Fakulta elektrotechniky a informatiky
Slovenskej Technickej Univerzity v Bratislave

Ing. Pavol Zajac

Autoreferát dizertačnej práce

Discrete Logarithm Problem in Degree Six Finite Fields

na získanie vedecko–akademickej hodnosti
philosophiae doctor, PhD.
v doktorandskom študijnom programe
9.1.9 aplikovaná matematika

Bratislava 2008

Dizertačná práca bola vypracovaná v dennej forme doktorandského štúdia na Katedre aplikovanej informatiky a výpočtovej techniky FEI STU v Bratislave.

Predkladateľ: Ing. Pavol Zajac
KAIVT FEI STU
Ilkovičova 3
812 19 Bratislava

Školiteľ: Prof. RNDr. Otokar Grošek, PhD.
FEI STU Bratislava

Oponenti: Prof. Igor A. Semaev
Institutt for informatikk
HIB - Thormøhlensgt. 55
N-5020 Bergen
Norway

Prof. Rainer Steinwandt
Department of Mathematical Sciences
Florida Atlantic University
777 Glades Road
Boca Raton, FL 33431
USA

Prof. RNDr. Štefan Porubský, DrSc.
Institute of Computer Science
Academy of Sciences of the Czech Republic
Pod Vodarenskou vezi 2
182 07 Prague 8
Czech Republic

Autoreferát bol rozoslaný dňa .....

Obhajoba dizertačnej práce sa koná ..... o ..... h
na Fakulte elektrotechniky a informatiky STU, Ilkovičova 3, 812 19 Bratislava,
v .....

doc. Ing. Ján Vajda, CSc.
Dekan FEI STU

Obsah

Úvod

Asymetrická kryptografia je základom veľkého množstva praktických aplikácií, od základnej výmeny kľúčov cez elektronický podpis až po komplexné riešenia elektronického obchodu. Bezpečnosť systémov asymetrickej kryptografie stojí na (zväčša nedokázaných) predpokladoch o náročnosti výpočtového riešenia niektorých matematických problémov, napr. systém RSA [1] je bezpečný iba v prípade, keď protivník nevie faktorizovať (dostatočne veľký) súčin dvoch prvočísel. DSA [2], Diffie-Hellmanova schéma výmeny kľúčov [3], a podobne aj množstvo ďalších protokolov, je možné narušiť v prípade, že oponent dokáže riešiť problém diskrétneho logaritmu (PDL), t.j. určenia neznámeho exponentu x v kongruencii $b \equiv a^x \pmod{p}$.

Na riešenie týchto dvoch problémov je možné použiť algoritmus NFS (*„Number Field Sieve"*, doslovne: sito číselných polí) [4, 5]. Tento algoritmus má subexponenciálnu zložitosť, čo spolu s rastom výkonu súčasných počítačov spôsobuje rýchle zastarávanie kľúčov asymetrickej kryptografie. V súčasnosti najčastejšie 1024-bitové kľúče sú na hranici použiteľnosti, a sú odporúčané len pre krátkodobé šifrovanie. Na zvýšenie bezpečnosti asymetrických systémov je potrebné tieto kľúče zväčšovať, čo vedie k nárastu nárokov na hardvér a zníženiu výkonu kryptosystému.

Jedným z riešení problému zastarávania kľúčov v prípade kryptosystémov založených na báze diskrétneho logaritmu je použitie XTR [6, 7]. Z pohľadu kryptoanalýzy dochádza k nahradeniu klasického PDL v multiplikatívnej grupe konečného poľa $\mathbb{F}_p$ zovšeobecneným problémom diskrétneho logaritmu v špeciálnej podgrupe $\mathbb{F}_{r^6}$ (XTR-DL). Pri vhodnej voľbe parametrov sa predpokladá, že zložitosť riešenia PDL závisí len na veľkosti poľa, t.j. pre $r \approx p/6$ by mali byť kryptosystém na báze klasického PDL a XTR systém rovnako bezpečný.

