Math-for-industry
Education & Research Hub

ISSN 2188-1200

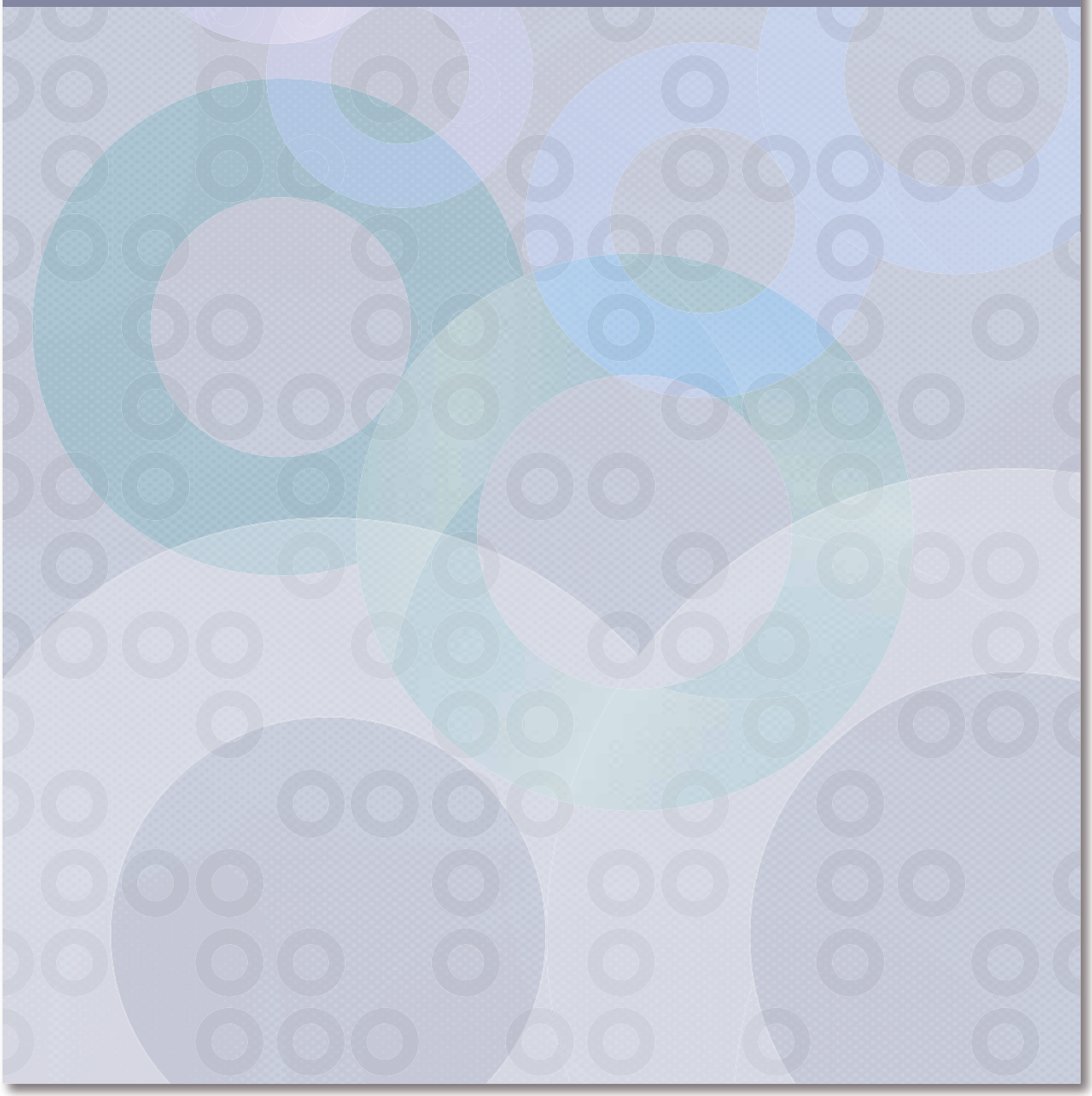
Workshop on

Algebraic constructions as a fundamental keystone of a safe and secure society

— Mathematics for guaranteeing the reliability of the cyber-society —

Editors: Yoshihiro SHIKATA, Kouichi SAKURAI, Takanori YASUDA, Xavier DAHAN

九州大学マス・フォア・インダストリ研究所



MI Lecture Note Vol.53 : Kyushu University

Workshop on

Algebraic constructions as a fundamental keystone of a safe and secure society

—Mathematics for guaranteeing the reliability of the cyber-society—

Editors:

Yoshihiro SHIKATA, Kouichi SAKURAI,

Takanori YASUDA, Xavier DAHAN

About MI Lecture Note Series

The Math-for-Industry (MI) Lecture Note Series is the successor to the COE Lecture Notes, which were published for the 21st COE Program "Development of Dynamic Mathematics with High Functionality," sponsored by Japan's Ministry of Education, Culture, Sports, Science and Technology (MEXT) from 2003 to 2007. The MI Lecture Note Series has published the notes of lectures organized under the following two programs: "Training Program for Ph.D. and New Master's Degree in Mathematics as Required by Industry," adopted as a Support Program for Improving Graduate School Education by MEXT from 2007 to 2009; and "Education-and-Research Hub for Mathematics-for-Industry," adopted as a Global COE Program by MEXT from 2008 to 2012.

In accordance with the establishment of the Institute of Mathematics for Industry (IMI) in April 2011 and the authorization of IMI's Joint Research Center for Advanced and Fundamental Mathematics-for-Industry as a MEXT Joint Usage / Research Center in April 2013, hereafter the MI Lecture Notes Series will publish lecture notes and proceedings by worldwide researchers of MI to contribute to the development of MI.

September 2013
Masato Wakayama
Director
Institute of Mathematics for Industry

Workshop on

Algebraic constructions as a fundamental keystone of a safe and secure society

—Mathematics for guaranteeing the reliability of the cyber-society—

MI Lecture Note Vol.53, Institute of Mathematics for Industry, Kyushu University
ISSN 2188-1200
Date of issue: 26 December 2013
Editors: Yoshihiro SHIKATA, Kouichi SAKURAI, Takanori YASUDA, Xavier DAHAN
Publisher:
Institute of Mathematics for Industry, Kyushu University
Graduate School of Mathematics, Kyushu University
Motooka 744, Nishi-ku, Fukuoka, 819-0395, JAPAN
Tel +81-(0)92-802-4402, Fax +81-(0)92-802-4405
URL http://www.imi.kyushu-u.ac.jp/

Printed by
Kijima Printing, Inc.
Shirogane 2-9-6, Chuo-ku, Fukuoka, 810-0012, Japan
TEL +81-(0)92-531-7102 FAX +81-(0)92-524-4411

Foreword

These pages are compiling the proceedings of the talks made during the workshop “Algebraic constructions as a fundamental keystone of a safe and secure society (Mathematics for the reliability and trustfulness of the cyber society)” hold in August 26th-30th 2013 at Kyushu University Nishijin Plaza, Fukuoka. As an industry-academia collaboration research workshop it was funded by the Institute of Mathematics for Industry of Kyushu University.

By the clever way in which public-key cryptography makes use of the structure of finite groups, it is becoming an indispensable fundamental tool to guarantee the security and the reliability of the digital society. In symmetric-key cryptography as well, the use of the theory of field extensions has make possible the efficient implementation of the block-cipher AES, the successor of DES and international standard block-cipher. In the design of such ciphers, the theory of groups and of field extensions is used proactively.

Moreover, lattices hold some properties with actual applications in computer security. Secret sharing, in the way of how matroids have permitted several achievements, is shaping a sub branch of discrete mathematics. However, researchers engaged in applying such algebraic structures to concrete industrial applications are quite dispersed, independent. In this collaborative research workshop, mathematicians could gather and discussed some applications of these algebraic structures to cryptography and information security in the industry.

The workshop was made of 13 talks addressed by 9 researchers including 3 invited speakers from abroad, and of a panel discussion. A broad range of recent topics was covered among Galois connections and Secret Sharing, lattice-based cryptography, multivariate polynomial based public-key cryptography. The panel discussion focuses on the use of multivariate polynomial systems in the recent Index Calculus attack on the Elliptic curve Discrete Logarithm Problem.

Along with addressing our gratitude to all the speakers, we hope that the workshop could accelerate the development of algebraic methods in cryptography/information security. Finally, we would like to thank the Institute of Mathematics for Industry for their financial support which permitted to invite speakers, and their help in the organization.

October 2013

Shikata Yoshihiro (Nagoya University)
Sakurai Kouichi (Kyushu University)
Yasuda Takanori (ISIT)
Xavier Dahan (Kyushu University)

序文

本報告集は，2013年8月26日から30日にかけて，九州大学西新プラザで開催されたIMI共同利用研究集会“安心・安全社会基盤構築のための代数構造～サイバー社会の信頼性確保のための数理学～” の報告集である．

公開鍵暗号は，有限群の構造を巧みに利用して，ネットワーク社会の安全性と信頼性確保に不可欠な基盤技術となっている．共通鍵暗号においても，DES の後継である国際標準ブロック暗号 AES では，拡大体の理論を用いて効率的実装を可能にしている．このように暗号の設計では，群や拡大体の理論が積極的に利用されている．代数構造は，符号や暗号で基本的な役割を演じており，すでに多くの研究集会や国際会議も活発である．また，束(lattice)もコンピュータセキュリティへの現実応用理論がある．秘密分散では，マトロイドを用いて記述される成果も多く，離散数学の一分野を形成している．束におけるガロア理論のアナロジーとして，ガロア接続がある．ソフトウエア工学では，形式検証において，このガロア接続も活用されている．最近では，ビッグデータの解析にも有効ということでさらに期待される．しかし，こうした具体的産業応用をもつ代数構造を研究している研究者は互いに独立・分散している状況にある．この共同利用研究集会は，国内外の著名な数理学者を招き，産学の暗号・セキュリティへの代数構造の応用，産学連携を見据えた研究・開発について交流討論することを目的とした．

講演は海外招聘者３名を含む講演者９名による１３講演とパネル討論会で構成された．ガロア接続や秘密分散，格子暗号，多変数多項式公開鍵暗号など暗号・セキュリティに関する最新の話題について多岐にわたって講演が行われた．パネル討論会では楕円曲線暗号の Index Calculus 攻撃として注目されている多変数多項式システムの解読を利用した攻撃法について議論した．講演者各位に感謝するとともに，本研究集会が，暗号・セキュリティと代数の連携研究の促進につながれば我々の喜びである．九州大学マス・フォア・インダストリ研究所には，本研究集会の開催にあたり，旅費の助成をはじめとする研究集会開催への助力をいただいた．ここに感謝申し上げる．

2013年10月

四方義啓（名古屋大名誉教授）
櫻井幸一（九州大学，九州先端科学技術研究所）
安田貴徳（九州先端科学技術研究所）
グザヴィエ・ダハン（九州大学）

平成25年度 九州大学マス・フォア・インダストリ研究所
共同利用研究集会

安全・安心社会基盤構築のための代数構造

～サイバー社会の信頼性確保のための数理学～

〈講演予定〉

海外招待講演	Avishek Adhikari（カルカッタ大学・インド） **"Applications of Algebraic Structures in Visual Cryptography"**
企業研究招待講演	櫻庭健年（日立製作所） **"ガロア接続をもちいた動的秘密情報の管理"**
基調講演	四方 義啓（名古屋大学・名誉教授） **"暗号解析とガロア理論"**
一般講演	安田貴徳（ISIT） **"非可換代数を用いた公開鍵暗号の設計と解析"** Xavier DAHAN（九州大学） **"楕円曲線上の離散対数問題のグレブナー基底計算に基づく攻撃"**

他数件の招待講演を予定

■日時 2013年
8月26日(月)～8月30日(金)

■会場
九州大学西新プラザ
〒814-0002 福岡県福岡市早良区西新2丁目

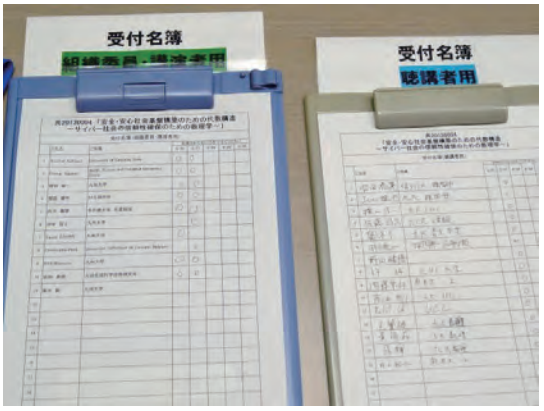
■共催機関：(公財)九州先端科学技術研究所(ISIT)
http://www.isit.or.jp/

■運営責任者：四方義啓(名古屋大学・名誉教授)
組織委員：櫻井幸一(ISIT、九州大学)
安田貴徳(ISIT)
Xavier DAHAN(九州大学)

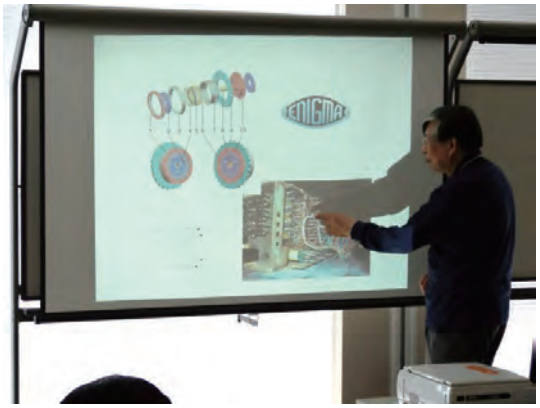
ISIT http://www.isit.or.jp/lab2/2013/05/29/imiworkshop/

■運営に関する問い合わせ先
E-mail：yasuda@isit.or.jp

■問い合わせ先 九州大学マス・フォア・インダストリ研究所
TEL：092-802-4402 E-mail：kyodo_riyou@imi.kyushu-u.ac.jp


受付名簿
受付名簿
聴講者用


名札


ENIGMA

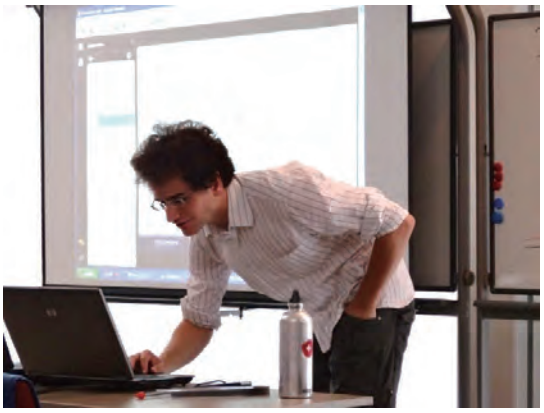

Lattice-based Crypto
Two Types of Techniques
Cryptography using trapdoors, i.e. se
short basis of a lattice. Similariti
RSA/Rabin cryptography.
Cryptography without trapdoors. S
with DL cryptography.
Historically, applied-lattice-crypto us
trapdoors.

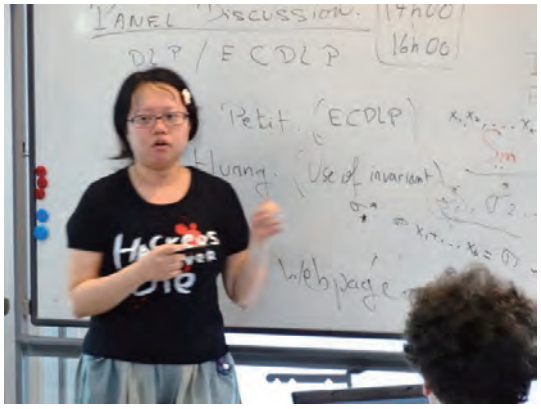

Classification of MPKC signature


Secret Sharing with Cheaters

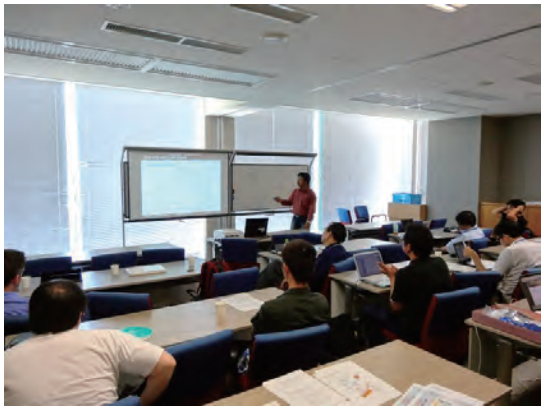

Multiplication on GPU


Some More Solutions




PANEL DISCUSSION
DLP / ECDLP
Petit (ECDLP)
Huang (Use of invariant)
Webpage


Computation of the eigenvalues
of Cayley graphs and applications



Participant List

"Algebraic constructions as a fundamental keystone of a safe and secure society
Mathematics for guaranteeing the reliability of the cyber-society"

No.	NAME	AFFILIATION
1	Advishek Adhikari	University of Calcutta
2	Phong Nguyen	INRIA, Tsinghua University,
3	Taketoshi Sakuraba	Hitachi, Ltd.
4	Christophe Petit	Universite catholique de Louvain
5	Kirill Morozov	Institute of Mathematics for Industry, Kyushu University
6	Satoshi Tanaka	Faculty of Information Science and Electrical Engineering, Kyushu University
7	Yoshihiro Shikata	Nagoya University (Emeritus)
8	Kouichi Sakurai	ISIT/Kyushu University
9	Takanori Yasuda	ISIT
10	Xavier Dahan	Faculty of Information Science and Electrical Engineering, Kyushu University
11	Tsuyoshi Takagi	Institute of Mathematics for Industry, Kyushu University
12	Shunichi Yokoyama	Institute of Mathematics for Industry, Kyushu University
13	Yuya Yamaguchi	Faculity of Mathematics, Kyushu University
14	Shinya Okumura	Faculity of Mathematics, Kyushu University
15	Takuya Hayashi	Faculity of Mathematics, Kyushu University
16	Hui Zhang	Faculity of Mathematics, Kyushu University
17	Yun-Ju Huang	Faculity of Mathematics, Kyushu University
18	Yuntao Wang	Faculity of Mathematics, Kyushu University
19	Rui Xu	Faculity of Mathematics, Kyushu University
20	Hirohito Inoue	Kumamoto University
21	Takashi Hori	Kobe University
22	Hideo Mori	Tokai University
23	Yasuhide Numata	Shinshu University
24	Kenji Kimura	Fukuoka Daiichi High School
25	Kengo Noda	Fukuoka Daiichi High School
26	Yoshihisa Sato	Kyushu Institute of Technology

Institute of Mathematics for Industry (IMI), Kyushu University, Workshop on

Algebraic constructions as a fundamental keystone of a safe and secure society

Mathematics for guaranteeing the reliability of the cyber-society

Date: August 26(mon) – August 30(fri) , 2013
Place: Nishijin Plaza, Kyushu University

Program

8/26(mon)

15:00—15:10 Opening
15:10—17:00 Research exchange meeting
explanation of the general purpose of this research gathering
self-introduction of participants

8/27(tue)

10:00—11:00 Keynote Lecture
Yoshihiro Shikata（Nagoya University, emeritus professor）
Cryptanalysis and Galois Theory
11:30—12:30 Avishek Adhikari（University of Calcutta, India）
Connections Among Algebra, Statistical Designs and Secret Sharing Schemes

14:00—15:00 Taketosi Sakuraba（HITACHI）
Control of Dynamical Secret Data by Using Galois Connections I
15:15—16:15 Phong Nguyen（INRIA, France and Tsinghua University, China）
Abstracting Lattice Cryptography
16:30—17:30 Xavier DAHAN（Kyushu University）
Greobner Bases Based Attacks of the Discrete Logarithm Problem on Elliptic Curves

8/28(wed)

10:00—11:00 Taketosi Sakuraba（HITACHI）
Control of Dynamical Secret Data by Using Galois Connections II

11:15—12:15 Christophe Petit (Université catholique de Louvain, Belgium)
Rubik's for Cryptographers

14:00—15:00 Takanori Yasuda（ISIT）
Design and Analysis of Public Key Cryptography using Non-commutative algebra

15:15—16:15 Avishek Adhikari（University of Calcutta, India）
Applications of Algebraic Structures in Visual Cryptography

16:30—17:00 Satoshi Tanaka（Kyushu University）
Efficient Solving of Multivariate Quadratic Polynomial System using GPU

8/29(thu)

10:00—10:30 Satoshi Tanaka（Kyushu University）
Efficient Implementation of Multiplication on Extension Field using GPU

10:40—11:10 Kirill Morozov（Kyushu University）
On Cheater Identifiable Secret Sharing Schemes Secure Against Rushing Adversary

11:20—11:50 Avishek Adhikari（University of Calcutta, India）
Plaintext Checkable Encryption with Designated Checker

14:00—16:00 Panel Discussion
About Attacks Methods on the ECDLP

8/30(fri)

10:00—12:00 Debate Session

Contents

29 August, 2013

Workshop

Keynote Lecture

Cryptanalysis and Galois Theory

Yoshihiro Shikata（Nagoya University）

From my experience during WW 2, I know Japanese took very light of information.
A part of which might be reflected in a certain characteristic of Japanese pure mathematics, not to mix well with practical mathematics, as informatics and/or statistics. For the future Japanese mathematics, it may be necessary to improve this situation, which could be the reason why we meet here together
First we take a look at coding and cipher:
As the coding system,we can count historical Caesar, Enigma method and modern RSA or algebraic curve method for future, Though the methods itself are different, every coding is based upon a permutation of alphabets. Therefore first attack on code may be done through comparison with linguistic rules as Magic decoding group, suggesting necessity of cooperation with linguistics.
On the other hand, Galois theory is a theory of the permutation group G, which asserts
1) To solve an algebraic equation of order k by algebraic method, the existence of a non trivial normal subgroup in G of order k is essential. Where we mean non trivial normal subgroup the normal subgroup except the normal subgroup of even permutation.
2) The permutation group G of order k (k>5) has no non trivial normal subgroup.
Thus we see, for example, that the normalizer of any subgroup of G essentially extends to G itself if k>5, which may give a theoretical background of successive replacement of alphabet in linguistic approach to attack code, .
Enigma system uses an embedding of alphabet into higher dimensional space and permutation of coordinate axis, plus rotations of the coordinate of the space, as a Rubik cube. Therefore it uses once a lift into a higher permutation group and then a splitting of the group into lower order permutation groups, plus the permutation of these small groups. Magic decoding group should have read the structure of thus obtained permutation. Here we may see fundamental symmetric polynomial help to find out the splitting, again a connection to Galois theory.
We can see a direct application of Galois theory to cipher in a sharing problem, proposed by Dr Aishiek. He proposed to decompose a word or picture printed in a sheet into two sheets, so that we read the original message if we lay these two sheets together. This

may be interpreted as a factorization problem of give message, and turns out to be a problem to find two roots (and another coefficient) of a quadratic equation for a given coefficient. Thus we may use direct Galois theory to measure the hardness of this cipher and the generalization possibility.

Another mathematical tool for coding and cipher may be topology for Galois simplex, which is Galois lattice admitting cell structure. Galois lattice is a lattice admitting hierarchy. If we introduce dimension and boundary to the component of the lattice so that they from a complex in accordance with the hierarchy, which we call Galois simplex, then they yield a homology of the lattice compatible with the hierarchy. we see that the homology is useful to measure the simplicity of the hierarchy.

The facts above are only several examples of the intersection of pure mathematics and the coding theory, other than well known prime number problem in RSA coding and algebraic curve approach for new coding theory. Thus we may expect a very fruitful results from further cooperation between pure mathematics and the coding theory.

My name is
Yoshihiro SHIKATA

四方義啓xysika@yahoo.co.jp

Born in 1936 in Kobe, JAPAN

Around 1936 many things happend

Military coup d'etat failed in Japan
Japan Germany anti communism treaty
Conflict between China

1936 was a turning point
Japan went direct to WW2

Japan US negotiation ended by Hull's note
Japan Russia peace treaty
Germans defeated at Moscow
Pearl harbor attack

The reality of the war made us realized
Japan makes light of information

Radio in Japanese fighter plane did not work well
Rader was considered a machine for cowards at first
Japanese pilots preferred Bomb than Rader

As for Cipher

Cipher decoding from Japenese side was not successful
American mathematicians breaked Japanese highest "purple cipher"

Around 1960

Graduated at Kyoto U
Master course
Specialized in topology and algebra
under Prof A.Komatsu

Around 1970

With Prof Klingenberg made
research on relation between
differential geometry and topology

Around 1975

Prof Thom of IHES
made aware of relation to
real world and mathematics

1980 was my turning point

Try to develop mathemaitics for real application
1980: Electronics and Mechanics → Gysi-simplex
1900:Medicine, Earthquake → EEG EMG
2000: Linguistics, Economy and Coding

Study of Coding and Pure math should be well related

Yoshi Shikata
四方義啓
xysika@yahoo.co.jp

Since Caesar, information is highly weighted not only in war field

Caesar cipher
Torch relay for exchange

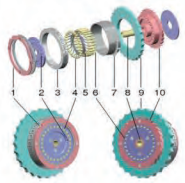
Cipher technique by machine are developed with war

Enigma coding and breaking
at the begining of WW2

Imbed alphabet into square matrix
Apply permutation to Raw and Column
↓
Enigma type coding

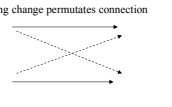
Real enigma system

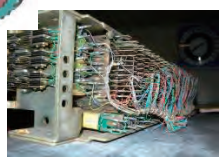
Combination of gear and wire
Gear rotates column and raw
Connecting wire switches connection



Gear rotation produce permutation

Wiring change permutates connection





Every coding at present depends on permutation of numbers

And embedding alphabet into
highler dimensional space of numbers

To realize permutation

Mathematical processing is useful
to generate the third number from given number
Add key number ⟶ Caesar cipher
Take a certain power ⟶ modern RSA
Algebraic curve and intersection for future coding
Enigma used decomposition and other besides arithmetic

Core of RSA coding is the following

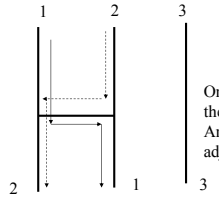
p^{th} power of x is x mod p
↓
$(p-1)^{th}$power of x=1 mod p
$(p-1)(q-1)^{th}$power of x=1 mod pq
$\{(p-1)(q-1)+1\}^{th}$power of x=x mod pq
↓
For any number KL=(p-1)(q-1)+1
KL^{th}power of x=x mod pq

Example in Mod 7 case

x	= 2,3,4,5,6
x square	= 4,2,2,4,1
x cube	= 1,6,1,6,6
x 4^{th}power	= 2,4,4,2,1
x 5^{th}power	= 4,5,2,3,6
x 6^{th}power	= 1,1,1,1,1

Representation of permutation by Amida kuji

One should take the woof line.till he meets the warp bar, then next woof line

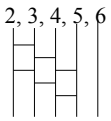


One can express all the permutations by Amida kuji adjusting the woof

Example of Amida kuji representation of 5th power in Mod 7

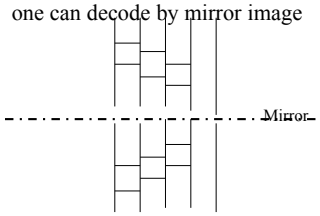
x = 2,3,4,5,6

$x^{5th power}$ = 4,5,2,3,6



Mirror image gives inverse or decoder

For given Amida kuji coding
one can decode by mirror image



Galois theory is a theory of Amida kuji

Problem: Does group of all Amida kuji decompose into smaller normal subgroups?

Answer: Over 5 woof lines it does not

↓

Even one seed grows to whole under "admissible operation"
indicates normal decoding is effective

Algebraic equation is equivalent to code the solution by its coefficient as fundamental symmetric polynomial

Galois thory

Possible to decode when the dgree is less than 5 by its normal subgroup

To transmit cipher 2 lines are used

One line to send the key of the cipher
Another line to send the cipher itself

Dr Avishiek's example
Sharing problem 1

He separates the 1 sheet image "IMBIC" into 2 sheets, each of which one not read but when the 2 is multiplied or doubled there appears letter "IMBIC"

This is interpreted as
the relation between solution and coefficient in quadratic eq

$\alpha\beta = c/a$

Avishiek send $\alpha\beta$ instead c/a

If the averaged use of lines are desirable

Then the fundamental polynomials should be used

↓

Up to 4th order it is possible

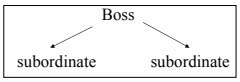
Over 5th order it looses "fairness"

For the sharing problem 2
we can use homology theory

Suppose there are
big bosses, bosses, subordinates

Topologist says

a boss and subordinates makes a family or 1 simplex if subordinates are connected to the boss by lines

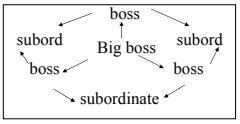


1-simplex

Suppose there are
big bosses, bosses, subordinates

Topologist says

a big, boss and subordinates makes a family or 2 simplex if they are well connected to the big boss



2-simplex

Those 1,2simplices have face

Every k-simplex are requested to have k-1 boundary to meet another family

The boundary of boundary is required to be zero

The relation boss and face can be replaced by priority of order

If here is no hole or
"homology is zero"
then the complex is well ordered

Workshop

Connections Among Algebra, Statistical Designs and Secret Sharing Schemes

Avishek Adhikari
Department of Pure Mathematics
Calcutta University
35 Ballygunge Circular Road, Kolkata 700019
E-mail : avishek.adh@gmail.com

Abstract

Due to the recent development of computers and computer networks, huge amount of digital data can easily be transmitted or stored. But the transmitted data in networks or stored data in computers may easily be destroyed or substituted by enemies if the data are not enciphered by some cryptographic tools. So it is very important to restrict access of confidential information stored in a computer or in a certain nodes of a system. Access should be gained through a secret key, password or token. Again storing the secret key or password securely could be a problem. The best solution could be to memorize the secret key. But for large and complicated secret key, it is almost impossible to memorize the key. As a result, it should be stored safely. While storing data in a hard disk, the threats such as troubles of storage devices or attacks of destruction make the situation even worse. In order to prevent such attacks, we may make as many copies of the secret data as possible. But, if we have many copies of the secret data, the secret may be leaked out and hence the number of the copies should be as small as possible. Under this circumstances, it is desirable that the secret key should be governed by a secure key management scheme. If the key or the secret data is shared among several participants in such a way that the secret data can only be reconstructed by a significantly large and responsible group acting in agreement, then a high degree of security is attained. Shamir and Blakley, independently, addressed this problem in 1979 when they introduced the concept of a threshold secret sharing scheme. A (t,n)-threshold scheme is a method whereby n pieces of information, called shares, corresponding to the secret data or key K, are distributed to n participants so that the secret key can be reconstructed from the knowledge of any t or more shares and the secret key can not be reconstructed from the knowledge of fewer than t shares. This this we we further emphasize on a special type of secret sharing scheme known as visual secret sharing scheme. Visual cryptographic scheme, for a set $\mathcal{P}$ of n participants, is a cryptographic paradigm that enables us to split a secret image, which may be some

handwritten note, printed text, picture, etc., into n shadow images called *shares*, where each *participant* in $\mathcal{P}$ receives one share. Certain qualified subsets of participants can "visually" recover the secret image with some loss of contrast, but other forbidden sets of participants have no information about the secret image. A "visual recovery" for a set $X \subseteq \mathcal{P}$ consists of photocopying the shares given to the participants in X onto the transparencies, and then stacking them. Since the reconstruction is done by human visual system, no computation is involved during decoding unlike traditional cryptographic schemes where a fair amount of computation is needed to reconstruct the plain text. In this talk, we shall describe how algebra and statistical designs play an important role in constructing visual cryptographic schemes.

References

[1] Avishek Adhikari, M R Adhikari, *Introduction to Linear Algebra with Application to Basic Cryptography*, Asian Books, India, 2007.

[2] Avishek Adhikari, M R Adhikari, *Basic Modern Algebra with Applications*, To be published by Springer.

[3] Avishek Adhikari, M R Adhikari, *Introduction to Linear Algebra with Application to Basic Cryptography*, Asian Books, India, 2007.

[4] Avishek Adhikari, M. R. Adhikari and Y. P Chaubey, *Contemporary Topics in Mathematics and Statistics with Applications*, Asian Books , India, 2013.

[5] Avishek Adhikari, *Linear Algebraic Techniques to Construct black and white Visual Cryptographic Schemes for General Access Structure and its Applications to Color Images*, Design, Codes and Cryptography, 2013, DOI 10.1007/s10623-013-9832-5.

[6] A. Shamir, *How to share a secret*, Communication of ACM, Vol. 22, No. 11, 612-613, 1979.

Connections Among Algebra, Statistical Designs and Secret Sharing Schemes

Avishek Adhikari

website: www.imbic.org/avishek.html

Research Team Members

Partha Sarathi Roy, Angsuman Das, Ushnish Sarkar, Sabyasachi Dutta

Department of Pure Mathematics
University of Calcutta, Kolkata.

What is secret sharing?

(t, w) threshold scheme

Let t and w be two positive integers, such that $t \leq w$. A (t, w) *threshold scheme* is a method of sharing a scheme key k among a set of w participants in such a way that any t participants can compute the value of k, but no group of $(t-1)$ participants can do so.

Secret Sharing for General Access Structure?

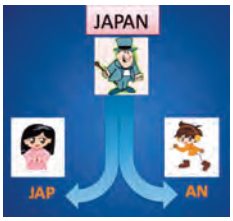
Secret Sharing for General Access Structure?

- Secret sharing refers to method for distributing a secret, say K, amongst a set $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ of n participants , each of which is allocated a share of the secret in such a way that certain qualified set of participants can reconstruct the secret by combining their shares while certain set of participants gets no information about the secret even when they combine their shares.
- The set of participants who are qualified to reconstruct the share is called qualified set of participants, while the set of participants who are not qualified to reconstruct the secret is known as forbidden set of participants.
- The collection of all qualified sets of participants is denoted by Γ_{Qual} while the set of all forbidden sets of participants are known as Γ_{Forb}.
- $(\Gamma_{Qual}, \Gamma_{Forb})$ is known as an access structure on the set of participants $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$.

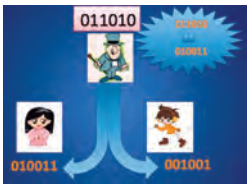
Secret Sharing for General Access Structure?

- The key is chosen by a special participant $\mathcal{D}$, called the *dealer*, and it is usually (for the classical SSS) assumed that $\mathcal{D} \notin \mathcal{P}$. The dealer gives partial information, called *share* or *shadow*, to each participant to share the secret key K.
- A secret sharing scheme is said to be *perfect* if the condition 2 of the above is strengthened as follows :
  Any unauthorized group of shares cannot be used to gain any information about the secret key that is if an unauthorized subset of participants $\mathcal{B} \subset \mathcal{P}$ pool their shares, then they can determine nothing more than any outsider about the value of the secret K.

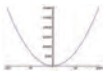
Simple Way!



Perfectly Secure (2,2)-SSS

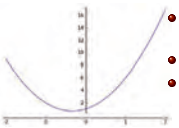


Shamir's (k, n)-Secret Sharing Scheme



- It takes two points to define a straight line, three points to fully define a quadratic, four points to define a cubic, and so on.
- One can fit a unique polynomial of degree $(k-1)$ to any set of k points that lie on the polynomial.

Shamir's (3, 4) threshold scheme



- Let $\mathcal{P}=\{P_1, P_2, P_3, P_4\}$ be a set of 4 participants.
- The key set, $\mathcal{K}=\mathbb{Z}_p$, where $p=5$ is a prime & $p > n$ Ket the secret be 1.
- The set of all possible shares, $\mathcal{S}=\mathbb{Z}_5$.
- The dealer constructs a random polynomial $f(x) \in \mathbb{Z}_5[x]$ of degree $t-1=3-1=2$, in which the constant term is the secret $K=1$.

$$f(x) = 1 + 2x + 3x^2$$

Shamir's (3, 4) threshold scheme

- Every participant P_i obtains a point (x_i, y_i) on this polynomial, where $y_i = f(x_i)$ and distinct $x_i \in \mathbb{Z}_p$.
- P_1 gets (1,a(1)=6=1), (P_2) gets (2,2), P_3 gets $(3, 4)$ and P_4 gets (4,2).

Recovery of Secret

- Suppose a subset B of $t=3$ participants wants to recollect the secret.
- Let the participants P_1, P_2, P_3 want to determine $K=1$.
- They know that $1=f(1)$, $2=f(2)$ and $4=f(3)$.
- They will assume the form of the secret polynomial as $y=f(x)=a_0+a_1x+a_2x^2$, where a_0, a_1 and a_2 are unknown and belong to $\mathbb{Z}$.
- Thus, these participants can obtain 3 linear equations in the 3 unknowns a_0, a_1, a_2.

