Fakulta elektrotechniky a informatiky
Slovenskej Technickej Univerzity v Bratislave

Mgr. Michal Mikuš

Autoreferát dizertačnej práce

Homomorfné kryptosystémy

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

Bratislava 2012

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

Predkladateľ: Mgr. Michal Mikuš
ÚIaM FEI STU
Ilkovičova 3
812 19 Bratislava

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

Oponenti: doc. RNDr. PaedDr. Pavel Trojovský, Ph.D.
Katedra matematiky
Přírodovědecká fakulta
Univerzity Hradec Králové
Rokitanského 62
500 03 Hradec Králové III

doc. RNDr. Martin Stanek, PhD.
Katedra Informatiky
Fakulta Matematiky, Fyziky a Informatiky
Univerzity Komenského
Mlynská dolina
842 48 Bratislava

Autoreferát bol rozoslaný dňa 19.12.2012

Obhajoba dizertačnej práce sa koná 15.1.2013 o 13:00 hod.
na Fakulte elektrotechniky a informatiky STU, Ilkovičova 3, 812 19 Bratislava,
v miestnosti C502.

prof. Ing. Gabriel Juhás, PhD.
Dekan FEI STU

Obsah

Úvod **2**

1 Ciele dizertačnej práce **3**

2 Dosiahnuté výsledky dizertačnej práce **4**

3 Literatúra **6**

4 Zoznam publikácií a citácií **8**
4.1 Publikované výsledky dizertačnej práce 8
4.2 Ostatné práce 8
4.3 Príspevky na konferenciách 8

Summary **10**

Úvod

Oblasť homomorfných kryptosystémov je skúmaná 34 rokov, problém existencie a prípadného využitia homomorfného kryptosystému bol prvýkrát otvorený v roku 1978 v práci [1]. Hovoríme, že kryptosystém je homomorfný, ak umožňuje počítanie určitej operácie (súčtu, násobenia) nad otvorenými textami, len pomocou zodpovedajúcich šifrových textov, t.j. bez odhalenia akejkoľvek informácie o otvorených textoch.

Sú známe viaceré kryptosystémy, ktoré umožňujú počítanie jednej takejto operácie. Najznámejší asymetrický kryptosystém RSA je multiplikatívne homomorfný, t.j. umožňuje výpočet zašifrovaného súčinu dvoch otvorených textov – jednoduchým súčinom zodpovedajúcich zašifrovaných textov. Príkladom aditívne homomorfného kryptosystému je napr. Paillierov kryptosystém, alebo ElGamalov kryptosystém založený na eliptických krivkách.

Hlavným problémom v tejto oblasti je existencia a konštrukcia homomorfného kryptosystému, ktorý by umožňoval homomorfné počítanie oboch operácií nad otvorenými textami. Takýto kryptosystém sa nazýva algebraicky, alebo plne homomorfný. Do roku 2009 bol problém existencie plne homomorfného kryptosystému otvorený, aj keď najvýznamnejšie konštrukcie plne homomorfných kryptosystémov [2], [3], [4], [5] umožňovali výpočet neobmedzene veľa sčítaní a niekoľkých násobení.

V roku 2009 bola publikovaná prelomová práca [6], kde bola prezentovaná všeobecná konštrukcia plne homomorfného systému založeného na diskrétnych mriežkach. Táto práca a následne [7] ukázali nový prístup ku konštrukcii plne homomorfného kryptosystému. Tento prístup spočíva v konštrukcii čiastočne (plne) homomorfnej schémy, ktorá dokáže korektne vyhodnotiť len určitý počet operácií. Za predpokladu, že táto čiastočne homomorfná schéma má dostatočne jednoduchý dešifrovací predpis, tak technikou tzv. „bootstrappingu" je možné z tejto schémy vytvoriť plne homomorfnú schému.

Následné práce [8], [9], [10], [11] a [12], [13], [14] boli zamerané na praktickú realizáciu tejto konštrukcie, pričom v [10] bola prezentovaná prvá plne homomorfná schéma. Spoločnou vlastnosťou týchto kryptosystémov je nízka efektivita a nepraktický prenosový pomer spôsobený použitou technikou „bootstrappingu".