Až donedávna, kedy na CRYPTO 2006 boli publikované nové výsledky [8], nebolo zrejmé, či sa algoritmus rovnakej zložitosti ako NFS dá aplikovať aj na rozšírenia konečných polí malého stupňa so stredne veľkou charakteristikou. Do tejto kategórie spadá aj XTR-DL v rozsahu prípadov, ktoré dokážeme prakticky riešiť (aj pri zapojení celosvetovej výpočtovej sily). Nové výsledky síce naznačili možný spôsob realizácie výpočtu a jeho teoretické zdôvodnenie, ale až doposiaľ, podľa nám dostupných informácií, neboli publikované žiadne výpočty XTR-DL pomocou NFS.

V dizertačnej práci (a súvisiacich doteraz zverejnených článkoch a konferenčných príspevkoch) sme zverejnili praktickú implementáciu upraveného NFS algoritmu, ktorý rieši XTR-DL problém. Vykonali sme preosievacie experimenty až do 240 bitovej veľkosti poľa, a realizácii väčších experimentov bránia už len praktické hranice na rozpočet a dĺžku trvania experimentov. Okrem popisu experimentov a ich výsledkov obsahuje dizertačná práca aj poznámky k rôznych technickým a matematickým aspektom realizácie NFS algoritmu. Tieto sú zväčša zamerané na náš špecifický prípad riešenia PDL v poliach stupňa 6, ale ich dôsledky môžu byť zaujímavé aj pre iné aplikácie NFS (faktorizáciu a klasický PDL).

Čiastočné výsledky boli doteraz zverejnené (alebo prijaté) v publikáciách uvedených v časti 5.1. Výskum bol spolufinancovaný z grantov VEGA 1/3115/06 a ESF SORO/JPD3-038/2005, a Národným Bezpečnostným Úradom SR. K dosiahnutiu výsledkov práce prispela aj odborná pomoc a pripomienky vedúceho práce prof. Otokara Grošeka a doc. Ladislava Satka. Na praktickej realizácii na KAIVT FEI STU sa podieľali aj Mgr. Marek Sýs, Ing. Vladislav Novák a Ing. Matúš Jókay.

1 Ciele dizertačnej práce

Využitie algoritmu NFS na faktorizáciu je známe približne od roku 1990 [4]. Gordonova adaptácia NFS pre riešenie klasického PDL (v poliach $\mathbb{F}_p$) pochádza z roku 1993 [9]. V tomto roku tiež bol zverejnený algoritmus Adlemana a DeMaraisa na riešenie PDL v ľubovoľnom konečnom poli [10]. Jeho zložitosť je však vyššia ako zložitosť NFS. V čase stanovenia pôvodných cieľov dizertácie nebolo známe, či je možné použiť algoritmus rovnakej zložitosti ako NFS na riešenie PDL v ľubovoľnom konečnom poli. Pre nás obzvlášť zaujímavá boli konečné polia stupňa 6, spojené s problematikou XTR.

Preto pôvodné ciele dizertačnej práce boli stanovené nasledovne:

1. Aplikovať algoritmus NFS na riešenie problému diskrétneho logaritmu v XTR grupe, resp. vyvinúť nový algoritmus so subexponenciálnou zložitosťou.
2. Preskúmať možnosti heuristickej optimalizácie algoritmu.
3. Dosiahnuť rekordné riešenie XTR-DL problému.

Počas riešenia dizertačnej práce na konferencii CRYPTO 2006 publikovali Joux et.al. článok [8], kde prezentovali spôsob riešenia PDL v ľubovoľnom konečnom poli algoritmom NFS. Základ tohto riešenia však už nadväzoval na predošlú publikáciu [11], ktoré sme mali rozpracované. Avšak vzhľadom na to, že jeden z pôvodných cieľov dizertácie bol teoreticky vyriešený, rozšírili sme záber dizertácie hlavne v oblasti praktickej realizácie o nasledujúce ciele:

4. Implementovať troj– a viacrozmerné sito.
5. Odvodiť a experimentálne overiť optimálnu parametrizáciu sita pre prípad využitia NFS na riešenie PDL v poliach stupňa 6.

