平成２９年度 共同利用研究報告書

平成 30 年 2 月 14 日

九州大学 マス・フォア・インダストリ研究所長 殿

所属・職名　九州大学マス・フォア・インダストリ研究所　准教授
提案者 氏名（ふりがな）　高島 克幸（たかしま かつゆき）・安田 雅哉（やすだ まさや）

下記の通り共同研究の報告をいたします.　　記

	※整理番号		20170015	
1.研究計画題目	代数的手法による数理暗号解析			
2.種別（○で囲む）	a. 研究集会Ⅰ　(b. 研究集会Ⅱ)　c.短期共同研究　d.短期研究員			
3.研究代表者	氏名（ふりがな）	高島 克幸（たかしま かつゆき）		
	所属部局名	三菱電機　情報技術総合研究所 松井暗号プロジェクト G	職名	主席技師長
	連絡先			
	e-mail		TEL	
4.研究実施期間	平成 30 年 2 月 5 日（ 月 曜日）～平成 30 年 2 月 7 日（ 水 曜日）			

5.参加者数・参加者リスト（＊別紙「共同利用研究報告書作成上の注意」参照）
(a,b は参加者数のみ記入し, 集会参加者リストを添付. c.の非公開プログラム参加者と d.は参加者リストに記入. c.は公開プログラムを含めた全参加者数を記入し，公開プログラム参加者リストを添付.）

参加者数：　37　人

参加者リスト（a,b は記入不要，c.は非公開プログラム参加者，d.は共同研究参加者を記入）

氏名（ふりがな）	所属	職名	氏名（ふりがな）	所属	職名
別紙添付					

6.本研究で得られた成果の概要

本研究集会では、暗号と代数学の両分野の研究交流を積極的に促進することができた。具体的な研究テーマとして、暗号分野で近年注目されているポスト量子暗号候補である格子暗号・符号ベース暗号・多変数公開鍵暗号などに関して、暗号と数学の研究アプローチ・考え方の違いを議論できたと共に、それぞれの専門知識・最新情報の共有を行うことができた。また、数学の暗号応用として、離散フーリエ変換や GAPN 関数の符号への応用可能性や、群論を用いた完全準同型暗号の構成などの新しい研究の芽を共有し、暗号と代数学の両分野における研究課題や研究の方向性を見つけることができた。また本研究集会では、産官学のそれぞれで著名な研究者に数多く参加して頂け、暗号と数学の両分野における長期的かつ永続的な研究交流を促進するための研究集会とすることができた。今後、今回のような研究集会を定期的に開催することで、複数の研究分野におけるシナジー効果が期待できると共に、産官学間の長期的な連携協力の礎にすることが強く期待できる。

九州大学 IMI 共同利用・研究集会（II）

代数的手法による数理暗号解析

日時： 2018年2月5日（月）13:00 ～ 2月7日（水）11:45
場所： 〒814-0002 福岡市早良区西新2-16-23
九州大学 西新プラザ 大会議室A
URL ： http://www.imi.kyushu-u.ac.jp/events/view/2227

2月5日（月）

13:00 開場

13:15－13:25 開会式

13:30－14:30 Mehdi Tibouchi (NTT)
Physical attacks on lattice-based schemes

14:45－15:45 Kim Taechan (NTT)
Use of algebraic subfield structure in cryptanalysis

16:00－17:00 玉置 卓（京都大学)
Fine-grained complexity and cryptography: A personal survey

2月6日（火）

9:00 開場

9:30－10:30 黒田 匡迪（北海道大学)
On monomial GAPN (Generalized Almost Perfect Nonlinear) functions and their classification

10:40－11:40 相川 勇輔（北海道大学)
Elliptic curve method with complex multiplication method

13:10－14:10 中島 規博（東京電機大学)
A modification of the discrete Fourier transform for the code defined by Garcia-Stichtenoth tower

14:20－15:20　Carlos Cid (Royal Holloway, University of London)
Code-based cryptography: design and security

15:30－16:30　高安 敦 (東京大学)
Solving RSA and factoring problems using LLL reduction

16:40－17:40　縫田 光司 (産業技術総合研究所/JST さきがけ)
Towards fully homomorphic encryption without ciphertext noise from group theory