Negatívne aspekty originálnej Gentryho konštrukcie – nízku efektivitu a veľa rôznych predpokladov na bezpečnosť – sa snažia obísť najnovšie konštrukcie plne homomorfných kryptosystémov v [15] a [16]. Hlavný prínos spočíva v postupnej redukcii šumu v zašifrovanom texte pri každej homomorfnej operácii. Toto sa dá dosiahnuť vhodne zvolenou zmenou modula q, ktorým je redukovaný každý šifrový text. Autori v [16] ukazujú, že takto je možno úplne vynechať operáciu bootstrappingu a vďaka tomu je možné takto konštruovať efektívnejšiu plne homomorfnú schému.

Dizertačná práca je zameraná na implementáciu čiastočne homomorfnej schémy z [10] a porovnanie homomorfných vlastností, ak by sme zväčšili priestor otvorených textov z dva na ľubovoľné prvočíslo. Ukázali sme spôsob, ako možno túto rozšírenú čiastočne homomorfnú schému využiť na obmedzené výpočty nad ľubovoľne veľkým priestorom otvorených textov.

V práci sme ďalej analyzovali bezpečnosť implementovanej schémy voči LLL-algoritmu na redukciu mriežok. Ukazujeme, že útok so znalosťou šifrového textu

pomocou LLL algoritmu je (využitím bežne dostupnej výpočtovej sily) realizovateľný len pre dimenzie 128 a menej. Prezentujeme však aj dve varianty útoku pomocou LLL algoritmu, ktoré 10000-násobne znižujú časovú náročnosť útoku. Tieto varianty však zatiaľ neboli úspešné pre dimenzie vyššie ako 128.

Čiastočné výsledky práce boli zverejnené (resp. prijaté) v publikáciách uvedených v časti 4.1. Výskum bol spolufinancovaný z projektov VEGA 1/3115/06, NIL-I-004, APVV-0513-10, APVV-0586-11 a Kritické mriežky - v rámci programu na podporu mladých výskumníkov.

1 Ciele dizertačnej práce

Táto dizertačná práca sa zaoberá problematikou homomorfných kryptosystémov. Tézy dizertačnej práce boli stanovené počas obdobia, kedy boli zverejňované prelomové práce [6], [7], [8] v tejto oblasti (na začiatku roku 2010). Boli zamerané na implementáciu základného kryptosystému z [6], analýzu jeho homomorfných vlastností a následnú kryptoanalýzu z pohľadu LLL algoritmu. Jednotlivé podúlohy boli špecifikované nasledovne:

1. realizovať kryptosystém podľa [6] s konkrétnymi parametrami,
2. preskúmať dopad LLL algoritmu na voľbu parametrov kryptosystému,
3. určiť efektivitu vyhodnocovania obvodov pomocou bootstrappingu a určiť časovú náročnosť.

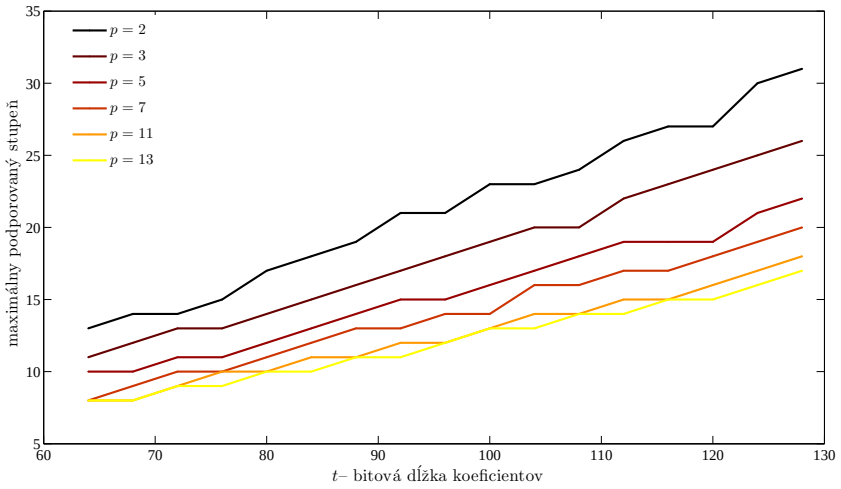
Avšak vzhladom na to, že tieto ciele boli prioritou aj iných výskumníkov, prvý a tretí z pôvodných cieľov dizertačnej práce boli čoskoro vyriešené v [10] (C.Gentry a S.Halevi). Keďže práca [10] obsahovala iba popis implementácie a samotné zdrojové kódy kryptosystému neboli zverejnené, pozmenili a rozšírili sme ciele týkajúce sa praktickej realizácie kryptosystému na:

