[053]MIレクチャーノート表紙奥付等

出版情報：MI lecture note series. 53, 2013-12-26. Institute of Mathematics for Industry, Kyushu University
バージョン：
権利関係：

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

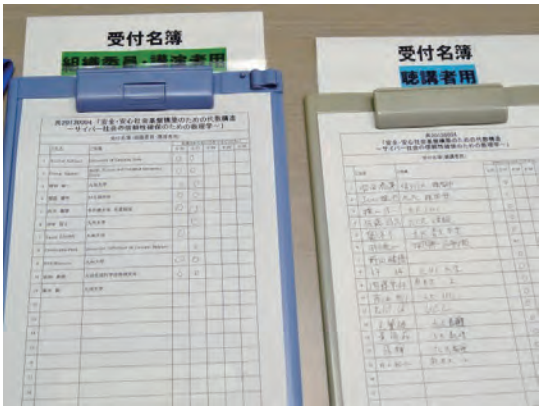
■共催機関：(公財)九州先端科学技術研究所(ISIT)
http://www.isit.or.jp/

■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)

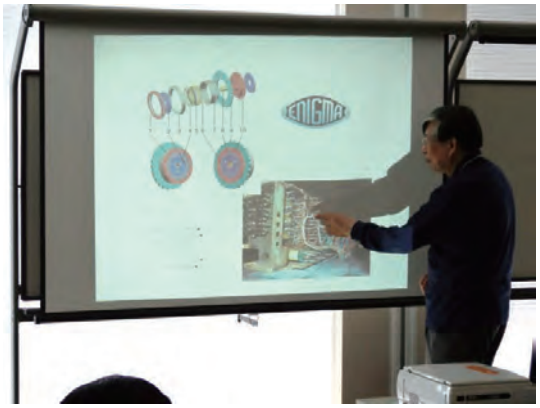
ISIT http://www.isit.or.jp/lab2/2013/05/29/imiworkshop/

■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

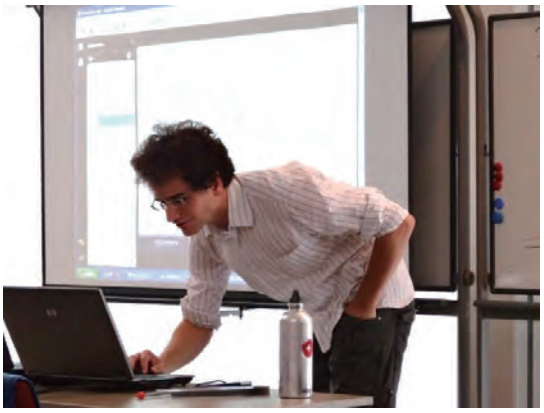

Lattice-based Crypto
Two Types of Techniques
Cryptography using trapdoors, i.e. se
short basis of a lattice. Similariti
RSA/Rabin cryptography.
Cryptography without trapdoors. S
with DL cryptography.
Historically, applied-lattice-crypto us
trapdoors.

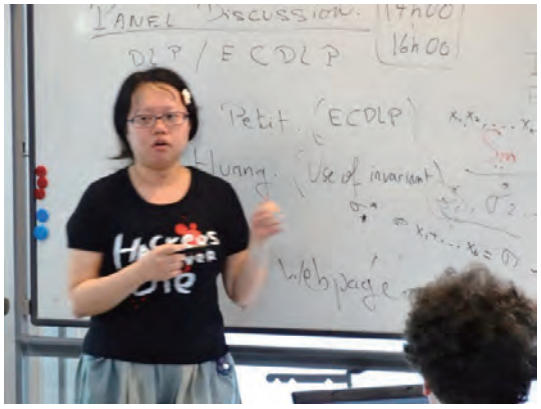

Classification of MPKC signature


Secret Sharing with Cheaters

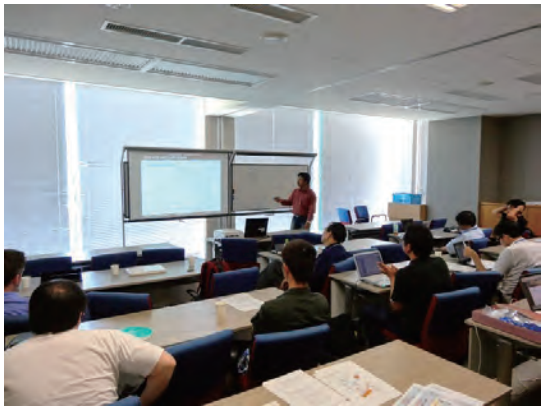

Multiplication on GPU


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