce je aj ukázať, ako kryptoanalýza úzko súvisí s kryptografiou. Konkrétne je v práci ukázané:

- ako je možné získané informácie z kryptoanalýzy jedného systému uplatniť v návrhu nového, bezpečnejšieho systému, a
- akých chýb sa treba vyvarovať pri budúcich návrhoch bezpečných kryptosystémov.

3 Výsledky dizertačnej práce

Dosiahnuté výsledky sú rozdelené do štyroch podkapitol, ktoré zhŕňajú informácie o štyroch skúmaných problémoch.

3.1 Šifrovacie systémy s verejným kľúčom na báze problému rozpoznávania slov vo voľnej grupe

Tento výskum bol publikovaný v článku [6]. Hlavné výsledky boli prezentované na konferencii *WartaCrypt '04* v Bedlewe v Poľsku v roku 2004. Časti tohoto výskumu boli tiež prezentované v roku 2004 na konferenciách *Southeastern Weekend Algebra Meeting* v Hammond v Louisiane a *69th Florida Academy of Sciences Annual Meeting* v Tampe na Floride.

Prvým publikovaným kryptosystémom založeným na probléme rozpoznávania slov vo voľnej grupe bol asymetrický kryptosystém Wagnera-Magyarikovej[45].

Ukázali sme, že tento kryptosystém nie je založený na pôvodnom probléme rozpoznávania slov vo voľnej grupe (tak ako ho zadefinoval Max Dehn v 1911), ale na jednoduchšom probléme výberu slov, ktorý sme zadefinovali nasledovne: Nech G je grupa s konečnou množinou generátorov X a nech $w_0, w_1 \in \{X \cup X^{-1}\}^*$ sú slová. Za predpokladu, že slovo $w \in \{X \cup X^{-1}\}^*$ je ekvivalentné s w_0 alebo w_1, *problém výberu slov* je problém zodpovedania otázky, či w je ekvivalentné s w_0. Dokázali sme, že ak je problém rozpoznávania slov vo voľnej pologrupe S coNP-kompletný, tak problém výberu slov je v S (NP $\cap$ coNP)-kompletný. Tvrdíme, že táto veta platí aj v grupách.

Okrem známeho reakčného útoku na tento kryptosystém sme ukázali, že Wagnerov-Magyarikovej kryptosystém nie je bezpečný ani voči útoku s možnosťou výberu zašifrovaných textov. Tento útok má polynomiálnu zložitosť $O(m^2)$, kde m je kardinalita množiny X (v pôvodnom návrhu je $m \in \{25, 50\}$).

Ďalším dôležitým výsledkom je návrh vlastného asymetrického systému založeného na podobnom princípe ako kryptosystém Wagnera-Magyarikovej. Náš návrh kryptosystému je založený na konečne prezentovanej grupe G, ktorá tranzitívne pôsobí na slová nad abecedou $\{1, 2, 3\}$. Takáto grupa je napríklad

$$G = \langle G_{3,1}^{\mathrm{mod}\,3}(0, 1; \#) \cup \{\kappa_{321}\} \rangle,$$

ktorá súvisí s Highman-Thompsonovou grupou $G_{3,1}$. Popis celého kryptosysému je však nad rámec tohoto autoreferátu.

3.2 Zrýchlená redukcia bázy niektorých grúp mrežových bodov

Tento výskum bol publikovaný v článku [41] a prezentovaný na konferencii *Third Pythagorean Conference* na ostrove Rodos v Grécku v roku 2003.

Najefektívnejší útok na kryptosystém NTRU[23] je založený na hľadaní najkratších vektorov v grupe mrežových bodov[10]. Problémy grupy mrežových bodov majú okrem toho uplatnenie v iných kryptosystémoch ako aj pri množstve útokov na ďalšie kryptosystémy.

Ukázali sme, že grupa mrežových bodov použitá pri útoku na NTRU kryptosystém má určitú symetrickosť, ktorú sme nazvali *birotácia*: Nech h je verejný polynóm a q celé číslo v definícii kryptosystému NTRU. Potom grupa mrežových bodov daná bázou

$$B = \left[\begin{array}{c|c} I & O \\ \hline \mathrm{cir}(h) & qI \end{array}\right],$$

kde O je nulová $N \times N$ matica, I je $N \times N$ jednotková matica a $\mathrm{cir}(h)$ je $N \times N$ ľavá cirkulantná matica pozostávajúca z koeficientov polynómu h, má nasledovnú vlastnosť: ak $v = (v_1, \ldots, v_{2N}) = (u, w) \in B$, kde $u = (v_1, \ldots, v_N)$ a $w = (v_{N+1}, \ldots, v_{2N})$, tak $\mathrm{birotate}_k(v) := (\mathrm{rotate}_k(u), \mathrm{rotate}_k(w)) \in B$, kde rotate_k je pravá cyklická rotácia vektora dĺžky N o k pozícií.