2 Teória a metódy

Nech p, q sú prvočísla také, $q|p^2 - p + 1$. Ďalej nech G je podgrupa rádu $p^2 - p + 1$ konečného poľa $\mathbb{F}_{p^6}$, a nech $g \in G$ je generátor podgrupy $S \subset G$ rádu q. Lenstra a Verheul [6, 7] popisujú spôsob efektívneho výpočtu stopy $Tr_{\mathbb{F}_{p^6}/\mathbb{F}_{p^2}}(g^d)$ zo známej stopy $Tr_{\mathbb{F}_{p^6}/\mathbb{F}_{p^2}}(g)$, pre ľubovoľné d. Táto operácia je ekvivalentná operácii umocnenia v $\mathbb{F}_{p^6}$. Keďže stopy sú prvky $\mathbb{F}_{p^2}$, na ich reprezentáciu potrebujeme len zhruba $2\log_2 p$ bitov, namiesto $6\log_2 p$ bitov potrebných na reprezentáciu celého prvku poľa $\mathbb{F}_{p^6}$. Navyše XTR aritmetika realizuje operáciu umocnenia asi 8-krát rýchlejšie ako pôvodná aritmetika celého poľa.

Problém XTR diskrétneho logaritmu (XTR-DL) definujeme ako problém výpočtu neznámeho parametra $d \in \mathbb{Z}_q$, ak poznáme $Tr_{\mathbb{F}_{p^6}/\mathbb{F}_{p^2}}(g^d)$. XTR-DL je polynomicky redukovateľný na problém diskrétneho logaritmu v poli $\mathbb{F}_{p^6}$ (pozri kapitolu 4 dizertačnej práce). Preto XTR je možné využiť vo veľkom množstve kryptosystémov, ktoré využívajú modulárne umocnenie, napr. ElGamalov kryptosystém, DSA, Diffie-Hellmanova schéma výmeny kľúčov a iné. XTR-DL je možné riešiť dvoma základnými spôsobmi (viac informácií v kapitole 3 dizertačnej práce):

1. Generickým algoritmom [12, 13] priamo v grupe S. Je možné použiť priamo XTR reprezentáciu a aritmetiku. Zložitosť útoku je však $O\left(q^{1/2}\right)$, t.j. exponenciálna a zdvojnásobuje sa každým pridaným bitom p (pri doporučenej voľbe maximálneho možného q).

2. Algoritmom na báze indexových metód [10, 8]. V tomto prípade je potrebné transformovať XTR-DL na problém diskrétneho logaritmu v poli $\mathbb{F}_{p^6}$. Algoritmy na báze indexových metód majú subexponenciálnu zložitosť danú vo forme funkcie
$$L_x(\alpha, c) = \exp\left(c(\ln x)^{\alpha}(\ln\ln x)^{(1-\alpha)}\right). \tag{1}$$
Najrýchlejším algoritmom tejto triedy je algoritmus NFS [8], ktorý má zložitosť $L_{p^6}(1/3, c + o(1))$, s heuristicky odvodenou $c = (64/9)^{1/3} \doteq 1.923$.

Podrobný popis algoritmu NFS je dostupný v kapitole 5 dizertačnej práce. V stručnosti: Nech $f_1, f_2 \in \mathbb{Z}[x]$ sú monické ireducibilné polynómy so spoločným koreňom t v $\mathbb{F}_{p^6}$. V praxi polynóm f_1 je vhodne zvolený polynóm s malými koeficientami, a $f_2(x) = f_1(x) \pm p$. Voľbou polynómov sa podrobne zaoberá kapitola 6 dizertačnej práce. Nech $\alpha_i \in \mathbb{C}$ je koreňom polynómu $f_i, i = 1, 2$. Potom $K_i = \mathbb{Q}(\alpha_i)$ je algebraické číselné pole. Nech ďalej $\phi_i : K_i \to \mathbb{F}_{p^n}$, $\phi(\sum a_k \alpha_i^k) = \sum a_i t^i \mod p$, $i = 1, 2$. Tieto dva zobrazenia sú okruhovým homomorfizmom so spoločným kernelom, ktorým je ideál stupňa n ležiaci nad p (t.j. konečné pole $\mathbb{F}_{p^6}$).