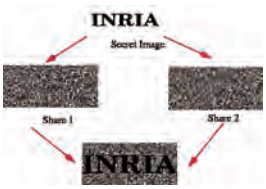
Shamir's (t, n) threshold scheme

- $$\begin{bmatrix} 1 & 1 & 1^2 \\ 1 & 2 & 2^2 \\ 1 & 3 & 3^2 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} f(1) \\ f(2) \\ f(3) \end{bmatrix}$$
- Now, the coefficient matrix A is the so called Vandermonde's matrix.

$$detA = \prod_{1 \le j < k \le t} (x_{i_k} - x_{i_j}) \mod p = (1-2)(2-3)(3-1) = 4*4*2 = 2 \neq 0$$

Thus multiplying both sides by the inverse of A, we can find the $a_0 = 1$.

Example of (2, 2)-VCS



Visual Cryptography

The **Visual cryptographic scheme**, introduced by ***Naor*** and ***Shamir*** in **1994**, for a set $\mathcal{P}$ of *n participants* is a cryptographic paradigm that enables a secret image to be split into *n* shadow images called *shares*, where each *participant* in $\mathcal{P}$ receives one share. Certain qualified subsets of participants can "visually" recover the secret image with some loss of contrast, but other forbidden sets of participants have no information about the secret image.

(2, 2)-VCS

For Black pixel

For White pixel

$$S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}.$$

Relative contrast

Let us consider a $(2, n)$-VCS on a set $\mathcal{P} = \{1, 2, \ldots, n\}$ of *n* participants with basis matrices S^0 and S^1 and having pixel expansion *m*. Then the *relative contrast* for the participants corresponding to *X*, $X \subseteq \mathcal{P}$, is denoted by $\alpha_X(m)$ and is defined as

$$\frac{w(S^1_X) - w(S^0_X)}{m}.$$

$(2, n)$-VCS by Naor and Shamir

$$S^0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \textit{and} \quad S^1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Here the *relative contrast* for any two participants is $\frac{1}{4}$ and the *pixel expansion* is 4.

$(2, n)$-VCS by Stinson at el

- Let v, k and λ be positive integers such that $v > k \geq 2$.
- a (v, k, λ)-balanced incomplete block design (BIBD) is a pair ($\mathcal{X}$,$\mathcal{A}$) such that the following properties are satisfied :
  1. $\mathcal{X}$ is a set of v elements called points,
  2. $\mathcal{A}$ is a collection of subsets of $\mathcal{X}$ called block,
  3. each block contains exactly k points,and
  4. every pair of distinct points is contained in exactly λ blocks.

$(2, n)$-VCS by Stinson at el

Example of a $(v = 7, b = 7, r = 3, k = 3, \lambda = 1)$-BIBD :

- $\mathcal{X} = \{1, 2, 3, 4, 5, 6, 7\}$.
- $\mathcal{A}$= $\{\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \{1, 5, 6\}, \{2, 6, 7\}, \{1, 3, 7\}\}$.
- the incidence matrix is : $\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$

Example of a (2,7)-VCS using BIBD

$S^1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$ & $S^0 = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$

Here the *pixel expansion* is 7 and the *relative contrast* is 2/7.

Latin Square

- A *latin square* L of order n is an $n \times n$ array with entries chosen from a set N of size n such that each element of N occurs precisely once in each row and in each column. Without loss of generality, N is assumed to be $\{1, 2, \cdots, n\}$.
- $$L = \begin{bmatrix} 1 & 4 & 3 & 2 \\ 2 & 3 & 4 & 1 \\ 4 & 1 & 2 & 3 \\ 3 & 2 & 1 & 4 \end{bmatrix}.$$

Back Circulant Latin Square

- A *back circulant* latin square is a particular latin square having the initial row in the standard form (i.e., in the first row the entries 1, 2, . . . , n occur in natural order) and subsequent rows are formed by translating the preceding row one element to the left.
- **Example of a back circulant latin square of order 3 :**

$$L = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}.$$

Lemma

For any $n \geq 3$, there exists a latin square (on symbols $\{1, 2, \ldots, n\}$), $L = [a_{ij}]_{n \times n}$ where $a_{ii} = i$ for $i = 1, 2, \ldots, n$.

(2,9)-VCS Using Latin Square

- $$\begin{matrix} 1 & 3 & 2 \\ 3 & 2 & 1 \\ 2 & 1 & 3. \end{matrix}$$
- Then we write the following arrangement as follows

$$\begin{matrix} 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 & 3 \\ 1 & 2 & 3 & 1 & 2 & 3 & 1 & 2 & 3 \\ 1 & 3 & 2 & 3 & 2 & 1 & 2 & 1 & 3 \end{matrix}$$

- Then we delete the column with the same entries. So we get

$$\begin{matrix} 1 & 1 & 2 & 2 & 3 & 3 \\ 2 & 3 & 1 & 3 & 1 & 2 \\ 3 & 2 & 3 & 1 & 2 & 1 \end{matrix}$$

(2,9)-VCS Using Latin Square

- Now we construct a new matrix M with elements as follows :

$$\begin{matrix} (1,1) & (1,1) & (1,2) & (1,2) & (1,3) & (1,3) \\ (2,2) & (2,3) & (2,1) & (2,3) & (2,1) & (2,2) \\ (3,3) & (3,2) & (3,3) & (3,1) & (3,2) & (3,1). \end{matrix}$$

- So there are 9 distinct entries. We rename as follows

$(1,1) = v_1$, $(1,2) = v_2$, $(1,3) = v_3$, $(2,1) = v_4$, $(2,2) = v_5$, $(2,3) = v_6$, $(3,1) = v_7$, $(3,2) = v_8$, $(3,3) = v_9$.

(2,9)-VCS Using Latin Square

- Thus the matrix becomes

$$\begin{matrix} v_1 & v_1 & v_2 & v_2 & v_3 & v_3 \\ v_5 & v_6 & v_4 & v_6 & v_4 & v_5 \\ v_9 & v_8 & v_9 & v_7 & v_8 & v_7. \end{matrix}$$

- $S^1 = \begin{bmatrix} 1&1&0&0&0&0 \\ 0&0&1&1&0&0 \\ 0&0&0&0&1&1 \\ 0&0&1&0&1&0 \\ 1&0&0&0&0&1 \\ 0&1&0&1&0&0 \\ 0&0&0&1&0&1 \\ 0&1&0&0&1&0 \\ 1&0&1&0&0&0 \end{bmatrix}$. $S^0 = \begin{bmatrix} 1&1&0&0&0&0 \\ 1&1&0&0&0&0 \\ 1&1&0&0&0&0 \\ 1&1&0&0&0&0 \\ 1&1&0&0&0&0 \\ 1&1&0&0&0&0 \\ 1&1&0&0&0&0 \\ 1&1&0&0&0&0 \\ 1&1&0&0&0&0 \end{bmatrix}$.
- The pixel expansion is 6 and the relative contrast is either $\frac{2}{6}$ or $\frac{1}{6}$.

Association Scheme with 2 Classes

Given v symbols $1, 2, \ldots, v$, a relation satisfying the following conditions is said to an **association scheme with** 2 **classes** :

1. Any two symbols are either 1st or 2nd associates, the relation being symmetrical; that is, if the symbol α is the ith associate of the β, then β is the ith associate of α.
2. Each symbol α has n_i ith associates, the number n_i being independent of α.
3. If any two symbols α and β are ith associates, then the number of symbols that are jth associates of α, and kth associates of β, is independent of the pair α and β.

PBIBD

If we have an association scheme with 2 classes and given parameters, we get a **PBIBD** with 2 associate classes if the v symbols are arranged into b sets of size k ($k < v$) such that every symbol occurs at most once in a set, every symbol occurs in exactly r sets and if two symbols α and β are ith associates, then they occur together in λ_i sets, the number λ_i being independent of the particular pair of ith associates α and β, $i = 1, 2$.
The **notation** $(v, b, r, k, \lambda_1, \lambda_2)$-PBIBD will be used to denote a PBIBD. Let $N = (n_{ij})$ denote the **incidence matrix** of a $(v, b, r, k, \lambda_1, \lambda_2)$-PBIBD.

Example of a PBIBD

Let us consider a
$(v = 6, b = 4, r = 2, k = 3, \lambda_1 = 0, \lambda_2 = 1)$-PBIBD.
Here $\mathcal{X} = \{1, 2, 3, 4, 5, 6\}$ and
$\mathcal{A} = \{\{1, 2, 3\}, \{1, 4, 5\}, \{2, 4, 6\}, \{3, 5, 6\}\}$ The insidence matrix of this PBIBD is given as follows :

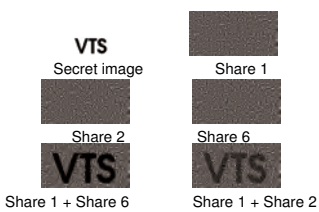
$$N = S^1 = \begin{bmatrix} 1&1&0&0 \\ 1&0&1&0 \\ 1&0&0&1 \\ 0&1&1&0 \\ 0&1&0&1 \\ 0&0&1&1 \end{bmatrix}$$

Example of a (2, 6)-VCS

$$S^1 = \begin{bmatrix} 1&1&0&0 \\ 1&0&1&0 \\ 1&0&0&1 \\ 0&1&1&0 \\ 0&1&0&1 \\ 0&0&1&1 \end{bmatrix} \text{ and } S^0 = \begin{bmatrix} 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \\ 1&1&0&0 \end{bmatrix}.$$

Clearly, *pixel expansion* is 4 ($m = 4$) and the *relative contrast* is either $\frac{1}{2}$ or $\frac{1}{4}$.

(2, 6)-VCS using PBIBD



$(2, n)$-VCS using PBIBD

Theorem : Let $\mathcal{P}$ be a set of participants. Suppose there exists an $(v, b, r, k, \lambda_1, \lambda_2)$-PBIBD. Then there exists a $(2, n)$-VCS with $n = v$ having pixel expansion $m = b$. For $X = \{\beta, \gamma\}$, $\beta, \gamma \in \mathcal{P}$, the relative contrast corresponding to the set of participants X is denoted by $\alpha_X(m)$ and is given by $\alpha_X(m) = \frac{r-\lambda_q}{m}$, if β and γ *are qth* associates, $q = 1, 2$.

Outline of the proof :

Take $S^1 = N$. Since the PBIBD is equireplicate with replication r, in each row of N there are exactly r 1's and $m - r$ 0's.

Construct S^2 such that it consists of n identical row vectors of length m, each row having r 1's and rest 0's.

n	m	α_p^1	α_p^2
6	4	·500	·250
9	6	·333	·167
10	5	·400	·200
15	6	·333	·167
21	7	·286	·143

A Comparison with respect to pixel expansion

Table: Comparison of pixel expansions

n	m_{B1}	m_{B2}	m_D	m_S	m_P
3	3	3	3	3	4
4	6	4	4	4	4
5	10	10	5	5	4
6	20	10	6	6	4
7	35	7	7	7	5
8	70	14	8	8	5
9	126	18	9	9	6
10	252	18	10	10	5
15	6435	15	15	15	6
21	352716	30	21	21	7

A Comparison with respect to relative contrast

Table: Comparison of relative contrasts

n	α_{B1}	α_{B2}	α_D	α_S	α_P^1	α_P^2
3	·333	·333	·333	·333	·500	·250
4	·333	·250	·250	·250	·500	·250
5	·300	·300	·200	·200	·500	·250
6	·300	·300	·167	·167	·500	·250
7	·286	·286	·143	·143	·400	·200
8	·286	·286	·125	·125	·400	·125
9	·278	·278	·111	·111	·333	·167
10	·278	·278	·100	·100	·400	·200
15	·267	·267	·067	·067	·333	·167
21	·262	·233	·048	·048	·286	·143

Bioliography

- Avishek Adhikari and S. Sikdar, *A New* $(2, n)$*-Color Visual Threshold Scheme for Color Images*, Indocrypt'03, Lecture Notes in Computer Science, Springer-Verlag, 2904, 148-161, 2003.
- Avishek Adhikari and M. Bose, *A New Visual Cryptographic Scheme Using Latin Squares*, IEICE Transactions on Fundamentals, E87-A, No. 5, 1998-2002, 2004.
- Avishek Adhikari, T. K. Dutta and B. Roy, *A New Black and White Visual Cryptographic Scheme for General Access Structures*, Indocrypt'04, Lecture Notes in Computer Science, Springer-Verlag, 3348, 399-413, 2004.
- Avishek Adhikari, *An overview of black and white Visual Cryptography using mathematics*, J. Calcutta Math. Soc, no. 2, 21-52, 2006.
- Avishek Adhikari, D. Kumar, M. Bose and B. Roy, *Applications of Partially Balanced and Balanced Incomplete Block Designs in developing Visual Cryptographic Schemes*, IEICE TRANS. FUNDAMENTALS, Japan, Vol. E-90A, No. 5, 949-951, 2007.

Bioliography

- Avishek Adhikari, M R Adhikari, *Introduction to Linear Algebra with Application to Basic Cryptography*, Asian Books, India, 2007.
- Avishek Adhikari, M R Adhikari, *Basic Modern Algebra with Applications*, To be published by Springer.
- Avishek Adhikari, M R Adhikari, *Introduction to Linear Algebra with Application to Basic Cryptography*, Asian Books, India, 2007.
- Avishek Adhikari, M. R. Adhikari and Y. P Chaubey, *Contemporary Topics in Mathematics and Statistics with Applications*, Asian Books , India, 2013.
- Avishek Adhikari, *Linear Algebraic Techniques to Construct black and white Visual Cryptographic Schemes for General Access Structure and its Applications to Color Images*, Design, Codes and Cryptography, 2013, DOI 10.1007/s10623-013-9832-5.
- A. Shamir, *How to share a secret*, Communication of ACM, Vol. 22, No. 11, 612-613, 1979.

Questions

Questions???

Galois Connection and Security (I)

ガロア接続を用いた動的秘密情報の管理 (I)

Application to Secure Information Flow

SAKURABA, Taketoshi[1,a)]

Abstract: As the part I of the presentation, we introduce concept of the lattice, the technology called formal concept analysis (FCA) and show their relation with the system security models. FCA is an application of the lattice theory and has been proposed as a method for the knowledge analysis. The basis of FCA is the Galois connection in the lattice theory, which derives a lattice from a context table. In the system security area, the lattice theory also plays important roles. One of the classical facts is that any secure information flow systems form lattices. It was explained in an axiomatic argument on property of secure information flow. In this presentation, we show this classical result by applying FCA to an access control table derived from a security policy.

1. Lattices

For lattice theory, refer [1].

A partially ordered set is a set equipped with a order relation "$\leq$" which satisfies following for elements x, y and z.

$$x \leq x \quad x \leq y \text{ and } y \leq z \Rightarrow x \leq z \quad x \leq y \text{ and } y \leq x \Rightarrow x = y$$

A lattice is a partial ordered set with more properties that any two elements x, y have the least common upper bound (lub) $x \vee y$ and the greatest common lower bound (glb) $x \wedge y$.

$$x \leq x \vee y \text{ and } y \leq x \vee y \quad \text{if } x \leq z \text{ and } y \leq z \;\Rightarrow\; x \vee y \leq z$$
$$x \wedge y \leq x \text{ and } x \wedge y \leq y \quad \text{if } z \leq x \text{ and } z \leq y \;\Rightarrow\; z \leq x \wedge y$$

Replacing "any two elements" with "any subset", the notion of complete lattices is obtained. But, considering only finite lattices, completeness does not matter.

Well known example of a partially ordered set P is non empty set of sets ordered by inclusion. If P is finite, it can be embedded in a lattice L, the intersection closure of P:

$$L = \{\cap A \mid A \subseteq P\} \qquad x \vee y = \bigcap \{z \mid x \leq z \text{ and } y \leq z\}$$

2. Galois Connection

Let G and M are non empty sets, and I is a relation between G and M, i.e. $I \subseteq G \times M$. $K = (G, M, I)$ is called a context. From the context, define maps γ and μ as follows. %

$$g \,\mathrm{I}\, m \Leftrightarrow (g, m) \in I$$
$$g \,\mathrm{I}\, N \Leftrightarrow g \,\mathrm{I}\, m \quad (\forall\, m \in N) \quad H \,\mathrm{I}\, m \Leftrightarrow g \,\mathrm{I}\, m \quad (\forall\, g \in H)$$

$$\gamma(\emptyset) = M \qquad \mu(\emptyset) = G$$
$$\gamma(g) = \{m \mid g \,\mathrm{I}\, m\} \qquad \mu(m) = \{g \mid g \,\mathrm{I}\, m\}$$
$$\gamma(H) = \{m \mid H \,\mathrm{I}\, m\} \qquad \mu(M) = \{g \mid g \,\mathrm{I}\, M\}$$
$$\mu\gamma(H) = \mu(\gamma(H)) = \{g \in G \mid g \,\mathrm{I}\, \{m \in M \mid H \,\mathrm{I}\, m\}\}$$
$$\gamma\mu(N) = \gamma(\mu(N)) = \{m \in N \mid g \,\mathrm{I}\, \{g \in G \mid g \,\mathrm{I}\, N\}\}$$
$$\gamma K = \{\gamma(H) \mid H \subseteq G\} \qquad \gamma\mu K = \{\gamma\mu(N) \mid N \subseteq M\}$$
$$\mu K = \{\mu(N) \mid N \subseteq M\} \qquad \mu\gamma K = \{\mu\gamma(H) \mid H \subseteq G\}$$

Then we get a lattice associated with the context $K = (G, M, I)$

Theorem 1 (Galois Connection)**.** *$\gamma\mu K$, γK, $\mu\gamma K$ and μK are all identical lattices. To be precise, $\gamma\mu K = \gamma K$, $\mu\gamma K = \mu K$, and γK and μK are dual each other. γ and μ are the order reversing isomorphism between them*

3. Formal Concept Analysis

Formal Concept Analysis (FCA) is an application of Galois-Connection. It was proposed by Wille [2] as a tool for analyzing data and knowledge. The settings of FCA are as follows [3].

G :	Set of objects (Gegenstände)
M :	Set of attributes (Merkmale)
I :	Context (Kontext)
$\gamma(H)$:	Intent of H, common attributes of all $g \in H \subseteq G$
$\mu(N)$:	Extent of N, objects satisfy attribute $m \in N \subseteq M$
(H, N) :	Formal concept of K, if $\gamma(H) = N$ and $\mu(N) = H$
$\mathfrak{B}(K)$:	Concept lattice, set of all formal concepts in K
	$(H_1, N_1) \leq (H_2, N_2) \;\Leftrightarrow\; H_1 \subseteq H_2 \;\Leftrightarrow\; N_1 \supseteq N_2$

Theorem 2 (Fundation of FCA)**.**

$$\bigwedge_t (H_t, N_t) = (\cap_t H_t, \gamma\mu(\cup_t N_t)) \qquad \bigvee_t (H_t, N_t) = (\mu\gamma(\cup_t H_t), \cap_t N_t)$$

As seen in the definition, an element of the concept lattice is

[1] Hitachi Yokohama Laboratory, Yokohama 244–0817, Japan
[a)] taketoshi.sakuraba.hc@hitachi.com

a pair of an intent and an extent, they are firmly related in the context K. Concrete but excessive concepts are reduced and included into the formal concepts. As the result of the construction, just enough formal concepts are remained. They are the essentially meaningful knowledge in the context K, and form a lattice.

4. Information Flow

A security model is a format of security policies. Information Flow Control (IFC) is one of the fundamental security model. Dividing users and information into some security classes, and monitoring and controlling flows of information and moves of information carriers. Let A and B are security classes. The order relation "$A \rightarrow B$" means that any information flow from A to B is permitted. The information flow relation can be seen as an order relation. Denning [4] showed that the security classes and secure information flow between them form a lattice. Thus this model also called the lattice model. Well known information flow policy is Bell-LaPadula model [6], which had been developed and used in US government. The lattice of BLP policy is simply linear-four-layers structure.

Important notions in IFC are NO-READ-UP and NO-WRITE-DOWN. the former means users in the lower security classes are not permitted to write anything into files of the upper security classes. This rule would be trivial. The latter means users of upper security classes are inhibited to write anything into files of the lower security classes, because upper secret may leak to the lower.

5. Application of FCA to IFC

A secresy security policy can be interpreted into an information flow control policy. As a consequence of the fact, one can see that, in a secure information flow policy, their security classes and the information flow relation form a lattice. These can be shown by using FCA as follows.

Define G as the set of users, and let M be the set of files. A file is considered as an attribute of a user, that means the user is permitted to access to the file by the security policy. This form of the security policy is called access control matrix (table). This information can be seen as a context of FCA. So, applying FCA to this context data, a concept lattice is derived. Each concept corresponds to a security class, and the order relation corresponds to the permitted information flow. In the access control theory, $\mu(m)$ is called access control list (ACL) of $m \in M$, and $\gamma(g)$ is called capability of $g \in G$. So, μK can be called ACL lattice, and γK can be called capability lattice.

Denning's explanation [4] was axiomatic, but in her another note [5], starting with partially ordered information flow models, and applying the intersection closure technic, she derived a lattice, which can be seen as a capability lattice in our argument.

6. Conclusion

The lattice and Galois connection thoery and FCA are introduced. Information flow and the lattice model of Denning are explained. Applying FCA to security policies, the lattice model is derived.

References

[1] Davey, B. A., Priestley, H. A.: *Introduction to Lattices and Order, second edition*, Cambridge University Press, Cambridge, UK, 2002.

[2] R. Wille, Restructuring lattice theory: an approach based on hierarchies of concept, D. Reidel, Ordered Sets (I. Rival eds.), pp.445–470, 1982

[3] Suzuki, O., Murofushi, T.: 形式概念分析 – 入門・支援ソフト・応用, 日本知能情報ファジイ学会, 知識と情報 vol.19, no. 2, pp. 103–142, 2007

[4] Denning, D. E. R.: A Lattice Model of Secure Information Flow, ACM, CACM, Vol.19, No.5, pp.236–243, 1976.

[5] Denning, D. E. R.: On the Derivation of Lattice Structures Information Flow Policies, Purdue University, CSD TR 180, 1976.

[6] Bell, D. E., LaPadula, J.: Secure Computer Systems: Unified Exposition and Multics Interpretation, MTR-2997, MITRE Corporation, ESD-TR-75-306, 1976.

[7] Sandhu, R. S., Coyne, E. J., Feinstein, H. L. and Youman, C. E.: Role-based access control models, IEEE Computer, Vol.29 No.2, pp.38–47, 1996.

HITACHI
Inspire the Next

IMI Workshop (2013/8/26—30)
安全・安心社会基盤構築のための代数構造
～サイバー社会の信頼性確保のための数理学～

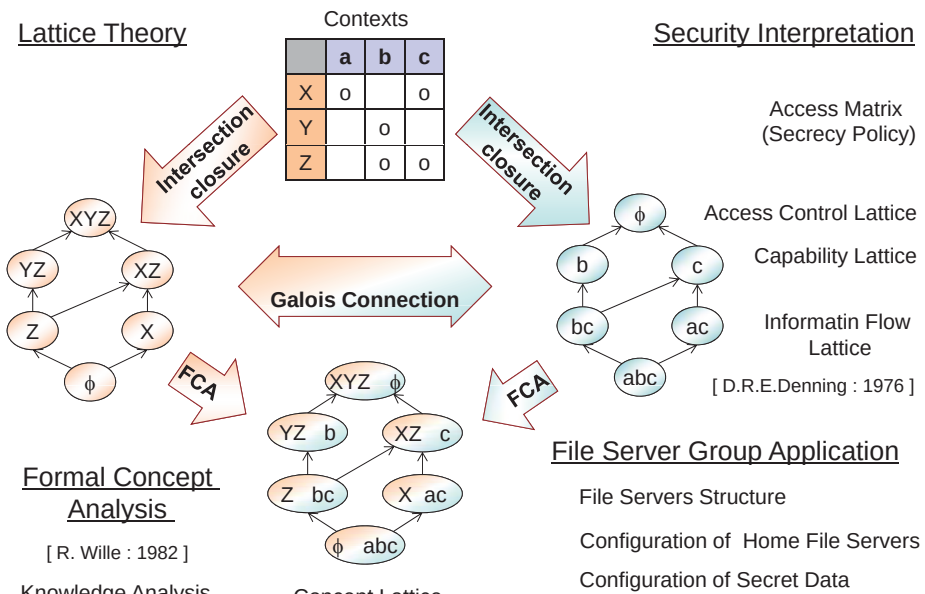
Galois Connection and Security (I)
ガロア接続を用いた動的秘密情報の管理 (I)
Application to Secure Information Flow

2013/08/27 Fukuoka, Japan

SAKURABA, Taketoshi Hitachi, Ltd.

Outline

HITACHI
Inspire the Next



 2

Agenda

HITACHI
Inspire the Next

- Galois Connection
  - Lattice Theory
  - Formal Concept Analysis
- Security
  - Information Flow Control
  - Lattice Model
- Application -- Hierarchical File Server Groups
  - Structure of HFSG
  - Security of HFSG
    - Information Flow Control,
    - Labeled Control without Labels,
    - RBAC
  - Management of HFSG
    - Comparison with Flat Structure
- Conclusions

Lattice

HITACHI
Inspire the Next

- Lattice
  - Partially Ordered Set (, not a subalgebra of Z x Z)
  - For any a and b in a lattice, they have both of
    lub [least upper bound, sup, join] of $\{a, b\}$, $= a \vee b$
    glb [greatest lower bound, inf, meet] of $\{a, b\}$, $= a \wedge b$
    - $a \vee b = b \vee a \quad a \vee (b \vee c) = (a \vee b) \vee c \quad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ etc.
- Example

  For $M \subseteq \mathbf{P}(X)$ $\mathbf{P}(X)$: powerset of X
  - Intersection-closure of M (= $\underline{M}$)

    $= \{ (\cap A) \cap (\cup M) \mid A \subseteq M \}$ (N.B. $(\cap \phi) \cap (\cup M) = \cup M \in \underline{M}$)
  - Complete lattice ordered by inclusion including M
    - $A \wedge B = A \cap B$
    - $A \vee B = \cap \{ C \mid A \cup B \subseteq C \in \underline{M} \}$

Galois Connection

HITACHI
Inspire the Next

Definitions

- $\mathbf{K} = (G, M, \mathbf{I})$: G, M : sets, $\mathbf{I} \subseteq G \times M$: relation

$g\ \mathbf{I}\ m \Leftrightarrow (g, m) \in \mathbf{I}$ $\quad g\ \mathbf{I}\ N \Leftrightarrow \forall m \in N\ (g\ \mathbf{I}\ m)$ $\quad H\ \mathbf{I}\ m \Leftrightarrow \forall g \in H\ (g\ \mathbf{I}\ m)$

$\gamma(g) = \{m \in M \mid g\ \mathbf{I}\ m\}$ $\quad \gamma(H) = \{ m \in M \mid H\ \mathbf{I}\ m\} = \cap \{ \gamma(g) \mid g \in H\}$

$\mu(m) = \{g \in G \mid g\ \mathbf{I}\ m\}$ $\quad \mu(N) = \{ g \in G \mid g\ \mathbf{I}\ N\} = \cap \{ \mu(m) \mid m \in N\}$

$\mu\gamma(H) = \mu(\gamma(H)) = \{ g \in G \mid g\ \mathbf{I}\ \{m \in M \mid H\ \mathbf{I}\ m\}\}$

$\gamma\mu(N) = \gamma(\mu(N)) = \{ m \in M \mid \{g \in G \mid g\ \mathbf{I}\ N\}\ \mathbf{I}\ m\}$

$\gamma\mathbf{K} = \{ \gamma(H) \mid H \subseteq G\}$ $\quad \gamma\mu\mathbf{K} = \{ \gamma\mu(N) \mid N \subseteq M\}$ N.B. : $\gamma(\phi) = M \in \gamma\mathbf{K}$

$\mu\mathbf{K} = \{ \mu(N) \mid N \subseteq M\}$ $\quad \mu\gamma\mathbf{K} = \{ \mu\gamma(H) \mid H \subseteq G\}$ $\quad \mu(\phi) = G \in \mu\mathbf{K}$

Theorem

- $\gamma\mu\mathbf{K} = \gamma\mathbf{K}$, $\mu\gamma\mathbf{K} = \mu\mathbf{K}$. These are lattices . ($\because$) $\cap$-closures
- $\gamma\mathbf{K}$ and $\mu\mathbf{K}$ are dual (order reversed, isomorphic) to each other

($\because$) $H \subseteq K \subseteq G \Rightarrow \gamma(H) \supseteq \gamma(K)$, $N \subseteq L \subseteq M \Rightarrow \mu(N) \supseteq \mu(L)$, $H \subseteq \mu\gamma(H)$, $N \subseteq \gamma\mu(N)$

$\therefore \gamma(H) \supseteq \gamma\mu\gamma(H)$, $\gamma(H) \subseteq \gamma\mu(\gamma(H))$, $\therefore \gamma(H) = \gamma\mu\gamma(H) \in \gamma\mu\mathbf{K}$, $\therefore \gamma\mathbf{K} \subseteq \gamma\mu\mathbf{K}$, …

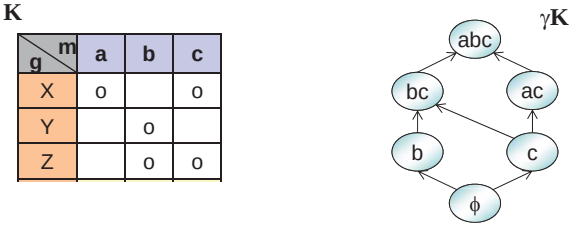
Example

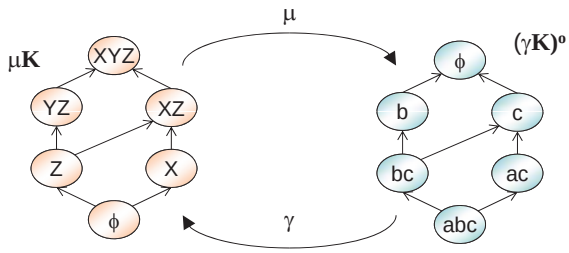
HITACHI
Inspire the Next

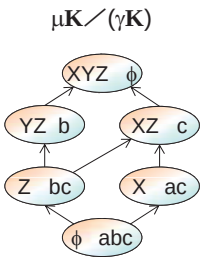
- $\mathbf{K} = (G, M, \mathbf{I})$ G, M : Sets, $\mathbf{I} \subseteq G \times M$
- $\gamma\mu\mathbf{K} = \gamma\mathbf{K}$, $\mu\gamma\mathbf{K} = \mu\mathbf{K}$: lattices. $\mu\mathbf{K} \equiv$ dual of $\gamma\mathbf{K}$

$\mathbf{K}$

g \ m	a	b	c
X	o		o
Y		o	
Z		o	o







ab denotes set {a, b}

FCA : Formal Concept Analysis

HITACHI
Inspire the Next

- **K**=(G, M, **I**)
  - G: Set of Objects, M: Set of Attributes, **I** (⊆G×M): “Formal” context
- γ(H) : Intent (H⊆G) μ(N) : Extent (N⊆M)
- (H, N) : “Formal” concept (H⊆G, N⊆M) ⇔ N=γ(H) and H=μ(N)
- **B**={(H,N) | (H,N) is a concept} : Concept Lattice

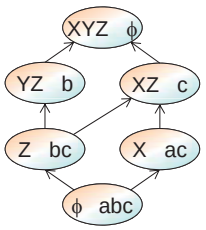
  (H1,N1)≦(H2, N2) ⇔ H1⊆H2 ⇔ N1⊇N2

  ⋀(Hi , Ni) = (∩Hi, γμ(∪Ni)) ⋁(Hi , Ni) = (μγ(∪Hi), ∩Ni))

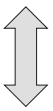
Context Table

g \ m	a	b	c	Intents	
X	o		o	ac	ϕ
Y		o		b	c
Z		o	o	bc	abc
Extents	X	YZ	XZ		
	ϕ	Z	XYZ		

Concept Lattice



Universal concept



Specific concept

Applications of FCA

HITACHI
Inspire the Next

- Rudolf Wille (1982).
  - “Restructuring lattice theory: an approach based on hierarchies of concepts”
- Data Analysis
- Healthcare
- Linguistics
- Software Design
- Security Models

- References

Davey, Priestley: Introduction to Lattices and Order, second edition, Ch.3, and Ch.7, Cambridge University Press (1990, 2002)

Suzuki, Murofushi: (in Japanese) Formal Concept Analysis – Introduction, Support Softwares and Applications –, **知識と情報** Vol.19, No.2 (2007)

Information Security

HITACHI
Inspire the Next

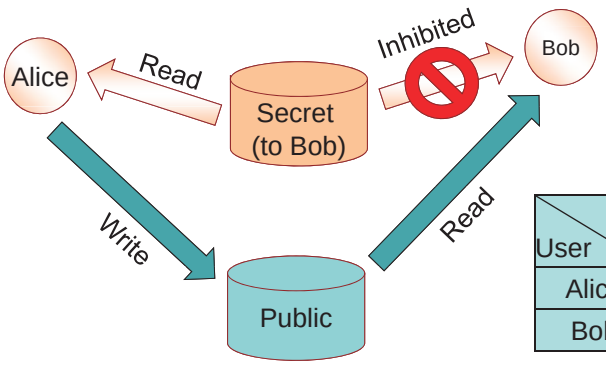
Technology for Protecting and Controlling “CIA”

- Confidentiality / Secret
  - Threats: Unauthorized access to information,
  - Measures: Information Flow Control, Cryptography, …
- Integrity / Consistency
  - Threats: Unauthorized modification of information
  - Measures: Rules for modification, Signature, …
- Availability
  - Threats: Unauthorized use of resources
  - Measures: Limiting resource allocation, Monitoring, …

Information Flow

HITACHI
Inspire the Next

- Information Flow
  - Secret ⇒Alice ⇒ Public ⇒ Bob
    - Against “the security Policy”



Secret may be known by Bob …

Access Matrix

User \ File	Secret	Public
Alice	Read	Write
Bob	-	Read

Security Policy Models

HITACHI
Inspire the Next

Format of Security Policy

- Access Matrix Model (Access Control Table)

		Objects			
		Secret A	Secret B	TopSecret	Public
Subjects	Alice	Read, Write			Read
	Bob		Read, Write		Read
	Chris	Read	Read	Read, Write	Read
	David				Read,Write

Alice's Capability

ACL of B

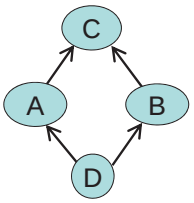
- Information Flow Model

A ∋ Alice、SecretA

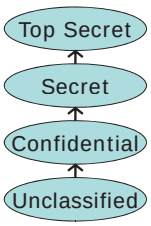
B ∋ Bob、SecretB

C ∋ Chris、TopSecret

D ∋ David、Public



Multi Level Security



 11

Order and Information Flow

HITACHI
Inspire the Next

A, B, … : security classes

≒ Set of "logical storage objects" sharing same information∋user, file, …

- A＝B : (members of) A and B share same information
- A⇒B : Information flow from A to B is permitted
  - Reflexive : A⇒A [may not be inhibited]
  - Transitive : A⇒B, B⇒C then A⇒C [B cannot keep secret]
  - Anti-Symmetric : A⇒B, B⇒A then A＝B
- Bell-LaPadula Model
  - A⇒B and A ≠ B then …
    - Read B by A : inhibited : No-Read-Up Read A by B : permitted
    - Write to A by B : inhibited : No-Write-Down Write to B by A : permitted
- Set of security classes forms partially ordered set furthermore, it becomes a Lattice [Denning,1976].

 12

FCA proof of Information Flow Lattice

HITACHI
Inspire the Next

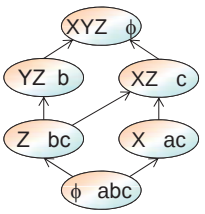
- Access Control Table ⇔ Context
- Information Flow : → ⇔ ≦ : Order Relation
- Security Classes ⇔ Concepts
- Structure of Security Classes ⇔ Lattice
- Access Control List (ACL) ⇔ Extent
- Capability ⇔ Intent

Access Matrix Model

file / user	a	b	c	Capability	
X	X can read a		o	ac	ϕ c ab
Y		o		b	
Z		o	o	bc	
ACL	X	YZ	XZ		
	ϕ Z XYZ				

⇔

Information Flow Model
Lattice Model



 13

Role Based Access Control

HITACHI
Inspire the Next

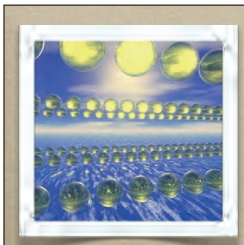
- RBAC
  - The most successful security model
  - Introduce Roles to describe Permission assignment rules
    - Subject ∈ Role ⇒ Permission, then Permission is assigned to Subject
      - Subject's actual/current role is determined dynamically [e.g. logon as an Admin]
      - Dr. Foo ∈ DOCTORS ⇒ May access his patient's medical record
  - Merits
    - Divide Permission Management into 2 parts, one is stable, another is easy
    - A subject may play different role in different context.
      - Dr. Foo on his day off, cannot access hospital's resource, except in emergency
- Modeling RBAC by using FCA
  - Dyadic Formal Context : Role-Permission relation
    ⇒ Role-lattice (Role hierarchy)
  - Triadic Formal Context :
    - K (R, D, P, **I**) ⇒ **I** ⊆ R × D × P = (R × D) × P
    - Roles, Documents, Permissions
      ⇒ Document types, classified by security point of view

 14

Conclusions (I)

HITACHI
Inspire the Next

- Galois Connection is a theorem of the Lattice theory
  $I \subseteq G \times M \Rightarrow$ derived two lattices are dual each other
- FCA is an application of Galois Connection for Knowledge Analysis
  considers extent lattice and intent lattice at once
- Security policy can be analyzed by FCA
  - Concept Lattice of given Security Policy represents appropriate Information Flow Policy
  - Another proof of Denning's theorem
- FCA is gathering attention from security point of view



Abstracting Lattice Cryptography

Phong Nguyễn

INVENTEURS DU MONDE NUMÉRIQUE

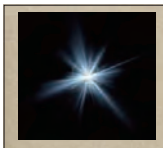
Tsinghua University

Fukuoka, August 2013

This Talk

- Present lattice cryptography as simply as possible, using analogies with classical public-key cryptography based on factoring and DL.