Navrhli sme algoritmus redukcie bázy takejto grupy mrežových bodov, a to nasledovne: Nech $B = [b_1^T, \ldots, b_{2N}^T]$ je báza pozostávajúca z transponovaných riadkových vektorov. Vyňatím vektora b_i s veľkou normou a jeho nahradením vektorom $\mathrm{birotate}_k(b_j)$, kde b_j má malú normu, pre rôzne k dostávame bázu B' pre danú grupu mrežových bodov alebo pre jej podgrupu. Keďže je triviálne zistiť či B' je báza pre celú pôvodnú grupu mrežových bodov, pre rôzne i, j, k dostávame redukovanú bázu tejto grupy mrežových bodov.

Popísaný algoritmus je súčasťou nami navrhnutej vysoko paralelizovateľnej metódy. Okrem algoritmu "birotate" využíva naša metóda aj algoritmus BKZ-L^3 a generický algoritmus (zostupovanie z kopca). Naša metóda je v súčasnosti najrýchlejším známym útokom na pôvodný kryptosystém NTRU. Je nutné poznamenať, že táto metóda je nedeterministická a nemusí viesť k výsledku (metóda je typu Las Vegas).

3.3 Problém konjugácie matíc permutačnou maticou

Tento výskum bol publikovaný v článku [11] a prezentovaný v roku 2005 na konferencii *MoraviaCrypt '05* v Brne.

V roku 1999 bol publikovaný blokový šifrátor[20] založený na báze Hopfieldových neurónových sietí (HNS). Konkrétne na faktoch, že neurónové siete realizujú nelineárne funkcie a vykazujú určité chaotické vlastnosti. V tomto prípade bolo ukázané, ako sa dá tento chaos v HNS kontrolovať a teda využiť ako šifrovacia a dešifrovacia funkcia.

Ukázali sme, že výsledný blokový symetrický šifrovací systém je neefektívny z hľadiska rýchlosti šifrovania, pamäťových nárokov, ako aj z hľadiska zväčšenia veľkosti otvorených textov pri šifrovaní - expanzný faktor je minimálne 2, obyčajne oveľa väčší.

Hlavnou nevýhodou tohoto kryptosystému je však nami objavená existencia útoku s možnosťou voľby šifrovaných textov. Pri realizácii tohoto útoku sa útočník dostáva k problému nájsť permutačnú maticu H v rovnici $V = H\sigma(T)H^{-1}$, kde matice V a $\sigma(T)$ sú štvorcové matice nad $\mathbb{Z}_2$. Tento problém je podobný známemu ťažkému problému izomorfizmu grafov, kde pre dané štvorcové matice A a B je potrebné nájsť permutačné matice P a Q tak, aby platilo

$$B = PAQ.$$

My sme ukázali metódu nájdenia permutačnej matice P v rovnici

$$B = PAP^{-1},$$

kde matice A a B sú štvorcové nad ľubovolným okruhom. Metóda je založená na niekoľkých základných vetách, ktoré nájdu jedno (prvé) riešenie pre danú rovnicu. Keďže táto rovnica môže mať viacero riešení, dokázali sme vety, ktoré pre dané jedno riešenie ukazujú cestu ako nájsť zvyšné riešenia. V práci sú uvedené konkrétne metódy na prístup k tomuto problému aj s odhadmi zložitosti.

Nezanedbateľným prínosom tejto metódy je nielen získanie šifrovacieho kľúča pre skúmaný kryptosystém založený na HNS, ale aj riešenie netriviálnych problémov v kombinatorike a bio-informatike.

3.4 Kryptoanalýza viacerých blokových video šifrátorov

Tento výskum bol publikovaný v článku [40] a prezentovaný v roku 2003 na medzinárodnej konferencii *TatraCrypt '03* v Bratislave.

Ochrana multimediálnych údajov pred pirátstvom je z hľadiska kryptológie zaujímavý problém. Bezpečnosť v tomto prípade má iné predpoklady a iné ciele ako pri tradičných aplikáciách. Avšak väčšina poznatkov z kryptografie a kryptoanalýzy je aplikovateľná proti pirátstvu.