1. implementácia (čiastočne homomorfného) kryptosystému podľa [10],
2. rozšírenie experimentov z práce C.Gentry a S.Halevi, ktoré určujú homomorfné vlastnosti schémy,
3. experimentálne overenie útoku pomocou LLL algoritmu na redukciu bázy diskrétnej mreže.

2 Dosiahnuté výsledky dizertačnej práce

Prvým krokom k naplneniu cieľov bola implementácia čiastočne homomorfnej schémy, zdrojové kódy základných algoritmov schémy sa nachádzajú v prílohe dizertačnej práce. Kompletné zdrojové kódy sú dostupné elektronicky v akademickom systéme AIS.

Druhým krokom bolo rozšírenie priestoru otvorených textov z pôvodnej množiny $\mathbb{Z}_2$ na $\mathbb{Z}_p$, kde p je vopred zvolené prvočíslo. Táto zmena sa týka len niekoľkých krokov algoritmu na generovanie kľúčov, šifrovania a dešifrovania a nepatrne zvýši časovú náročnosť generovania kľúčov. Prenosový pomer schémy sa zlepší v pomere $p/2$, pretože veľkosť šifrového textu ostane taká istá a vzrastie veľkosť otvoreného textu. Homomorfné vlastnosti schémy sa samozrejme znížia. Na Obr.1 je zobrazené, ako sa mení maximálny podporovaný stupeň elementárneho symetrického polynómu o 80 premenných, ktorý schéma ešte vyhodnotí korektne. Porovnanie ostatných vlastností rozšírenej schémy sa nachádza v práci v časti 4.2.



Obrázok 1: Závislosť maximálneho podporovaného stupňa od t pre voľby $N = 128$, $m = 80$ a rôzne p.

Rozšírená čiastočne homomorfná schéma dokáže pre $p = 13$ korektne spočítať polynomiálne výrazy zhruba polovičného stupňa oproti $p = 2$. Z hľadiska praktických výpočtov je to už zlepšenie, pretože pomocou tejto rozšírenej schémy dokážeme s číslami do 13 spočítať zložitejšie výrazy. Nevýhodou tohto rozšírenia priestoru otvorených textov je, že už nie je možné využiť metódu bootstrappingu na konštrukciu plne homomorfnej schémy.

Pomocou viacerých rozšírených schém (s rôznymi prvočíslami p) vieme zostrojiť aj čiastočne homomorfnú schému, ktorá bude pracovať nad ľubovoľne veľkým priestorom otvorených textov. Zároveň bude schopná korektne vyhodnocovať také množstvo homomorfných operácií ako je minimum z použitých schém. Nech b je ohraničenie pre veľkosť otvorených textov. Hlavná myšlienka, postavená na známej

parametre schémy	priemerný čas(s)	úspešnosť
$N = 64$, $t = 64$	5200	16/16
$N = 128$, $t = 64$	160000	1/1
$N = 256$, $t = 128$	-	-

Tabuľka 1: Čas a úspešnosť redukcie bázovej matice základným LLL algoritmom knižnice NTL.