- Many lattice-crypto papers hide lattices and finite abelian groups using matrices.



Thesis

- Lattice cryptography can be described without matrices, by focusing on a (large) finite abelian group G generated by many random elements.
- Claim: avoiding matrices gives better insight and clarifies the use of duality.

Summary

- Finite groups in public-key cryptography
- Background on lattices
- Cryptography from lattices
  - Hard problems: SIS, LWE and generalizations
  - Cryptography without trapdoors
  - Cryptography with trapdoors
  - Advanced cryptography

Finite Groups in Public-Key Cryptography

Groups in Asymmetric Cryptography

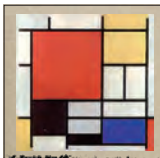
- Most public-key schemes known rely on groups, usually finite and abelian.
- The RSA family: groups whose order is secret, except for the party who constructed the group.
  - Ex: $(\mathbf{Z}/N\mathbf{Z})^\times$ whose order is $\varphi(N)$ and $N=pq$
- The DL family: cyclic groups whose order is a large public prime.
  - Ex: Subgroups of $(\mathbf{Z}/p\mathbf{Z})^\times$ and elliptic curves $E(\mathbf{F}_q)$ over finite fields.

Other Groups

- Non-abelian groups: braids, linear groups, etc. Not very popular.
- 'Post-quantum' crypto:
  - Finite fields used in multivariate crypto and coding-based crypto.
  - Lattices, which are infinite abelian groups!

Groups in Lattice Cryptography

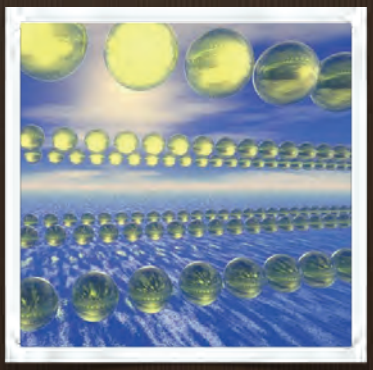
- Lattices are infinite abelian groups.
- But integer lattices are actually related to finite abelian groups, which are used implicitly in lattice cryptosystems. We will make this use explicit.



Why Abstracting?

- Abstracting can simplify descriptions and give better insight:
  - Ex: El Gamal encryption is best described with an arbitrary group, rather than with just $(\mathbf{Z}/p\mathbf{Z})^{\times}$.
  - Ex: Pollard's p-1 factoring method is best described with an arbitrary group. Using elliptic curves, one obtains ECM!

Background on Lattices



楕円曲線上の離散対数問題へのグレブナー基底を用いた攻撃
Attacks on the ECDLP using Groebner bases

安全・安心社会基盤構築のための代数構造
8月27日

Xavier Dahan
九州大学 システム情報科学府
情報科学専攻

Purpose of the talk

- Account of recent progresses in the Discrete Logarithm Problem over the group of rational points of elliptic curves Prepare the panel discussion session of Thursday 14:00-16:00
- Highlight the role of polynomial systems and tools for solving them : Groebner bases
- Toward practical subexponential algorithms ?

Discrete Logarithm Problem (DLP)

Given a cyclic group G and a generator g
$For\ h \in G, find\ t \in \mathbb{N}\ such\ that\ [t]g = h$

Computationally difficult problem on which relies:

- Diffie-Hellmann protocol
- ElGamal cryptosystem
- Digital signature algorithms
- Pairing

- With RSA, a keystone of the whole public-key cryptography.
- Evaluating its security is critical

Generic attacks: yardsticks for security

- "Generic": alglorithms that does not depend on a particular cyclic group G

$n \stackrel{\text{def}}{=} \#G$

- Brute force: compute $[t]g$ and test $[t]g =?\ h$ for $t = 1, \dots, n \rightarrow$ up to $O(n)$ operations in G
- Most efficient: Pollard ρ-method → $O(\sqrt{n})$ op. in G

- Efficiency vs security: For Elliptic Curves, NIST recommends to use finite fields of size 2^{224} (or2^{160})

Two important families of cyclic groups

- Invertible elements of a finite field:
  $\mathbb{F}_q^*$, q a prime power $\left|\mathbb{F}_q^*\right| = q - 1$

- (Large cyclic subgroup) of the group of rational points of an elliptic curve C.

  $E_C(\mathbb{F}_{q^n})$ $\left|E_C(\mathbb{F}_{q^n})\right| \approx q^n + O\left(q^{\frac{n}{2}}\right)$
  Often contains a large cyclic subgoup.

Motivation for Elliptic Curves

(V. Miller and N. Koblitz, 1985)

- More secure than finite fields.
  Not as efficient attacks for finite fields exist for EC
  ⇒ for a same level of security, shorter finite fields (=shorter key)

- More choice ⇒ for each prime power $q = p^r$ there are only one finite field $\mathbb{F}_q$ whereas there are approximately $2q$ elliptic curves defined over $\mathbb{F}_q$

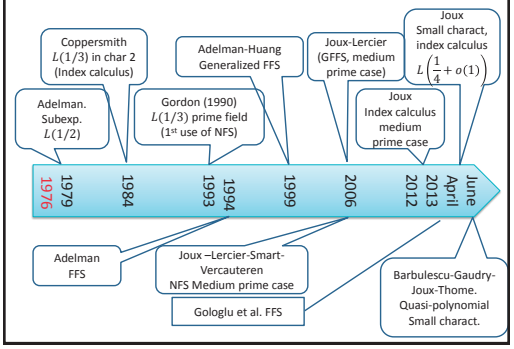
Running time complexity classes

- Measure of complexity against bit-length: $\log(n) = \log(\#G)$

$$L_N(\alpha) = \exp(O(\log(N)^{\alpha}\ (\log(\log(N))^{1-\alpha})$$

- Exponential: $n^c = L_n(1)$ Pollard ρ : $\approx n^{\frac{1}{2}}$
- Subexponential: $e^{\mathrm{O}(\log(n)^c)} = L_n(c),\ c < 1$
- Quasi-Polynomial: $\log(n)^{O(\log(n))} < L_n(\epsilon), \forall \epsilon$
- Polynomial: $\log(n)^{O(1)} = L_n(0)$

Milestones in DLP: finite fields



Conclusion (of the intro)

- 2013's results suggest that in a near future the DLP over finite field may not be secure enough.
- This motivates to study further the security of ECDLP.

Generalities about elliptic curves

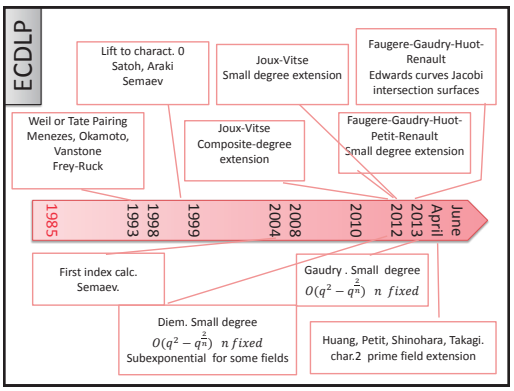
Elliptic Curves

- Most commonly defined by the Weierstrass model. In the plane of coordinates x, y:

$$y^2 = x^3 + a_4x + a_6 \quad if\ char(K) \neq 2$$
$$y^2 + xy = x^3 + ax^2 + b \quad if\ \ char\ (K) = 2$$
$$a_4, a_6, a, b \in K$$

- These are curves of genus 1 and are the only curves whose set of rational points is endowed naturally of a group structure:

$$E_C(K) \quad (or\ \ E(K)\ \ if\ no\ ambiguity\ about\ C)$$



Index calculus: an attack to the DLP

Input: group G $(= E_C(\mathbb{F}_q))$ of order n. $P, Q \in G$
Output: $t \in \mathbb{N}$ such that $[t]P = Q$

Step 1: Construct a factor base $\mathcal{F} = \{P_1, \dots, P_s\} \subset G$
Step 2: Setup product relations (sieving)
$[a_i]P + [b_i]Q = [e_{i,1}]P_1 + \cdots + [e_{i,s}]P_s,\ i = 1, \dots, s+1$
Step 3: Linear algebra
$A = (e_{i,j})_{\substack{1 \le i \le s \\ 1 \le j \le s}}$ matrix obtained at Step 2
$v = (e_{s+1,1}, \dots, e_{s+1,s})$ Solve $x^t A = v$.
Let $\alpha = (a_1, \dots, a_s)x^t$ and $\beta = (b_1, \dots, b_s)x^t$
Then $[\alpha]P + [\beta]Q = x^t A(P_1, \dots, P_s)^t = v(P_1, \dots, P_s)^t = [a_{s+1}]P + [b_{s+1}]Q$
Step 4 : Return $t = (\alpha - a_{s+1})(\beta - b_{s+1})^{-1} \bmod n$

Difficulties of index calculus for ECDLP

- How to choose a good decomposition basis $\mathcal{F} \subset E(\mathbb{F}_q)$?
  - Easy to describe
  - A lot of points can decompose in this basis
  - PDP is solved efficiently
- How to decompose effectively (Point Decomposition Problem = PDP) ?

For all $R \in E(\mathbb{F}_q)$, find $P_1, \dots, P_m \subset \mathcal{F}$ such that $R = P_1 + \cdots + P_m$

Solving the PDP efficiently

- Weil restriction (Frey, 2001)
  Choose $\mathcal{F} = \{(x, y) \in \mathbb{F}_q{}^n \mid y \in \mathbb{F}_q\}$
  But leads to up to $n(n+1)$ equations in $n(n+1)$ unknowns too much !
- Summation polynomials (Semaev, 2004)

To any elliptic curve, ∃ polynomials $f_1, f_2, \dots$:
$f_m(x_1, \dots, x_m) = 0 \Leftrightarrow \exists\ P_1, \dots, P_m \in E(\overline{\mathbb{F}_q})$
such that $P_1 + \cdots + P_m = O_C$
and $P_i = (x_i, y_i)$ $(here\ y_i \in \overline{\mathbb{F}_q})$

Semaev's summation polynomials (1)

- $char(\mathbb{F}_q) \ge 3$
  Weierstrass equation: $y^2 = x^3 + a_4 x + a_6$
- $f_2(x_1, x_2) = x_1 - x_2$
  $f_3(x_1, x_2, x_3) = (x_1 - x_2)^2 x_3^2 - 2((x_1 x_2 + a_4)(x_1 + x_2) + 2a_6)x_3 + (x_1 x_2 - a_4)^2 - 4a_6(x_1 + x_2)$
  $f_m(x_1, \dots, x_m) = Res_X(f_{m-k}(x_1, \dots, x_{m-k-1}, X), f_{k+2}(x_{m-k}, \dots, x_m, X))$
  for all $m \ge 4$ and for all $m - 3 \ge k \ge 1$

Resultant

$$A(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0, \quad a_m \neq 0, \quad m \ge 1$$
$$B(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0, \quad b_n \neq 0, \quad n \ge 1.$$

$$\mathrm{Syl}(A, B) = \begin{pmatrix} a_m & \cdots & a_1 & a_0 & & \\ & a_m & & a_0 & & \\ & & \ddots & & \ddots & \\ & & a_m & \cdots & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & \cdots & b_1 & b_0 \\ & b_n & \cdots & \cdots & \cdots & b_0 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ (n+m) \text{ lines} \\ (n+m) \text{ columns} \end{matrix}$$

$Res_x(A, B) = \det(Syl(A, B)) = \pm Res_x(B, A)$

Enjoy nice properties under projection.
Can be computed efficiently.....until some point !

Semaev's summation polynomial (2)

- $char(\mathbb{F}_q) = 2$
  Weierstrass equation: $y^2 + xy = x^3 + a_2 x^2 + a_6$
- $f_2(x_1, x_2) = x_1 - x_2$
  $f_3(x_1, x_2, x_3) = x_1^2 x_2^2 + x_1^2 x_3^2 + x_1 x_2 x_3 + x_2^2 x_3^2 + a_6$
  $f_m(x_1, \dots, x_m) = Res_X(f_{m-k}(x_1, \dots, x_{m-k-1}, X), f_{k+2}(x_{m-k}, \dots, x_m, X))$
  for all $m \ge 4$ and for all $m - 3 \ge k \ge 1$
- Coefficient a_2 does not appear in Semaev's polynomials
- Therefore the polynomials are simplified compared to $char(\mathbb{F}_q) > 2$

Semaev's polynomials $f_2, \dots, f_m$:

$f_m(x_1, \dots, x_m) = 0 \Leftrightarrow \exists\, P_1, \dots, P_m \in E(\overline{\mathbb{F}}_q)$
$such\ that \quad P_1 + \cdots + P_m = O_C$
$and \quad P_i = (x_i, y_i) \quad (here\ y_i \in \overline{\mathbb{F}}_q)$

- Allow to solve PDP in the index calculus attack more efficiently (for ECDLP).
- How?
- Let $R_i := [a_i]P + [b_i]Q$ (sieving step)
  Write $R_i = (x(R_i), y(R_i)) \in E_C(\mathbb{F}_q)$
- To find a relation $R_i = P_1 + \cdots + P_m$ it suffices to solve $f_{m+1}(x_1, \dots, x_m, x(R_i)) = 0$

Solving Semaev's polynomials (1)

- Properties: $f_m(x_1, \dots, x_m)$ verifies:
  - $\forall\, m \geq 3, \quad \deg_{x_i}(f_m) = 2^{m-1}$
  - f_m is symmetric: permuting some variables do not change f_m $(m \geq 3)$
  - f_m is irreducible (no simplification possible)
- f_m grows quickly with m :
  - It has at most $2^{m(m-1)}$ monomials.
  - Even a small fraction of the above number is huge.
  - f_7 has never been computed

Descent technique (1)

Let $h_{m+1}(x_1, \dots, x_m) := f_{m+1}(x_1, \dots, x_m, x(R))$.
Finding a solution in $(\mathbb{F}_{q^n})^m$ of h_{m+1} is not easy

Let $\{1, \omega, \dots, \omega^{n-1}\}$ be an $\mathbb{F}_q -$ basis of $\mathbb{F}_{q^n}$
$\mathbb{F}_{q^n} = \oplus_{j=0} \mathbb{F}_q \omega^j$

$\Rightarrow \quad \mathbb{F}_{q^n}[x_1, \dots, x_m] = \oplus_{j=0} \mathbb{F}_q[x_1, \dots, x_m]\omega^j$ and it follows:

$$h_{m+1}(x) = \sum_{j=0} h_{m+1}^{\downarrow j}(x)\omega^j$$

Solving h_{m+1} over $\mathbb{F}_{q^n}$ ⇔ solving n equations over $\mathbb{F}_q$ in m unknowns

Application to small degree extension

- Solving h_{m+1} over $\mathbb{F}_{q^n}$ ⇔ solving n equations over $\mathbb{F}_q$ in m unknowns.
- Unfortunately if $n < m$ the system $\{h_{m+1}^{\downarrow j}, j = 0, \dots, n-1\}$ isn't easily solvable (dim>0)
- Unfortunately, if $m > 6$, f_{m+1} is very hard to compute.
- If $m = n$
  This means looking for PDP with n points $R = P_1 + \cdots + P_n$ (put m=n)
- And choose as factor base:
  $\mathcal{F} := \{(x, y) \in E(\mathbb{F}_{q^n}) \mid y \in \mathbb{F}_q\}$

Application to composite degree extension field

- If $n = mn'$, then choose:
  $\mathcal{F} := \{(x, y) \in E(\mathbb{F}_{q^n}) \mid y \in \mathbb{F}_{q^{n'}}\}$
- For $R = [a]P + [b]Q$, the PDP is:
  $R = P_1 + \cdots + P_m$
- As before we compute the $m + 1^{th}$ Semaev polynomial f_{m+1} and its evaluation at $x(R)$:
  $h_{m+1}(x_1, \dots, x_m) = f_{m+1}(x_1, \dots, x_m, x(R))$
- We deploy it over $\mathbb{F}_{q^{n'}}$:

$$h_{m+1} = \sum_{j=0} h_{m+1}^{\downarrow j}\, \omega^j$$

….composite degree extension fied(2)

- To solve the system over $\mathbb{F}_{q^{n'}}$:

$$\begin{cases} f_{m+1}^{\downarrow 0}(x_1, \dots, x_m, x(R)) = 0 \\ \vdots \\ f_{m+1}^{\downarrow m-1}(x_1, \dots, x_m, x(R)) = 0 \end{cases}$$

It is often more efficient to solve it over $\mathbb{F}_q$:
We add the n' field equations if q is small:

$$\{x_i^q - x_i\}\ 1 \leq i \leq n'$$

Polynomial System Solving with Groebner bases

Polynomial System Solving

多変数多項式方程式系

$x^4y^2z^3 - 4x^2yz^2 + x^3 - z = 0$
$x^3y^2 - xyz + x^3 - zy = 0$
$\vdots$
$x^3y^2z + 3x^2y^2z + x^4 + 1 = 0$

グレブナー基底（辞書式順序）

$x^4y^2z^3 - 4x^2yz^2 + x^3 - z = 0$
$-xyz + x^3y^2 + x^3 - zy = 0$
$\vdots$
$y^3 + y^2x^3 - yx + 1 = 0$ 変数xとyだけ
$x^2y + xy + y + 2 = 0$
$x^3 + x^2 + 1 = 0$ 変数xだけ

線形方程式系

$a_{11}x_1 + \cdots + a_{1n}x_n = y_1$
$a_{21}x_1 + \cdots + a_{2n}x_n = y_2$
$\vdots\ \vdots\ \vdots\ \vdots$
$a_{m1}x_m + \cdots + a_{mn}x_m = y_m$

Row echelon form

$b_{11}x_1 + \cdots\cdots + b_{1n}x_n = y'_1$
$b_{23}x_3 + \cdots + b_{2n}x_n = y'_2$
$\ddots$
$b_{mr}x_r + \cdots = y'_m$

Groebner Bases

- Depends on a monomial order:
  ① Lex. Order: $x \prec y \prec z$

$$x^{10} \prec y \prec x^{100}y^2 \prec z \prec y^{100}z^2 \prec x^{10^{10}}y^{101}z^2$$

② Degree Reverse Lexicographic Order: $x \prec y \prec z$
This is a degree order: first compare the degree

$$xyz \prec x^4 \prec y^5 \prec z^6 \prec x^7 \prec x^3y^2z^3$$

If the degree is equal, then do like $lex(x \succ y \succ z)$

$$z^7 \prec y^7 \prec xy^6 \prec x^2yz^5 \prec x^2y^3z^3 \prec x^3y^2z^3$$

Leading Monomial

- $lex(x \prec y \prec z)$
  What is the largest monomial in p ?
  $p(x,y,z) = 2 + x^2 + xy - 2xyz^2 + x^2y^5z$
  $-\ LM(p) = xyz^2$
  $-\ LC(p) = -2$

- $p(x,y,z), q(x,y,x) \in k[x,y,z]$

$$LM(\langle p,q\rangle) \stackrel{\text{def}}{\equiv} LM(\{ap + bq \mid \forall a,b \in k[x,y,z]\})$$

$$LM(\langle p,q\rangle) \supseteq \{aLM(p) + bLM(q)\} \stackrel{\text{def}}{\equiv} \langle LM(p), LM(q)\rangle$$

Groebner Bases, outline

- Family of polynomials: $G = (g_1, g_2, \ldots, g_s)$
  $LM(\langle G\rangle) = \langle LM(g_1), \ldots, LM(g_s)\rangle$

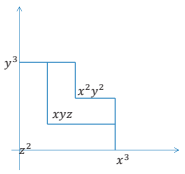
- Challenge: Given a polynomial system
  $f_1, \ldots, f_t \in k[x_1, \ldots, x_n]$
  compute a Groebner basis G
  $\langle LM(g_1), \ldots, LM(g_s)\rangle = LM(\langle f_1, \ldots, f_t\rangle)$

- Buchberger: 1965 (introduces S-polynomials)
  Faugere (2000~) F4/F5 : Linear algebra on a big matrix “Macaulay matrix”

Groebner “staircase”

- Let $G = (g_1, g_2, g_3, \cdots, g_s)$ be a GB for $\prec$.
- Then the exponent of the leading monomials $LM(g_1), \ldots, LM(g_s)$ can be represented in a the space.

Ex: $G \subset k[x,y,z]$,
$lex(x \prec y \prec z)$
$LM(g_1) = x^3$, $LM(g_2) = x^2y^2, LM(g_3) = y^3$,
$LM(g_4) = xyz$, $LM(g_5) = z^2$



Efficient Computation of Groebner bases: choice of monomial order

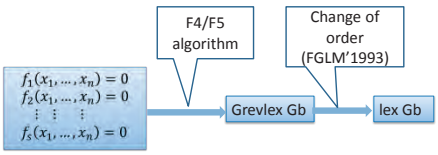
Theorem (Bayer-Stillmann '1987): The most efficient monomial order for computing a Groebner basis is the degree reverse lex. order (grevlex)

But a grevlex Groebner basis is not very useful.

The most useful lex Gb are unfortunately the hardest to compute.

If number of solutions is finite: "**change of order**" strategy.

Change of order strategy



- FGLM: Linear algebra in the quotient ring $k[X]/I$
- Requires the system to have a finite number of solutions (dimension 0)

Symmetries of Semaev's polynomials

Preliminary

- Even for $m < 7$, the polynomial systems arising from the m^{th} Semaev's f_m polynomial are very hard to solve.
- In order to reduce its hardness, we can use the fact that f_m is symmetric:

$\forall$ permutation σ on m elements:
$f_m(x_{\sigma(1)},\dots,x_{\sigma(m)}) = f_m(x_1,\dots,x_m)$

Invariant polynomial system

- it follows that the polynomials in the system arising by scalar restriction are also symmetric:
$$h_{n+1}^{\downarrow j}(x_1,\dots,x_n) \quad j=0,\dots,n-1$$
- In this case the set of solution $Sol_n(h_{n+1}^{\downarrow j}, j=0,\dots,n-1)$ is invariant by exchange of coordinates:
- If one has 1 solution, automoatically gives $n!$ solutions.
- Complexity can "theoretically" be divided by $n!$

Rewriting symmetric polynomials

Theorem: if $F(x_1,\dots,x_m)$ is symetric then there exist $G \in k[x_1,\dots,x_n]$ such that:
$$F = G(\sigma_1,\dots,\sigma_n)$$

$$\sigma_1(x_1,\dots,x_n) = x_1+\cdots+x_n$$
$$\sigma_2(x_1,\dots,x_n) = x_1x_2+x_1x_3+\cdots+x_{n-1}x_n$$
$$\vdots$$
$$\sigma_n(x_1,\dots,x_n) = x_1\cdots x_n$$

G has smaller degree than F

- Rewrite Semaev's polynomial f_m in term of symetric polynomials:
- Ex:
  $f_3 = \sigma_2^2 + \sigma_3 + a_6$ (elliptic curves in char 2)
  $f_3'(y_1, y_2, y_3) = y_2^2 + y_3 + a_6$
- $f_3{}'$ is smaller than f_3
- $f_m'(\sigma_1, \dots, \sigma_m) = f_m(x_1, \dots, x_m)$

Use of symetrization

- Choose a $\mathbb{F}_q \subset V \subset \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-vector subspace.
  Consider the factor base (Diem, 2008)
  $\mathcal{F}_V := \{(x, y) \in E_C(\mathbb{F}_{2^n}) \mid x \in V\}$
- Case 1 $V = \mathbb{F}_{q^{n'}}$ is an intermediate field.
- Case $V = \{1, \omega, \omega^2, \dots, \omega^{n'-1}\}$

Use of symetrization in case 1

Composite degree extension $V = \mathbb{F}_{q^{n'}} \subset \mathbb{F}_{q^n}$
Let be a basis of the extension $\mathbb{F}_{q^n} | \mathbb{F}_{q^{n'}}$

For $1 \le j \le m \quad \sigma_j = d_{j,0}$ * ($d_{j,0}$ are variables)
$x_{m+1} = r_1 + r_2\omega_2 + \cdots + r_{\frac{n}{n'}}\omega_{\frac{n}{n'}} \qquad r_\ell \in \mathbb{F}_{q^{n'}}$

Let $h'_{m+1} \in \mathbb{F}_{q^n}[\sigma_1, \dots, \sigma_m]$ the $(m+1) - th$ Semaev's polynomial with $x_{m+1} = x(R)$

Substitute relations * in h'_{m+1} and deploy over $\mathbb{F}_{q^{n'}}$ using the basis $\{1, \omega_2, , \dots, \omega_{\frac{n}{n'}}\}$ obtain $\frac{n}{n'}$ equations in m variables.

Symmetrization with intermediate field

- If $m \approx n/n'$ the systen has likely a solution.
- This system is easier to solve than the direct approach thanks to the symmetry.

Application to prime degree extension (case 2 of symmetrization) (HPST'2013)

- Setting: $\mathbb{F}_{2^n} | \mathbb{F}_2$, n is prime.
  $\{1, \omega, \omega^2, \dots, \omega^{n-1}\}$ a basis
- Difficulty: since n is prime no intermediate extension. Therefore the previous technique cannot be used.
- Following (Diem, 08) choose $V = \{1, \omega, \dots, \omega^{n'-1}\}$
- Again using symmetries, the aim is to simplify the PDP w.r.t. the following factor base:
- $\mathcal{F}_V := \{(x, y) \in E_C(\mathbb{F}_{2^n}) \mid x \in V\}$

- $V = \{1, \omega, \dots, \omega^{n'-1}\} \qquad n \approx mn'$
- $\alpha_1, \dots, \alpha_m \in V \Rightarrow \sigma_1(\alpha) \in V$
- $\sigma_2(\alpha) \in \langle 1, \omega, \dots, \omega^{2n'-2} \rangle$
- ⋮
- $\sigma_m(\alpha) \in \langle 1, \omega, \dots, \omega^{n-m} \rangle$ because $n \approx mn'$

- Next: rewrite the polynomials σ_j in the above bases.

- $\sigma_1 = d_{1,0} + d_{1,1}\omega + \cdots + d_{1,n'-1}\omega^{n'-1}$
- $\sigma_2 = d_{2,0} + d_{2,1}\omega + \cdots + d_{2,2n'-2}\omega^{2n'-2}$

$\vdots$

- $\sigma_m = d_{m,0} + d_{m,1}\omega + \cdots + d_{m,,n-m}\omega^{n-m}$

- Let $h'_{m+1} \in \mathbb{F}_{q^n}[\sigma_1, \ldots, \sigma_m]$ the $(m+1) - th$ Semaev's polynomial with $x_{m+1} = x(R)$
- Replace the σ_j in h'_{m+1} and apply descent techniques in $\mathbb{F}_q$.

- Obtain $h'_j \in \mathbb{F}_q[d_{j,\ell}] \quad 1 \leq j \leq n$
- Replace σ_j in the system below
- $\sigma_1 = x_1 + \cdots + x_n$

$\sigma_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n$

$\vdots$

$\sigma_n = x_1 \cdots x_n$

- Obtain a lot of new equations with new N:=m $+ n'm + \frac{(n'-1)m(m+1)}{2}$ variables
- Impossible that is easy to solve !
- But this is indeed the case ! symmetrization has reduced the degree, and the system is very structured.

Not talked about

- Use of symmetry in the Edwards curves and Jacobi intersection surfaces (F.,G.,H.,R., 2013)
- Joux-Vitse (2012,2013): combining cover attack with this decomposition attack.
- Petit-Quisquater (2012) : conjecture subexponential algorithm in the binary case first fall degree $\approx$ degree of regularity

ありがとう

Galois Connection and Security (II)

ガロア接続を用いた動的秘密情報の管理 (II)

Hierarchical File Server Groups for Implementing Mandatory Access Control

Summary of the presentation

SAKURABA, TAKETOSHI[1,a)]

Abstract: As the continuation of the previous manuscript, an application of Formal Concept Analysis for Information Flow Control between file servers is presented. A File Server Group is a system of plurality of file servers organized for controlling secure information flow among them. The configuration of files servers is derived from an organizational security policy by using formal concept analysis. Role-Based Access Control also can be implemented with a File Server Group. The File Server Group implements the Mandatory Access Control among sensitive files and users in an organization without introducing any "exotic" MAC tools such as secure OSs, security labels and global reference monitors. Those are virtually embedded into the configuration of the File Server Group. Adopting lattice structure and FCA, the configuration cost of File Server Group is lower than that of flat structured file server systems.

Keywords: Formal Concept Analysis, File Server Group, lattice model, Mandatory Access Control

1. File Server Group

1.1 Enforcement of distributed MAC

To enforce mandatory access control (MAC) in a modern distributed computing environment, some tools such as global reference monitors have been introduced [8], [9], [10]. But they had to introduce new tools, which people are unfamiliar with, and those have not got popularity in any level. The Hierarchical File Server Group (HFSG) we propose here is also a new mechanism for supporting MAC, but uses ordinal file servers which is familiar to many people.

1.2 HFSG, and Use of FCA

A HFSG system consists of plurality of file servers which are connected via read-only mounts. Each file server stores files of similar security class, and the mount option limit the flow of information in those files.

Assume that an organization has a security policy, and interpret it into an access control table as seen in **Table 1**. Analyzing the table by using Formal Concept Analysis (FCA), a concept lattice is derived as in **Fig. 1**. The node 2 represents the concept (Y, ab). The edge connecting 2 and 5 represents a secure information flow from 5 to 2. Upward flow is secure and downward flows should be limited.

Applying the concept lattice, the HFSG system shown in **Fig. 2** is obtained as follows. Each triangle represents a file server and corresponds to a security class of the information flow policy, and each arrow represents information flow that should be enforced. The information flow enforcement is implemented by the read-only mount mechanism. A file server corresponding to an upper security class is mounting file servers corresponding to lower security classes with Read-Only option, which allows the upper file servers to read data in the lower file servers, and prohibits writing data through the mount point. From the lower file servers, the upper file servers are invisible. As a consequence, only information flows from the lower file server to the upper occur.

Table 1 Example Policy

	Sensitive Data		
User	a	b	c
X	×		
Y	×	×	
Z		×	×

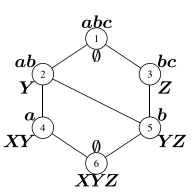


Fig. 1 Concept Lattice

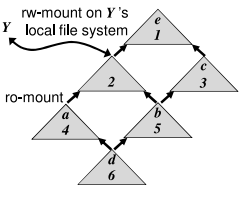


Fig. 2 File Server Group

[1] Hitachi Yokohama Laboratory, Yokohama 244–0817, Japan
[a)] taketoshi.sakuraba.hc@hitachi.com

1.3 Home file server

To each user of HFSG, his/her "home file server" in HFSG is assigned according with the user's capability. The user is forced to use a computer mounting the his/her home file server, or the user can mount only his/her home file server. In Fig. 2, the home file server of user Y is the server numbered 2, and Y is using the file server by mounting file server 2 to Y's local file system. Then Y can make read-and-write access to the files on the file server 2, and read-only access to the files on the file servers 3, 4, 5 and 6. User Y does not know about file servers 1 and 3 because they are invisible to Y.

1.4 Placement of Files and Users

Location of files and home file servers of users in the HFSG are determined by the concept lattice explicitly. In the concept lattice Fig. 1, user Y appears in nodes 2, 4, 5 and 6, and because the **lub** of those nodes is 2, the home file server of Y is 2. Similarly, b is seen in nodes 1, 2, 3 and 5, and the **glb** of them is 5. So file b should be stored in file server 5. Note that in (finite) lattices, lub and glb of any subset of the lattice are uniquely determined. Also note that the intents and the extents are used explicitly and directly in the construction of HFSG.

2. Application to RBAC

Changing the correspondence between the concept lattice and the computing environment, HFSG system can be applied to implement Role-Based Access Control (RBAC) policy. One of the characteristic concept of RBAC is session, and correspondence from a session to a role the user are working with. Capability of a user differs depending on the role selected for the session,

To implement such mechanism, analyze relations between a role and resources which are neccessary to play the role, and allocate file servers to each role, and prepare client computers as an entry point to roles. Using a client computer can be seen as working in a session. A client computer (or a user account in the computer) is corresponfing to a role, and is mounting the home file server of the role.

3. Security of FSG

HFSG implements access control policy represented in the form of access control table. In particular, No Write Down policy is enforced by the Read-only mount, and No Read Up policy is enforced because upper file server is invisible. The settings and configuration are done only in the file servers. The mount options are done by administrators of HFSG. Users cannot make downgrade of files, cannot move files from upper files server to lower file server. These are characteristic of a Mandatory Access Control. To implement MAC, use of security labels are common and essential security mecanism for implementing and managing the seurity of an organization. HFSG does not introduce security labels explicitly, but the file server itself can be regarded as a security label. The home file server of a user can be seen as the label of the user. If a file is stored in a file server, then the file server is the label of the file.

4. Configuration Cost of FSG

One of the merits of HFSG is the management cost.

The same access control can be implemented without hierarchical structure. Let us call such configuration flat structure. In a flat structured file servers, security policy enforcement mechanism is only file system's access control. The configuration in the flat structure may be complicated and hard to understand, because access control parameters must be prepared for each pair of user and server which may be accessd by the user. So the number of the parameter is estimated as $F * U/2$, where F is number of file servers, which is the same with the number of the security classes, and U is the number of users of the system.

On the other hand, HFSG's hierarchical structure helps administrators to understand the structure. HFSG is adopting the read-only mount to enforce the information flow. Utilizing the lattice structure, configuration of HFSG is simplified. Neccesary configuration parameters are only for user and user's home file server, and for some of file servers pair. So the number of the parameter can be estimated as $U + F^2$. In actual system, U is big but F would be so small that it can be negrected.

5. Conclusion

We introduced the hierarchical file server group system, HFSG. HFSG enforces lattice-based information flow control policy. HFSG uses plural file servers and conguration of those file servers is based heavily on the formal concept analysis technology which is an application of Galois connection in the lattice theory. One of the prerequisit to implement HFSG is that the file server used in HFSG is capable to export the imported file system. Some distributed file system need enhancement. Utilizing the lattice structure, HFSG's adoministration cost is considered to be low.

References

[1] Davey, B. A., Priestley, H. A.: *Introduction to Lattices and Order, second edition*, Cambridge University Press, Cambridge, UK, 2002.

[2] R. Wille, Restructuring lattice theory: an approach based on hierarchies of concept, D. Reidel, Ordered Sets (I. Rival eds.), pp.445–470, 1982

[3] Suzuki, O., Murofushi, T.: 形式概念分析 – 入門・支援ソフト・応用, 日本知能情報ファジイ学会, 知識と情報 vol.19, no. 2, pp. 103–142, 2007

[4] Denning, D. E. R.: A Lattice Model of Secure Information Flow, ACM, CACM, Vol.19, No.5, pp.236–243, 1976.

[5] Denning, D. E. R.: On the Derivation of Lattice Structures Information Flow Policies, Purdue University, CSD TR 180, 1976.

[6] Bell, D. E., LaPadula, J.: Secure Computer Systems: Unified Exposition and Multics Interpretation, MTR-2997, MITRE Corporation, ESD-TR-75-306, 1976.

[7] Sandhu, R. S., Coyne, E. J., Feinstein, H. L. and Youman, C. E.: Role-based access control models, IEEE Computer, Vol.29 No.2, pp.38–47, 1996.

[8] M. Zakrewski, "Mandatory Access Control for Linux Clustered Servers," Proc. of the Ottawa Linux Symposium, pp. 618–631, 2002.

[9] McCune, J. M., Jaeger, T., Berger, S., Cáceres, R., Sailer, R.: Shamon: A System for Distributed Mandatory Access Control, Proc. of the 22nd Annual Computer Security Applications Conference, pp.23–32, 2006.