Pri kryptoanalýze šifrátorov zameraných na ochranu dôvernosti multimédií, sme sa zamerali na šifrátory zabezpečujúce ochranu MPEG-1 videa. Množstvo šifrovacích systémov je v tomto prípade viazané na konkrétny multimediálny protokol za účelom zvýšenia rýchlosti. Pravdaže je možné celé MPEG-1 video zašifrovať tradičnou blokovou alebo prúdovou šifrou, ale takéto riešenie je pomalé a nákladné.

Úspešne sme kryptoanalyzovali tri šifrátory určené pre MPEG-1 videá. V dvoch prípadoch sme ukázali, že navrhované šifrovanie je ekvivalentné s klasickou šifrou (Vigenère). Pri šifrovaní videí je ho teda možné úspešne napadnúť prostredníctvom útoku so známymi otvorenými textami a získať tak (de)šifrovací kľúč pre celé video.

V treťom prípade sme pre daný kryptosystém redukovali veľkosť kľúča z 2^{718} kombinácií na 2^{38} kombinácií. Cenou za túto redukciu sú ojedinelé chybné body vo videu. Experimentálne je to však len 0.1% 8×8 bodových blokov (4 bloky z 4096).

V prípade týchto troch šifrovacích systémov sme ukázali, že aj špecifické kryptosystémy určené na ochranu multimediálnych informácií, ktoré sú kompromisom medzi rýchlosťou a bezpečnosťou, potrebujú rigoróznu previerku z kryptoanalýzy.

4 Zoznam použitej literatúry

[1] Bharat Bhargava and Changgui Shi. Light-Weight MPEG Video Encryption Algorithm. In *Proc. of the Int'l Conf. on Multimedia - Multimedia 98, Shaping the Future*, pages 55–61, New Delhi, India, 1998.

[2] Bharat Bhargava, Changgui Shi, and Sheng-Yih Wang. MPEG Video Encryption Algorithms. *Multimedia Tools and Applications*, 24(1):57–79, 2004.

[3] Jean-Camille Birget. Time-complexity of the word problem for semigroups and the Higman Embedding Theorem. *International Journal of Algebra and Computation*, 8:235–294, 1998.

[4] Jean-Camille Birget. Circuits, coNP-completeness, and the groups of Richard Thompson. *International Journal of Algebra and Computation*, to appear. Preprint (2003), `http://arxiv.org/pdf/math/0310335`.

[5] Jean-Camille Birget. The groups of Richard Thompson and complexity. *International Journal of Algebra and Computation*, to appear. Preprint (2002), `http://arXiv.org/abs/math.GR/0204292`.

[6] Jean-Camille Birget, Spyros S. Magliveras, and Michal Sramka. On public-key cryptosystems based on combinatorial group theory. *Tatra Mt. Math. Publ.*, to appear. Cryptology ePrint Archive, Report 2005/070, `http://eprint.iacr.org/2005/070`.

[7] Jean-Camille Birget, Alexander Yu. Olshanskii, Eliyahu Rips, and Mark V. Sapir. Isoperimetric functions of groups and computational complexity of the word problem. *Annals of Mathematics*, 156(2):467–518, 2002.

[8] Garret Birkhoff. Three Observations on Linear Algebra. *Univ. Nac. Tucuman*, Rev. Ser. A(5):147–151, 1946.

[9] Greg Butler. An Inductive Schema for Computing Conjugacy Classes in Permutation Groups. *Math. Comp.*, 62(205):363–383, 1994.

[10] Don Coppersmith and Adi Shamir. Lattice attacks on NTRU. In *Advances in Cryptology - EUROCRYPT '97*, LNCS 1233, pages 52–61. Springer, 1997.

[11] Dubravko Culibrk, Daniel Socek, and Michal Sramka. Cryptanalysis of the Block Cipher based on the Hopfield Neural Network. *Tatra Mt. Math. Publ.*, submitted.

[12] Philip J. Davis. *Circulant Matrices.* John Wiley & Sons, New York, 2^{nd} edition, 1994.

[13] Ding-Zhu Du and Ker-I Ko. *Theory of Computational Complexity.* Wiley, 2000.

[14] L. Dulmage and I. Halperin. On a Theorem of Frobenius-Konig and J. von Neumann's Game of Hide and Seek. *Trans. Roy. Soc. Canada*, 3(49):23–29, 1955.

[15] Didier Le Gall. MPEG: A Video Compression Standard for Multimedia Applications. *Communications of the ACM*, 34(4):46–58, 1991.