Nech $\mathcal{O}_K$ označuje okruh celých čísel poľa K. Nech $\xi \in \mathcal{O}_K$ má normu $N(\xi) = \prod p_j^{e_j}$, pričom $p_j < B$. Potom sa dá hlavný ideál $(\xi) = \xi\mathcal{O}_K$ jednoznačne faktorizovať na súčin prvoideálov ležiacich nad p_j. Takéto ξ budeme označovať ako B-hladké algebraické celé číslo.

Nech pre pár B-hladkých algebraických čísel $\xi_1 \in \mathcal{O}_{K_1}$ a $\xi_2 \in \mathcal{O}_{K_2}$ platí $\phi_1(\xi_1) = \phi_2(\xi_2)$. Pre takýto pár vieme zostaviť rovnicu v tvare

$$\sum_{j=0}^{r_1} \lambda_j^{(1)}(\xi_1)\Lambda_j^{(1)} + \sum_j v_{\mathfrak{p}_j}(\xi_1)x_j^{(1)} \equiv \sum_{k=0}^{r_2} \lambda_k^{(2)}(\xi_2)\Lambda_k^{(2)} + \sum_k v_{\mathfrak{p}_k}(\xi_2)x_k^{(2)} \pmod q, \tag{2}$$

kde $\Lambda_j^{(1)}, \Lambda_k^{(2)}, x_j^{(1)}$, a $x_k^{(2)}$ sú neznáme „virtuálne logaritmy" [14]. Pár hladkých čísel a k nim prislúchajúcu rovnicu označíme zjednodušene „hladká rovnica".

Množina všetkých prvoideálov $\mathcal{O}_K$, ktoré ležia nad prvočíslami $p_j < B$ nazývame (algebraická) faktorová báza. Nech c_1, c_2 sú počty prvkov faktorových báz v K_1, K_2. Potom počet možných neznámych virtuálnych logaritmov v ľubovoľnej hladkej rovnici je najviac $c = c_1 + c_2 + o(1)$. Ak sa nám podarí nájsť viac ako c lineárne nezávislých hladkých rovníc, je možné nájsť hodnoty virtuálnych logaritmov ako netriviálne riešenie takéhoto systému rovníc. Za pomoci virtuálnych logaritmov je potom možné podobným postupom vypočítať diskrétne logaritmy prvkov $\mathbb{F}_{p^n}^*$, a teda aj riešiť XTR-DL problém.

Pre efektívnu implementáciu algoritmu NFS je nutné vedieť rýchlo hľadať hladké rovnice. Na to slúži algoritmus preosievania (angl. *„sieve"*). Aby bolo možné nazbierať dostatočné množstvo hladkých relácií v prípade polí stupňa 6, je nutné preosievať trojrozmerný región. To znamená, že čísla ξ_i zapíšeme v tvare $\xi_i = x + y\alpha_i + z\alpha_i^2$. Pri preosievaní využívame fakt, že je ľahké určiť všetky algebraické čísla, ktorých normy sú deliteľné daným prvočíslom p_j. Samotné sito a jeho efektívnu

realizáciu popisuje kapitola 7 dizertačnej práce. Okrem toho sa v tejto kapitole zaoberáme nastavením parametrov sita, jeho optimálnou implementáciou, a rôznymi variantami realizácie.