čínskej zvyškovej vete, spočíva v tom, že b rozložíme na súčin prvočísel p_i pre $i = 1, \ldots, k$ a pre každé z nich definujeme osobitný kryptosystém ξ_i s priestorom otvorených textov $\mathbb{Z}_{p_i}$. Každý otvorený text $m \in \mathbb{Z}_b$ sa dá jednoznačne rozložiť na časti m_i a tejto bude prislúchať zašifrovaný text c_i. Každá homomorfná operácia sa vykoná po zložkách modulo každé prvočíslo p_i a pri dešifrovaní sa dešifrujú jednotlivé časti m'_i a pomocou čínskej zvyškovej vety sa dopočíta naspäť otvorený text zo $\mathbb{Z}_b$.

Podrobný popis tejto konštrukcie je v práci v časti 4.2.3. Výhodou tejto konštrukcie je zlepšenie jednej z nevýhod Gentryho konštrukcie – vysoký prenosový pomer. Nevýhodou ostáva použitie len čiastočne homomorfnej schémy, t.j. obmedzenie homomorfných výpočtov len po určitú hranicu.

Tretím cieľom dizertačnej práce bola kryptoanalýza implementovanej schémy z pohľadu LLL-algoritmu na redukciu diskrétnych mriežok. Realizovali sme útok, ktorého cieľom je získanie otvoreného textu len pomocou verejných parametrov schémy a šifrového textu. Podstatou útoku bola konštrukcia diskrétnej mriežky tak, aby najkratší vektor obsahoval informáciu o otvorenom texte. Bázu tejto mriežky sme potom redukovali pomocou LLL-algoritmu implementovaného v známej knižnici NTL (Number Theory Library) [17].

Výsledky útoku vykonaného na bežnom osobnom počítači (procesor Intel 2.6GHz) sú v Tab.1. Ukázalo sa, že útok trval už pre dimenziu $N = 128$ viac ako 40 hodín a že najväčším problémom bude časová náročnosť. Pre dimenziu $N = 256$ je odhadované trvanie útoku 55 dní.

Realizovali sme preto dve varianty LLL algoritmu, ktorých cieľom bolo zníženie časovej náročnosti na úkor úspešnosti. Základom bol približný variant LLL_FP implementovaný v knižnici NTL, podrobný popis metód LLL_FP_cut a LLL_FP_block uvádzame v časti 4.3.1 dizertačnej práce. V Tab.2 prezentujeme výsledky pre dimenziu 128. Je vidieť, že časová náročnosť výrazne klesla (v najlepšom prípade 40000-krát).

Popísané varianty útoku dosiahli pre dimenziu $N = 256$ nulovú úspešnosť, predmetom ďalšieho výskumu je voľba rozumnejšieho kompromisu medzi rýchlosťou a úspešnosťou a využitie paralelných redukcií mriežok pre rôzne poradia bázových vektorov.

dimenzia	bit. dĺžka	metóda redukcie	priem. čas(s)	úspešnosť
128	64	LLL	160000	1/1
128	64	LLL_XD	1580	20/20
128	96	LLL_XD	3800	20/20
128	128	LLL_XD	7800	12/12
128	64	LLL_FP_block	515	9/20
128	96	LLL_FP_block	1090	9/20
128	128	LLL_FP_block	1980	10/20
128	64	LLL_FP_cut	4.2	3/20
128	96	LLL_FP_cut	4.2	3/20
128	128	LLL_FP_cut	4.2	3/20

Tabuľka 2: Čas a úspešnosť jednotlivých metód pre dimenziu $N = 128$.

Referencie

[1] R. Rivest, L. Adleman, and M. Dertouzos. On data banks and privacy homomorphisms. *Foundations of Secure Computation*, pages 169–177, 1978.

[2] A. Sadeghi F. Armknecht. A new approach for algebraically homomorphic encryption. *Cryptology ePrint Archive, Report 2008/422*. `http://eprint.iacr.org/2008/422` .

[3] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-DNF Formulas on Ciphertexts. In Joe Kilian, editor, *TCC*, volume 3378 of *Lecture Notes in Computer Science*, pages 325–341. Springer, 2005.

[4] C. Melchor, P. Gaborit, and J. Herranz. Additively homomorphic encryption with t-operand multiplications. *Cryptology ePrint Archive, Report 2008/378*, 2008. `http://eprint.iacr.org/2008/378` .