[10] Zeldovich, N., Wickizer, S. B., Mazières, D.: Securing distributed systems with information flow control, Proc. of the 5th NSDI, pp. 293–308, 2008.

[11] Sakuraba, T.: Proposal of the Hierachical File Server Groups for Omplementeing Mandatory Access Control, IEEE, International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 639–644, 2012,

HITACHI
Inspire the Next

IMI Workshop (2013/8/26—30)
安全・安心社会基盤構築のための代数構造
～サイバー社会の信頼性確保のための数理学～

Galois Connection and Security (II)
ガロア接続を用いた動的秘密情報の管理 (II)

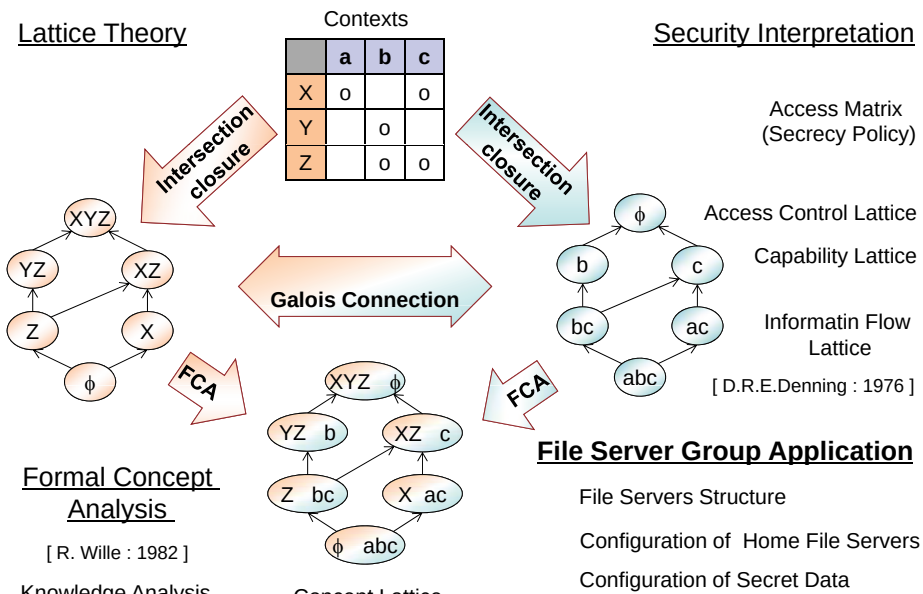
Hierarchical File Server Groups for Implementing Mandatory Access Control

2013/08/28 Fukuoka, Japan

SAKURABA, Taketoshi Hitachi, Ltd.

Outline

HITACHI
Inspire the Next



Agenda

HITACHI
Inspire the Next

- Galois Connection
  - Lattice Theory
  - Formal Concept Analysis
- Security
  - Information Flow Control
  - Lattice Model
- Application -- Hierarchical File Server Groups
  - Structure of HFSG
  - Security of HFSG
    - Information Flow Control,
    - Labeled Control without Labels,
    - RBAC
  - Management of HFSG
    - Comparison with Flat Structure
- Conclusions

Background of HFSG

HITACHI
Inspire the Next

- To Enforce Security Policy, Mechanisms are necessary
- Mechanisms

  ～ 1980's : Centralized Computing,
  Information Flow inside a single computer was the concern
  OS was the mechanism (Reference Monitor)

  1985 ～: Distributed Computing
  Information Flow over network may be concern,
  but there is no Reference Monitor over network

  Recently : Centralized Security Management returning (partially ?)
  Needs of Organizational security is increasing,
  New mechanisms: Thin Clients, Monitoring utility on each PC,
  ⇒ Information Flow Control becoming meaningful
- HFSG : Hierarchical File Server Group
  - Information Flow Control Mechanism in distributed systems
  - HFSG uses FCA for configuration management

MAC

HITACHI
Inspire the Next

Two Basic Access Controls Policies

- DAC (Discretionary Access Control)
  - It is owner of information that is responsible about protection of info.
  - So, Individual owner can set protection parameters for the information
- MAC (Mandatory Access Control)
  - It is Organization that is responsible about security
  - So, system's security setup is prior to individual owner's setup
  - Adopted mainly in Government , and Defense systems
- Properties of MAC
  - Mandatory : System overrides users' intention
  - Labels are often used
    - Label ⇔ Security Class), Attach a security label to protected file, document, user, …
  - Information Flow Control (No Read Up, No Write Down) is a MAC
  - RBAC (Role Based Access Control) is a MAC

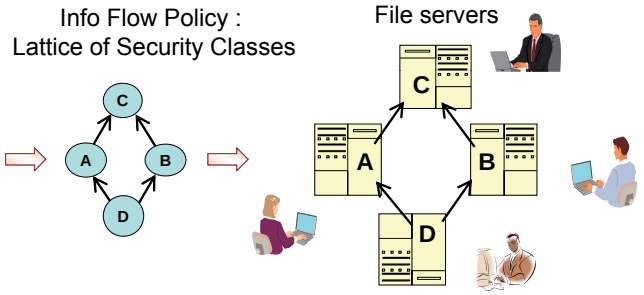
Idea of HFSG

HITACHI
Inspire the Next

- Install File servers along the lattice of the security policy

Security Policy

		Objects			
		A	B	Secret	Public
Subjects	Alice	Read, Write			Read
	Bob		Read, Write		Read
	Chris	Read	Read	Read, Write	Read
	David				Read, Write



- File servers are integrated by read only mount
  - In file server A, file system D is mounted on file system A,
    ※ mount D on A : arrange so that File system D is seen as a part of file system A
  - Similarly, File system A is mounted on file system C
  - Limiting the mount option read-only, Alice cannot write to D (nor b,c)
  - As a result, Information flow goes up only.

Idea of HFSG (Detailed)

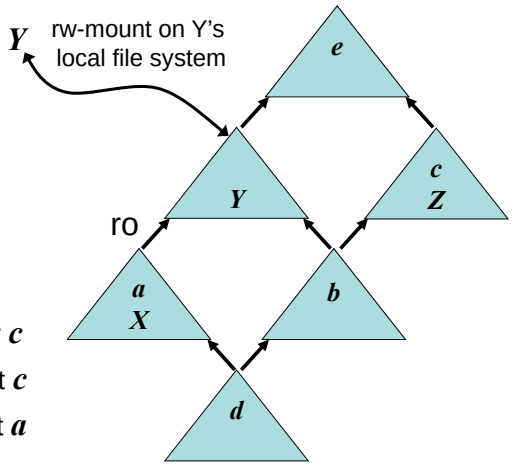
HITACHI
Inspire the Next

X Y Z : Users

a b c d e : Secrets

: File Server

: Info flow via mount point



Observe that

- ***X*** can read ***a***, but ***b*** nor ***c***
- ***Y*** can read ***a*** and ***b***, but ***c***
- ***Z*** can read ***b*** and ***c***, but ***a***
- All users can read ***d***
- No users can read ***e***

 7

Mount Point Protection

HITACHI
Inspire the Next

Semantics of file access control in Unix/Linux NFS:

- for Files
  - { User (Owner), Group member, Other People }
    x { **r** : Read Right, **w** : Write Right, **x** : Execution Right, … }
- for Directories
  - { **u**, **g**, **o**} x { **r**, **w**, **x**: Search Right }
- for Mount Points
  - /etc/exports :
    { ***mount points*** } x { ***clients*** } x { **rw**, **ro**, etc. }
    - Info flow over a **ro**-mount point is one directional
  - Protection is effective for all files under the mount point

 8

Merits of HFSG

HITACHI
Inspire the Next

- Merits
  - Using ordinal administration settings
  - Direct interpretation of the lattice model
- Issues
  - Deduction of configuration from given security policy
    - FCA is used
  - Management cost
    - Measured by number of mount parameters
  - Performance

Review : Policy Compatible Structure

HITACHI
Inspire the Next

- Any secrecy security policy should determines Policy table : “Who can read which object”

Users	Secrets		
	a	***b***	***c***
X	***X*** can access ***a***		
Y	○	○	
Z		○	○

- From the policy table, derive info flow policy
- Map the info flow policy into structure of HFSG

Review : From Policy Table to Lattice

HITACHI
Inspire the Next

- Derivation of Information Flow Lattice by using Formal Concept Analysis (FCA)
  - FCA [Wille, 1982] : a Lattice based Knowledge derivation method
    - { (object, property) } ➔ Concept Lattice
  - { (User, Secret) } ➔ Information Flow Lattice
    - Almost same with the Lattice model [Denning, 1976]
    - Classifies Users and Secrets at once

Review : Derivation of Security Lattice

HITACHI
Inspire the Next

- ' : $U' = \{ d \mid (U, d)=○ \}$ $\quad d' = \{ U \mid (U, d)=○ \}$

Users	Secrets				
	a	*b*	*c*	' (γ)	∩
X	○			*a*	*ϕ*
Y	○	○		*ab*	*b*
Z		○	○	*bc*	*abc*
' (μ)	*XY*	*YZ*	*Z*	*Legend:*	
∩	*ϕ*	*Y*	*XYZ*	$XY = \{X, Y\}$	

- User Lattice = { *ϕ* *Y* *Z* *XY* *YZ* *XYZ* }
- Secret Lattice = { *abc* *ab* *bc* *a* *b* *ϕ* }

: dual

Review : Concept Lattice to HFSG

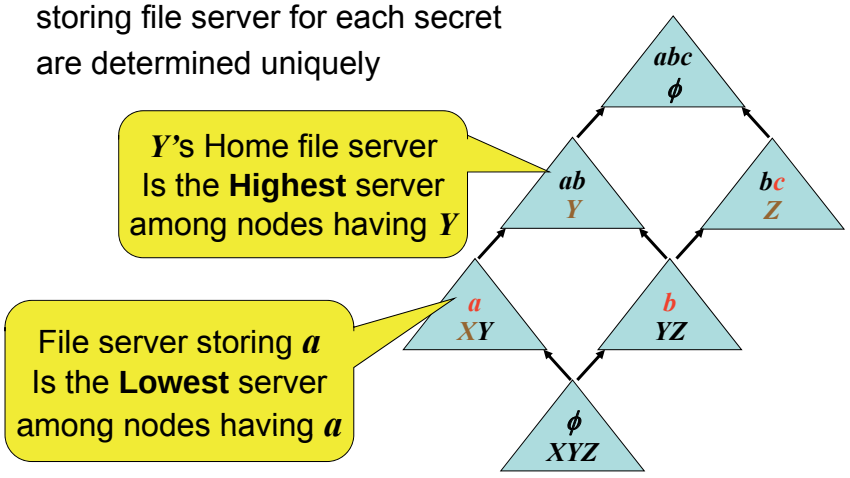
HITACHI
Inspire the Next

- Correspondence between the Lattice and HFSG
  - Node ←→ File Server
  - Order ←→ Read-Only Mounts
  - LUB of a Secret ←→ File Server storing the Secret
  - GLB of a User ←→ Home File Server of the User

Interpretation into HFSG

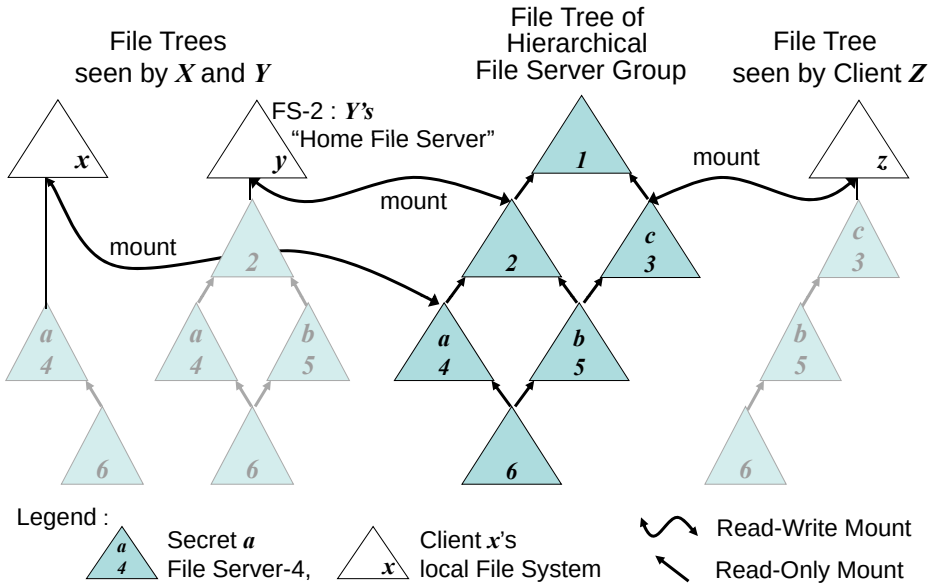
HITACHI
Inspire the Next

- Due to the fact that the structure is a Lattice,
  - Home file server for each user, and storing file server for each secret are determined uniquely



HFSG (again)

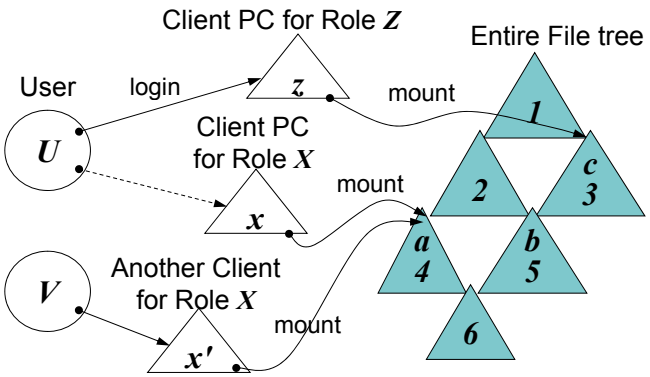
HITACHI
Inspire the Next



RBAC by using HFSG

HITACHI
Inspire the Next

- {(Role,Resource)} ➔ Role Hierarchy
- Setup a client PC as a Role-dedicated terminal
  - Authenticates only users assigned to the role
  - Authorized to mount the role's home file server



Security of HFSG

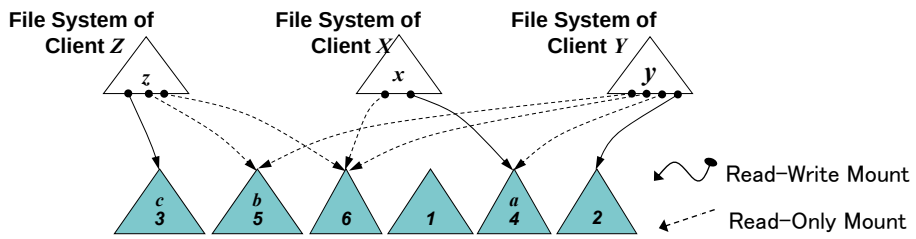
HITACHI
Inspire the Next

- Policy-Compatible
- Info Flow Control
  - No Write-Down : Because lower file servers are read-only
  - No Read-Up : Because upper file serves are invisible
- Mandatory
  - Mount options are controlled by system admins
  - Users can make new files in their home file servers only
  - Users cannot move files to lower file servers
- Labels
  - No explicit security labels are used
  - Virtually, file servers play roles of security labels
    - User's home file server can be seen as the label of the user

Management Merits of HFSG

HITACHI
Inspire the Next

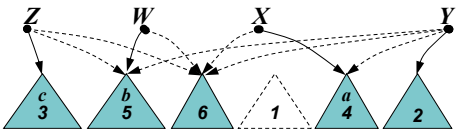
- It is possible to install the equivalent access control without providing special structure to the file servers (ordinal way).
- But there are demerits in the security management area
  - Difficult to understand
  - Client needs to mount lower FSs
  - Lower FSs need to know all Users of upper FSs

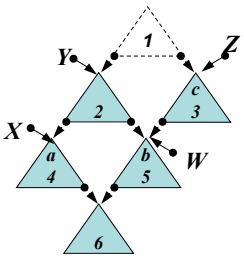


Comparison of Management Cost

HITACHI
Inspire the Next

- Measure the complexity by counting arrows (mounts)
  - Omit ***FS1*** and add user ***W***, C = number of clients
  - Assume the example files servers structure
- FLAT case :
  - Client - Server Mounts =2+4+3+2=11, No S - S mounts
- HFSG case :
  - Client - Server Mounts =4, Server - Server Mounts=5
- Scalability against number of users
  - FLAT : 11C/4 vs HFSG : C+5





 19

Implementation Issues

HITACHI
Inspire the Next

- Prerequisites of file servers of HFSG
  - （1） Possible to export the imported File
    - File server can export files which the file server imports from other file server to its clients
  - （2） Possible to control Read-Only mounts in server side
- NFS satisfies （2）, but unfortunately, not （1）
  - exports local file systems only
  - In Linux NFS 3.0, File server cannot distinguish file identifier of other servers and itself
- Implementation in NFS is under consideration
  - Proto typing : Implementation in User land（using Fuse)
  - Performance : Cache, in-Kernel implementation

 20

Conclusions (II)

HITACHI
Inspire the Next

- Hypothesis:
  necessity and effectiveness of MAC is increasing.
- Propose HFSG which implements MAC using ordinal IT
- HFSG provides Lattice-based Information Flow Control
  and Role-based Access Control
- Configuration of FSG can be Calculated by FCA
- Structure of HFSG is more effective
  than Ordinal Flat Structure
- Enhancement of distributed File Systems
  necessary to implement HFSG is under consideration.

Existing Technology

HITACHI
Inspire the Next

- MAC over Distributed Environment
  - Common Idea :
    - Let Co-operating Secure OSs across Computers
      Implement a Global Distributed Reference Monitor,
    - Common Security Label and Consistent Security Policy

    Zakrewski : DSI (2002)
    - Distributed Access Control over Linux Cluster using LSM

    McCune et al : Shamon (2006)
    - MAC and Labeled Communication across VMs by Hypervisors

    Zeldovitch et al : Dstar (2008)
    - Protocol for Info-Flow Control Units to Cooperate each other
  - In Practice :
    - Current office systems would not accept those Exotic Technologies

Rubik's for Cryptographers

Christophe Petit*

UCL Crypto Group,
Université catholique de Louvain
Place du Levant 3
1348 Louvain-la-Neuve (Belgium)
christophe.petit@uclouvain.be

This abstract and this talk are based on joint work with Jean-Jacques Quisquater [1]

Abstract. Hard mathematical problems are at the core of security arguments in cryptography. In this talk, we describe three mathematical generalizations of the famous Rubik's cube puzzle, namely the factorization, representation and balance problems in non-Abelian groups.
These problems arise naturally when describing the security of Cayley hash functions, a class of cryptographic hash functions with very interesting properties. The factorization problem is also strongly related to a famous long-standing conjecture of Babai, at the intersection of group theory and graph theory. A constructive proof of Babai's conjecture would make all Cayley hash functions insecure, but on the other hand it would have many positive applications in graph theory and computer science.
We review existing attacks against Cayley hash functions and known results on Babai's conjecture, and we infer some general lessons from these results.
Despite recent cryptanalytic progress on particular instances, we show that the factorization, representation and balance problems presumably remain good sources of cryptographic hard problems. In particular, we argue that Cayley hash functions deserve further interest by the cryptography community.

References

1. Christophe Petit and Jean-Jacques Quisquater. Rubik's for cryptographers. *Notices of the American Mathematical Society*, 60:733–739, 2013.

* Supported by an F.R.S.-FNRS postdoctoral research fellowship at Université catholique de Louvain, Louvain-la-Neuve.

Rubik's for Cryptographers

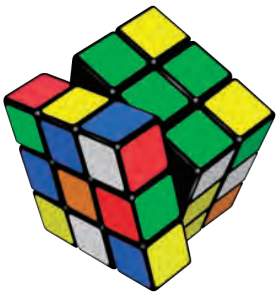
Based on joint work with Jean-Jacques Quisquater

Christophe Petit
UCL Crypto Group

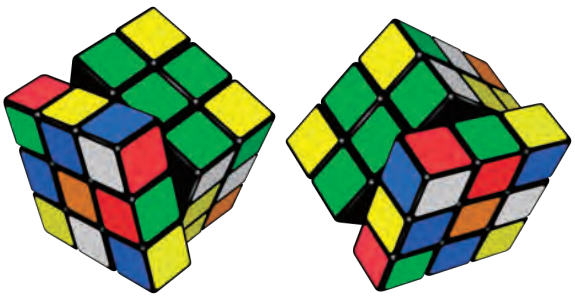
Cryptographic hard problems

- Classical hard problems
  - Integer factoring
  - Discrete logarithms over finite fields, elliptic curves
- Less classical hard problems
  - Lattice problems
  - Solving multivariate polynomial systems
  - Syndrome decoding
- Motivations for new assumptions
  - Avoid function field sieve and variants
  - Resist quantum computing
  - Use NP-hard problems
  - Build new cryptographic protocols

Another "hard" problem ?



Make it harder ?



Make it harder ?

Could we make it really hard ?

Outline

The Rubik's cube as a finite group

- Rubik's cube $\sim$ subgroup of all permutations of the corners, the central edge elements and their orientations
- Generated by the faces' rotations
- Neutral element $\sim$ Rubik's cube when solved
- Solution $=$ combination of the elementary permutations leading to the neutral element

Representation problem in finite groups

- Let G be a finite (non Abelian) group
- Let $S := \{s_1, ..., s_k\}$ generating G
- Let $e \in G$ be the neutral element
- How to write e as a product of the generators s_i ?
- "Short" products ? with less than $p(\log |G|)$ terms ? (p a polynomial)
- Can we do that in polynomial time ?
- Is this problem useful for cryptography ?

Factorization problem in finite groups

- Let G be a finite (non Abelian) group
- Let $S := \{s_1, ..., s_k\}$ generating G
- Let $g \in G$
- How to write g as a product of the generators s_i ?
- "Short" products ? with less than $p(\log |G|)$ terms ? (p a polynomial)
- Can we do that in polynomial time ?
- Is this problem useful for cryptography ?

Outline

Factoring in finite groups : motivations

- **Cryptography**
  - Cryptographic hash functions with nice properties
  - Factoring problem $\sim$ preimage resistance security
- **Babai's conjecture**
  - Existence of short products when G is simple
  - Factoring problem $\sim$ constructive proof
- **Expander graphs**
  - Highly connected graphs with few edges
  - Factoring problem $\sim$ routing problem in Cayley graphs

Cryptographic hash functions

$$H : \{0,1\}^* \rightarrow \{0,1\}^n$$

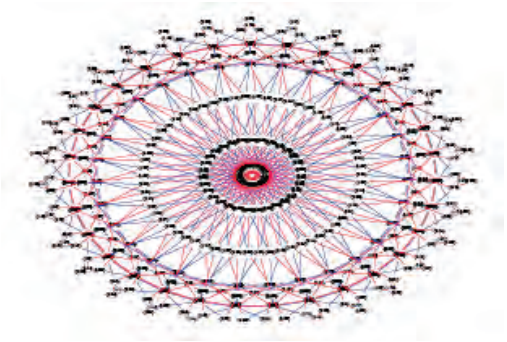
- Message authentication codes
- Digital signatures
- Password storage
- Pseudorandom number generation
- Entropy extraction
- Key derivation techniques
- ...
- ...

Hash functions security requirements

- **Preimage resistance :**
  given h, hard to find m such that $H(m) = h$
- **Collision resistance :**
  hard to find m, m' such that $H(m) = H(m')$
- **Second preimage resistance :**
  given m, hard to find m' such that $H(m') = h$
- "**Random oracle**"

Typical hash function construction

Hash functions from factoring in groups



Hash functions from factoring in groups

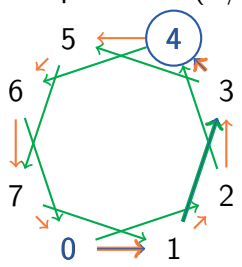
- Let G a non-abelian group and $S := \{s_0, ..., s_{k-1}\} \subset G$
- Write $m = m_1 m_2 ... m_N$ with $m_i \in \{0, ..., k-1\}$
  Define
$$H(m) := s_{m_1} s_{m_2} ... s_{m_N}$$
- **Preimage resistance = factoring problem**
  Given $g \in G$, find $m_1, ..., m_N \in \{0, ..., k-1\}$ such that
$$g = \prod_{i=1}^{N} s_{m_i}$$

Example : Tillich-Zémor hash function [TZ94]

- $p \in \mathbb{F}_2[X]$ irreducible of degree n
  $K = \mathbb{F}_2[X]/(p(X)) \approx \mathbb{F}_{2^n}$
- $G = SL(2, K)$
  $S = \{A_0 = \left(\begin{smallmatrix} X & 1 \\ 1 & 0 \end{smallmatrix}\right), A_1 = \left(\begin{smallmatrix} X & X+1 \\ 1 & 1 \end{smallmatrix}\right)\}$
- $H(m_1 m_2 ... m_N) := A_{m_1} A_{m_2} ... A_{m_N} \bmod p(X)$
- Efficient arithmetic

Cayley graph perspective

- *Computation* $\sim$ *walk* in the Cayley graph
- Example : $G = (\mathbb{Z}/8\mathbb{Z}, +)$, $S = \{1, 2\}$



$m = 101$
$H(m) = 0 + 1 + 2 + 1 = 4$

- These hash functions are called *Cayley hash functions*

Cayley hash functions properties

- **Preimage resistance $\sim$ factorization problem :**
  Given G, $g \in G$ and $S = \{s_0, ..., s_{k-1}\} \subset G$,
  find a short product $\prod s_{m_i} = g$
- 2^{nd} **preimage resistance $\leftarrow$ representation problem :**
  Given G and $S = \{s_0, ..., s_{k-1}\} \subset G$,
  find a short product $\prod s_{m_i} = 1$
- **Collision resistance $\sim$ balance problem :**
  Given G and $S = \{s_0, ..., s_{k-1}\} \subset G$,
  find two short products $\prod s_{m_i} = \prod s_{m'_i}$
- **Output distribution $\sim$ expander properties**
- **Parallelism** $H(m||m') = H(m)H(m')$

Cayley hash function proposals

Zémor [Z91]
p prime
$G = SL(2, \mathbb{F}_p)$
$S = \{\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)\}$

Tillich-Zémor [TZ94]
$p \in \mathbb{F}_2[X]$ irreducible
$G = SL(2, \mathbb{F}_{2^n})$
$S = \{\left(\begin{smallmatrix}X & 1\\ 1 & 0\end{smallmatrix}\right), \left(\begin{smallmatrix}X & X+1\\ 1 & 1\end{smallmatrix}\right)\}$

LPS [CGL09]
p prime
$G = PSL(2, \mathbb{F}_p)$
S as in
Lubotsky-Philips-Sarnak's
Ramanujan graphs

Morgenstern [PLQ07]
$p \in \mathbb{F}_2[X]$ irreducible
$G = PSL(2, \mathbb{F}_{2^n})$
S as in Morgenstern's
Ramanujan graphs

Factoring in finite groups : motivations

- Cryptography
- **Babai's conjecture**
- Expander graphs

Babai's conjecture [BS92]

There is a constant c such that, for any non-Abelian finite simple group G, for all generator sets S, the diameter of the Cayley graph arising from G and S is smaller than $(\log |G|)^c$.

- Not true for cyclic groups
- Factorization problem $\sim$ **constructive proof** of Babai's conjecture
- Recently attracted many mathematicians such as Bourgain, Gamburd, Green, Helfgott, Kantor, Lubotzky, Tao,...

State of Babai's conjecture [BS92]

- Non constructive results
  - True for $SL(2, \mathbb{F}_p)$ [H05]
  - True for all groups of Lie type and bounded rank [PS10,BGT10]
- Constructive results
  - $SL(2, K)$: $\exists$ 2 or 3 generators such that the diameter is $O(\log |K|)$ [BHKLS90]
  - $SL(m, \mathbb{F}_p)$ with $m > 2$: $\exists$ 2 generators such that the diameter is $O(m^2 \log p)$ [KR05]
  - Symmetric/alternate groups : almost all generator pairs [BH05]

State of Babai's conjecture

- Except for symmetric/alternate groups, all proofs are either *non constructive*
  or only valid for (very) *particular* generators sets
- No **constructive** proofs for **generic** generator sets in **matrix groups**,

Factoring in finite groups : motivations

- Cryptography
- Babai's conjecture
- **Expander graphs**

Expander graphs

- Families of highly connected regular graphs : $\exists c > 0$ such that
$$\min_{S \subset V, |S| \leq |V|/2} \frac{|\delta(S)|}{|S|} = c.$$
- Large spectral gap ; random walks mix quickly
- Cayley graphs tend to be good expanders (theoretical and experimental evidence)

Expander graphs

- Applications : [HLW06]
  - Randomness amplification
  - Error correcting codes
  - Optimal circuits for linear transformations
  - ...
- Factorization problem $\sim$ **routing/path-finding problem**
  Potentially useful in all applications of expander graphs

Factoring in finite groups : motivations

- **Cryptography**
  - Cryptographic hash functions with nice properties
  - Factoring problem $\sim$ preimage resistance security
- **Babai's conjecture**
  - Existence of short products when G is simple
  - Factoring problem $\sim$ constructive proof
- **Expander graphs**
  - Highly connected graphs with few edges
  - Factoring problem $\sim$ routing problem in Cayley graphs

Outline

Cayley hash function proposals

Zémor [Z91]
p prime
$G = SL(2, \mathbb{F}_p)$
$S = \{\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)\}$

Tillich-Zémor [TZ94]
$p \in \mathbb{F}_2[X]$ irreducible
$G = SL(2, \mathbb{F}_{2^n})$
$S = \{\left(\begin{smallmatrix}X & 1\\ 1 & 0\end{smallmatrix}\right), \left(\begin{smallmatrix}X & X+1\\ 1 & 1\end{smallmatrix}\right)\}$

LPS [CGL09]
p prime
$G = PSL(2, \mathbb{F}_p)$
S as in
Lubotsky-Philips-Sarnak's
Ramanujan graphs

Morgenstern [PLQ07]
$p \in \mathbb{F}_2[X]$ irreducible
$G = PSL(2, \mathbb{F}_{2^n})$
S as in Morgenstern's
Ramanujan graphs

Many angles of attacks

Exhaustive search
Birthday attacks

Multicollisions
Meet-in-the-middle

Trapdoor attacks

Subgroup attacks

Lifting attacks
Euclidean algorithm

Babai's conjecture

Subgroup attacks

- Assume $G = G_0 \supset G_1 \supset G_2 ... \supset G_N = \{1\}$

Subgroup attacks

- Assume $G = G_0 \supset G_1 \supset G_2 ... \supset G_N = \{1\}$ and $|G_i|/|G_{i+1}|$ "small"
- **Factorization of 1**
  - Random products of s_0 and s_1 to get two elements s'_0 and s'_1 of G_1
  - Random products of s'_0 and s'_1 to get two elements s''_0 and s''_1 of G_2
  - ...

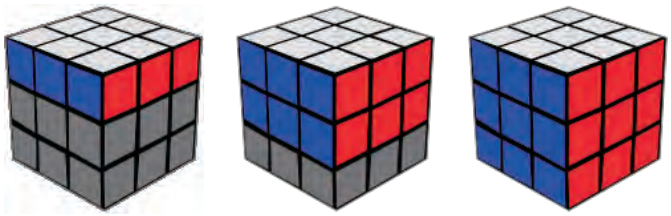
  = second preimage attack
  - $H(m) = 1 \Rightarrow H(m'||m) = H(m')H(m) = H(m')$
- Can be extended to a **preimage attack**

Subgroup attacks

- Assume $G = G_0 \supset G_1 \supset G_2 ... \supset G_N = \{1\}$
- More generally, the attack works if "going from G_i to G_{i+1} is easy"
  Ex. : if G_i/G_{i+1} is Abelian and DLP easy in it
- [SGGB00] : subgroup attack on Tillich-Zémor when n is composite
- [PQTZ09] : generic subgroup attacks on $SL(2, \mathbb{F}_{2^n})$ and variants that "remove easy quotients"

Subgroup attacks on the Rubik's cube

$$|G| = \frac{1}{12} 12!8!3^8 2^{12}$$



Lessons learned

- Subgroup attacks are independent of the generators
- We should choose the group carefully

Trapdoor attacks

- Choose the parameters such that you know a collision
- [SGGB00] against Tillich-Zémor
- Can be prevented easily
- Sometimes useful ! [CP10]

Lifting attacks

- Very successful approach !
- Intuition : factorization easier over infinite groups, often unique, at least the length is leaked
- Principle : lift the factorization problem to some infinite group where it is easier to solve
  - Define the lifted set appropriately
  - Find a way to lift elements
  - Factor elements in the lifted set

Lifting attacks : Zémor [TZ94]

- Zémor $G = SL(2, \mathbb{F}_p)$, $S = \{\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)\}$
- Given $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in SL(2, \mathbb{F}_p)$
  1. **Lifting :** find $\left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right) \in SL(2, \mathbb{Z}_+)$ such that $\left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right) = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \bmod p$
  2. **Solving :** factor $\left(\begin{smallmatrix}A & B\\ C & D\end{smallmatrix}\right)$ as a product of $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$ with Euclidean algorithm :

     If $A \geq B$, apply Euclidean algorithm to (A, B)
     else apply Euclidean algorithm to (C, D)

  Indeed :
  - $a_{i-1} = q_i a_i + a_{i+1}$
    $\Leftrightarrow \left(\begin{smallmatrix}a_{i-2}\\ a_{i-1}\end{smallmatrix}\right) = \left(\begin{smallmatrix}1 & q_{i-1}\\ & 1\end{smallmatrix}\right) \left(\begin{smallmatrix}1 & \\ q_i & 1\end{smallmatrix}\right) \left(\begin{smallmatrix}a_i\\ a_{i+1}\end{smallmatrix}\right)$
  - $\left(\begin{smallmatrix}1 & q\\ 0 & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)^q$ and $\left(\begin{smallmatrix}1 & 0\\ q & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)^q$

Lessons learned

- Lifting part trivial here
  $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$ generate the whole set $SL(2, \mathbb{Z}_+)$
- More generally, the generators should not generate a dense subset of the infinite group above G
- Attack thwarted if we replace $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ by $\left(\begin{smallmatrix}1 & 2\\ 0 & 1\end{smallmatrix}\right)$

Lifting attacks : LPS [TZ08]

- LPS : $G = PSL(2, \mathbb{F}_p)$ and $S \sim$ integral quaternions with a given small norm ℓ as in LPS Ramanujan graphs [LPS88]
- Lift from $PSL(2, \mathbb{F}_p)$ to $\Omega \subset SL(2, \mathbb{Z}[i])$
  Here $\Omega := \langle$lifts of generators$\rangle \subsetneq SL(2, \mathbb{Z}[i])$
  $\Omega =$ set of ℓ-power norm elements in $SL(2, \mathbb{Z}[i])$
  Very small (not dense) subset, but well structured
- Factoring lifted elements easy...
  What about lifting ?

Lifting the identity : LPS [TZ08]

- Lifting the identity $\sim$ finding λ, w, x, y, z, e such that $(\lambda + wp)^2 + 4(xp)^2 + 4(yp)^2 + 4(zp)^2 = \ell^e$
- The equation is solved as follows :
  - Fix e even, large enough
  - Fix λ to solve modulo $2p$
  - Simplify by $4p^2 \Rightarrow$ get $x^2 + y^2 + z^2 = N$
  - Pick random x and solve with Lagrange's method (Continued fractions / Euclidean algorithm)
- The lifted identity is then easily factored
- **Factorization of I = 2nd preimages**

Factoring for LPS generators

- Factoring for LPS generators
  $\sim$ Preimages against LPS function
  $\sim$ finding λ, w, x, y, z, e such that
  $(A\lambda + wp)^2 + (B\lambda + xp)^2 + (C\lambda + yp)^2 + (D\lambda + zp)^2 = \ell^e$
- Resolution attempt :
  - Fix e even, large enough
  - Fix λ to solve modulo p
  - Simplify by $p \Rightarrow$ some coefficients p remain
  - Quadratic diophantine equation with **large** coefficients
  - Does not work

Factoring for LPS generators [PLQ08]

- Lift *diagonal matrices*
  $(A\lambda + wp)^2 + (B\lambda + xp)^2 + (yp)^2 + (zp)^2 = \ell^e$
  - Fix e even, large enough
  - Fix λ to solve modulo p
  - Fix w and x to solve modulo p^2
  - Simplify modulo p^2 and get $y^2 + z^2 = N$
  - Use Lagrange's method
- Decompose any matrix as a product of diagonal matrices and generators
  $\left(\begin{smallmatrix} M_1 & M_2 \\ M_3 & M_4 \end{smallmatrix}\right) = \lambda \left(\begin{smallmatrix} 1 & 0 \\ 0 & \alpha \end{smallmatrix}\right) s_1 \left(\begin{smallmatrix} 1 & 0 \\ 0 & \beta_1 \end{smallmatrix}\right) s_1 \left(\begin{smallmatrix} 1 & 0 \\ 0 & \beta_2 \end{smallmatrix}\right) s_1 \left(\begin{smallmatrix} 1 & 0 \\ 0 & \omega \end{smallmatrix}\right)$
- Similar attacks for Morgenstern parameters [PLQ08]

Lessons learned

- Lifting simplified by generators' special structure (amounted to solve a norm equation in this case)
- Attack thwarted if we remove or replace one generator

Collision attack for Tillich-Zémor [GIMS09]

$$G = SL(2, \mathbb{F}_{2^n}),\ S = \{\left(\begin{smallmatrix} X & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} X & X+1 \\ 1 & 1 \end{smallmatrix}\right)\}$$

1. Change generators $S' = \{\left(\begin{smallmatrix} X & 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} X+1 & 1 \\ 1 & 0 \end{smallmatrix}\right)\}$
   - $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \langle S' \rangle \Rightarrow$ when applying Euclidean algorithm to (a, b), all the quotients are X or $X+1$
2. Lift a matrix with shape $\left(\begin{smallmatrix} 0 & b \\ c & d \end{smallmatrix}\right)$
   Apply [MS87] to $p(X)$ to get $m = m_1 ... m_n$ such that
   $$H(m) = \left(\begin{smallmatrix} p & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & b \\ c & d \end{smallmatrix}\right) \bmod p(X)$$
3. Build the palindrome $\tilde{m} = m_n ... m_2 \bar{m}_1 \bar{m}_1 m_2 ... m_n$, then one can show $H(0\tilde{m}0) = H(1\tilde{m}1)$.