I keď asymptotické správanie algoritmu NFS je známe, konkrétna realizácia je silne ovplyvnená výberom parametrov a využitím rôznych heuristík. Viaceré takéto heuristiky spôsobujú pseudonáhodné správanie algoritmu. Napríklad pre zrýchlenie preosievania nepoužívame príliš malé prvočísla, ale ich príspevok nahrádzame zvolenou konštantou. Celkový príspevok sa dá modelovať náhodnou premennou. Pri správnom pravdepodobnostnom modele potom vieme vhodne sito parametrizovať. Vplyv niektorých heuristík je však ťažko modelovateľný, hlavne ak závisí na rozdelení hladkých noriem v celom trojrozmernom preosievanom regióne, alebo na konkrétnej softvérovej a hardvérovej implementácii. Naším prístupom bolo teda pokúsiť sa preniknúť do podstaty jednotlivých heuristík a ich kombinácií jednak teoreticky, a jednak prostredníctvom experimentov. Výsledky viacerých takýchto experimentov sú zhrnuté v kapitole 8 dizertačnej práce. V tejto kapitole sú aj uvedené hlavné experimentálne výsledky konkrétnych preosievaní určených pre riešenie XTR-DL s čoraz väčším parametrom p. Výsledky experimentov, resp. pri implementačne závislých experimentoch metodika, s ktorou boli vykonávané, môžu slúžiť aj ďalším odborníkom zaoberajúcim sa problematikou NFS aj v iných aplikáciách.

3 Dosiahnuté výsledky dizertačnej práce

Dizertačná práca dosiahla stanovené ciele. Podarilo sa nám implementovať riešenie XTR-DL problému pomocou aplikácie algoritmu NFS. Na jeho fungovanie bolo potrebné vyvinúť a efektívne implementovať algoritmus viacrozmerného sita. Teoreticky a experimentálne sme preskúmali problémy voľby vhodného preosievacieho polynómu, optimálneho nastavenia preosievacieho regiónu a voľby tolerancie pre stochastickú realizáciu preosievania. Okrajovo sme sa zaoberali aj využitím viac ako dvoch preosievacích polynómov v NFS a tiež využitím metódy veľkých faktorov. Tieto sa však ukázali ako nezaujímavé v oblasti parametrov aktuálne riešených inštancií problému XTR-DL, a teda pre dosiahnutie cieľov dizertácie.

V tabuľke 1 sú zhrnuté výsledky preosievania pre rôzne inštancie XTR-DL problému. Ich náročnosť je daná veľkosťou prvočísla. Nami dosiahnuté rekordné riešenie používalo 40-bitové p, t.j. veľkosť poľa bola približne 2^{240}. Na samotný výpočet bolo potrebných približne 266 MIPS rokov. Riešenie vyšších inštancií problému je obmedzené len možnosťou alokácie dostatočného výpočtového výkonu, pričom v tabuľke 1 je uvedená odhadovaná doba riešenia na 1 počítači typu AMD Athlon 2 GHz.

Okrem aplikácie na riešenie XTR-DL problému sú výsledky práce dôležité aj z hľadiska súvisu s inými kryptografickými algoritmami, ktoré je možné riešiť pomocou algoritmu NFS. Implementácia NFS pre PDL v poliach stupňa 6 je rádovo asi až 1000-krát pomalšia ako je softvér použitý na dosiahnutie súčasných svetových rekordov v oblasti faktorizácie/PDL stupňa 1. Rozdiel čiastočne spočíva v nízkoúrovňových optimalizáciách algoritmu (približne 55 % času je možné ušetriť len na ďalšej cache optimalizácii). Hlavný rozdiel je však vo vyššej náročnosti algoritmu, napr. je nutné používať polynómy vyšších stupňov, taktiež na výpočet noriem sa používa zložitejší polynóm až v 3 premenných. Preto narušenie systému na báze

$\log_2 p$	$\log_2 B$	Báza	Čas [s]	Očakávaný čas
20	16	12325	24691	—
24	18	43828	2746	$<$ 1.0 hod
28	19	97816	13636	4.0 hod
32	20	200137	78891	22.0 hod
36	21	365666	449744	4.9 deň
40	23	893707	2087070	26.1 deň
50	25	—	—	0.6 rok
60	27	—	—	4 rok
70	29	—	—	29 rok
80	31	—	—	200 rok
90	33	—	—	1400 rok
100	34	—	—	3704 rok

Tabuľka 1: Súhrn výsledkov preosievania s extrapoláciou pre väčšie p.