[16] Maria Isabel Gonzalez-Vasco. *Criptosistemas Basados en Teoria de Grupos.* Tesis doctoral, Universidad de Oviedo, Spain, July 2003. `http://www.criptored.upm.es/paginas/investigacion.htm`.

[17] Maria Isabel Gonzalez-Vasco, Consuelo Martinez, and Rainer Steinwandt. *Toward a uniform description of several group based cryptographic primitives.* Cryptography ePrint Archive, Report 2002/048, `http://eprint.iacr.org/2002/048`, 2002.

[18] Maria Isabel Gonzalez-Vasco and Rainer Steinwandt. Reaction attacks on public key cryptosystems based on the word problem. Cryptography ePrint Archive, Report 2002/139, `http://eprint.iacr.org/2002/139`, 2002.

[19] Martin Grotschel, Laszlo Lovasz, and Alexander Schrijver. *Geometric Algorithms and Combinatorial Optimization.* Springer-Verlag, Berlin, New York, 1991.

[20] Donghui Guo, L. M. Cheng, and L. L. Cheng. A New Symmetric Probabilistic Encryption Scheme Based on Chaotic Attractors of Neural Networks. *Applied Intelligence*, 10:71–84, 1999.

[21] Chris Hall, Ian Goldberg, and Bruce Schneier. Reaction attacks against several public-key cryptosystems. In *Information and Communication Security - ICICS'99*, LNCS 1726, pages 2–12. Springer, 1999.

[22] Graham Higman. Finitely presented infinite simple groups. *Notes on Pure Mathematics, The Australian National University, Canberra*, 8, 1974.

[23] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A Ring Based Public Key Cryptosystem. In *Algorithmic Number Theory - ANTS III*, LNCS 1423, pages 267–288. Springer, 1998.

[24] John J. Hopfield. Neural networks and physical systems with emergent collective computational abilities. In *Proc. Natl. Acad. Sci. USA*, vol. 79, pages 2554–2558. Plenum Press, 1982.

[25] Nick Howgrave-Graham, Phong Q. Nguyen, David Pointcheval, John A. Proos, Joseph H. Silverman, Ari Singer, and William Whyte. The Impact of Decryption Failures on the Security of NTRU Encryption. In *Advances in Cryptology - CRYPTO '03*, LNCS 2729, pages 226–246. Springer, 2003.

[26] International Telecommunication Union (ITU-T). *Standard T.81 - Digital compression and coding of continuous-tone still images.* Switzerland, 1992.

[27] Birgit Jenner, Johannes Kobler, Pierre McKenzie, and Jacobo Toran. Completeness Results for Graph Isomorphism. *Journal of Computer and System Sciences*, 66:549–566, 2003.

[28] David Kahn. *Commemorating the 50th Anniversary of the National Security Agency.* A speech delivered at NSA, Fort Meade, MD, `http://www.fas.org/irp/eprint/kahn.html`, 2002.

[29] Auguste Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, IX:5–38 (Jan), 161–191 (Feb), 1883.

[30] Arjen K. Lenstra, Hendrik W. Lenstra, and Laszlo Lovasz. Factoring Polynomials with Rational Coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[31] Roger C. Lyndon and Paul E. Schupp. *Combinatorial group theory.* Springer-Verlag, New York, 1977.

[32] Klaus Madlener and Friedrich Otto. Pseudo-natural algorithms for the word problem for finitely presented monoids and groups. *Journal of Symbolic Computation*, 1:383–418, 1985.

[33] Wilhelm Magnus, Abraham Karrass, and Donald Solitar. *Combinatorial group theory; presentations of groups in terms of generators and relations.* Interscience Publishers, New York, 1966.

[34] Juergen Meyer and Frank Gadegast. *Security mechanisms for multimedia-data with the example MPEG-1-video.* Proj. description of SECMPEG, Technische Universitat Berlin, Germany, 1995.

[35] John A. Proos. *Imperfect Decryption and Partial Information Attacks in Cryptography*. Ph.d. thesis, University of Waterloo, Ontario, Canada, 2003.

[36] Mark V. Sapir, Jean-Camille Birget, and Eliyahu Rips. Isoperimetric and isodiametric functions of groups. *Annals of Mathematics*, 156(2):345–466, 2002.

[37] Bruce Schneier. A Self-Study Course in Block-Cipher Cryptanalysis. *Cryptologia*, 24(1):18–34, 2000.

[38] Claus P. Schnorr. Block Korkin-Zolotarev Bases and Successive Minima. Technical Report TR-92-063, Berkeley, CA, 1992.