[5] M. Fellows and N. Koblitz. Combinatorial cryptosystems galore! *Contemporary Mathematics*, vol. 168 of Finite Fields: Theory, applications and Algorithms:51–61, 1993.

[6] C. Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the 41st annual ACM symposium on Theory of computing (STOC'09)*, pages 169–178, 2009.

[7] C. Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Standford University, 2009.

[8] Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully Homomorphic Encryption over the Integers. In Henri Gilbert, editor, *EUROCRYPT*, volume 6110 of *Lecture Notes in Computer Science*, pages 24–43. Springer, 2010.

[9] Nigel P. Smart and Frederik Vercauteren. Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. In Phong Q. Nguyen and David

Pointcheval, editors, *Public Key Cryptography*, volume 6056 of *Lecture Notes in Computer Science*, pages 420–443. Springer, 2010.

[10] Craig Gentry and Shai Halevi. Implementing Gentry's fully-homomorphic encryption scheme. In *Proceedings of the 30th Annual international conference on Theory and applications of cryptographic techniques: advances in cryptology*, EUROCRYPT'11, pages 129–148, Berlin, Heidelberg, 2011. Springer-Verlag.

[11] Jean-Sébastien Coron, Avradip Mandal, David Naccache, and Mehdi Tibouchi. Fully Homomorphic Encryption over the Integers with Shorter Public Keys. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 487–504. Springer Berlin / Heidelberg, 2011.

[12] Gu Chunsheng. New Fully Homomorphic Encryption over the Integers. Cryptology ePrint Archive, Report 2011/118, 2011. `http://eprint.iacr.org/`.

[13] Gu Chunsheng. More Practical Fully Homomorphic Encryption. Cryptology ePrint Archive, Report 2011/121, 2011. `http://eprint.iacr.org/`.

[14] Gu Chunsheng. Fully Homomorphic Encryption Based on Approximate Matrix GCD. Cryptology ePrint Archive, Report 2011/645, 2011. `http://eprint.iacr.org/`.

[15] Zvika Brakerski and Vinod Vaikuntanathan. Efficient Fully Homomorphic Encryption from (Standard) LWE. In Rafail Ostrovsky, editor, *FOCS*, pages 97–106. IEEE, 2011.

[16] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In Shafi Goldwasser, editor, *ITCS*, pages 309–325. ACM, 2012.

[17] Viktor Shoup. A library for doing Number Theory, v.5.5.2. New York University, New York, Available online at: `http:shoup.net/ntl/`.

4 Zoznam publikácií a citácií

4.1 Publikované výsledky dizertačnej práce

Mikuš, M. *Ciphertext-only attack on Gentry-Halevi implementation of somewhat homomorphic scheme.* Accepted for publication: Proceedings of Mathematical and Engineering Methods in Computer Science, 8th Doctoral Workshop (MEMICS 2012), Revised Selected Papers, Vol. 7721 of LNCS, Springer, 2012.

Mikuš, M. *Experiments with the Plaintext Space in Gentry's Somewhat Homomorphic Scheme.* Accepted for publication: Tatra Mountains Mathematical Publications Vol. 53, 2012.

Mikuš, M. *Experiments on the Gentry-Halevi Somewhat Homomorphic Scheme.* International Journal of Mathematics and Computers in Simulation Vol. 5, s. 462-469, 2011. ISBN 1998-0159.

4.2 Ostatné práce

Semaev, I., Mikuš, M. *Methods to Solve Algebraic Equations in Cryptanalysis.* Tatra Mountains Mathematical Publications Vol. 45 : NILCRYPT '10. s. 107–136. ISSN 1210-3195.

Mikuš, M., Savický, P. *Remarks on Gödel's Code as a Hash Function.* Remarks on Gödel's Code as a Hash Function. Tatra Mountains Mathematical Publications Vol. 47, s. 67–80, 2010. ISSN 1210-3195.

Mikuš, M., Zajac, P. *Projekt NIL-I-004 podporuje spoluprácu medzi národmi.* Spektrum : periodikum Slovenskej technickej univerzity v Bratislave Roč.17, č.4. s. 10–11. ISSN 1336-2593.