XTR je prakticky zložitejšie, ako narušenie ekvivalentného RSA/DSA systému.

Experimentálne výsledky práce môžu slúžiť aj ako podklad pre ďalší výskum v tejto oblasti, napr. výsledky týkajúce sa optimálnej voľby preosievacieho regiónu sa týkajú aj implementácií NFS určených na faktorizáciu. Ukazuje sa, že i keby postačovalo preosievanie dvojrozmerného regiónu, je vhodné tento región afinne posunúť v smere osi z. To má za následok odstránenie nutnosti kontrolovať $\gcd(x, y)$, čo by pri nezmenenej hustote hladkých noriem viedlo približne ku štvornásobnému množstvu preosiatych rovníc. Dodatočné rovnice sa potom dajú využiť na zefektívnenie štruktúrovanej Gausovej eliminácie. Pre plnohodnotné využitie tejto metódy je však zrejme nutné zmeniť spôsob a kritériá výberu preosievacích polynómov.

Referencie

[1] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[2] NIST. Digital Signature Standard (DSS). FIPS PUB 186-2, January 2000.

[3] Whitfield Diffie and Martin Hellman. New direction in cryptography. *IEEE Trans. Info. Theory. IT*, 22(1-2):644–654, 1976.

[4] A.K. Lenstra, H.W. Jr. Lenstra, M.S. Manasse, and J.M. Pollard. The number field sieve. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, pages 564–572, 1990.

[5] Arjen K. Lenstra and Hendrik W. Lenstra, editors. *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1993. ISBN: 978-3-540-57013-4.

[6] Arjen K. Lenstra and Eric R. Verheul. The XTR public key system. *Lecture Notes in Computer Science*, 1880:1+, 2000.

[7] A.K. Lenstra and E.R. Verheul. An overview of the XTR public key system. In *Publickey cryptography and computational number theory (Warsaw, 2000)*, pages 151–180. de Gruyter, Berlin, 2001.

[8] Antoine Joux, Reynald Lercier, Nigel Smart, and Frederick Vercauteren. The number field sieve in the medium prime case. In *Advances in Cryptology - CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 326–334. Springer-Verlag, 2006.

[9] D. Gordon. Discrete logarithms in $GF(p)$ using the Number Field Sieve. *SIAM Journal on Discrete Mathematics*, 6(1):124–138, 1993.

[10] Leonard M. Adleman and Jean DeMarrais. A subexponential algorithm for discrete logarithms over all finite fields. In Douglas Stinson, editor, *Proceedings of CRYPTO'93*, volume 773 of *Lecture Notes in Computer Science*, pages 147–158. Springer, 1993.

[11] A. Joux and R. Lercier. Improvements to the general number field sieve for discrete logarithms in prime fields: a comparison with the gaussian integer method. *Mathematics of Computation*, 72:953–967, 2003.

[12] Daniel Shanks. Class number, a theory of factorization, and genera. In Donald J. Lewis, editor, *Proc. Symp. Pure Math.*, volume 20, pages 415–440. Amer. Math. Soc., 1971. MR 47:4932.

[13] John M. Pollard. Monte Carlo methods for index computation mod p. *Mathematics of Computation*, 32:918–924, 1978.

[14] Oliver Schirokauer. Virtual logarithms. *Journal of Algorithms*, 57:140–147, 2005.

5 Zoznam publikácií a citácií

5.1 Publikované výsledky dizertačnej práce

Sýs, M., and Zajac, P. Discrete logarithm problem and its applications in cryptography. *Begabtenförderung im MINT Bereich 12* (2005), 129–146.

Zajac, P. Generalized line sieve algorithm. In *ELITECH '07*. The 9th Conference for PhD Students Electrical Engineering and Information Technology : Bratislava, Slovak Republic, 16.5.2007. STU (2007), CD-Rom.