[39] Elizabeth A. Scott. A construction which can be used to produce finitely presented infinite simple groups. *Journal of Algebra*, 90:294–322, 1984.

[40] Tanya E. Seidel, Daniel Socek, and Michal Sramka. Cryptanalysis of Video Encryption Algorithms. *Tatra Mt. Math. Publ.*, 29:1–9, 2004.

[41] Tanya E. Seidel, Daniel Socek, and Michal Sramka. Parallel Symmetric Attack on NTRU using Non-Deterministic Lattice Reduction. *Design, Codes and Cryptography*, 32(1-3):369–379, 2004.

[42] Adi Shamir. A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem. In *Advances in Cryptology - CRYPTO '82*, pages 279–288. Plenum Press, 1983.

[43] Charles C. Sims. Determining the Conjugacy Classes of a Permutation Group. In *Computers in Algebra and Number Theory, Proc. of Symposium in Applied Mathematics*, SIAM-AMS Proc. vol. 4, pages 191–195. AMS, 1971.

[44] Douglas R. Stinson. *Cryptography: Theory and Practice*. Chapman & Hall/CRC Press, Boca Raton, FL, 2^{nd} edition, 2002.

[45] Neal R. Wagner and Marianne R. Magyarik. A public-key cryptosystem based on the word problem. In *Advances in Cryptology - CRYPTO '84*, LNCS 196, pages 19–36. Springer-Verlag, 1985.

[46] Celia Wrathall. The word problem for free partially commutative groups. *Journal of Symbolic Computation*, 6:99–104, 1988.

5 Zoznam prác dizertanta

5.1 Zoznam prác dizertanta priamo súvisiacich s dizertačnou prácou

- Dubravko Culibrk, Daniel Socek, Michal Šrámka: *Cryptanalysis of the Block Cipher based on the Hopfield Neural Network*, zaslané do Tatra Mt. Math. Publ. ako príspevok konferencie MORAVIACRYPT '05, Brno, Česká Republika, 15-17. jún 2005.

- Jean-Camille Birget, Spyros S. Magliveras, Michal Šrámka: *On public-key cryptosystems based on combinatorial group theory*, prijaté do Tatra Mt. Math. Publ. ako príspevok konferencie WARTACRYPT '04, Bedlewo, Poĺsko, 1-3. júl 2004. Cryptology ePrint Archive, Report 2005/070. `http://eprint.iacr.org/2005/070`

- Tanya E. Seidel, Daniel Socek, Michal Šrámka: *Cryptanalysis of Video Encryption Algorithms*, Tatra Mt. Math. Publ. 29 (2004), pp. 1-9.

- Tanya E. Seidel, Daniel Socek, Michal Šrámka: *Parallel Symmetric Attack on NTRU using Non-Deterministic Lattice Reduction*, Design, Codes and Cryptography, Vol. 32(1-3), 2004, pp. 369-379.

5.2 Zoznam ďalších prác dizertanta

- Michal Šrámka: *Cryptanalysis of the Cryptosystem Based on DLP* $\gamma = \alpha^a \beta^b$, zaslané do International Journal of Network Security, 2006.

- Shanzhen Gao, Michal Šrámka, Zhonghua Tan: *Graphs on Surfaces*, prijaté do Congressus Numerantium, 2005.

- Michal Šrámka, Otokar Grošek: *Efficiency of Elliptic Curve Cryptography*, JEEE, Vol. 54(12/s), 2003, pp. 10-14.

6 Summary

The submitted dissertation presents four research papers that in one way or another contribute to the area of study of cryptanalysis. Although the four papers explore different cryptographic schemes with different underlying mathematical problems, the outcome of the research exhibits the wide impact a cryptanalysis may result in.

In the first part, the cryptanalysis of a public-key encryption scheme based on the word problem led to design of another, more secure one. This was an example of straightforward application of cryptanalytic results in cryptography. In the second part, the symmetry of the NTRU-like lattice, namely birotation, was explored and led to the design of a faster algorithm for a basis reduction of such a lattice. The proposed algorithm is non-deterministic. In addition, the algorithm can be highly parallelized. In this case, the careful analysis of the underlying problem of a public-key encryption scheme allowed for a speedup in a known attack.

The third part, cryptanalysis of a block cipher based on the Hopfield neural network, resulted in a solution for an old matrix conjugacy problem with many applications. The block cipher itself become obsolete because of the insecurities found. Last but not least, the fourth part of the dissertation dealt with recently proposed, poorly designed symmetric ciphers proposed for fast video encryption that are susceptible to classical and trivial attacks.