Lessons learned

- The matrices $\left(\begin{smallmatrix} X & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} X+1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ generate a non dense subset of $SL(2, \mathbb{F}_2[X])$, but a lifting attack was still possible
- In fact, "only one component" of the matrix is lifted $\left(\begin{smallmatrix} 0 & b \\ c & d \end{smallmatrix}\right) \rightarrow \left(\begin{smallmatrix} p & b \\ c & d \end{smallmatrix}\right)$
- Lifting requires an old algorithm by Mesirov-Sweet [MS87] only works for these two specific matrices
- Attack thwarted if we replace $\left(\begin{smallmatrix} X & 1 \\ 1 & 0 \end{smallmatrix}\right)$ by $\left(\begin{smallmatrix} X^2 & 1 \\ 1 & 0 \end{smallmatrix}\right)$

Preimages for Tillich-Zémor [PQ10]

- $H(m) = \left(\begin{smallmatrix} 0 & b \\ c & d \end{smallmatrix}\right)$
  $\Rightarrow H(0\tilde{m}) = \left(\begin{smallmatrix} 1 & X+b^2 \\ 0 & 1 \end{smallmatrix}\right)$ and $H(\tilde{m}0) = \left(\begin{smallmatrix} 1 & 0 \\ X+b^2 & 1 \end{smallmatrix}\right)$
- The red matrices belong to Abelian subgroups, isomorphic to $\mathbb{F}_2^n$

$$\left(\begin{smallmatrix} 1 & 0 \\ \sum \alpha_i & 1 \end{smallmatrix}\right) = \prod \left(\begin{smallmatrix} 1 & 0 \\ \alpha_i & 1 \end{smallmatrix}\right)$$

- Factor any matrix with red matrices and the generators

$$\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ \alpha & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} X & 1 \\ 1 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & \beta \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} X & 1 \\ 1 & 0 \end{smallmatrix}\right)^3 \left(\begin{smallmatrix} 1 & 0 \\ \gamma & 1 \end{smallmatrix}\right)$$

- It remains to precompute enough blue matrices producing "linearly independent" red matrices

Preimages for Tillich-Zémor [PQ10]

- Two precomputing algorithms
  1. Obtain new matrices $\begin{pmatrix} 0 & b_i \\ c_i & d_i \end{pmatrix}$ recursively
     $\Rightarrow$ deterministic algorithm ; full proof when n is prime
  2. Apply (an extension of) [MS87] to $a_i = pq_i$
     $\Rightarrow$ probabilistic algorithm ; some heuristic assumptions ;
     $\Rightarrow$ performs better in practice
- [MS87] only works for partial quotients X and $X + 1$
- If we change one, density problem again

Lessons learned

- Attacks become more and more sophisticated
- They still only apply to specific parameters

Cryptanalysis results

Zémor [Z91]
Collisions and preimages
[TZ94]

Tillich-Zémor [TZ94]
Partial attacks
[CP94,AK98,SGGB00,PQTZ09]
Collisions [GIMS09]
Preimages [PQ10]

LPS [CGL09]
Collisions [TZ08]
Preimages [PLQ08]

Morgenstern [PLQ07]
Collisions and preimages
[PLQ08]

Rubik's for cryptographers ?

- All particular instances proposed have been broken
- BUT all of them used **special parameters** for efficiency or maximal expansion
- Generic parameters ?
  - Avoid permutation and alternate groups [BH05]
  - Subexponential algorithms producing subexponential length factorizations for $SL(2, 2^n)$ [P12,FPPR11]

Outline

Conclusion

- Factoring in finite groups is an interesting problem
  - From a theoretical point of view
  - Many applications in computer science (if easy)
  - At least one nice application in crypto (if hard)
  - Fun anyway
- Cayley hash functions are appealing. Are they secure ?
  - Zémor, LPS, Morgenstern, Tillich-Zémor broken
  - Security of other / generic instances ?
- Interactions with mathematicians needed !

References

- [TZ94] JP Tillich & G Zémor, *Group-theoretic hash functions*
- [Z91] G Zémor, *Hash functions and graphs with large girths*
- [CGL09] D Charles, E Goren, K Lauter, *Cryptographic hash functions from expander graphs*
- [PLQ07] C Petit, K Lauter, JJ Quisquater, *Cayley Hashes : A Class of Efficient Graph-based Hash Functions*
- [B92] L Babai, A Seress, *On the diameter of permutation groups*

References

- [H05] H Helfgott, *Growth and generation in SL2(Z/pZ)*
- [LS10] L Pyber, E Szabï¿½, *Growth in finite simple groups of Lie type*
- [BGT10] E Breuillard, B Green, T Tao, *Approximate subgroups of linear groups*
- [BH05] L Babai, T Hayes, *The probability of generating the symmetric group when one of the generators is random*
- [BHKLS90] L Babai, G Hetyei, W Kantor, A Lubotzky, A Seress, *On the diameter of finite groups*

References

- [KR05] M Kassabov, T Riley, *Diameters of Cayley graphs of Chevalley groups*
- [HLW06] S Hoory, N Linial, A Wigderson, *Expander graphs and their applications*
- [SGGB00] R Steinwandt, M Grassl, W Geiselmann, T Beth, *Weaknesses in the $SL_2(F_2^n)$ Hashing Scheme*
- [PQTZ09] C Petit, JJ Quisquater, JP Tillich, G Zémor, *Hard and easy Components of Collision Search in the Zémor-Tillich Hash Function : New Instances and Reduced Variants with equivalent Security*

References

- [TZ08] JP Tillich, G Zémor, *Collisions for the LPS Expander Graph Hash Function*
- [LPS88] A Lubotzky, R Phillips, P Sarnak, *Ramanujan Graphs*
- [PLQ08] C Petit, K Lauter, JJ Quisquater, *Full Cryptanalysis of LPS and Morgenstern Hash Functions*
- [GIMS09] M Grassl, I Ilic, S Magliveras, R Steinwandt, *Cryptanalysis of the Tillich-Zémor hash function*
- [MS87] JP Mesirov, MM Sweet, *Continued fraction expansions of rational expressions with irreducible denominators in characteristic 2*

References

- [PQ10] C Petit, JJ Quisquater, *Preimage algorithms for the Tillich-Zémor hash function*
- [R05] T Riley, *Navigating in the Cayley Graphs of* $SL_N(\mathbb{Z})$ *and* $SL_N(\mathbb{F}_p)$
- [P12] C Petit, *Towards factoring in* $SL(2, \mathbb{F}_{2^n})$
- [FPPR11] JC Faugère, L Perret, C Petit, G Renault, *New subexponential algorithms for factoring in* $SL(2, \mathbb{F}_{2^n})$

Design and Analysis of Public Key Cryptography using Non-commutative Algebra

Takanori Yasuda

Institute of Systems, Information Technologies and Nanotechnologies

Abstract. Multivariate Public Key Cryptosystems (MPKC) can be potentially applied to post-quantum cryptography. Rainbow is a digital signature scheme in MPKC that affords relatively efficient encryption and decryption. However, the security of MPKC depends on the difficulty in solving a system of multivariate polynomials, and a substantial number of their coefficients is required to attain a reasonable level of security.
For a public key cryptosystem, it is important to study the reduction of key size. In the case of RSA with a small key size, the lattice attack works efficiently [7, 2], whereas in the case of cryptosystems based on discrete logarithm, Pollard's λ-method [6, 4] works efficiently [3]. Moreover, the key size of the McEliece cryptosystem, which is another candidate for post-quantum cryptography, has been reduced by Berger et al. [1]. In the case of Rainbow, it is known that CyclicRainbow [5] reduces the size of the public key while maintaining the security of the original Rainbow. In this paper, we reduce the secret key size of Rainbow by using non-commutative rings. The proposed scheme is constructed by replacing a definition field with a non-commutative ring in the original Rainbow scheme. Non-commutative rings are a well-established topic in mathematics; for examples, quaternion algebras and group rings have been studied in depth.

References

1. Berger, T.P., Cayrel, P.-L., Gaborit, P. and Otmani, A., "Reducing Key Length of the McEliece Cryptosystem", Progress in Cryptology, AFRICACRYPT'09, Springer LNCS, vol. 5580, pp. 77–97, 2009.
2. Boneh, D. and Durfee, G., "Cryptanalysis of RSA with Private Key d Less Than $N^{0.292}$", IEEE Trans. Inform. Theory, vol. 46, no. 4, pp. 1339–1349, 2000.
3. Galbraith, S. D. and Ruprai, R. S., "Using Equivalence Classes to Accelerate Solving the Discrete Logarithm Problem in a Short Interval", PKC'10, Springer LNCS vol. 6056, pp. 368–383, 2010.
4. van Oorschot, P.C. and Wiener, M.J., "Parallel Collision Search with Cryptanalytic Applications", Jornal of Cryptology, vol. 12, pp. 1–28, 1999.
5. Petzoldt, A., Bulygin, S. and Buchmann, J., "CyclicRainbow - A multivariate Signature Scheme with a Partially Cyclic Public Key based on Rainbow", INDOCRYPT'10, Springer LNCS vol. 6498, pp. 33–48, 2010.
6. Pollard, J.M., "Monte Carlo Methods for Index Computation mod p", Mathmatics of Computation vol. 143, no. 32, pp. 918–924, 1978.
7. Wiener, M.J., "Cryptanalysis of Short RSA Secret Exponents", IEEE Trans. Inform. Theory, vol. 36, no. 3, pp. 553–558, 1990.

Design and Analysis of Public Key Cryptography using Non-commutative algebra

Takanori Yasuda (ISIT)

Commutative vs Non-commutative

- **Public Key Cryptography using Commutative Algebra.**
  1. Discrete Logarithm Problem.
  2. Multivariate Public Key Cryptosystem.
- **Public Key Cryptography using Non-Commutative Algebra.**
  3. Discrete Logarithm Problem using Non-commutative Group.
  4. Multivariate Public Key Cryptosystem using Non-commutative algebra.

Application of Non-commutative Group

Discrete Logarithm Problem

G: commutative cyclic group

- g: generator of G
- h: element in G

DLP

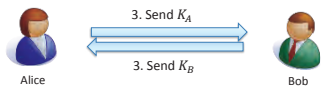
Find an integer a such that $h = g^a$.

We can change G into a non-commutative group.
But, essentially same to use its cyclic subgroup.

Diffie-Hellman Key Exchange

g: generator — Public information

4. Compute $(K_B)^a$ | 4. Compute $(K_A)^b$



1. Choose a (secret) integer a | 1. Choose a (secret) integer b

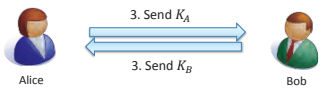
2. Compute $K_A = g^a$ | 2. Compute $K_B = g^b$

Share the Secret Key: $(K_B)^a = (K_A)^b$

Stickel's Key Exchange

$a, b \in G$: $ab \neq ba$ — Public information

4. Compute $a^n K_B b^m$ | 4. Compute $a^r K_A b^s$



1. Choose a (secret) integer n, m | 1. Choose a (secret) integer r, s

2. Compute $K_A = a^n b^m$ | 2. Compute $K_B = a^r b^s$

Share the Secret Key: $a^n K_B b^m = a^r K_A b^s$

Platform Example

- Braid group

$$B_n = \left\langle x_1, \cdots x_{n-1} \;\middle|\; \begin{array}{ll} x_i x_j x_i = x_j x_i x_j & \text{if } |i-j|=1 \\ x_i x_j = x_j x_i & \text{if } |i-j|>1 \end{array} \right\rangle$$

- Other examples
  - Group of matrices
  - Thomson's group
  - Artin group

Multivariate Public Key Cryptosystem

Multivariate Polynomials

- F: field (or commutative ring)
- $A = F[x_1, \ldots, x_n]$

Multivariate (quadratic) equations

$$\begin{cases} f_1(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(1)} x_i x_j + \sum_{1\le i\le n} b_i^{(1)} x_i + c^{(1)} = d_1 \\ f_2(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(2)} x_i x_j + \sum_{1\le i\le n} b_i^{(2)} x_i + c^{(2)} = d_2 \\ \vdots \\ f_m(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(m)} x_i x_j + \sum_{1\le i\le n} b_i^{(m)} x_i + c^{(m)} = d_m \end{cases}$$

Non-commutative Polynomials

- R: non-commutative ring
- $A = R[x_1, \ldots, x_n]$

Multivariate (quadratic) equations

$$\begin{cases} f_1(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(1,1)} x_i x_j + \sum_{1\le i,j\le n} x_i a_{ij}^{(1,2)} x_j + \sum_{1\le i,j\le n} x_i x_j a_{ij}^{(1,3)} + \cdots + c^{(1)} = d_1 \\ f_2(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(2,1)} x_i x_j + \sum_{1\le i,j\le n} x_i a_{ij}^{(2,2)} x_j + \sum_{1\le i,j\le n} x_i x_j a_{ij}^{(2,3)} + \cdots + c^{(2)} = d_2 \\ \vdots \\ f_m(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(m,1)} x_i x_j + \sum_{1\le i,j\le n} x_i a_{ij}^{(m,2)} x_j + \sum_{1\le i,j\le n} x_i x_j a_{ij}^{(m,3)} + \cdots + c^{(m)} = d_m \end{cases}$$

Non-commutative rings

- R : non-commutative ring
  - R : finite dimensional algebra over a finite field K (dimension=r)

    Fix a K –linear isomorphism $\phi : K^r \xrightarrow{\sim} R$
- Example (quaternion algebra Q_q (q : order of K))

$$\begin{cases} (set)\ \ Q_q = K\cdot 1 \oplus K\cdot i \oplus K\cdot j \oplus K\cdot ij, & (r=4), \\ (product)\ \ i^2 = j^2 = -1, \quad ij = -ji. \end{cases}$$

There is a natural isomorphism $\phi : K^4 \xrightarrow{\sim} Q_q$

Fundamental Structure of Multivariate Public Key Cryptosystems

Multivariate Public Key Cryptosystems (MPKC)

Security is based on the difficulty of solving MQ problem.

MQ equations (coefficients belongs to a finite field)

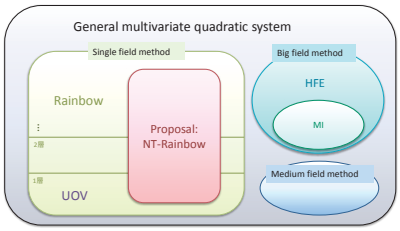
$$\begin{cases} f_1(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(1)} x_i x_j + \sum_{1\le i\le n} b_i^{(1)} x_i + c^{(1)} = d_1 \\ f_2(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(2)} x_i x_j + \sum_{1\le i\le n} b_i^{(2)} x_i + c^{(2)} = d_2 \\ \vdots \\ f_m(x_1,\ldots,x_n) = \sum_{1\le i,j\le n} a_{ij}^{(m)} x_i x_j + \sum_{1\le i\le n} b_i^{(m)} x_i + c^{(m)} = d_m \end{cases}$$

MQ problem: Find a solution of this MQ equations.

Features of MPKC

- Encryption
  - Matsumoto-Imai(MI), HFE, *l*-IC
- Signature
  - UOV, Rainbow
- Advantage
  - A candidate for post-quantum cryptosystem.
  - High efficiency for encryption (verification) and decryption (signature generation)
- Problem
  - Huge size of public key
  - Provable Security

Classification of MPKC signature



History of MPKC

- 1988 Proposal by Matsumoto-Imai (MI)
  - Attack by Patarin(1995)
- 1996 HFE (Hidden Field Equation) encryption
  - Applied to Quartz(1996)as a signature scheme
- 1997 (Balanced) Oil and Vinegar signature scheme
  - Attack by Kipnis-Shamir(1998)
- 1999 UOV(Unbalanced Oil and Vinegar)scheme
  - Improvement of Kipnis-Shamir's attack (UOV attack)
- 2005 Rainbow (layered UOV) signature scheme
  - Enhanced the security against UOV attack

Signature schemes based on RSA

- Ong-Schnorr-Shamir(OSS) signature scheme(1984)
  - Based on hardness of solving an equation,

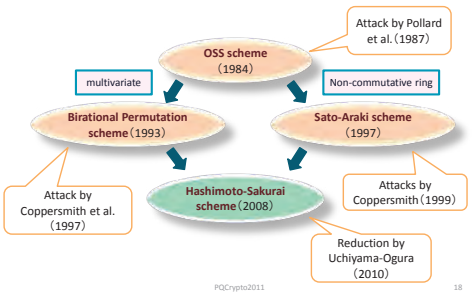
$$x^2 + hy^2 = m \pmod N, \qquad (N = pq)$$

easy to solve it mod p or mod q.
⇒ need the difficulty of factorization of $N = pq$.

1987 Pollard-Schnorr : attack not using factorization

- RSA-based schemes extended from OSS scheme
  - Shamir's Birational Permutation scheme(1994)
  - Sato-Araki scheme(1997)
  - Hashimoto-Sakurai(HS) scheme(2008)

History of extensions of OSS scheme



Reduction of Uchiyama-Ogura

- Reduction of Uchiyama-Ogura
  - They reduced HS scheme to Rainbow, (whose base ring is $\mathbb{Z}/NZ$, not a finite field)
  - This implies that attacks against Rainbow may be applicable.
- Rainbow
  - A signature in Multivariate Public Key Cryptosystems(MPKC).
  - Base field is a finite field with small order.
  - Fast signature generation and verification (A.I.Chen et al. "SSE Implementation of Multivariate PKCs on Modern x86 CPUs", CHES'09)
  - Security analysis against many attacks (direct attacks, Rank attacks, UOV attack ...).

Redefinition of HS signature

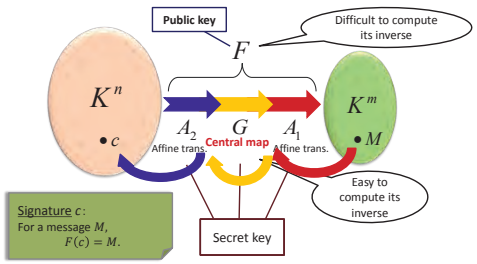
- Change base field (ring) in HS scheme:

  $Z/NZ \longrightarrow$ finite field K

  (Other Reasons)
  1. Huge key size (in Original HS scheme)
  2. A scheme in MPKC (one of candidates of Post-Quantum cryptosystems)

  Need to analyze security against attacks which has been already analyzed once and again.
- Attacks analyzed
  - i. Attacks against Birational Permutation scheme and Sato-Araki scheme.
  - ii. Attacks against Rainbow.

Fundamental structure of MPKC



HS scheme (Redefinition)

$\mathrm{HS}(R, n)$

Non-commutative ring R

- Non-commutative ring R
  - R : finite dimensional K-algebra (of r dimension)

    Fix a K–linear embedding $\phi : R \xrightarrow{\sim} M(m, K)$

    Assume R is closed by transpose operation.
- Ex. Quaternion algebra Q_q (q :order of K)

$$\begin{cases} (set)\ \ Q_q = K\cdot 1 \oplus K\cdot i \oplus K\cdot j \oplus K\cdot ij, & (r=4), \\ (product)\ \ i^2 = j^2 = -1, \quad ij = -ji. \end{cases}$$

$$Q_q \ni a_0\cdot 1 + a_1\cdot i + a_2\cdot j + a_3\cdot ij \leftrightarrow \begin{pmatrix} a_0 + a_1\cdot i & a_3 + a_2\cdot i \\ a_3 - a_2\cdot i & a_0 - a_1\cdot i \end{pmatrix} \in M(2, K(i))$$

Ring with Involution

- Involution $*: R \to R$
  1. $(a+b)^* = a^* + b^*$
  2. $(ab)^* = b^* a^*$
  3. $(a^*)^* = a$
  4. $1^* = 1$
- In quaternion case
  - Main involution

$$Q_q \ni a_0\cdot 1 + a_1\cdot i + a_2\cdot j + a_3\cdot ij \to a_0\cdot 1 - a_1\cdot i - a_2\cdot j - a_3\cdot ij \in Q_q$$

Examples of Non-commutative Ring

1. (Subring of) Square Matrix algebra $Mat(n, F)$
   - Involution is transpose.
2. Group Ring $F[G]$
   - G: non-commutative group

$$F[G] = \{\sum a_g g \mid a_g \in F\}$$

   - Involution is the linear map extended

$$G \ni g \to g^{-1} \in G$$

HS scheme HS(R, n)

n : natural number

- Secret key

  Central map $G = (g_2, \ldots, g_n) : R^n \to R^{n-1}$, two affine transformations

  $A_1 : R^{n-1} \to R^{n-1}, \quad A_2 : R^n \to R^n.$

- Public key $F = A_1 \circ G \circ A_2 : R^n \longrightarrow R^{n-1}$

  Central map G

$$g_k(x_1, \ldots, x_n) = \sum_{i=1}^{k-1} (x_i' \alpha_i^{(k,1)} x_k + x_k' \alpha_i^{(k,2)} x_i) + \sum_{1 \le i,j \le k-1} x_i' \beta_{ij}^{(k)} x_j,$$

$$(\alpha_i^{(k,1)}, \alpha_i^{(k,1)}, \beta_{ij}^{(k)} \in R, \quad k = 2, \ldots, n)$$

Example (Sato-Araki scheme)

- HS(Q_q,2) ($R = Q_q$)
  - $G(x_1, x_2) = g_2(x_1, x_2) = \frac{1}{2}(x_1' x_2 + x_2' x_1),$
  - $A_1 = Id_R : R \to R,$
  - $A_2 : R^2 \to R^2,$

    $A_2(z_1, z_2) = (z_1 + uz_2, z_1 - uz_2), \qquad (u \in R^\times),$
  - $F(x_1, x_2) = A_1 \circ G \circ A_2(x_1, x_2) = x_1' x_1 + h x_2' x_2, \quad (h = -(u')^{-1} u^{-1} \in R).$

  - **Signature generation** (Message $M \in R$)

    $c = (c_1, c_2) = (\rho^{-1} M + \rho', u(\rho^{-1} M - \rho'))$ $(\rho \in R^\times$: random)
  - **Verification**

    $F(c) = M$

Extension to Ring with involution

- Non-commutative ring used in HS scheme
  - A matrix subring which is closed by transpose operation.

  ⇒ cannot use general non-commutative rings (group rings etc.)

  HS scheme can be extended by using "Ring with involution".

- Ex. (group rings)
  - G: finite (non-commutative) group
  - $R = K[G]$: group ring of G
  - $\vartheta : K[G] \to K[G]$: linear isomorphism defined by $\vartheta(g) = g^{-1}$ $(g \in G)$

Rainbow$(K; v_1, o_1, o_2, \ldots, o_t)$

n : natural number

$$0 < v_1 < v_2 < \cdots < v_t < v_{t+1} = n$$

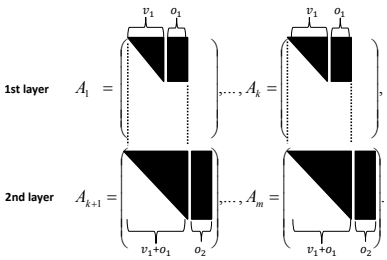
For $i = 1, \ldots, t$,

- $S_i = \{1, \ldots, v_i\}, \; O_i = \{v_i + 1, \ldots, v_{i+1}\},$
- $o_i = v_{i+1} - v_i.$

Central map $G = (g_{v_1+1}, \ldots, g_n) : K^n \to K^m, \quad (m = n - v_1)$

$$g_k(x_1, \ldots, x_n) = \sum_{i \in O_\alpha, j \in S_\alpha} \alpha_{ij}^{(k)} x_i x_j + \sum_{i,j \in O_\alpha, i \le j} \beta_{ij}^{(k)} x_i x_j \quad (\alpha_{ij}^{(k)}, \ldots, \eta^{(k)} \in K)$$
$$+ \sum_{i \in S_{\alpha+1}} \gamma_i^{(k)} x_i + \eta^{(k)}, \qquad (k = v_1 + 1, \ldots, n)$$

Secret key of Rainbow



Public key of Rainbow

$n = v_1 + o_1 + o_2$

$B_1 = \left(\begin{array}{|c|c|c|}\hline \blacksquare & \blacksquare & \blacksquare \\ \hline \blacksquare & \blacksquare & \blacksquare \\ \hline \blacksquare & \blacksquare & \blacksquare \\ \hline \end{array}\right), \ldots, B_k = \left(\begin{array}{|c|c|c|}\hline \blacksquare & \blacksquare & \blacksquare \\ \hline \blacksquare & \blacksquare & \blacksquare \\ \hline \blacksquare & \blacksquare & \blacksquare \\ \hline \end{array}\right),$

There are no layers.

$B_{k+1} = \left(\begin{array}{|c|c|c|}\hline \blacksquare & \blacksquare & \blacksquare \\ \hline \blacksquare & \blacksquare & \blacksquare \\ \hline \blacksquare & \blacksquare & \blacksquare \\ \hline \end{array}\right), \ldots, B_m = \left(\begin{array}{|c|c|c|}\hline \blacksquare & \blacksquare & \blacksquare \\ \hline \blacksquare & \blacksquare & \blacksquare \\ \hline \blacksquare & \blacksquare & \blacksquare \\ \hline \end{array}\right).$

NC-Rainbow$(R; \tilde{v}_1, \tilde{o}_1, \tilde{o}_2, \ldots, \tilde{o}_s)$ (1/2)

$\tilde{n}$: positive number

$$0 < \tilde{v}_1 < \tilde{v}_2 < \cdots < \tilde{v}_s < \tilde{v}_{s+1} = \tilde{n}$$

For $i = 1, \ldots, s$

- $\tilde{S}_i = \{1, \ldots, \tilde{v}_i\}$, $\tilde{O}_i = \{\tilde{v}_i + 1, \ldots, \tilde{v}_{i+1}\}$,
- $\tilde{o}_i = \tilde{v}_{i+1} - \tilde{v}_i$.

Central map $\tilde{G} = (\tilde{g}_{\tilde{v}_1+1}, \ldots, \tilde{g}_{\tilde{n}}) : K^{\tilde{n}} \to K^{\tilde{m}}, \quad (\tilde{m} = \tilde{n} - \tilde{v}_1)$

$$\begin{aligned} \tilde{g}_k(x_1, \ldots, x_n) = & \sum_{i \in \tilde{O}_k, j \in \tilde{S}_k} (x_i \alpha_{ij}^{(k)} x_j + x_j \alpha_{ij}^{(k)} x_i) \\ & + \sum_{i,j \in \tilde{S}_k} x_i \beta_{ij}^{(k)} x_j + \sum_{i \in \tilde{S}_{k+1}} (\gamma_i^{(k,1)} x_i + x_i \gamma_i^{(k,2)}) \\ & + \eta^{(k)} \quad (k = \tilde{v}_1 + 1, \ldots, \tilde{n}, \ \alpha_{ij}^{(k)}, \ldots \in R). \end{aligned}$$

32

NC-Rainbow$(R; \tilde{v}_1, \tilde{o}_1, \tilde{o}_2, \ldots, \tilde{o}_s)$ (2/2)

- Key Generation
  - Secret key $(n = \tilde{n}r, m = \tilde{m}r)$
    - $\hat{G}$, two affine transformations, $A_1 : K^m \to K^m$, $A_2 : K^n \to K^n$.
  - Public key
    - $\tilde{F} = A_1 \circ \phi^{-\tilde{m}} \circ \tilde{G} \circ \phi^{\tilde{n}} \circ A_2 : K^n \to K^m$.
- Signature Generation

  For message $M \in K^m$, calculate

  (1) $a = \phi^{\tilde{m}}(A_1^{-1}(M))$, (2) $b = \tilde{G}^{-1}(a)$, (3) $c = \phi^{-\tilde{n}}(A_2^{-1}(b))$

  in this order. c is a signature.
- Verification

  If $\tilde{F}(c) = M$, the signature is accepted.

  Original Rainbow

  If R=K, then this becomes $\boxed{\text{Rainbow}(K; \tilde{v}_1, \tilde{o}_1, \tilde{o}_2, \ldots, \tilde{o}_s)}$

33

Correspondence between NC-Rainbow and Rainbow

Theorem

There exists a correspondence

$$\text{NC-Rainbow}(R; \tilde{v}_1, \tilde{o}_1, \tilde{o}_2, \ldots, \tilde{o}_s) \to \text{Rainbow}(K; r\tilde{v}_1, r\tilde{o}_1, r\tilde{o}_2, \ldots, r\tilde{o}_s)$$

which holds public key.

- Secret key size of NC-Rainbow

  $m(m+1) + n(n+1) + \sum_{h=1}^{s} r\tilde{o}_h (2\tilde{v}_h \tilde{o}_h + \tilde{v}_h^2 + 2\tilde{v}_{h+1} + 1)$ field elements
- Secret key size of corresponding Rainbow

  $m(m+1) + n(n+1) + \sum_{h=1}^{s} r\tilde{o}_h \left(r^2 \tilde{v}_h \tilde{o}_h + \frac{r\tilde{v}_h (r\tilde{v}_h + 1)}{2} + r\tilde{v}_{h+1} + 1 \right)$ field elements

34

Comparison of Secret key size

$K = GF(256)$,
$R = Q_{256}$ $(r = 4)$.

Comparison of NC-Rainbow$(Q_{256}; \tilde{v}_1, \tilde{o}_1, \tilde{o}_2)$ *and* Rainbow$(GF(256); 4\tilde{v}_1, 4\tilde{o}_1, 4\tilde{o}_2)$

$(\tilde{v}_1, \tilde{o}_1, \tilde{o}_2)$	NC-size	Corr. Rainbow	R-size	ratio
(4,3,3)	4.2kB	(16,12,12)	15.9kB	26.7%
(5,4,4)	8.0kB	(20,16,16)	33.6kB	23.9%
(7,5,5)	15.1kB	(28,20,20)	70.7kB	21.5%
(9,6,6)	25.5kB	(36,24,24)	128.2kB	19.9%

NC-size : Secret key size of NC-Rainbow
R-size : Secret key size of corresponding Rainbow
ratio = NC-size/R-size

35

Reason of reduction of key size

- Property of "regular action"
  - R is expressed by a subring of matrix algebra of size r.

$Q_q \ni (\square \ \square \ \square \ \square) \longrightarrow \begin{pmatrix} \square & \square & \square & \square \\ \square & \square & \square & \square \\ \square & \square & \square & \square \\ \square & \square & \square & \square \end{pmatrix} \in M(4, K)$

4 entries — 16 entries

$M(d, Q_q) \longrightarrow M(4d, K)$

$4d^2$ entries — $16d^2$ entries

$\text{NC-Rainbow}(Q_q; \tilde{v}_1, \tilde{o}_1, \tilde{o}_2, \ldots, \tilde{o}_s)$

(Map in Theorem) $\to \text{Rainbow}(K; 4\tilde{v}_1, 4\tilde{o}_1, 4\tilde{o}_2, \ldots, 4\tilde{o}_s)$

36

Conclusion

- Non-commutative rings can be applied to MPKC in order to reduce key sizes.

- Thank you for your attention.

Applications of Algebraic Structures in Visual Cryptography

Avishek Adhikari
Department of Pure Mathematics
Calcutta University
35 Ballygunge Circular Road, Kolkata 700019
E-mail : avishek.adh@gmail.com

Abstract

Most of the secret sharing schemes are based on algebraic calculations in their realizations. But there are some different realizations from ordinal secret sharing schemes. Visual cryptography is one such secret sharing scheme. In visual cryptography, the problem is to encrypt some written material (handwritten notes, printed text, pictures, etc.) in a perfectly secure way in such a manner that the decoding may be done visually, without any cryptographic computations. The concept of visual cryptography was first proposed by Naor and Shamir in 1994. Visual cryptographic scheme for a set P of n participants is a cryptographic paradigm that enables a secret image to be split into n shadow images called shares, where each participant in P receives one share. Certain qualified subsets of participants can "visually" recover the secret image with some loss of contrast, but other forbidden sets of participants have no information about the secret image. In this talk, we shall explore how linear algebra and statistical design theory play an important role in constructing visual cryptographic schemes. We further emphasize on some of the open problems related to visual cryptographic schemes for both (k, n)-threshold and general access structures.

References

[1] Avishek Adhikari, M R Adhikari, *Introduction to Linear Algebra with Application to Basic Cryptography*, Asian Books, India, 2007.

[2] Avishek Adhikari, M R Adhikari, *Basic Modern Algebra with Applications*, To be published by Springer.

[3] Avishek Adhikari, M R Adhikari, *Introduction to Linear Algebra with Application to Basic Cryptography*, Asian Books, India, 2007.

[4] Avishek Adhikari, M. R. Adhikari and Y. P Chaubey, *Contemporary Topics in Mathematics and Statistics with Applications*, Asian Books , India, 2013.

[5] Avishek Adhikari, *Linear Algebraic Techniques to Construct black and white Visual Cryptographic Schemes for General Access Structure and its Applications to Color Images*, Design, Codes and Cryptography, 2013, DOI 10.1007/s10623-013-9832-5.

[6] A. Shamir, *How to share a secret*, Communication of ACM, Vol. 22, No. 11, 612-613, 1979.

Applications of Algebraic Structures in Visual Cryptography

Avishek Adhikari

website: www.imbic.org/avishek.html

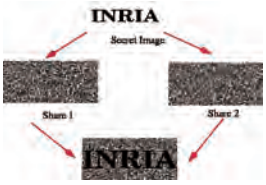
Research Team Members

Partha Sarathi Roy, Angsuman Das, Ushnish Sarkar, Sabyasachi Dutta

Department of Pure Mathematics
University of Calcutta, Kolkata.

Secret Sharing for General Access Structure?

Example of $(2, 2)$-VCS



$(2, 2)$-VCS

For Black pixel

For White pixel

$(2, 2)$-VCS

For Black pixel

For White pixel

0	0	1	1
0	1	0	1
0	1	1	1

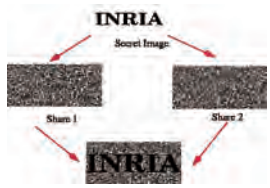
$(2, 2)$-VCS

For Black pixel

For White pixel

$$S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}.$$

Example of (2, 2)-VCS



Relative contrast

Let us consider a $(2, n)$-VCS on a set $\mathcal{P} = \{1, 2, \ldots, n\}$ of n participants with basis matrices S^0 and S^1 and having pixel expansion m. Then the *relative contrast* for the participants corresponding to X, $X \subseteq \mathcal{P}$, is denoted by $\alpha_X(m)$ and is defined as

$$\frac{w(S^1_X) - w(S^0_X)}{m}.$$

Secret Sharing for General Access Structure?

- Secret sharing refers to method for distributing a secret, say K, amongst a set $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ of n participants , each of which is allocated a share of the secret in such a way that certain qualified set of participants can reconstruct the secret by combining their shares while certain set of participants gets no information about the secret even when they combine their shares.
- The set of participants who are qualified to reconstruct the share is called qualified set of participants, while the set of participants who are not qualified to reconstruct the secret is known as forbidden set of participants.
- The collection of all qualified sets of participants is denoted by Γ_{Qual} while the set of all forbidden sets of participants are known as Γ_{Forb}. Γ_0 denotes the set of minimal qualified sets of participants.
- $(\Gamma_{Qual}, \Gamma_{Forb})$ is known as an access structure on the set of participants $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$.