Zajac, P. How to solve XTR-DL using NFS. In *Mikulášska Kryptobesídka 2007*, Sborník příspěvků. Praha, 6.-7.12.2007. Trusted Network Solutions (2007), 91–97.

Zajac, P. Remarks on the NFS complexity. Submited to: *TATRACRYPT 2007*, Tatra Mountains Math. Publ. (2008).

Zajac, P. Smoothness probability in degree six number fields. *Journal of Electrical Engineering 58*, 7/s (2007), 14–16.

5.2 Ostatné práce

Grošek, O., Horák, P., and Zajac, P. On complexity of round transformations. To appear: *Discrete Mathematics*, Elsevier (2008).

Grošek, O., Vojvoda, M., and Zajac, P. *Klasické šifry*, STU v Bratislave (2007). ISBN 978-80-227-2653-5.

Grošek, O., Vojvoda, M., Zanechal, M., and Zajac, P. *Základy kryptografie*, STU v Bratislave (2006). ISBN 80-227-2415-7.

Grošek, O., and Zajac, P. Automated cryptanalysis of classical ciphers. To appear: *Encyclopedia of Artificial Intelligence*, Juan R. Rabuñal, Julian Dorado, and Alejandro Pazos Sierra, Eds., Information Science Reference (2008). ISBN 978-1-59904-849-9.

Grošek, O., and Zajac, P. Automated cryptanalysis — Language processing. To appear: *Encyclopedia of Artificial Intelligence*, Juan R. Rabuñal, Julian Dorado, and Alejandro Pazos Sierra, Eds., Information Science Reference (2008). ISBN 978-1-59904-849-9.

Grošek, O., and Zajac, P. Efficient Selection of the AES-Class MixColumns Parameters. *WSEAS Transactions on Information Science and Applications 4*, Iss. 4 (2007), 663–668.

Grošek, O., and Zajac, P. Graphs Connected with Block Ciphers. *WSEAS Transactions on Information Science and Applications 3*, Iss. 2 (2006), 439–443.

Zajac, P. Automated Attacks on Transposition Ciphers. *Begabtenförderung im MINT Bereich 14* (2006), 27–42.

Zajac, P. Ciphertext Language Identification. *Journal of Electrical Engineering 57*, 7/s (2006), 26–29.

Zajac, P. Generating the Suitable ECDSA Domain Parameters. *Journal of Electrical Engineering 55*, 12/s (2004), 43–45.

Zajac, P. Remark to the Mixing Layer of SPN Ciphers. *Journal of Electrical Engineering 56*, 12/s (2005), 32–35.

5.3 Príspevky na konferenciách

Grošek, O., Novák, V., Sýs, M., and Zajac, P. Dlhodobá archivácia elektronických dokumentov. In: *PKI 2004 : Realizácia elektronického podpisu v praxi.*, Bratislava, (2004).

Grošek, O., Novák, V., Sýs, M., and Zajac, P. Problémy elektronickej archivácie. Rump session, *Mikulášska kryptobesídka*, Praha, TNS (2004).

Grošek, O., and Zajac, P. A bridge between design of block ciphers and Boolean matrices. In: *MoraviaCrypt 2005 : 5th Central European Conference on Cryptography.* Brno, Masaryk University (2005).

Grošek, O., and Zajac, P. A remark to minimal graphs connected with block ciphers. In: *Proceedings of 4th WSEAS International Conference on Information Security, Communications and Computers (ISCOCO 2005).* Tenerife, WSEAS Press (2005), 78–82.

Grošek, O., and Zajac, P. Searching for a Different AES-Class MixColumns Operation. In: *Proceedings of the WSEAS Conference: 6th International Conference on Applied Computer Science.* Tenerife, WSEAS Press (2006), 307–310.

Zajac, P. Generating suitable ECDSA domain parameters. In: *ISCAM 2004: International Conference in Applied Mathematics for Undergraduate and Graduate Students.* Abstracts. Bratislava, STU (2004).