Spoluautor 3 technických správ pre NBÚ SR, ktoré podliehajú utajeniu podľa zákona č. 215/2004 Z.z.

4.3 Príspevky na konferenciách

Mikuš, M. *On implementation of the Gentry-Halevi somewhat homomorphic scheme.* Proceedings of the 2011 international conference on Computers and computing, ICCC'11, s. 131-134. ISBN 978-1-61804-000-8, 2011.

Mikuš, M. *Experiments with the Plaintext Space in Gentry's Somewhat Homomorphic Scheme.* In Tatracrypt 2012 : 12th Central European Conference on Cryptology. Smolenice, Slovak Republic, July 2-4, 2012. Bratislava: Slovak Academy of Sciences, 2012, s. 31–33.

Mikuš, M., Sýs, M. *Algorithm for Finding Critical Lattices.* In KOZÁKOVÁ, A. ELITECH´12 [elektronický zdroj] : 14th Conference of Doctoral Students. Bratislava, 22 May 2012. Bratislava: Nakladateľstvo STU, 2012, s. 6. ISBN 978-80-227-3705-0.

Mikuš, M., Sýs, M. *Computing the Pseudoprimes up to* 10^{13}. In KHOLOSHA, A. – NEMOGA, K. – SÝS, M. Proceedings. 1st Plenary Conference of the NIL-I-004

Development of Norwegian-Slovak Cooperation in Cryptology : Bergen, Norway, 24.-27.8.2009. Bratislava: STU, 2009, s. 7–8. ISBN 978-80-227-3230-7.

Mikuš, M., Sýs, M. *MELP Value of Two Rounds AES with Different Parameters.* In KHOLOSHA, A. – NEMOGA, K. – SÝS, M. Proceedings. 1st Plenary Conference of the NIL-I-004 Development of Norwegian-Slovak Cooperation in Cryptology : Bergen, Norway, 24.-27.8.2009. Bratislava: STU, 2009, s. 17–20. ISBN 978-80-227-3230-7.

Mikuš, M. *New Way of Factoring Numbers.* In ELITECH ´08 : PhD Students Conference. Bratislava, Slovak Republic, 20.5.2008. Bratislava: STU v Bratislave, 2008, ISBN 978-80-227-2878-2.

Mikuš, M. *Remarks on Gödel's Code as a Hash Function.* In 9th Central European Conference on Cryptography. Třebíč, Czech Republic, 23.-26.6.2009. Brno: University of Technology, 2009, s. 16–17.

Summary

The thesis deals with the area of homomorphic cryptosystems. The goals of the thesis were

1. the implementation of the somewhat homomorphic scheme of a cryptosystem from [10],

2. analysis of its homomorphic properties,

3. analysis of its resistance against LLL lattice reduction algorithm.

The chapter 3 of the thesis describes the implementation of the somewhat homomorphic scheme. We extended the plaintext space of the scheme to $\mathbb{Z}_p$ for an arbitrary prime p. This modification slightly increased the time complexity of the key generation algorithm but significantly decreased the CT-to-PT ratio of the scheme. Also the modified somewhat homomorphic scheme cannot be further extended to a fully homomorphic one via the bootstrapping procedure. The source codes of our implementation are available for download in the Academic Information System.

The homomorphic properties of both the original and the modified scheme are assessed in sections 4.1. and 4.2. of the thesis. The results show that the modification of the plaintext space improved the homomorphic potential of the scheme. In section 4.2.3 we describe how to combine the modified somewhat homomorphic schemes to further extend the plaintext space via the Chinese remainder theorem.

The cryptanalysis of the scheme is based on a ciphertext-only attact. The attact uses lattice reduction algorithms with the same principle as in the knapsack problem. Our results from section 4.3. show that the scheme is resistant to the basic LLL-algorithm as long as the dimension is greater than 512. We further proposed two variants of the basic attack that significantly reduce the time complexity at the cost of decreased success rate. Both variants were not successful for dimension higher than 128, but we propose ideas for improvements for further research.