Basis Matrix

Definition

Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure on a set $\mathcal{P}$ of n participants. A $(\Gamma_{Qual}, \Gamma_{Forb}, m)$-VCS with relative difference $\alpha(m)$ and a set of thresholds $\{t_X\}_{X \in \Gamma_{Qual}}$ is realized using the $n \times m$ basis matrices S^0 and S^1 if the following two conditions hold:

1. *If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Qual}$, then S^0_X, the "or" of the rows $i_1, i_2, \ldots, i_p$ of S^0, satisfies $w(S^0_X) \leq t_X - \alpha(m) \cdot m$; whereas, for S^1 it results in $w(S^1_X) \geq t_X$.*
2. *If $X = \{i_1, i_2, \ldots, i_p\} \in \Gamma_{Forb}$, the two $p \times m$ matrices obtained by restricting S^0 and S^1 to rows $i_1, i_2, \ldots, i_p$ are equal up to a column permutation.*

$(2, n)$-VCS by Naor and Shamir

$$S^0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \text{and} \quad S^1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Here the *relative contrast* for any two participants is $\frac{1}{4}$ and the *pixel expansion* is 4.

Linear Algebraic Techniques to construct VCS for General Access Structures

- $(\Gamma_{Qual}, \Gamma_{Forb})$ with $\Gamma_0 = \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3,4\}\}$.
- $\{\{1,2\}, \{1,3\}\}$ and $\{\{1,4\}, \{2,3,4\}\}$.
- $\left.\begin{matrix} x_1 + x_2 = 0 \\ x_1 + x_3 = 0 \\ x_4 = 0 \end{matrix}\right\} \cdots (1)$ and $\left.\begin{matrix} x_1 + x_2 = 1 \\ x_1 + x_3 = 1 \\ x_4 = 0 \end{matrix}\right\} \cdots (2)$
- $\left.\begin{matrix} x_1 + x_4 = 0 \\ x_2 + x_3 + x_4 = 0 \end{matrix}\right\}$ (3) and $\left.\begin{matrix} x_1 + x_4 = 1 \\ x_2 + x_3 + x_4 = 1 \end{matrix}\right\} \cdots (4)$

$$S^0_1 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, S^1_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

$$S^0_2 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, S^1_2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}.$$

Linear Algebraic Techniques to construct VCS for General Access Structures

- $(\Gamma_{Qual}, \Gamma_{Forb})$ with $\Gamma_0 = \{\{1,2\},\{1,3\},\{1,4\},\{2,3,4\}\}$.
  - $S^0 = S_1^0 || S_2^0 = \left[\begin{array}{cc|cccc} 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right]$

$$S^1 = S_1^1 || S_2^1 = \left[\begin{array}{cc|cccc} 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right]$$

Main Theorem

Theorem

For any given strong strong access structure $(\Gamma_{Qual}, \Gamma_{Forb})$ on a set $\mathcal{P} = \{1,2,\ldots,n\}$ of n participants with $\Gamma_0 = \{B_1, B_2, \ldots, B_k\}$ where $B_i \subseteq \mathcal{P}, \forall\ i = 1,2,\ldots,k$ and for any permutation $\sigma \in S_k$, the symmetric group of degree k, there exists a strong visual cryptographic scheme $(\Gamma_{Qual}, \Gamma_{Forb}, m)$ on $\mathcal{P}$ with $m = m_\sigma$, where m_σ is given as follows:

$$m_\sigma = \begin{cases} \sum_{i=1}^{l} 2^{|B_{\sigma(2i-1)} \cup B_{\sigma(2i)}|-2} & \text{if } k = 2l,\ l \geq 1 \\ \sum_{i=1}^{l} 2^{|B_{\sigma(2i-1)} \cup B_{\sigma(2i)}|-2} + 2^{|B_{\sigma(2l+1)}|-1} & \text{if } k = 2l+1,\ l \geq 0. \end{cases}$$

Construction of Basis Matrices

- Suppose we want to construct a scheme on a set of 6 participants $\mathcal{P} = \{1,2,3,4,5,6\}$ in which the minimal qualified set is $\Gamma_0 = \{\{1,2,3\},\{2,3,4\},\{2,4,5\},\{1,2,5\},\{1,3,6\},\{2,4,6\},\{3,4,5\}\}$.
- Note that $\Gamma_0 = \{\{1,2,3\},\{1,2,5\},\{2,4,3\},\{2,4,6\},\{2,4,5\},\{3,4,5\},\{1,3,6\}$
- Let us start with $\{1,2,3\}$ and $\{1,2,5\}$. Consider the following two associated system of linear equations over the binary field $\mathbf{Z_2}$

$$\begin{array}{rcl} x_1 + x_2 + x_3 &=& 0 \\ x_1 + x_2 + x_5 &=& 0 \\ x_4 &=& 0 \end{array} \quad ---(3) \qquad \begin{array}{rcl} x_1 + x_2 + x_3 &=& 1 \\ x_1 + x_2 + x_5 &=& 1 \\ x_4 &=& 0 \end{array} \quad ---(4)$$

$$G_0 = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \begin{array}{c} \\ \leftarrow 1 \rightarrow \\ \leftarrow 2 \rightarrow \\ \leftarrow 3 \rightarrow \\ \leftarrow 5 \rightarrow \end{array} \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} = G_1$$

Important Observations

- $\{\{1,2,3\},\{1,2,5\},\{2,4,3\},\{2,4,6\},\{2,4,5\},\{3,4,5\},\{1,3,6\}\}$
- $G_0 =$

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \left[\begin{array}{cccc|cccc|cccc} 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{array}\right] \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \left[\begin{array}{cccc|cccc|cccc} 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

- $G_1 =$

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \left[\begin{array}{cccc|cccc|cccc} 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{array}\right] \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \left[\begin{array}{cccc|cccc|cccc} 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{array}\right]$$

Open Problem: Find a suitable permutation to get minimum pixel expansion.

(k,n)-Threshold Scheme: as a particular case

Theorem

Let $(\Gamma_{Qual}, \Gamma_{Forb})$ be an access structure on a set $\mathcal{P} = \{1,2,\ldots,n\}$ of n participants with $\Gamma_0 = \{A \subseteq \mathcal{P} : |A| = k\}$, $2 \leq k \leq n$. Then there exists a strong (k,n)-VCS with

$$m_{our} = \begin{cases} l \cdot 2^{k-2}, & \text{if } l = \binom{n}{k} \text{ is even} \\ (l+1) \cdot 2^{k-2}, & \text{if } l = \binom{n}{k} \text{ is odd} \end{cases}$$

and relative contrast $\alpha(m) = \frac{1}{m_{our}}$.

$(4,5)$-Threshold Scheme: An Efficient Construction

Let us consider the $(4,5)$-VCS with
$\{\{1,2,3,4\},\{1,2,3,5\},\{1,2,4,5\},\{1,3,4,5\},\{2,3,4,5\}\}$.

$S^0 =$

$$\left[\begin{array}{cccccccccccccccccccc} 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}\right].$$

$S^1 =$

$$\left[\begin{array}{cccccccccccccccccccc} 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \end{array}\right].$$

Open Problem: For a future problem, one may think of finding exact number of common columns in S^0 and S^1.

Open Problems

- $\Gamma_0 = \{\{1,2\},\{2,3\},\{3,4\},\{1,4\}\}$.
- $$\left.\begin{array}{l} x_1 + x_2 = 0 \\ x_2 + x_3 = 0 \\ x_3 + x_4 = 0 \end{array}\right\} \cdots (5) \text{ and } \left.\begin{array}{l} x_1 + x_2 = 1 \\ x_2 + x_3 = 1 \\ x_3 + x_4 = 1 \end{array}\right\} \cdots (6).$$
- $S^0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}$ and $S^1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}$.

Open Problem: Characterize a given access structure on which we can take 3 equations together to get less pixel expansion.

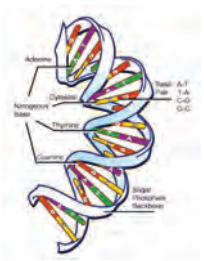
Introduction

- Secret Sharing Schemes,
- DNA Computing,
- Mathematics.

Aim of Our Work

Suppose we want to distribute a secret binary string to a set $\{P_1, P_2, \ldots, P_n\}$ of n participants in such a way that certain designated set of participants can reveal the secret by pulling their shares, but no forbidden set of participants has any information about the secret binary string.

Why DNA?

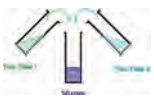


- The very small size,
- The huge storage capacity,
- Easy to carry or hide,
- Made up of A, T, G, C,
- Huge parallel computing,
- Stable as a DNA double strand,
- High longevity,
- Easy to get synthesized DNA

DNA encoding of binary strings

- a binary string can be represented as a set of integers that corresponds the positions where the bits are 1 from left to right.
- 1011 can be represented as a set $\{1,3,4\}$,
- each integer i can be represented in a DNA double strand notation as follows $ds_i = \updownarrow (GAATT)^i$.
- if $\alpha = 1011$, the DNA double strand representation of α is the test tube $T[\alpha] = \{ds_1,\ ds_3,\ ds_4\}$.

Mixing operation



- Take the content of two test tubes.
- Mixing can be done by dehydrating the tube contents (if not already in solution) and then combining the fluids together into a new tube, by pouring and pumping.

Bio-mathematical operations

- Boolean "*or*" operation between two binary strings
- if $\alpha = 1011$ and $\beta = 1001$,
- the binary "*or*" of two strings will be 1011.
- $T[\alpha]$ ($T[\beta]$) the test tube corresponding to the binary string α (β).
- pore the contents of the two test tubes to get binary "*or*".

Automated DNA Sequencing

- To read the DNA double strands in the test tube we need the process called DNA sequencing.

Outlay of our scheme

- Consider the secret sharing scheme on $\mathcal{P} = \{1, 2, 3, 4\}$ of 4 participants, where $\Gamma_0 = \{\{1, 2\}, \{2, 3\}, \{2, 4\}, \{1, 4\}\}$.
- $\Gamma_{Qual} = \{Y \subseteq \mathcal{P} : X \subseteq Y \text{for some } X \in \Gamma_0\}$ and $\Gamma_{Forb} = 2^{\mathcal{P}} \setminus \Gamma_{Qual}$.
- let the secret binary string be $x = x_1x_2x_3 = 011$.
- Assume that the DNA encoding, the mixing process are public.

Share Distribution

- The dealer chooses two Boolean matrices
$$G_0 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \text{ and } G_1 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$
- Since $x_1 = 0$, the dealer considers the matrix G_0 and apply a random permutation to the columns of G_0 and produces a matrix M_1.
- Similarly, for x_2 and x_3 on G_1 to produce matrices M_2 and M_3.
- Assume that the DNA encoding, the mixing process are public.

Share Distribution

- Let $M = M_1||M_2||M_3$.
- first row of M is $\alpha_1 = 010110101010$. Similarly $\alpha_2 = 010101100110$, $\alpha_3 = 010010001000$ and $\alpha_4 = 000100010001$.
- dealer converts the binary strings to DNA representations to get the test tubes
$T[\alpha_1] = \{ds_2, ds_4, ds_5, ds_7, ds_9, ds_{11}\}$,
$T[\alpha_2] = \{ds_2, ds_4, ds_6, ds_7, ds_{10}, ds_{11}\}$,
$T[\alpha_3] = \{ds_2, ds_4, ds_5, ds_9\}$,
$T[\alpha_4] = \{ds_4, ds_8, ds_{12}\}$,

Share Distribution

- $T[\alpha_i]$ is given to the participants P_i, $i = 1, 2, \ldots, n$ through a secret channel.
- Also the values $m = 4$ and $k = 3$ are given to the participants even through an insecure channel.

Decryption by the Qualified participants

- Let P_1, P_2 come together.
- They use mixing procedure with test tubes $T[\alpha_1]$ and $T[\alpha_2]$ to get $T[\alpha_1] \cup T[\alpha_2] = \{ds_2, ds_4, ds_5, ds_6, ds_7, ds_9, ds_{10}, ds_{11}\}$.
- Execute automated DNA sequencing method to read the DNA double strands.
- With the knowledge of decoding the DNA representation to the binary string, the values of $k = 3$ and $m = 4$, the participants P_1 and P_2 can convert the DNA representation to the binary string $y = 010111101110$.

Decryption by the Qualified participants

- Since, the value of m is known to the participants, P_1 and P_2 can break y as $y = (0101)(1110)(1110)$.
- Next they will find the value of w as 3 and then they will compute $z = 011$, as $BW(0101) < 3$, $BW(1110) = 3$. Thus P_1 and P_2 can recover the secret 011.

Forbidden set of participants

- Let $Y = \{P_3, P_4\}$ come together.
- They use mixing procedure with test tubes $T[\alpha_3]$ and $T[\alpha_4]$ to get $T[\alpha_1] \cup T[\alpha_2] = \{ds_2, ds_4, ds_5, ds_8, ds_9, ds_{12}\}$.
- they will convert the DNA representation to the binary string $y = (0101)(1001)(1001)$.
- Thus looking at those it is not possible to predict whether they correspond to 0 or 1.

DNA Microarray

- Affymetrix chips has more than 3,50,000 oligos per chip
- Around 48,000 different DNA spots can fit on a glass of this array.
- Statistical data analysis using computers gives less error.

Bibliography

- Avishek Adhikari, *Linear Algebraic Techniques to Construct black and white Visual Cryptographic Schemes for General Access Structure and its Applications to Color Images*, Design, Codes and Cryptography, 2013, DOI 10.1007/s10623-013-9832-5.
- Avishek Adhikari, "DNA Secret Sharing", IEEE World Congress on Evolutionary Computation 2006, CEC 2006, July 16-21, 1407-1411, 2006.
- Avishek Adhikari and Bimal Roy, *On some constructions of monochrome visual cryptographic schemes*, Page(s): 1-6, Digital Object Identifier 10.1109/INFTECH.2008.4621609, appeared in the IEEE Conference Proceedings, 1st International Conference on Information Technology, Faculty of Electronics, Telecommunications & Informatics Gdansk University of Technology, Poland, May 18-21, 2008.
- Avishek Adhikari, M. Bose, D. Kumar and Bimal Roy, *Applications of Partially Balanced and Balanced IncompleteBlock Designs in developing Visual Cryptographic Schemes*, IEICE TRANS. FUNDAMENTALS, Japan, Vol. E-90A, No. 5, pp. 949-951, May 2007.
- Avishek Adhikari, and M. Bose, "A New Visual Cryptographic Scheme Using Latin Squares," IEICE Transactions on Fundamentals, E87-A, No. 5, 1998-2002, 2004.
- Avishek Adhikari, T. K. Dutta, and B Roy, *A New Black and White Visual Cryptographic Scheme for General Access Structures*, Recent Advances in Cryptology : Indocrypt 2004, Lecture Notes in Computer Science, Springer, 2004, 399-413.
- Avishek Adhikari, and S. Sikdar, "A New (2, *n*) Color Visual Threshold Scheme for Color Images," Indocrypt'03, Lecture Notes in Computer Science, Springer-Verlag, 2904, 148-161, 2003.
- Avishek Adhikari, M R Adhikari, *Introduction to Linear Algebra with Application to Basic Cryptography*, Asian Books, India, 2007.
- Avishek Adhikari, M R Adhikari, *Basic Modern Algebra with Applications*, To be published by Springer.

Questions


Thank You!

Efficient Implementation of Multiplication on Extension Field Using GPU

Satoshi Tanaka[*,**], Takanori Yasuda[**], Kouichi Sakurai[*,**]

* : Kyushu University

** : Institute of Systems, Information Technologies and Nanotechnologies

Abstract:

Evaluating non-linear multivariate polynomial systems over finite fields is an important subroutine for encryption and signature verification in multivariate public-key cryptography (MPKC). The security of MPKC definitely becomes lower if a larger field is used instead of $GF(2)$ given the same number of bits in the key. However, we still would like to use larger fields because MPKC tends to run faster at the same level of security if a larger field is used. The heaviest computation of evaluating non-linear multivariate polynomial system is multiplication. Therefore, we must find the best way of multiplications.

Nowadays, graphics processing units (GPUs) have over 100 times computational power than CPU. They are constructed by hundreds cores. Hence, it seems that GPUs are suited as parallel general computing machines. Therefore, researchers applied parallel algorithms to GPUs.

In this work, we compare the efficiency of several techniques for multiplication methods over $GF(2^{16})$ via their implementations on a CPU and a GPU. In CPU implementations, Zech's method is fastest, and it multiplies 67,108,864 instances in 1.2 seconds. On the other hand, for GPU implementations, it seems that $GF(2^4)$ is a very efficient intermediary field for building extension fields over $GF(2^{16})$. The time of 67,108,864 multiplications is about 60.3 milliseconds. GPU implementations are about 20 times faster than CPU implementations.

Efficient Solving of Multivariate Quadratic Polynomial System using GPU

Satoshi Tanaka[†, ‡] Bo-Yin Yang[*],
Chen-Mou Cheng,[**] Kouichi Sakurai[†,‡]

†: Kyushu University, Japan
‡: Institute of Systems, Information Technologies and Nanotechnologies, Japan
*: Academia Sinica, Taiwan
**: National Taiwan University, Taiwan

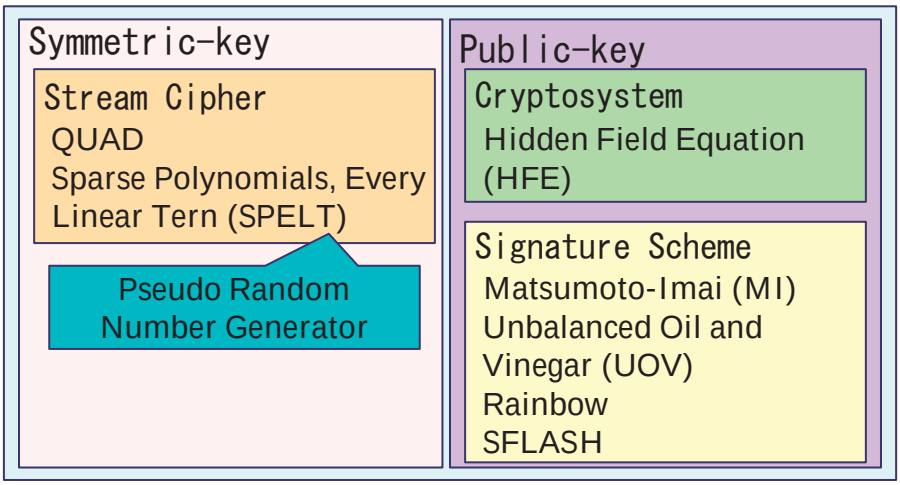
Multivariate Public-Key Cryptography (MPKC)

- Using multivariate polynomial system for encryption

$M = (x_1, \ldots, x_n)$ ⇒ $\begin{cases} y_1 = p_1(x_1, \ldots, x_n) \\ \vdots \\ y_m = p_m(x_1, \ldots, x_n) \end{cases}$ ⇒ $C = (y_1, \ldots, y_m)$

Message — system — Ciphertext

MPKC Family



Security of MPKC

- Solving multivariate polynomial system over finite field $GF(q)$
  - Particular, quadratic polynomial (MQ)

$$\begin{cases} y_1 = p_1(x_1, \dots, x_n) \\ \vdots \\ y_m = p_m(x_1, \dots, x_n) \end{cases} \Rightarrow (x_1, \dots, x_n)$$

NP-Complete problem

Example of MQ

- Over $GF(2)$, with 4 unknowns and 4 polynomials

$$\begin{cases} x_1x_2 + x_1x_4 + x_2x_3 + x_1 + x_3 = 1 \\ x_1x_3 + x_1x_4 + x_2x_4 + x_3x_4 + 1 = 1 \\ x_1x_2 + x_2x_4 + x_1 + x_3 + x_4 + 1 = 0 \\ x_1x_4 + x_2x_3 + x_3x_4 + x_1 + x_4 = 1 \end{cases}$$

$$(x_1, x_2, x_3, x_4) = (1, 0, 0, 0)$$

Solving Method for MQ

- Gröbner basis method
  - Find the Gröbner basis from MQ
- Relinearization method
  1. Linearize quadratic terms: $y_{i,j} = x_i x_j$
  2. Express y_{ij} as a linear combination of new parameters $t_1, \ldots, t_l$: $y_{i,j} = \sum_k a_{i,j,k} t_k$
  3. Create additional equations:

$$y_{i,j}\, y_{i',j'} = y_{i,j'} y_{i',j}$$

XL(eXtended Linearization) algorithm

1. Multiply

$$f_i = \prod_{j=1}^{k} x_{ij} * p_i(x_1, \ldots, x_n),$$

$$(k \leq D - 2, D = \max(|f_i|))$$

2. Linearize
3. Solve
4. Repeat

XL(eXtended Linearization) algorithm

1. Multiply
2. Linearize
   - Consider $\prod_j^k x_{ij}$ $(k \leq D)$ as a new variable y_i
   - Perform elimination to get univariate equations (e.g. with Gaussian Elimination)
3. Solve
4. Repeat

XL(eXtended Linearization) Algorithm

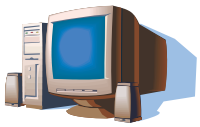
1. Multiply
2. Linearize
3. Solve
   - Solve the univariate equation (e.g. with Berlekamp's algorithm)
4. Repeat
   - Simplify the equations
   - Repeat the process

Parallel Computing Technique

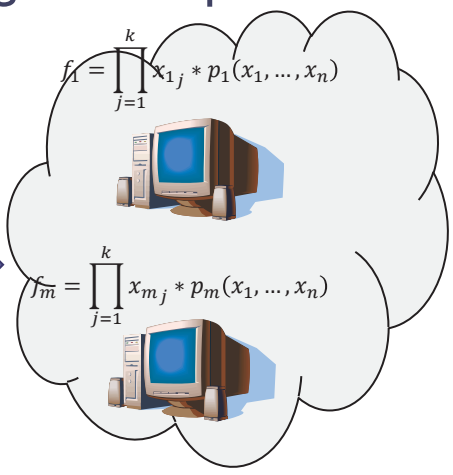
$$f_1 = \prod_{j=1}^{k} x_{1j} * p_1(x_1, \ldots, x_n)$$

$$\vdots$$

$$f_m = \prod_{j=1}^{k} x_{mj} * p_m(x_1, \ldots, x_n)$$



1 PC



m PCs

Graphics Processing Unit(GPU)

- Processing Graphics (particular for 3DCG)
- GPUs have many cores
  - Strong Computing Power
- General Purpose computing on GPUs (GPGPU)
  - Use for non-graphical computing

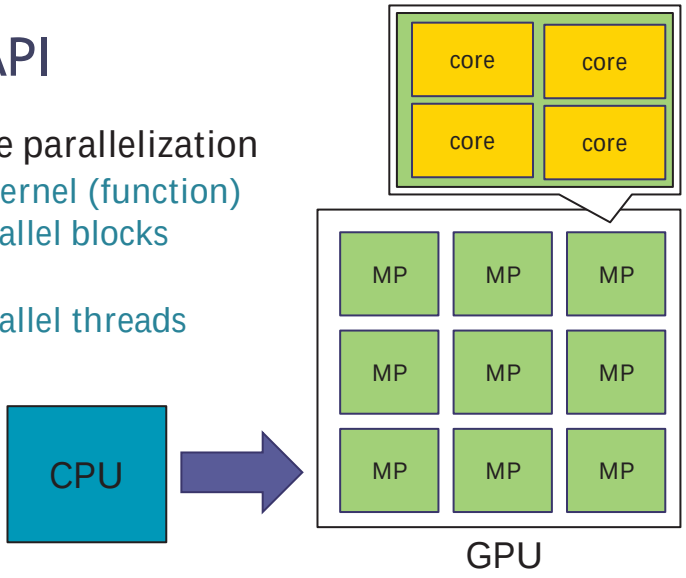
GPGPU environment

- CUDA API
  - For NVIDIA GPU Hardware
  - Language: C, Fortran
- ATI Stream
  - For ATI GPU Hardware
  - Language: Brook+ (C-based language)
- OpenCL
  - Framework for multicore and heterogeneous programs (not only for GPUs)
  - Language: C

13

CUDA API

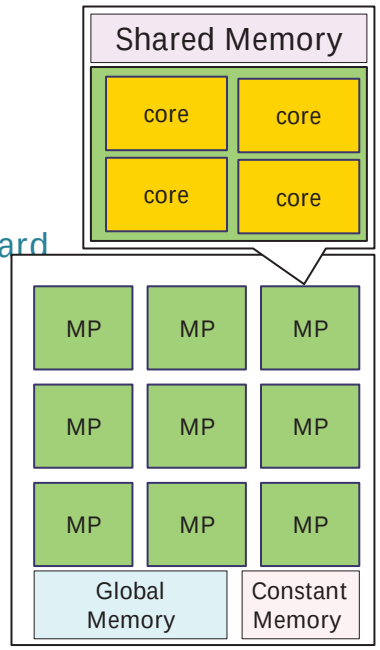
- Multiple parallelization
  - CPU kernel (function)
    → parallel blocks
  - Block
    → parallel threads



14

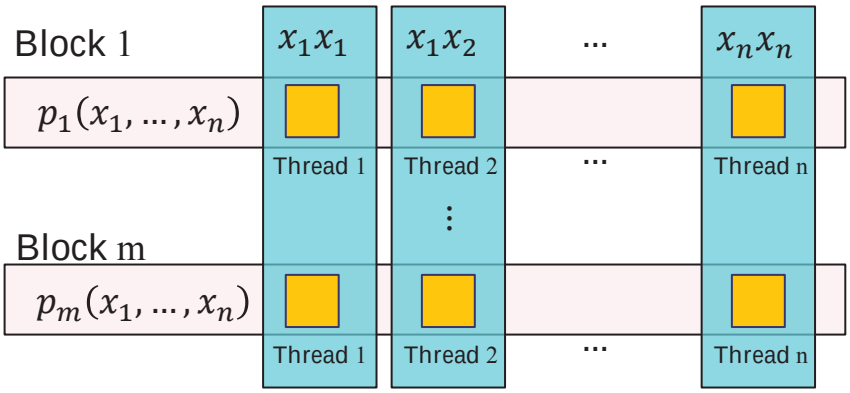
CUDA API

- Limitations (e.g. GTX 580)
  - Not the full C (C++) standard
  - Maximum threads/block
    - 1024 threads/block
  - Memory construction
    - Shared memory: 48 kB
    - Constant memory: 64kB
    - Global memory: 3GB
  - The number of registers:
    - 32,768 registers/block



Parallel XL Algorithm

1. Multiply



Parallel XL Algorithm

2. Linearize
   - E.g. Gaussian elimination for $n \times n$ matrix
     i. $i \leftarrow 1$
     ii. Find non-zero element $a_{j,i}$, $i \leq j \leq n$
     iii. Swap row i and row j
     iv. Normalize row i
     v. $a_{j,k} \leftarrow a_{j,k} - a_{j,i}a_{i,k}$, $i < j \leq n, i \leq k \leq n$
     vi. $i \leftarrow i + 1$
     vii. If $i < n$ then back to step ii.

1	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$
0	1	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$
0	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$
0	$a_{4,2}$	$a_{4,3}$	$a_{4,4}$	$a_{4,5}$
0	$a_{5,2}$	$a_{5,3}$	$a_{5,4}$	$a_{5,5}$

Parallel XL Algorithm

3. Solve
   - Solving with exhaustive search with each core
     - E.g. $f(x) = x^2 + x + 4 = 0$ over $GF(5)$

       $f(0) = 0^2 + 0 + 4 = 4 \neq 0$

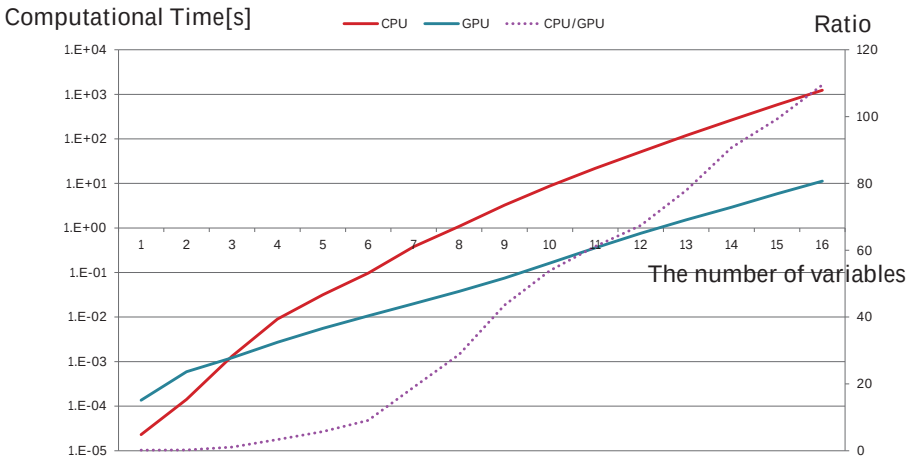
       $f(1) = 1^2 + 1 + 4 = 1 \neq 0$

       $f(2) = 2^2 + 2 + 4 = 0$

       $f(3) = 3^2 + 3 + 4 = 1 \neq 0$

       $f(4) = 4^2 + 4 + 4 = 4 \neq 0$
4. Repeat
   - Simplify the equations in parallel (like step 1)

Experimental Results



Conclusion and Future Work

- GPGPU technique has the potential of efficient solving multivariate quadratic polynomial system over a finite field.

- Improve the linearize step of XL algorithm
- Comparing with Parallel Gröbner basis method

Efficient Implementation of Multiplication on Extension Field Using GPU

Satoshi Tanaka[*,**], Takanori Yasuda[**], Kouichi Sakurai[*,**]

* : Kyushu University

** : Institute of Systems, Information Technologies and Nanotechnologies

Abstract:

Evaluating non-linear multivariate polynomial systems over finite fields is an important subroutine for encryption and signature verification in multivariate public-key cryptography (MPKC). The security of MPKC definitely becomes lower if a larger field is used instead of $GF(2)$ given the same number of bits in the key. However, we still would like to use larger fields because MPKC tends to run faster at the same level of security if a larger field is used. The heaviest computation of evaluating non-linear multivariate polynomial system is multiplication. Therefore, we must find the best way of multiplications.

Nowadays, graphics processing units (GPUs) have over 100 times computational power than CPU. They are constructed by hundreds cores. Hence, it seems that GPUs are suited as parallel general computing machines. Therefore, researchers applied parallel algorithms to GPUs.

In this work, we compare the efficiency of several techniques for multiplication methods over $GF(2^{16})$ via their implementations on a CPU and a GPU. In CPU implementations, Zech's method is fastest, and it multiplies 67,108,864 instances in 1.2 seconds. On the other hand, for GPU implementations, it seems that $GF(2^4)$ is a very efficient intermediary field for building extension fields over $GF(2^{16})$. The time of 67,108,864 multiplications is about 60.3 milliseconds. GPU implementations are about 20 times faster than CPU implementations.

Efficient Implementation of Multiplication on Extension Field Using GPU

Satoshi Tanaka, Takanori Yasuda, Kouichi Sakurai
†: Kyushu University
‡: Institute of Systems, Information Technologies and Nanotechnologies

Multivariate Public-Key Cryptography (MPKC)

- Using multivariate polynomial system for encryption

$$M = (x_1, \dots, x_n) \Rightarrow \begin{cases} y_1 = p_1(x_1, \dots, x_n) \\ \vdots \\ y_m = p_m(x_1, \dots, x_n) \end{cases} \Rightarrow C = (y_1, \dots, y_m)$$

Message

system

Ciphertext

Computational Cost of MPKC

- $\frac{m(n^2+3n)}{2}$ additions, $m(n^2+2n)$ multiplications, n variables, m polynomials,

Unknowns	Polynomials	Additions	Multiplications
40	60	51,600	100,800
60	90	170,100	334,800
80	120	398,400	787,200
128	256	2,146,304	4,259,840
256	512	16,973,824	33,816,576
320	640	33,075,200	65,945,600
512	1024	135,004,160	269,484,032

Extension Field of Finite Field

- Field extension K/F, $K = GF(p^k)$, $F = GF(p)$
  - Primitive polynomial $f_0(x)$:
    $f_0(x) = x^k + c_{k-1}x^{k-1} + \cdots + c_1x + c_0,\ (c_0, \ldots, c_{k-1} \in F)$
  - Element $e = (e_1, \ldots, e_k)$:
    e: $e(x) = e_{k-1}x^{k-1} + \cdots + e_1x + e_0, \quad (e_0, \ldots, e_{k-1} \in F)$
- Addition:
  $a + b = (a_0 + b_0 \bmod p, \ldots, a_{k-1} + b_{k-1} \bmod p)$

Multiplications on Extension Field

- Multiplication:

$$a * b = a(x) * b(x) \; mod \; f_0(x)$$
$$= \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} a_i b_j x^{i+j} \; mod \; f_0(x)$$

  - Computational Cost:
    $(k-1)^2$ additions, k^2 multiplications on F,
    1 modulo $f_0(x)$

Reduce Multiplication Cost

- Transform multiplication formula
- Zech's method
- Use multiplication table

Transform Multiplication Formula

- Precompute modulo $f_0(x)$
  - E.g. $GF(2^2)$, $f_0(x) = x^2 + x + 1 = 0$
    $c = a * b = (a_0, a_1) * (b_0, b_1)$:
    $c_0 = a_0 b_0 + a_1 b_1$
    $c_1 = a_1 b_0 + a_0 b_1 + a_1 b_1$
- Computational cost:
  $2(k-1)^2$ additions, k^2 multiplications,
  $(k-1)^2$ constant multiplications on F

Zech's method

- Precompute
  $x^t \bmod f_0(x), \qquad (0 \le t < p^k - 1)$
- $c = a * b = x^{t_a} * x^{t_b}$:
  $x^{(t_a + t_b) \bmod p^k - 1} \bmod f_0(x)$
  - E.g. . $GF(2^2)$, $f_0(x) = x^2 + x + 1 = 0$

elements	(0,0)	(0,1)	(1,0)	(1,1)
index	$-\infty$	0	1	2

- Computational cost:
  3 lookups, 1 additions, 1 modulo $(p^k - 1)$
- Memory cost: $2p^k \lceil k \log_2 p \rceil$ bits

Use Multiplication Table

- Precompute all multiplications on K
  - E.g. $GF(2^2), f_0(x) = x^2 + x + 1 = 0$

$*$	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(0,1)	(0,0)	(0,1)	(1,0)	(1,1)
(1,0)	(0,0)	(1,0)	(1,1)	(0,1)
(1,1)	(0,0)	(1,1)	(0,1)	(1,0)

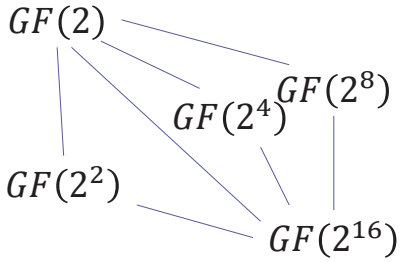
- Computational cost: 1 lookup
- Memory cost: $\left(p^k\right)^2 \lceil k \log_2 p \rceil$ bits

Which is the Best Way?

- Use multiplication table:
  - $GF(2^8)$: 64 kB
  - $GF(2^{16})$: 8 GB
- Zech's method:
  - $GF(2^{16})$: 256 kB
  - $GF(2^{32})$: 32 GB

Use Intermediary Field

- Intermediary field L of K/F
  - $L = GF(p^l)$, (l is a divisor of k)
- Multiplications on K with K/L, L/F:
  - $2(k/l-1)^2$ additions on L, $(k/l)^2$ multiplications on L
  - Multiplications on L:
    - Multiplication table
    - Zech's method



Example: Multiplication on $GF(2^{16})$

- $GF(2^{16})/GF(2^8)/GF(2)$:
  - $GF(2^8)/GF(2)$: Multiplication table
    $f_0(x) = x^8 + x^4 + x^3 + x^2 + 1 = 0$
  - $GF(2^{16})/GF(2^8)$: Polynomial
    $f_0(y) = y^2 + y + (x^5 + x) = 0,$

Multiplication on GPU

- Should parallelize about multiplication on GPU?
  - Should parallelize about evaluating multivariate polynomial system
    - Evaluating system needs many computaions
    - Reduce communications between CPU and GPU

Experimental Result of $GF(2^{16})$

- Computational time of 67,108,864 multiplications

CPU	Zech's method	Polynomial
$GF(2^{16})/GF(2)$	1,174.1971 ms	21,982.8976 ms
$GF(2^{16})/GF(2^2)/GF(2)$	N.A.	9,591.4002 ms
$GF(2^{16})/GF(2^4)/GF(2)$	N.A.	3,500.0024 ms
$GF(2^{16})/GF(2^8)/GF(2)$	N.A.	1,357.0016 ms

GPU	Zech's method	Polynomial
$GF(2^{16})/GF(2)$	88.5837 ms	346.5904 ms
$GF(2^{16})/GF(2^2)/GF(2)$	N.A.	149.7266 ms
$GF(2^{16})/GF(2^4)/GF(2)$	N.A.	60.3309 ms
$GF(2^{16})/GF(2^8)/GF(2)$	N.A.	92.5700 ms

Conclusion

- We present how to multiply on extension field
  - Show example of multiplications on $GF(2^{16})$, CPU, GPU implementation result
- Future works
  - Generalize to all finite fields of multiplications.
  - Apply to MPKC

On Cheater-Identifiable Secret Sharing Schemes Secure Against Rushing Adversary[1]

Kirill MOROZOV

Institute of Mathematics for Industry, Kyushu University, Japan
morozov@imi.kyushu-u.ac.jp

(joint work with Rui Xu, Graduate School of Mathematics, Kyushu University and Tsuyoshi Takagi, Institute of Mathematics for Industry, Kyushu University)

In this talk, we present our recent result on a k-out-of-n *cheater-identifiable* secret sharing. In a k-out-of-n secret sharing scheme [4], a party called *dealer* splits his secret data into n pieces (called *shares*) which are to be given to n parties. Any subset of $k-1$ shares contains no information on the secret, while any subset of k shares allows efficient reconstruction.