Zajac, P. N-Gram-Based Cryptanalysis of Classical Substitution Ciphers. In: *ISCAM 2006: International Conference in Applied Mathematics for Undergraduate and Graduate Students.* Abstracts. Bratislava, STU (2006).

Zajac, P. Remark to the mixing layer of SPN ciphers. In: *ISCAM 2005: International Conference in Applied Mathematics for Undergraduate and Graduate Students.* Abstracts. Bratislava, STU (2005).

Zajac, P. Remarks on Polynomial Selection for the NFS. In: *ISCAM 2007: International Conference in Applied Mathematics for Undergraduate and Graduate Students.* Abstracts. Bratislava, STU (2007).

Zajac, P. Remarks on Using NFS to Solve DLP in XTR Supergroup. In: *Tatracrypt 2007: 7th Central European Conference on Cryptography.* Smolenice, SAV (2007).

Zajac, P. Using n-Gram Ranking in Ciphertext Analysis. In: *Nyírcrypt 2006: 6th Central European Conference on Cryptography.* Debrecen, University of Debrecen, (2006).

Summary

The aim of the thesis was to solve the XTR-discrete logarithm (XTR-DL) problem [6, 7], i.e. the problem of finding unknown private key d of the XTR based cryptosystem with parameters p, q using public XTR traces $Tr(g)$ and $Tr(g^d)$. Chapter 3 of the thesis summarizes the state-of-the-art in the area of the discrete logarithm problem (DLP) and basic methods to solve it. Chapter 4 shows, that the exact value of d can be determined by computing two discrete logarithms in $\mathbb{F}_{p^6}$ modulo q, and at most 5 exponentiations in XTR group. All operations in transforming the problem from XTR-DL to DL problem in $\mathbb{F}_{p^6}$ have polynomial complexity.

The asymptotically fastest algorithm to solve the DLP in $\mathbb{F}_{p^6}$ is the Number Field Sieve (NFS). NFS can also be seen as a class of algorithms. Specific algorithms in this class can be applied to either solve the integer factoring problem for special, and general numbers respectively, and the DLP in various finite fields. However, to our best knowledge, until now the algorithm of this class to solve the DLP in extension fields of degree 6 have not been practically implemented. In the thesis, we present a practical implementation of the said algorithm based on the ideas of [8].

Chapter 5 of the thesis summarizes the Number Field Sieve and its adaptation to degree 6 finite fields. Remarks and basic complexity estimates for applications of NFS to $\mathbb{F}_{p^6}$-DLP are discussed, as well as various applicable NFS variants and implementation options. Although the asymptotic complexity of the NFS is known, these options have a strong impact on performance of the algorithm for "smaller instancesöf the problem. However, in the XTR-DL case, the notion "small instance"covers the whole range of problem instances, that are solvable by the current technology.

A very problem specific part of each algorithm from the NFS class is the polynomial selection. As shown in Chapter 6 of the thesis, the difference between the good and the bad choice of the sieve polynomial can lead in ideal case to a four times smaller factor base size. Unfortunately, we were unable to find a significant distinguishing factor determining the suitability of the sieve polynomial (although some possible candidate factors are presented). On the other hand, it is possible to evaluate the fitness of sieve polynomials using statistical methods.

Chapter 7 summarizes our most important results connected with sieving algorithm. Classical sieve algorithms sieve a bounded two-dimensional region (of algebraic integers). These sieves are unable to find enough smooth equations required for the success of the NFS, as the smoothness density in the sieve region is too small. We have extended the sieving algorithm to higher dimensions, as the optimal sieving region for degree 6 DLP is three dimensional. Using this extended sieve we have collected enough smooth equations, and were able to finish the DLP computation. Results of various experiments aimed at optimal NFS parametrization, and final sieving results are summarized in Chapter 8 of the thesis.

The thesis covers also some minor mathematical problems that are specific to the NFS and the line sieving algorithm, such as contribution of small primes, probabilistic sieve behavior, optimal sieve region and others. Although the results are derived for the specific instance of NFS, they can influence also the mainstream NFS applications (factoring of integers, classical DLP).