It is well known that Shamir secret sharing scheme [4] is not protected against malicious parties who contribute an incorrect share at the reconstruction [2, 5].

At Eurocrypt 2011, Obana [3] proposed a k-out-of-n secret sharing scheme capable of identifying up to t cheaters with probability $1-\epsilon$ under the condition $t < k/3$. In that scheme, the share size $|V_i|$ satisfies $|V_i| = |S|/\epsilon$, which is almost optimal. However, Obana's scheme is known to be vulnerable to attacks by rushing adversary who can observe the messages sent by the honest parties prior to deciding her own messages.

In this talk, we present a new scheme, which is secure against rushing adversary, with $|V_i| = |S|/\epsilon^{n-t+1}$, assuming $t < k/3$. The share size of our proposal is substantially smaller compared to $|V_i| = |S|(t+1)^{3n}/\epsilon^{3n}$ in the scheme by Choudhury at PODC 2012 [1] when the secret is a single field element. A modification of the later scheme is secure against rushing adversary under a weaker $t < k/2$ condition.

Therefore, our scheme demonstrates an improvement in share size (at least 3 times smaller compared to the related works) achieved for the price of strengthening the assumption on t.

References

[1] Choudhury, A.: Brief announcement: optimal amortized secret sharing with cheater identification. In: PODC 2012. (2012) 101-102.
[2] McEliece, R., Sarwate, D.: On sharing secrets and reed-solomon codes. Commun. ACM 24(9) (1981) 583-584.
[3] Obana, S.: Almost optimum t-cheater identifiable secret sharing schemes. In: EUROCRYPT 2011. (2011) 284-302.
[4] Shamir, A.: How to share a secret. Commun. ACM 22(11) (1979) 612-613.
[5] Tompa, M., Woll, H.: How to share a secret with cheaters. J. Cryptology 1(2) (1988) 133-138.

[1]The paper on this result will appear in Proc. of the 8th International Workshop on Security (IWSEC 2013), Okinawa, Japan, November 18-20, 2013.

On Cheater Identifiable Secret Sharing Schemes Secure Against Rushing Adversary

Kirill Morozov

Institute of Mathematics for Industry
Kyushu University

Joint work with Rui Xu and Tsuyoshi Takagi

安全・安心社会基盤構築のための代数構造ワークショップ

ISIT, Fukuoka

August 29, 2013

Plan of This Talk

- Motivation
- Secret sharing: introduction
- Cheater Identification
- Our Proposal
- Conclusion

Secret Sharing

Applications:

- Threshold cryptography
- Multi-party computation
- Perfectly secure message transmission
- …

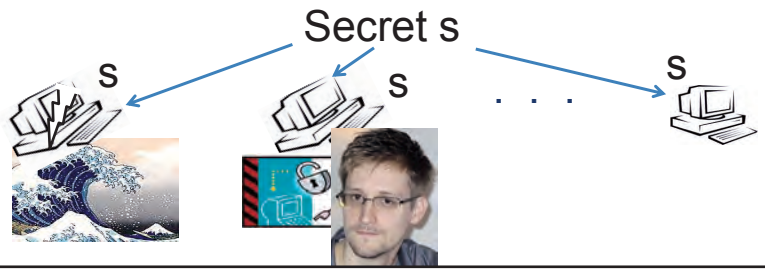
Secure Cloud Storage

- Confidentiality of data stored “in the cloud”
- Single server: encryption
- Multiple servers: encryption or secret sharing

"Secret Sharing": Naïve Approach

- Reliability: **O**
- Privacy: **X**

[http://www.cs.tau.ac.il/~erezalon/]



5

Computational vs Information-Theoretic Security

- Hardness of some mathematical problem
  - E.g. no polynomial-time algorithm for discrete log

Example: El Gamal public-key encryption

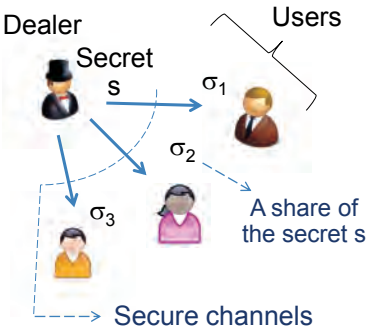
- "Physical" assumption:
  - E.g. at least k out of n servers are intact

Example: Secret sharing

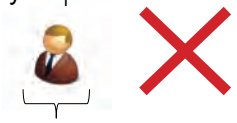
6

Secret Sharing

- Dealer distributes shares among n users (parties)
- A collection A of subsets of parties (access structure) can reconstruct the secret
- A collection *not in* A (adversary structure) cannot reveal any information on the secret



Privacy: σ_1 => secret = ?

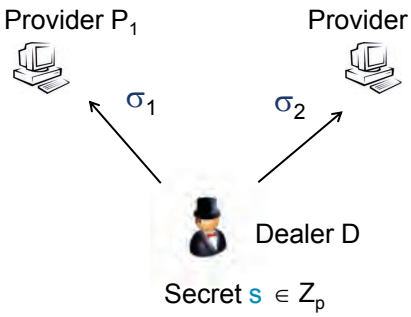


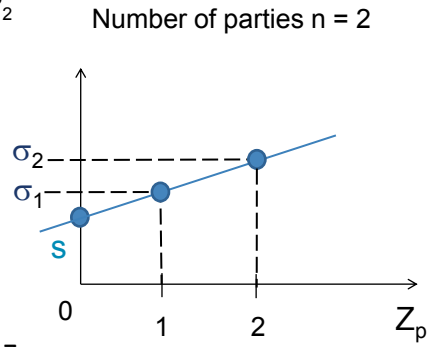
Unqualified set

Reconstruction: (σ_1, σ_2,…) => secret = s

Qualified set

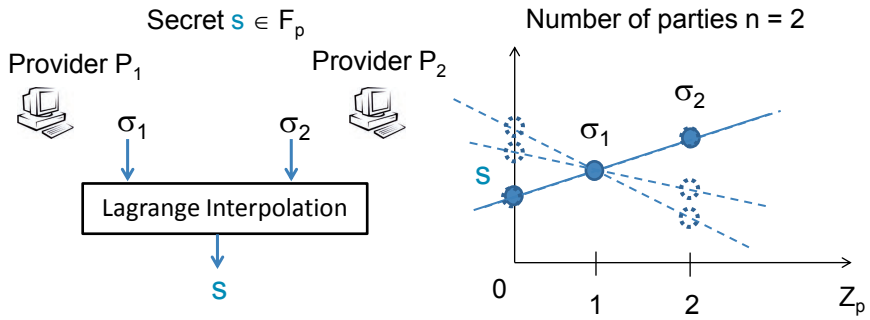
(k=2,n=2) Scheme





- Fix prime p>n, computation over Z_p
- Dealer randomly chooses $f_s(X) \in F_p[X]$, $\deg(f_s) \leq k-1 = 1 : f_s(X) = s + b_1X$
  - I.e. $b_0 = b(0) = s$ and $b_1 \leftarrow_R Z_p$
- $\sigma_1 = f_s(1)$, $\sigma_2 = f_s(2)$ – shares of the secret

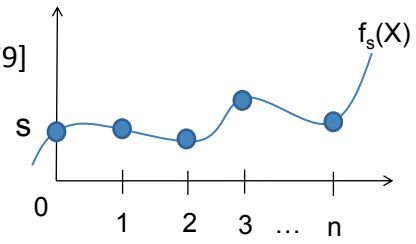
(2,2) Scheme: Reconstruction and Security



- Reconstruction: $s = f_s(0) = \Sigma^k_{i=1} \sigma_i \prod^k_{j=1,j\neq i} j / (j - i)$
- Privacy: ∃ p polynomials of degree ≤ k-1 = 1, which are consistent with the share σ_1
  - This means that any value of s is equiprobable (perfect privacy)

9

Shamir (k,n) Threshold Secret Sharing



- [Shamir, Commun. ACM 22(11) '79]
- **Share Generation:**
  Dealer chooses
  $f_s(X) \in_R F_p[X]$: $\deg(f_s) \leq k-1$,
  $f_s(X) = s + \Sigma_{j=1}^{k-1} b_j X^j$
  - s is the secret, $b_j \leftarrow_R F_p$, $1 \leq j \leq n$
- Shares $\sigma_i = f_s(i)$, $1 \leq i \leq n$
- **Reconstruction:** Using Lagrange interpolation, any subset of k parties reconstructs "s"

10

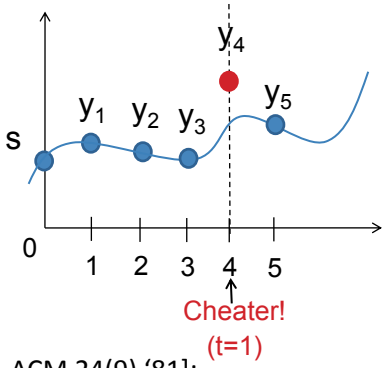
Secret Sharing with Cheaters

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{k-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_n & x_n^2 & \dots & x_n^{k-1} \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \dots \\ b_{k-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \dots \\ y_n \end{pmatrix}$$

Generator matrix of Reed-Solomon code (Vandermonde matrix)

"information symbols" (randomness)

"codeword" (shares)



- Observation [McEliece, Sarwate: Comm. ACM 24(9) '81]: Shamir's scheme is closely related to Reed-Solomon code that corrects both erasures and errors
- Recovery of t errors (i.e. cheaters) is possible, if # reconstructing parties is $l \geq k + 2t$

11

Cheater-Identifiable Secret Sharing

- (k,n) threshold secret sharing scheme
- (t,ε) secret sharing with cheater identification (SSCI): ≤t cheaters succeed with probability ≤ε
- At reconstruction, a list of cheaters L is output

12

Adversary Model

- Adversary controls cheaters
- Adversary succeeds if
  1) She imposes reconstruction of an incorrect secret, AND
  2) She is not included into L
- (Honest parties never get to L)

13

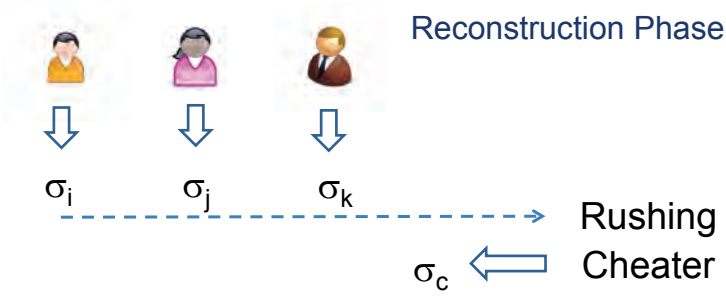
Remarks

- Robust secret sharing:
  - Only correctness of the secret is required…
  - … But cheater identification sometimes possible ☺
- Basic idea from [Rabin, Ben-Or '89]: Authenticate shares
- Our focus: Public identification
- => $t < \lfloor (k-1)/2 \rfloor$ is the weakest assumption

14

Rushing Cheater

- Observes all the shares of honest users, prior to submitting his own



Reminder:

- k = threshold for reconstruction
- t = # cheaters

15

Lower Bound

- [Kurosawa, Obana, Ogata '95]
- In SSCI, the share size is at least

$$|V_i| \geq (|S|-1)/\varepsilon + 1,$$

where $|V_i|$ is the share size,
$|S|$ is the size of the secret,
ε - cheaters' success probability

16

Our Result and Comparison

Scheme	# Cheaters	Share Size	Adversary	# Players at Reconstruction
Obana [11]	$t < k/3$	$\|V_i\| = \|S\|/\epsilon$	Non-rushing	$m \geq k$
Choudhary [4]	$t < k/2$	$\|V_i\| = \|S\|(t+1)^{3n}/\epsilon^{3n}$	Rushing	$m \geq k$
Cevallos et al [3]	$t < n/2$	$\|V_i\| = \|S\|[\frac{1}{t+1}(\frac{\epsilon}{e})^{\frac{2}{t}}]^{3n}$	Rushing	$m = n$
Our Proposal	$t < k/3$	$\|V_i\| = \|S\|/\epsilon^{n-t+1}$	Rushing	$m \geq k$

Optimal schemes:

- [Choudhary [4] PODC'12] t<k/2
  - Optimal in asymptotics when the secret is a vector
- [Cevallos et al [3] Eurocrypt'12] t<n/2
  - Note: all n parties must reconstruct
- (RSS!): [Jhanwar & Safavi-Naini, FC'13] t<n/2-1
  - (Ideal!) but reconstruction is inefficient

17

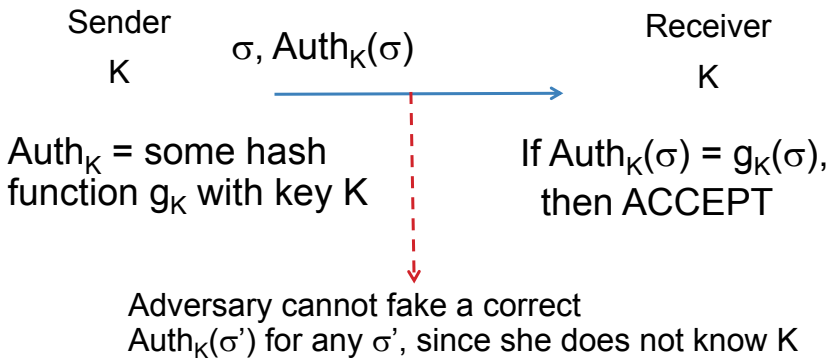
Share Size Estimation

- Closest competitor [Choudhury '12] (for a single secret)
- "Red" - an overhead for cheater identification
- Take n = $\lfloor$(t-1)/3$\rfloor$, $\varepsilon = 2^{-80}$

n	Red_{Cho}	Red_{Our}	Red_{Cho}/Red_{Our}
4	120.6 B	26.7 B	4.5
1024	33.2 KB	6.7 KB	5.0
2^{18}	9.0 MB	1.7 MB	5.4

18

Unconditional Authentication



- Strongly universal (SU) hash functions can be used [Carter Wegman '79]

Instantiation of SU Function

- Set $\{g(x) \mid g(x) \in F_q[X], \deg(g) \leq t\}$ is a class of strongly universal$_{t+1}$ hash functions $F_q \rightarrow F_q$
- Def.: $\forall$distinct $x_1,\ldots,x_{t+1} \in F_q$ and $y_1,\ldots,y_{t+1} \in F_q$: $\Pr[g(x_{t+1})=y_{t+1} \mid g(x_1)=y_1,\ldots,g(x_t)=y_t]=1/q$
- The polynomial g(x) is the key of the hash function

Obana's Scheme

- [Eurocrypt 2011]
- Basic idea: Authenticate shares (using SU hash function) + share the authentication tag using Shamir
- $\sigma_i = (f_s(i) , Auth)$
- $Auth = SU(f_s(i)) = g(f_s(i))$

21

Obana's Scheme (cont)

- **Share Generation:**
  Let $q \geq n \cdot p$, $\phi : F_p \times [n] \rightarrow F_q$
  1. $f_s(x) \leftarrow_R \{F_p[X], deg(g) \leq k-1\}$ s.t. $f_s(0)=s$, $v_{s,i}=f_s(i)$
  2. $g(x) \leftarrow_R \{F_q[X], deg(g) \leq t\}$, $v_{c,i}=g(\phi(v_{s,i},i))$
  3. Output a share $\sigma_i=(v_{s,i},v_{c,i})$

22

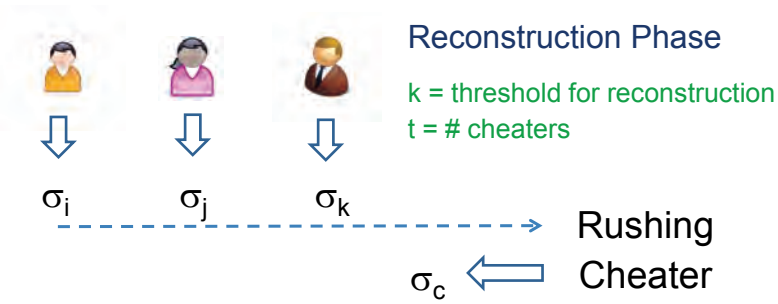
Obana's Scheme (cont)

Reconstruction: Let $m \geq k$, and L - the list of cheaters
On input $(\sigma_{i_1},\ldots,\sigma_{i_m})=((v_{s,i_1},v_{c,i_1}),\ldots,(v_{s,i_m},v_{c,i_m}))$:

1. From $(v_{c,i_1},\ldots,v_{c,i_m})$ reconstruct g(x) using Reed-Solomon decoding
   - Up to "t" errors (i.e. cheater's shares) may be identified; if so, then add them to L
2. Use g(x) for share authentication
   - If $v_{c,i_j}=g(\phi(v_{s,i},j))$ does not hold, add "j" to L
3. If $|L|>m-k$ then output $(\perp,L)$, otherwise
   reconstruct $f_s'(x)$ using Lagrange interpolation;
   If $\deg(f_s'(x)) \leq k-1$, output $f_s'(0)$, o/w output $(\perp,L)$

23

Rushing Cheater



- Obana's scheme is not secure now:
- Adv will learn the key g(x) from $\{v_{c,i}\}_{1\leq i\leq m}$
- Then forge authentication for an arbitrary share

24

Our Proposal: Share Generation

- [To appear at IWSEC'13]
- Basic idea: Reconstruction in *two rounds*
- **Share Generation:**
  Let $q \geq n \cdot p$, $\phi : F_p \times [n] \rightarrow F_q$
  1. $f_s(x) \leftarrow_R \{F_p[X], \deg(g) \leq k-1\}$ s.t. $f_s(0)=s$, $v_{s,i}=f_s(i)$
  2. $g(x) \leftarrow_R \{F_q[X], \deg(g) \leq t\}$, $v_{c,i}=g(\phi(v_{s,i},i))+k_i$
  3. For j=1,…,n:
     - $f_j(x) \leftarrow_R \{F_p[X], \deg(g) \leq t\}$ s.t. $f_j(0)=k_j$, $k_{j,i}=f_j(i)$
  4. Output a share $\sigma_i=(v_{s,i},v_{c,i},k_{1,i},\ldots, k_{n,i})$
- Obs. (Saving share size): For t parties the masking key is not needed

25

Reconstruction and Security Intuition

- User i: $\sigma_i=(v_{s,i},v_{c,i},k_{1,i},\ldots, k_{n,i})$
- Reconstruction:
  - Round 1: Submit ($v_{s,i}=f_s(i)$, $v_{c,i} = g(\phi(v_{s,i},i))+k_i$)
  - Round 2: Submit $k_{1,i},\ldots, k_{n,i}$
- Security intuition: Rushing Adv cannot see Auth = $g(\phi(v_{s,i},i))$ after Round 1
- => Adv must forge k_i
- **Impossible** due to cheater identification using RS decoding

26

Security Intuition (cont)

- Cheater must fake Auth before seeing the key
- Her success probability is $\varepsilon=1/q$
- $|V_i| = p \cdot q^{n-t+1} = |S|/\varepsilon^{n-t+1}$

Open Questions

- Further reduction of the share size
  (Maybe constant? I.e. independent of n,k,t)
- "Killer application"?

Plaintext Checkable Encryption with Designated Checker

Avishek Adhikari*
Department of Pure Mathematics
Calcutta University
35 Ballygunge Circular Road, Kolkata 700019
E-mail : avishek.adh@gmail.com

Abstract

Plaintext checkable encryption (PCE), proposed by Canard et. al., in CT-RSA 2012, is a public-key primitive with an added functionality that given a plaintext, a ciphertext and the public key under which the ciphertext is created, anyone can check whether the ciphertext encrypts the plaintext under the key. However, in many situations, users may not want everybody to have plaintext checking right on their ciphertexts. In this paper, we introduce a primitive called designated plaintext checkable encryption (DPCE), where only a designated checker can perform the plaintext checking operation. We note that, unlike PCE, there can be two types of DPCE (of Type I and II), depending upon whether the user delegates (at his will) or is bound to provide the plaintext checking right to a designated checker. We also provide various generic random-oracle and standard model constructions for DPCE of both the types based on any probabilistic or deterministic encryption scheme.

References

[1] Boneh, D., Crescenzo, G.D., Ostrovsky, R., Persiano, G.: Public Key Encryption with Keyword Search, EUROCRYPT 2004, LNCS 3027, 506-522, 2004.

[2] Baek, J., Safavi-Naini, R., Susilo, W.: Public Key Encryption with Keyword Search Revisited, ICCSA 2008, Part I, LNCS 5072, 1249-1259, 2008.

[3] Lu, Y., Zhang, R., Lin, D.: Stronger Security Model for Public-Key Encryption with Equality Test, PAIRING 2012, LNCS 7708, 65-82, 2013.

*This work is the joint collaboration with Angsuman Das of University of Calcutta and Professor K Sakurai of Kyushu University

[4] Canard, S., Fuchsbauer, G., Gouget, A. Laguillaumie, F.: Plaintext-Checkable Encryption, CT-RSA 2012, LNCS 7178, 332-348, 2012.

Plaintext Checkable Encryption with Designated Checker

Avishek Adhikari

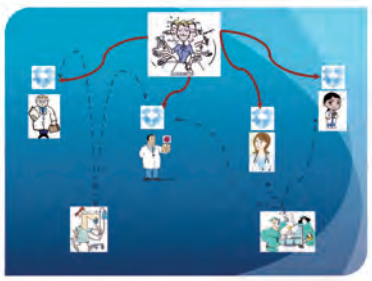
website: www.imbic.org/avishek.html

Joint Work with

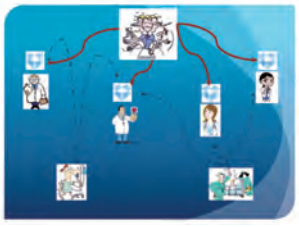
Angsuman Das and Professor K Sakurai

Department of Pure Mathematics
University of Calcutta, Kolkata.

Some Scenario in a Hospital



Some Solutions



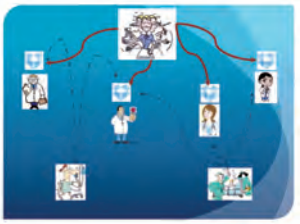
Trivial Solution

Decryption Power to the Secretary.

Problem

But for security reasons, the patients or the Hospital Management may not want.

Some More Solutions



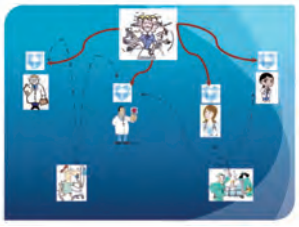
Boneh et. al. [Eurocrypt 2004]

Public Key Encryption with Keyword Search.

Problem

- Message dependent trapdoor.
- Secure Channel.
- Not decryptable.

Some More Solutions



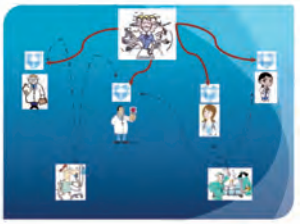
Beak et. al. [ICCSA 2008]

Public Key Encryption with Keyword Search: Revisited.

Problem

- Message dependent trapdoor.
- No Secure Channel.
- Not decryptable.

Some More Solutions



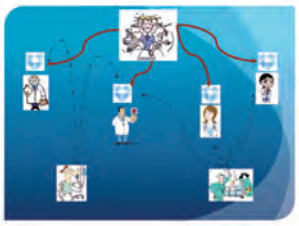
Ibraimi et. al. [ACNS 2011]

Public Key Encryption with Delegated Search.

Problem

- Encryptable and decryptable.
- Master trapdoor.
- Secure Channel.
- Different master keys for different users.

Some More Solutions



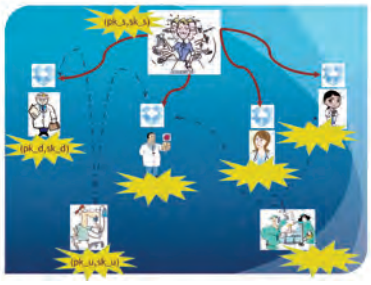
Canard et. al. [CT-RSA 2012]

Plain Text Checkable Encryption.

Problem

- Any body can check.

DPCE Type-I



Some Scenario in an Office

DPCE Type-II

Definition of DPCE (both Type I & II)

Let $k \in \mathbb{N}$ be a security parameter. A DPCE (both Type I & II) is composed of the following algorithms:

- $\mathsf{Setup}(1^k) \rightarrow PP$, where PP contains the public system parameters (particularly includes descriptions of the message space $\mathcal{M}$ and the randomness space $\mathcal{R}$).
- $\mathsf{KeyGen}_C(PP) \rightarrow (pk_C, sk_C)$, the checker's public key/private key pair.
- $\mathsf{KeyGen}_U(PP) \rightarrow (pk_U, sk_U)$, the user's public key/private key pair (pk_U, sk_U). *(In Type II,* KeyGen_U *takes additionally* pk_C *as input along with* PP*.)*
- $\mathsf{Encrypt}(PP, pk_U, pk_C, m) \rightarrow c$, where $m \in \mathcal{M}$.
- $\mathsf{Decrypt}(PP, sk_U, c) \rightarrow m$ or $\perp$.
- $\mathsf{PCheck}(PP, pk_U, sk_C, c, m) \rightarrow 1$ or 0. It outputs 1 if c is an encryption of m and 0 otherwise.

Definition of DPCE (contd.)

The above algorithms must abide by the following correctness properties:

- *Correctness of Decryption:*
  $\forall PP, \forall (pk_C, sk_C) \leftarrow \mathsf{KeyGen}_C, \forall (pk_U, sk_U) \leftarrow \mathsf{KeyGen}_U, \forall m \in \mathcal{M},$
  $\mathsf{Decrypt}(PP, sk_U, \mathsf{Encrypt}(PP, pk_U, pk_C, m)) = m.$
- *Correctness of Plaintext Check:*
  $\forall PP, \forall (pk_C, sk_C) \leftarrow \mathsf{KeyGen}_C, \forall (pk_U, sk_U) \leftarrow \mathsf{KeyGen}_U, \forall m \in \mathcal{M},$
  $\mathsf{PCheck}(PP, sk_C, m, \mathsf{Encrypt}(PP, pk_U, pk_C, m)) = 1.$

Security Notions for DPCE

Security notions for DPCE consists of three types of adversary:

- External Adversary (other than designated checker or user) may try to get some partial information about the messages being encrypted.
- Designated Checker, *Charlie* may try to get something '**more**' than plaintext checkability, and
- Users (both sender *Alice* and receiver *Bob*) may try to '**fool**' the boss by communicating the intended message without being traced.

The last security notion is needed only for DPCE of Type-II.

Indistinguishability against External Adversary

IND-DPCE-CPA

IND-DPCE-CPA is defined as an abstract game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ in a DPCE as follows:

- **Set up:** $\mathcal{C}$ runs Setup$(1^k) \rightarrow PP$, $KeyGen_U(PP) \rightarrow (pk_U, sk_U)$, $KeyGen_C(PP) \rightarrow (pk_C, sk_C)$ and gives PP, pk_U, pk_C to $\mathcal{A}$.
- **Challenge Phase:** $\mathcal{A}$ chooses and sends two plaintexts m_0, m_1 with $|m_0| = |m_1|$ to $\mathcal{C}$. $\mathcal{C}$ chooses a bit $b \in_R \{0,1\}$, computes $c^* = \text{Encrypt}(PP, pk_U, pk_C, m_b)$ and gives c^* to $\mathcal{A}$.
- **Output Phase:** $\mathcal{A}$ outputs a bit b'.

The *advantage of* $\mathcal{A}$ in this game is given by

$$\text{Adv}_{\mathcal{A}} = 2Pr[b = b'] - 1.$$

Unlinkability against Designated Checker

- The classical property of indistinguishability (for public-key encryption schemes) cannot be achieved for the designated checker due to its ability to check the plaintext messages.
- Though one-wayness against the designated checker is sufficient in most of the cases, in some applications it is not enough.
- In the unlinkability game, the adversary's task is to decide whether two encryptions given as challenge are encryptions of same message or not.
- As an alternative, unlinkability stop the adversary from deciding whether two encryptions are of same message.

UNLINK-CPA against Designated Checker

- **Set up:** $\mathcal{C}$ runs Setup$(1^k) \rightarrow PP$, $KeyGen_U(PP)$ $\rightarrow (pk_U, sk_U)$, $KeyGen_C(PP) \rightarrow (pk_C, sk_C)$ and gives $1^k, PP, pk_U, pk_C, sk_C$ to $\mathcal{A}_1$ and $\mathcal{A}_2$.
- **Challenge Phase:** $\mathcal{A}_1 \rightarrow m_0, m_1$. $\mathcal{C}$ chooses a random bit $b \in_R \{0,1\}$ and computes ${c_0}^* = \text{Encrypt}(pk_U, pk_C, m_b)$ & ${c_1}^* = \text{Encrypt}(pk_U, pk_C, m_1)$ and gives $({c_0}^*, {c_1}^*)$ to $\mathcal{A}_2$.
- **Output Phase:** $\mathcal{A}_2$ outputs a bit b'.

The *advantage of* $\mathcal{A}$ in this game is given by

$$\text{Adv}_{\mathcal{A}} = 2Pr[b = b'] - 1.$$

It is assumed that $\mathcal{A}_1$ & $\mathcal{A}_2$ share neither state nor coins and m_0, m_1.

Security against Malicious Users

The users, in DPCE of Type-II, can be malicious in two ways:

- The sender may send a ciphertext c to the receiver, who decrypts it to get the intended message m, but the PCheck algorithm of Boss outputs 0, when fed with (sk_C, c, m).
- The sender may send c which decrypts to m for the receiver, but for some other message m', PCheck(sk_C, c, m') is 1.

This motivates the notions of completeness and soundness, which we define next.

Completeness and Soundness

Completeness

This property states if a ciphertext decrypts to a plaintext then PCheck matches them i.e., that no adversary should be able to output a ciphertext c which decrypts to a message that is refused by PCheck on input c.

Formally, for every $(pk_U, sk_U), (pk_C, sk_C)$ and every ppt. algorithm $\mathcal{A}$ that, on inputs pk_U, pk_C, outputs a ciphertext c, the following probability should be negligible:

$$Pr[\forall (pk_U, sk_U), (pk_C, sk_C), c \leftarrow \mathcal{A}(pk_U, pk_C), m \leftarrow \text{Decrypt}(sk_U, c) : \text{PCheck}(sk_C, pk_U, m, c) = 0]$$

Completeness and Soundness

Soundness

This property states if PCheck matches a ciphertext to a plaintext then the former encrypts the latter i.e., that no adversary should be able to produce a plaintext and ciphertext such that the decryption and the check procedures do not agree on the plaintext related to c.

Formally, for every $(pk_U, sk_U), (pk_C, sk_C)$ and every ppt. algorithm $\mathcal{A}$ that, on inputs pk_U, pk_C, outputs a ciphertext c and a plaintext m, the following probability should be negligible:

$$\Pr[\forall (pk_U, sk_U), (pk_C, sk_C), (c, m') \leftarrow \mathcal{A}(pk_U, pk_C), m \leftarrow \text{Decrypt}(sk_U, c) : m \neq m' \wedge \text{PCheck}(sk_C, pk_U, m', c) = 1]$$

DPCE of Type-I

Construction-I

We construct $\overline{\Pi} = (\overline{\text{Setup}}, \overline{\text{KeyGen}_U}, \overline{\text{KeyGen}_C}, \overline{\text{Encrypt}}, \overline{\text{Decrypt}}, \overline{\text{PCheck}})$ with the message space $\mathcal{M}$ and the ciphertext space as $\{0,1\}^{t+l}$, using

- a probabilistic PKE, $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$, with message space $\mathcal{M}$, randomness space $\mathcal{R}$ and ciphertext space $\{0,1\}^t$.
- a hash function $H : \mathcal{M} \times \mathcal{R} \rightarrow \mathcal{R}$.
- a one-way (injective) trapdoor function $f : \mathcal{R} \rightarrow \{0,1\}^l$

as shown in figure below:

Construction-I

$\overline{\text{Setup}}(1^\sigma) \rightarrow$	$\overline{\text{KeyGen}_U}(PP)$	$\overline{\text{KeyGen}_C}(PP)$
Public Parameter PP Message space $\mathcal{M}$, Randomness space $\mathcal{R}$	$\text{Gen}(PP) \rightarrow (pk, sk)$ Set $pk_U = pk$ $sk_U = sk$	Choose $f : \mathcal{R} \rightarrow \{0,1\}^l$ with trapdoor tr and a hash fn. $H : \mathcal{M} \times \mathcal{R} \rightarrow \mathcal{R}$ Set $pk_C = (f, H)$, $sk_C = \text{tr}$

$\overline{\text{Encrypt}} : (m \in \mathcal{M}, pk_U, pk_C)$	$\overline{\text{Decrypt}} : (\overline{c} = (c, \alpha), sk_U)$	$\overline{\text{PCheck}} : (m \in \mathcal{M}, \overline{c} = (c, \alpha), sk_C)$
Choose $r \in_R \mathcal{R}$ Compute $\alpha = f(r)$, $\rho = H(m\|\|r)$ $c = \text{Enc}(pk_U, m, \rho)$ Output $\overline{c} = (c, \alpha)$	Output $\text{Dec}(sk_U, c)$	Compute $r' = \text{tr}(\alpha)$, $\rho' = H(m\|\|r')$ and $c' = \text{Enc}(pk, m, \rho')$ If $c = c'$, output 1, else 0.

Construction-I: Security Analysis

Theorem

$\overline{\Pi}$ is IND-CPA secure from an external adversary in random oracle model if Π is IND-CPA secure and f is one-way.

Theorem

$\overline{\Pi}$ is UNLINK against a designated checker in random oracle model, if Π is IND-CPA.

DPCE of Type-I

Construction-II

We construct $\overline{\Pi} = (\overline{\text{Setup}}, \overline{\text{KeyGen}_U}, \overline{\text{KeyGen}_C}, \overline{\text{Encrypt}}, \overline{\text{Decrypt}}, \overline{\text{PCheck}})$ with the message space $\{0,1\}^l$ and the ciphertext space as $\{0,1\}^{t+2l}$, using

- a deterministic PKE, $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$, with message space $\{0,1\}^l$ and ciphertext space $\{0,1\}^t$.
- two hash functions $H_1, H_2 : \{0,1\}^* \rightarrow \{0,1\}^l$.
- a one-way (injective) trapdoor function $f : \{0,1\}^l \rightarrow \{0,1\}^l$

as shown in figure below:

Construction-II

$\overline{\text{Setup}}(1^\sigma) \rightarrow$	$\overline{\text{KeyGen}_U}(PP)$	$\overline{\text{KeyGen}_C}(PP)$
Public Parameter PP Message space $\{0,1\}^l$,	$\text{Gen}(PP) \rightarrow (pk, sk)$ Set $pk_U = pk$ $sk_U = sk$	Choose $f : \{0,1\}^l \rightarrow \{0,1\}^l$ with trapdoor tr and 2 hash fns. $H_1, H_2 : \{0,1\}^* \rightarrow \{0,1\}^l$ Set $pk_C = (f, H_1, H_2)$, $sk_C = \text{tr}$

$\overline{\text{Encrypt}} : (m \in \{0,1\}^l, pk_U, pk_C)$	$\overline{\text{Decrypt}} : (\overline{c}, sk_U)$	$\overline{\text{PCheck}} : (m \in \{0,1\}^l, \overline{c}, sk_C)$
Choose $r \in_R \{0,1\}^l$ Compute $\alpha = f(r)$, $\rho = H(m\|\|r)$, $c_1 = \text{Enc}(pk, \rho)$, $c_2 = m \oplus H_2(\rho)$, Output $\overline{c} = (c_1, c_2, \alpha)$	Set $\rho = \text{Dec}(sk_U, c_1)$ Return $m = c_2 \oplus H_2(\rho)$	Compute $r' = \text{tr}(\alpha)$, $\rho' = H_1(m\|\|r')$ $c_1' = \text{Enc}(pk, \rho')$, $c_2' = m \oplus H_2(\rho')$ If $(c_1', c_2') = (c_1, c_2)$, output 1, else 0.

Construction-II: Security Analysis

Theorem

$\overline{\Pi}$ *is IND-CPA secure from an external adversary in random oracle model if* Π *and* f *are one-way.*

Theorem

$\overline{\Pi}$ *is UNLINK against a designated checker in random oracle model, if* Π *is one-way.*

Construction-I & II does not satisfy completeness

- In case of Construction-I, $\mathcal{A}$ chooses $m \in \mathcal{M},\ r, r' \in \mathcal{R}$ and computes $\rho = H(m||r), \alpha = f(r'), c = \mathsf{Enc}(m, \rho)$ and outputs $\overline{c} = (c, \alpha)$. Now, it is obvious that $\overline{\mathsf{Dec}}(\overline{c}) = m$, but $\overline{\mathsf{PCheck}}(sk_C, pk_U, \overline{c}, m) = 0$.
- In case of construction-II, $\mathcal{A}$ chooses $m \in \{0,1\}^l,\ r, r' \in \{0,1\}^l$ and computes $\rho = H(m||r), \alpha = f(r'), \overline{c_1} = \mathsf{Enc}(pk, \rho), \overline{c_2} = m \oplus H_2(\rho)$ and outputs $\overline{c} = (\overline{c_1}, \overline{c_2}, \alpha)$. Now, it is obvious that $\overline{\mathsf{Dec}}(\overline{c}) = m$, but $\overline{\mathsf{PCheck}}(sk_C, pk_U, \overline{c}, m) = 0$.

DPCE of Type-II

Construction-III

We construct $\overline{\Pi} = (\overline{\mathsf{Setup}}, \overline{\mathsf{KeyGen}_U}, \overline{\mathsf{KeyGen}_C}, \overline{\mathsf{Encrypt}}, \overline{\mathsf{Decrypt}}, \overline{\mathsf{PCheck}})$ with message space $\{0,1\}^{l'}$ and ciphertext space as $\{0,1\}^{t+t'}$, using

- a deterministic PKE, $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$, with message space $\{0,1\}^{l'}$ and ciphertext space $\{0,1\}^{t'}$.
- a PKE with double decryption mechanism (DD-PKE), $\Pi = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec1}, \mathsf{Dec2})$, with message space $\{0,1\}^{l}$ and ciphertext space $\{0,1\}^{t}$.
- a pseudo-random generator $G : \{0,1\}^{l} \to \{0,1\}^{l'}$.

as shown in figure below:

Construction-III

$\overline{\mathsf{Setup}}(1^k) \to$	$\overline{\mathsf{KeyGen}_C}(PP)$	$\overline{\mathsf{KeyGen}_U}(PP, PK)$
Public Parameter $PP = (l, l')$,	$\mathsf{Setup}(PP) \to (PK, SK)$ Choose a PRG $G : \{0,1\}^l \to \{0,1\}^{l'}$, Set $pk_C = (PK, G)$, $sk_C = SK$	$\mathsf{Gen}(PK) \to (pk, sk)$ $\mathsf{Gen}'(PP) \to (pk', sk')$ Set $pk_U = (pk, pk')$, $sk_U = (sk, sk')$

$\overline{\mathsf{Encrypt}} : (m \in \{0,1\}^{l'}, pk_U, pk_C)$	$\overline{\mathsf{Decrypt}} : (\overline{c}, sk_U)$	$\overline{\mathsf{PCheck}} : (m \in \{0,1\}^{l'}, \overline{c}, sk_C)$
Choose $r \in_R \{0,1\}^l$ Set $\alpha = \mathsf{Enc}(PK, pk, r)$, $c = \mathsf{Enc}'(pk', m \oplus G(r))$. Output $\overline{c} = (c, \alpha)$	Set $r = \mathsf{Dec1}(sk, \alpha)$ Return $m = \mathsf{Dec}'(sk', c) \oplus G(r)$	Compute $\hat{r} = \mathsf{Dec2}(SK, \alpha)$ If $\mathsf{Enc}'(pk', m \oplus G(\hat{r})) = c$, output 1, else 0.

Construction-III: Security Analysis

Theorem

$\overline{\Pi}$ *is IND-CPA secure from an external adversary in random oracle model if* Π *is one-way.*

Theorem

$\overline{\Pi}$ *is one-way against a designated checker in standard model if* Π' *is one-way.*

Theorem

$\overline{\Pi}$ *satisfies completeness and soundness against a malicious user.*

DPCE of Type-II

Construction-IV

We construct $\overline{\Pi} = (\overline{\mathsf{Setup}}, \overline{\mathsf{KeyGen}_U}, \overline{\mathsf{KeyGen}_C}, \overline{\mathsf{Encrypt}}, \overline{\mathsf{Decrypt}}, \overline{\mathsf{PCheck}})$ with message space $\{0,1\}^{l}$, using

- a deterministic PKE, $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$, with message space $\{0,1\}^{l}$ and ciphertext space $\{0,1\}^{t}$.
- a PKE with double decryption mechanism (DD-PKE), $\Pi = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec1}, \mathsf{Dec2})$, with message space $\{0,1\}^{t}$.

as shown in figure below:

Construction-IV

$\overline{\text{Setup}}(1^\lambda) \rightarrow$	$\overline{\text{KeyGen}_C}(PP)$	$\overline{\text{KeyGen}_U}(PP, PK)$
Public Parameter $PP = l$	Setup$(PP) \rightarrow (PK, SK)$ Set $pk_C = PK$, $sk_C = SK$	Gen$(PK) \rightarrow (pk, sk)$ Gen$'(PP) \rightarrow (pk', sk')$ Set $pk_U = (pk, pk')$, $sk_U = (sk, sk')$

$\overline{\text{Encrypt}} : (m \in \{0,1\}^l,$ $pk_U, pk_C)$	$\overline{\text{Decrypt}} : (\overline{\sigma}, sk_U)$	$\overline{\text{PCheck}} : m \in \{0,1\}^l, \overline{\sigma}, sk_C$
Output $\overline{\sigma} =$ Enc$(PK, pk,$ Enc$'(pk', m))$	Compute Dec1$(sk, \overline{\sigma}) = \hat{c}$ or $\perp$ If Dec1$(sk, \overline{\sigma}) \neq \perp$, Output $m =$ Dec$'(sk, \hat{c})$	If Dec2$(SK, \overline{\sigma}) =$ Enc$'(pk', m)$, output 1, else 0.

Construction-IV: Security Analysis

Theorem

$\overline{\Pi}$ *is IND-CPA secure from an external adversary in standard model if* Π *is IND-CPA secure.*

Theorem

$\overline{\Pi}$ *is one-way against a designated checker if* Π' *is one-way.*

Theorem

$\overline{\Pi}$ *satisfies completeness and soundness against a malicious user.*

Comparison

Construction	I	II	III	IV
DPCE of Type	I	I	II	II
External adversary	IND-CPA ROM	IND-CPA ROM	IND-CPA ROM	IND-CPA Std.M
Completeness & Soundness	No	No	Yes Std.M	Yes Std.M
Designated Checker	UNLINK ROM	UNLINK ROM	OW Std.M	OW Std.M

Table: Comparison between Construction I, II, III and IV

Bibliography

Boneh, D., Crescenzo, G.D., Ostrovsky, R., Persiano, G.: Public Key Encryption with Keyword Search, EUROCRYPT 2004, LNCS 3027, 506-522, 2004.

Baek, J., Safavi-Naini, R., Susilo, W.: Public Key Encryption with Keyword Search Revisited, ICCSA 2008, Part I, LNCS 5072, 1249-1259, 2008.

Lu, Y., Zhang, R., Lin, D.: Stronger Security Model for Public-Key Encryption with Equality Test, PAIRING 2012, LNCS 7708, 65-82, 2013.

Canard, S., Fuchsbauer, G., Gouget, A. Laguillaumie, F.: Plaintext-Checkable En- cryption, CT-RSA 2012, LNCS 7178, 332-348, 2012.

Questions

Questions???

Improvement of Faugère *et al.*'s method to solve ECDLP

○ Huang Yun-Ju *
Christophe Petit *
Naoyuki Shinohara †
Tsuyoshi Takagi ‡

*Graduate School of Mathematics, Kyushu University
* UCL Crypto Group
† NICT
‡ Institute of Mathematics for Industry, Kyushu University

August 29, 2013

Abstract

- Target : ECDLP problem.
- Motivation : A new technique for index calculus method algorithm to solve ECDLP proposed by Faugère *et al.* at Eurocrypt 2012.
- Contribution :
  1. Give a new idea to improve the algorithm proposed by Faugère *et al.*
  2. Implements different strategies solving ECDLP and compares them.

Outline

Elliptic Curve Discrete Log Problem (ECDLP)

Let F_{2^n} is a binary field of prime degree n over F_2.

Let $E_{\alpha,\beta} : y^2 + xy = x^3 + \alpha x^2 + \beta$ over field F_{2^n}, where $\alpha, \beta \in F_{2^n}$.
Given $P \in E_{\alpha,\beta}$, $Q \in \langle P \rangle$,

Target

Find smallest non-negative integer k such that $Q = [k]P$

Known Algorithm

- Exhaustive Search
  Time Complexity : $O(2^n)$
- Pollard-rho Mehod
  Time Complexity : $O(2^{\frac{n}{2}})$
- Index Calculus Method
  Time Complexity : claimed to be sub-exponential $O(2^{cn^{2/3}\log n})$ by Petit *et al.* at Asiacrypto 2012.

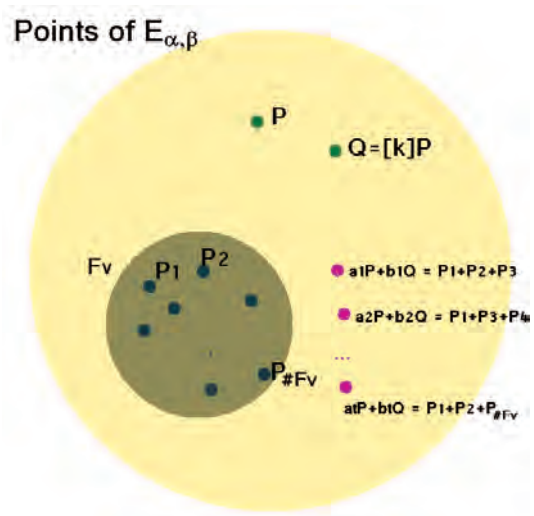
Generic Index Calculus Mehod

Generic Index Calculus Method

Input :	$P, Q \in E_{\alpha,\beta}$
Output :	$k \in N$ such that $Q = [k]P$
phase 1:	Setup factor base $F_V = \{P_i \in E_{\alpha,\beta} \mid x(P_i) \in V\}$
phase 2: Relation Search	Find sufficient relations $sol_m = \{\sum_{1\le j\le m} P'_j = [a]P + [b]Q\}$ for random $a, b \in N$, $P'_j \in F_V$.
phase 3:	Transform the relation to matrix M.
phase 4:	Find reduced echelon form M_- of M.
phase 5:	Solve the relation $[a']P + [b']Q = O$ in M_-. $k = \frac{-a'}{b'}$.

$x(P_i)$ means x-coordinate of P_i.

Generic Index Calculus



Generic Index Calculus Method

$$\begin{array}{c} \begin{matrix} P_1 & P_2 & \dots & P_{\#F_V} & P & Q \end{matrix} \\ \begin{pmatrix} 1 & 1 & & 0 & a_1 & b_1 \\ 1 & 0 & & 0 & a_2 & b_2 \\ \vdots & & \ddots & \vdots & & \vdots \\ 1 & 1 & \dots & 1 & a_t & b_t \end{pmatrix} \end{array}$$

$\Downarrow$ reduced row echelon form

$$\begin{pmatrix} 1 & 0 & & 0 & & \\ 0 & 1 & & 0 & & \\ \vdots & & \ddots & \vdots & & \\ 0 & 0 & \dots & 1 & & \\ 0 & 0 & & 0 & a' & b' \end{pmatrix}$$

Semaev's Polynomials[1]

Property - Semaev's summation polynomial

For $R = [a]P + [b]Q$, **Semaev's summation polynomials** s_{m+1} are multivariate polynomials where :
$\forall x_1, ..., x_m \in F_{2^n}$,

$$s_{m+1}(x_1, x_2, ..., x_m, x_r) = 0$$

if and only if $\exists P'_j, 1 \leq j \leq m$ such that

$$\sum_{1 \leq j \leq m} P'_j + R = O,$$

where $x_j = x(P'_j)$, $x_r = x(R)$.

The problem to find P'_j s.t, $\sum P'_j = R$ is now reduced to solve $s_{m+1}(x_1, , x_m, x_r) = 0$. x_j is variable and x_r is known value.

Version by Faugère *et al.* (FPPR)

In Eurocrypt 2012, Faug'ere, Perret, Petit and Renault proposed a new version to solve the Semaev's summation polynomials by Gröbner basis for phase 2 (Relation Search).

Variable Rewritten

We can regard F_{2^n} as the vector space defined by the basis $\{v_0, v_1, ..., v_{n'-1}\}$.

Variable Substitution

Let $x_j = x(P'_j), P'_j \in F_v$, if we rewrite $x_j = \sum_{0 \le \ell \le n'-1} c_{j,l} v_\ell$, then

$s_{m+1}(x_1, ..., x_m, x_r)$
$= s_{m+1}(\sum_{0 \le \ell \le n'-1} c_{1,\ell} v_\ell, ..., \sum_{0 \le \ell \le n'-1} c_{m,\ell} v_\ell, \sum_{0 \le l \le n-1} r_\ell v_\ell)$

where $c_{j,\ell} \in F_2$ is unknown and r_ℓ is known.

Multivariable Polynomial System

Multivariable Polynomial System

$s_{m+1}(\sum_{0 \le \ell \le n'-1} c_{1,\ell} v_\ell, ..., \sum_{0 \le l \le n'-1} c_{m,\ell} v_\ell, \sum_{0 \le \ell \le n-1} r_\ell v_\ell)$
$= f_0(c_{j,\ell}) v_1 + f_1(c_{j,\ell}) v_2 + ... + f_{n-1}(c_{j,\ell}) v_n$
where $1 \le j \le m, 1 \le \ell \le n'$, $c_{j,\ell} \in F_2$

$s_{m+1} = 0$ over $F_{2^n} \iff f_0 = 0, f_1 = 0, f_{n-1} = 0$ over F_2.

Outline

Symmetric function

Using the fact that Semaev's summation polynomials are symmetric, substitute the polynomials with elementary symmetric functions.

For example :

$$s_3 = (x_1x_2 + x_1x_r + x_2x_r)^2 + x_1x_2x_r + \beta$$
$$= (\sigma_2 + \sigma_1x_r)^2 + \sigma_2x_r + \beta$$

where
$\sigma_1 = x_1 + x_2, \sigma_2 = x_1x_2$, β is the parameter of $E_{\alpha,\beta}$.

Rewritten system for symmetric function

- Variables rewritten
  $x_1 = c_{1,0}v_1 + c_{1,1}v_2 + \ldots + c_{1,n'-1}v_{n'}$
  $x_2 = c_{2,0}v_1 + c_{2,1}v_2 + \ldots + c_{2,n'-1}v_{n'}$
  $\ldots$
  $x_m = c_{m,0}v_1 + c_{m,1}v_2 + \ldots + c_{m,n'-1}v_{n'}$
- Symmetric function rewritten
  $\sigma_1 = d_{1,0}v_1 + d_{1,1}v_2 + \ldots + d_{1,n-1}v_n$
  $\sigma_2 = d_{2,0}v_1 + d_{2,1}v_2 + \ldots + d_{2,n-1}v_n$
  $\ldots$
  $\sigma_m = d_{m,0}v_1 + d_{m,1}v_2 + \ldots + d_{m,n-1}v_n$
- Relation of variables and symmetric function
  $d_{1,0} = f_{1,0}(c_{i,j})$
  $d_{1,1} = f_{1,1}(c_{i,j})$
  $\ldots$
  $d_{m,n-1} = f_{m,n-1}(c_{i,j})$

Symmetric function

- Using symmetric function for s_{m+1} is not a new idea. Gaudry, Diem, Joux and Vitse proposed this in composite extension degree.[2, 3, 4, 5]
- However, in prime extension degree makes the number of variables and number of polynomials grows too large. This makes it impracticable.

Special factor base V

Let $F_{2^n} = F_2[\omega]/h(\omega)$, where $h(\omega)$ is an irreducible polynomial of prime degree n over F_2.

Using the special factor base $V = \{1, \omega, ..., \omega^{n'-1}\}$.

Rewritten system for symmetric function

- Variables rewritten
  $x_1 = c_{1,0} + c_{1,1}\omega + ... + c_{1,n'-1}\omega^{n'-1}$
  $x_2 = c_{2,0} + c_{2,1}\omega + ... + c_{2,n'-1}\omega^{n'-1}$
  ...
  $x_m = c_{m,0} + c_{m,1}\omega + ... + c_{m,n'-1}\omega^{n'-1}$
- Symmetric function rewritten
  $\sigma_1 = d_{1,0} + d_{1,1}\omega + ... + d_{1,n'-1}\omega^{n'-1}$
  $\sigma_2 = d_{2,0} + d_{2,1}\omega + ... + d_{2,n'-2}\omega^{2n'-2}$
  ...
  $\sigma_2 = d_{m,0} + d_{m,1}\omega + ... + d_{m,n'-m}\omega^{n-m}$
- Relation of variables and symmetric function
  $d_{1,0} = f_{1,0}(c_{i,j})$
  $d_{1,1} = f_{1,1}(c_{i,j})$
  ...
  $d_{m,n'-m} = f_{m,n'-m}(c_{i,j})$

Symmetric function with specific vector base V

	s_{m+1}	s'_{m+1}	s'_{m+1} with specific V
#var	mn'	$mn' + mn$	$mn' + (n'-1)\frac{m(m+1)}{2} + m$
#poly	n	$n + mn$	$n + (n'-1)\frac{m(m+1)}{2} + m$
$\deg_{reg}$	7 or 6	4 or 3	4 or 3

Table: Comparison for different multivariate polynomial system

The time and memory costs are respectively roughly $\#var^{2*deg_{reg}}$ and $\#var^{3*deg_{reg}}$.

Experimental Results

CPU : AMD Opteron 6276*4, 16 cores, 2.3GHz, L3 cache 16MB
OS : CentOS 6.3
RAM : 512 GB
Platform : Magma V2.18-9 64-bit version

Experimental Results

Using Magma to finding one relation $\sum P_i = [a]P + [b]Q$.

	n	n'	sol: yes						
			D_{reg}	var	poly	mono	t_{trans}	t_{groe}	mem
Imp_{FPPR}	23	3	6	9	23	2792.97	5.47	1.06	29.10
Imp_{Ours}	23	3	3	24	38	1079.60	0.91	1.04	15.59
Imp_{FPPR}	53	3	6	9	53	6358.94	12.86	1.03	72.06
Imp_{Ours}	53	3	3	24	68	2348.50	2.12	0.79	24.89
Imp_{FPPR}	23	4	6	12	23	12059.19	21.06	6.83	95.66
Imp_{Ours}	23	4	3	33	44	2173.29	1.83	3.19	29.63
Imp_{FPPR}	53	4	6	12	53	27655.34	50.63	1.86	272.55
Imp_{Ours}	53	4	3	33	74	4701.09	4.19	1.75	40.46

Table: Comparison of the relation search ($m = 3$, $n' = 3, 4$) with two strategies, Imp_{FPPR} and Imp_{Ours}. Units are sec and MB

Experimental Results

Using Magma to finding one relation $\sum P_i = [a]P + [b]Q$.

	n	n'	sol: yes						
			D_{reg}	var	poly	mono	t_{trans}	t_{groe}	mem
Imp_{FPPR}	23	5	7	15	23	40168.90	64.67	70.46	475.55
Imp_{Ours}	23	5	4	42	50	3572.00	3.01	157.86	323.60
Imp_{FPPR}	53	5	6	15	53	91642.50	147.66	80.76	810.08
Imp_{Ours}	53	5	3	42	80	8034.10	6.83	6.68	59.58
Imp_{FPPR}	23	6	7	18	23	107008.67	163.45	3888.70	6656.13
Imp_{Ours}	23	6	4	51	56	5270.00	4.36	5150.12	4791.31
Imp_{FPPR}	53	6	7	18	53	245891.33	366.92	2967.03	7311.44
Imp_{Ours}	53	6	3	51	86	11748.00	10.48	34.82	151.04

Table: Comparison of the relation search ($m = 3$, $n' = 4, 5$) with two strategies, Imp_{FPPR} and Imp_{Ours}. Units are sec and MB

Experimental Results

Using Magma to solve ECDLP.

n	$\#E_{\alpha,\beta}$	Imp_{FPPR}	Imp_{Ours}
7	4*37	1.574	0.864
11	4*523	8.625	6.702
13	4*2089	49.698	31.058
17	4*32941	2454.470	1364.742
19	4*131431	22474.450	9962.861

Table: Comparison of two ECDLP strategies, Imp_{FPPR} and Imp_{Ours}. The last two columns are computing time in seconds.

Conlusion

- This work has been accepted by IWSEC2013.
- We give the experimental evidence of our improvements.
- Future work - parallization.

Thanks

Q & A

Reference I

I. Semaev, "Summation polynomials and the discrete logarithm problem on elliptic curves," *IACR Cryptology ePrint Archive*, vol. 2004, p. 31, 2004.

C. Diem, "An index calculus algorithm for plane curves of small degree," in Hess *et al.* [14], pp. 543–557.

P. Gaudry, "Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem," *Journal of Symbolic Computation*, vol. 44, no. 12, pp. 1690 – 1702, 2009.

C. Diem, "On the discrete logarithm problem in elliptic curves," *Compositio Mathematica*, vol. 147, pp. 75–104, 2011.

A. Joux and V. Vitse, "Elliptic curve discrete logarithm problem over small degree extension fields," *Journal of Cryptology*, pp. 1–25, 2011.

C. Petit and J.-J. Quisquater, "On polynomial systems arising from a weil descent," in *Advances in Cryptology ASIACRYPT 2012* (X. Wang and K. Sako, eds.), vol. 7658 of *Lecture Notes in Computer Science*, pp. 451–466, Springer Berlin Heidelberg, 2012.

D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003.

I. Blake, G. Seroussi, N. Smart, and J. W. S. Cassels, *Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series)*. New York, NY, USA: Cambridge University Press, 2005.

T. Saito, S. Yokoyama, T. Kobayashi, and G. Yamamoto, "Some relations between semaev's summation polynomials and stange's elliptic nets," *Journal of Math-for-Industry*, vol. 3 (2011A-9), pp. 89–92, 2011.

Reference II

- R. P. Brent, "An improved monte carlo factorization algorithm," *BIT Numerical Mathematics*, vol. 20, pp. 176–184, 1980.
- J. M. Pollard, "A monte carlo method for factorization," *BIT Numerical Mathematics*, vol. 15 (3), pp. 331–334, 1975.
- J.-C. Faugre, L. Perret, C. Petit, and G. Renault, "Improving the complexity of index calculus algorithms in elliptic curves over binary field," in *Proceedings of Eurocrypt 2012*, vol. 7237 of *Lecture Notes in Computer Science*, pp. 27–44, Springer Verlag, 2012.
- J. H. Silverman, "The xedni calculus and the elliptic curve discrete logarithm problem," *Designs, Codes and Cryptography*, vol. 20, pp. 5–40, 1999.
- F. Hess, S. Pauli, and M. E. Pohst, eds., *Algorithmic Number Theory, 7th International Symposium, ANTS-VII, Berlin, Germany, July 23-28, 2006, Proceedings*, vol. 4076 of *Lecture Notes in Computer Science*, Springer, 2006.
- J.-C. Faugère, "A new efficient algorithm for computing gröbner bases (f_4)," *Journal of Pure and Applied Algebra*, vol. 139, no. 1-3, pp. 61–88, 1999.
- J. C. Faugère, "A new efficient algorithm for computing gröbner bases without reduction to zero (f_5)," in *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, ISSAC '02, (New York, NY, USA), pp. 75–83, ACM, 2002.
- J. Faugère, P. Gianni, D. Lazard, and T. Mora, "Efficient computation of zero-dimensional gröbner bases by change of ordering," *Journal of Symbolic Computation*, vol. 16, no. 4, pp. 329 – 344, 1993.

Reference III

- J. M. Pollard, "Kangaroos, monopoly and discrete logarithms," *Journal of Cryptology*, vol. 13, pp. 437–447, 2000.
- D. Shanks, "Class number, a theory of factorization, and genera," in *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pp. 415–440, 1971.
- D. Bernstein, H.-C. Chen, C.-M. Cheng, T. Lange, R. Niederhagen, P. Schwabe, and B.-Y. Yang, "Ecc2k-130 on nvidia gpus," in *Progress in Cryptology - INDOCRYPT 2010* (G. Gong and K. Gupta, eds.), vol. 6498 of *Lecture Notes in Computer Science*, pp. 328–346, Springer Berlin Heidelberg, 2010.
- L. Judge, S. Mane, and P. Schaumont, "A hardware-accelerated ecdlp with high-performance modular multiplication," *International Journal of Reconfigurable Computing*, vol. 2012, 2012.

MI レクチャーノートシリーズ刊行にあたり

本レクチャーノートシリーズは、文部科学省 21 世紀 COE プログラム「機能数理学の構築と展開」(H.15-19 年度) において作成した COE Lecture Notes の続刊であり、文部科学省大学院教育改革支援プログラム「産業界が求める数学博士と新修士養成」(H19-21 年度) および、同グローバル COE プログラム「マス・フォア・インダストリ教育研究拠点」(H.20-24 年度) において行われた講義の講義録として出版されてきた。平成 23 年 4 月のマス・フォア・インダストリ研究所 (IMI) 設立と平成 25 年 4 月の IMI の文部科学省共同利用・共同研究拠点として「産業数学の先進的・基礎的共同研究拠点」の認定を受け、今後、レクチャーノートは、マス・フォア・インダストリに関わる国内外の研究者による講義の講義録、会議録等として出版し、マス・フォア・インダストリの本格的な展開に資するものとする。

平成 25 年 9 月
マス・フォア・インダストリ研究所
所長　若山正人

平成25年度　九州大学マス・フォア・インダストリ研究所　共同利用研究集会

安全・安心社会基盤構築のための代数構造

～サイバー社会の信頼性確保のための数理学～

発　行　　2013年12月26日
編　集　　四方義啓、櫻井幸一、安田貴徳、グザヴィエ・ダハン
発　行　　九州大学マス・フォア・インダストリ研究所
九州大学大学院数理学府
〒819-0395 福岡市西区元岡744
九州大学数理・IMI 事務室
TEL 092-802-4402　FAX 092-802-4405
URL http://www.imi.kyushu-u.ac.jp/

印　刷　　城島印刷株式会社
〒810-0012 福岡市中央区白金 2 丁目 9 番 6 号
TEL 092-531-7102　FAX 092-524-4411

シリーズ既刊

Issue	Author／Editor	Title	Published
COE Lecture Note	Mitsuhiro T. NAKAO Kazuhiro YOKOYAMA	Computer Assisted Proofs - Numeric and Symbolic Approaches - 199pages	August 22, 2006
COE Lecture Note	M.J.Shai HARAN	Arithmetical Investigations - Representation theory, Orthogonal polynomials and Quantum interpolations- 174pages	August 22, 2006
COE Lecture Note Vol.3	Michal BENES Masato KIMURA Tatsuyuki NAKAKI	Proceedings of Czech-Japanese Seminar in Applied Mathematics 2005 155pages	October 13, 2006
COE Lecture Note Vol.4	宮田　健治	辺要素有限要素法による磁界解析 - 機能数理学特別講義 21pages	May 15, 2007
COE Lecture Note Vol.5	Francois APERY	Univariate Elimination Subresultants - Bezout formula, Laurent series and vanishing conditions - 89pages	September 25, 2007
COE Lecture Note Vol.6	Michal BENES Masato KIMURA Tatsuyuki NAKAKI	Proceedings of Czech-Japanese Seminar in Applied Mathematics 2006 209pages	October 12, 2007
COE Lecture Note Vol.7	若山　正人 中尾　充宏	九州大学産業技術数理研究センター キックオフミーティング 138pages	October 15, 2007
COE Lecture Note Vol.8	Alberto PARMEGGIANI	Introduction to the Spectral Theory of Non-Commutative Harmonic Oscillators 233pages	January 31, 2008
COE Lecture Note Vol.9	Michael I.TRIBELSKY	Introduction to Mathematical modeling 23pages	February 15, 2008
COE Lecture Note Vol.10	Jacques FARAUT	Infinite Dimensional Spherical Analysis 74pages	March 14, 2008
COE Lecture Note Vol.11	Gerrit van DIJK	Gelfand Pairs And Beyond 60pages	August 25, 2008
COE Lecture Note Vol.12	Faculty of Mathematics, Kyushu University	Consortium “MATH for INDUSTRY” First Forum 87pages	September 16, 2008
COE Lecture Note Vol.13	九州大学大学院 数理学研究院	プロシーディング「損保数理に現れる確率モデル」 ― 日新火災・九州大学 共同研究 2008 年 11 月 研究会 ― 82pages	February 6, 2009

シリーズ既刊

Issue	Author／Editor	Title	Published
COE Lecture Note Vol.14	Michal Beneš, Tohru Tsujikawa Shigetoshi Yazaki	Proceedings of Czech-Japanese Seminar in Applied Mathematics 2008 77pages	February 12, 2009
COE Lecture Note Vol.15	Faculty of Mathematics, Kyushu University	International Workshop on Verified Computations and Related Topics 129pages	February 23, 2009
COE Lecture Note Vol.16	Alexander Samokhin	Volume Integral Equation Method in Problems of Mathematical Physics 50pages	February 24, 2009
COE Lecture Note Vol.17	矢嶋　　徹 及川　正行 梶原　健司 辻　　英一 福本　康秀	非線形波動の数理と物理 66pages	February 27, 2009
COE Lecture Note Vol.18	Tim Hoffmann	Discrete Differential Geometry of Curves and Surfaces 75pages	April 21, 2009
COE Lecture Note Vol.19	Ichiro Suzuki	The Pattern Formation Problem for Autonomous Mobile Robots —Special Lecture in Functional Mathematics— 23pages	April 30, 2009
COE Lecture Note Vol.20	Yasuhide Fukumoto Yasunori Maekawa	Math-for-Industry Tutorial: Spectral theories of non-Hermitian operators and their application 184pages	June 19, 2009
COE Lecture Note Vol.21	Faculty of Mathematics, Kyushu University	Forum “Math-for-Industry” Casimir Force, Casimir Operators and the Riemann Hypothesis 95pages	November 9, 2009
COE Lecture Note Vol.22	Masakazu Suzuki Hoon Hong Hirokazu Anai Chee Yap Yousuke Sato Hiroshi Yoshida	The Joint Conference of ASCM 2009 and MACIS 2009: Asian Symposium on Computer Mathematics Mathematical Aspects of Computer and Information Sciences 436pages	December 14, 2009
COE Lecture Note Vol.23	荒川　恒男 金子　昌信	多重ゼータ値入門 111pages	February 15, 2010
COE Lecture Note Vol.24	Fulton B.Gonzalez	Notes on Integral Geometry and Harmonic Analysis 125pages	March 12, 2010
COE Lecture Note Vol.25	Wayne Rossman	Discrete Constant Mean Curvature Surfaces via Conserved Quantities 130pages	May 31, 2010
COE Lecture Note Vol.26	Mihai Ciucu	Perfect Matchings and Applications 66pages	July 2, 2010

シリーズ既刊

Issue	Author／Editor	Title	Published
COE Lecture Note Vol.27	九州大学大学院 数理学研究院	Forum “Math-for-Industry” and Study Group Workshop Information security, visualization, and inverse problems, on the basis of optimization techniques 100pages	October 21, 2010
COE Lecture Note Vol.28	ANDREAS LANGER	MODULAR FORMS, ELLIPTIC AND MODULAR CURVES LECTURES AT KYUSHU UNIVERSITY 2010 62pages	November 26, 2010
COE Lecture Note Vol.29	木田　雅成 原田　昌晃 横山　俊一	Magma で広がる数学の世界 157pages	December 27, 2010
COE Lecture Note Vol.30	原　　隆 松井　　卓 廣島　文生	Mathematical Quantum Field Theory and Renormalization Theory 201pages	January 31, 2011
COE Lecture Note Vol.31	若山　正人 福本　康秀 高木　　剛 山本　昌宏	Study Group Workshop 2010 Lecture & Report 128pages	February 8, 2011
COE Lecture Note Vol.32	Institute of Mathematics for Industry, Kyushu University	Forum “Math-for-Industry” 2011 “TSUNAMI-Mathematical Modelling” Using Mathematics for Natural Disaster Prediction, Recovery and Provision for the Future 90pages	September 30, 2011
COE Lecture Note Vol.33	若山　正人 福本　康秀 高木　　剛 山本　昌宏	Study Group Workshop 2011 Lecture & Report 140pages	October 27, 2011
COE Lecture Note Vol.34	Adrian Muntean Vladimír Chalupecký	Homogenization Method and Multiscale Modeling 72pages	October 28, 2011
COE Lecture Note Vol.35	横山　俊一 夫　　紀恵 林　　卓也	計算機代数システムの進展 210pages	November 30, 2011
COE Lecture Note Vol.36	Michal Beneš Masato Kimura Shigetoshi Yazaki	Proceedings of Czech-Japanese Seminar in Applied Mathematics 2010 107pages	January 27, 2012
COE Lecture Note Vol.37	若山　正人 高木　　剛 Kirill Morozov 平岡　裕章 木村　正人 白井　朋之 西井　龍映 栄　伸一郎 穴井　宏和 福本　康秀	平成 23 年度 数学・数理科学と諸科学・産業との連携研究ワークショップ　拡がっていく数学　～期待される “見えない力” ～ 154pages	February 20, 2012

シリーズ既刊

Issue	Author／Editor	Title	Published
COE Lecture Note Vol.38	Fumio Hiroshima Itaru Sasaki Herbert Spohn Akito Suzuki	Enhanced Binding in Quantum Field Theory 204pages	March 12, 2012
COE Lecture Note Vol.39	Institute of Mathematics for Industry, Kyushu University	Multiscale Mathematics: Hierarchy of collective phenomena and interrelations between hierarchical structures 180pages	March 13, 2012
COE Lecture Note Vol.40	井ノ口順一 太田　泰広 筧　三郎 梶原　健司 松浦　望	離散可積分系・離散微分幾何チュートリアル 2012 152pages	March 15, 2012
COE Lecture Note Vol.41	Institute of Mathematics for Industry, Kyushu University	Forum “Math-for-Industry” 2012 “Information Recovery and Discovery” 91pages	October 22, 2012
COE Lecture Note Vol.42	佐伯　修 若山　正人 山本　昌宏	Study Group Workshop 2012 Abstract, Lecture & Report 178pages	November 19, 2012
COE Lecture Note Vol.43	Institute of Mathematics for Industry, Kyushu University	Combinatorics and Numerical Analysis Joint Workshop 103pages	December 27, 2012
COE Lecture Note Vol.44	萩原　学	モダン符号理論からポストモダン符号理論への展望 107pages	January 30, 2013
COE Lecture Note Vol.45	金山　寛	Joint Research Workshop of Institute of Mathematics for Industry (IMI), Kyushu University “Propagation of Ultra-large-scale Computation by the Domain-decomposition-method for Industrial Problems (PUCDIP 2012)” 121pages	February 19, 2013
COE Lecture Note Vol.46	西井　龍映 栄　伸一郎 岡田　勘三 落合　啓之 小磯　深幸 斎藤　新悟 白井　朋之	科学・技術の研究課題への数学アプローチ ―数学モデリングの基礎と展開― 325pages	February 28, 2013
COE Lecture Note Vol.47	SOO TECK LEE	BRANCHING RULES AND BRANCHING ALGEBRAS FOR THE COMPLEX CLASSICAL GROUPS 40pages	March 8, 2013
COE Lecture Note Vol.48	溝口　佳寛 脇　隼人 平坂　貢 谷口　哲至 島袋　修	博多ワークショップ「組み合わせとその応用」 124pages	March 28, 2013

シリーズ既刊

Issue	Author／Editor	Title	Published
COE Lecture Note Vol.49	照井　章 小原　功任 濱田　龍義 横山　俊一 穴井　宏和 横田　博史	マス・フォア・インダストリ研究所　共同利用研究集会 II 数式処理研究と産学連携の新たな発展　137pages	August 9, 2013
MI Lecture Note Vol.50	Ken Anjyo Hiroyuki Ochiai Yoshinori Dobashi Yoshihiro Mizoguchi Shizuo Kaji	Symposium MEIS2013: Mathematical Progress in Expressive Image Synthesis　154pages	October 21, 2013
MI Lecture Note Vol.51	Institute of Mathematics for Industry, Kyushu University	Forum “Math-for-Industry” 2013 “The Impact of Applications on Mathematics”　97pages	October 30, 2013
MI Lecture Note Vol.52	佐伯　修 岡田　勘三 髙木　剛 若山　正人 山本　昌宏	Study Group Workshop 2013 Abstract, Lecture & Report 142pages	November 15, 2013