2月7日（水）

9:00　開場

9:30－10:30　橋本 康史 (琉球大学)
A survey on multivariate public key cryptosystem

10:45－11:45　奥村 伸也 (大阪大学)
Security analysis of Arita-Handa's subring homomorphic encryption scheme

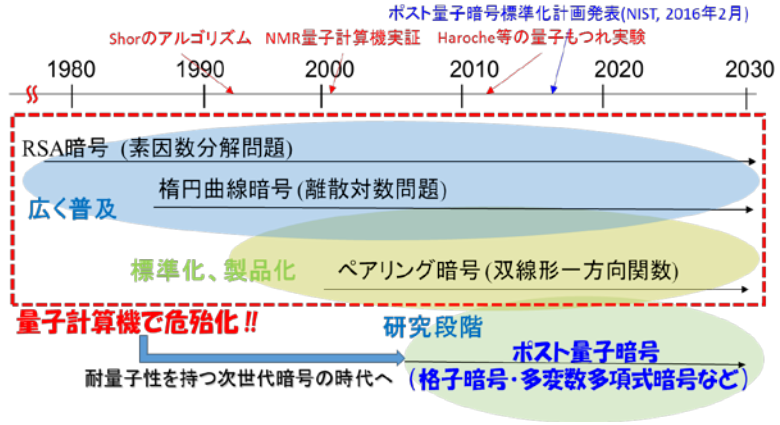
世話人：
阿部 拓郎 (九州大学 IMI)
高島 克幸 (三菱電機株式会社)
縫田 光司 (産業技術総合研究所 / JST さきがけ)
安田 雅哉 (九州大学 IMI)

平成 30 年 2 月 14 日

成果報告書

【研究背景】

現代の情報社会において情報セキュリティを支える暗号技術は必須であり、その安全性はある数学問題の計算量困難性に依存している。例えば、現在広く普及している RSA 暗号と楕円曲線暗号の安全性は、それぞれ素因数分解問題と楕円曲線暗号離散対数問題の計算量困難性に基づいている。一方、研究開発が活発に行われている量子計算機が実現すると、現代暗号技術が危殆化することが知られており、量子計算機でも耐性を持つ「ポスト量子暗号」の研究が盛んに行われている。実際、2016 年 2 月に開催された国際会議 PQCrypto2016 において、米国標準技術研究所 NIST はポスト量子暗号の標準化計画を発表し、2017 年 11 月末に公募〆切を迎え、格子暗号・符号ベース暗号・多変数公開鍵暗号などの数学ベースの暗号方式が多数提案された。このように、暗号と数学（主に代数学）は密接に関係している分野であり、両分野の研究交流・議論が常に求められている。



【本研究集会の目的】

本研究集会では、暗号と代数学の研究者間の積極的な交流を促すことを目的とする。より具体的には、双方の各専門分野における高度な専門知識・最新情報を共有すると共に、互いの研究課題に対して他分野からのアプローチを試みることで、既存研究では得られなかった新しい研究の芽や方向性を探索することを目的とする。

【本研究集会の講演内容と得られた成果】

本研究集会において、暗号と代数学の研究者からの講演内容は以下である：

- 暗号研究者からの講演内容：格子暗号方式に対するサイドチャンネル攻撃、代数体の整数環上の格子基底簡約、NIST 公募提案の符号ベース暗号方式の紹介、LLL 基底簡約を用いた RSA 暗号解読、群論からの完全準同型暗号の構成アプローチ、多変数公開鍵暗号とその攻撃の紹介、分解体上の Ring-LWE 問題ベースの準同型暗号に対する格子攻撃評価
- 代数学研究者からの講演内容：Fine-grained による計算量と暗号との関係、monomial GAPN 関数とその分類理論、虚数乗法を持つ楕円曲線上の素因数分解アプローチ、離散フーリエ変換と符号

今回、格子暗号・符号暗号・多変数公開鍵暗号などの NIST 公募に提案されているポスト量子暗号に関する提案方式や攻撃可能性などの講演があり、暗号と代数学の両分野からの研究アプローチ・考え方の違いを積極的に議論することができた。また、数学の暗号応用として、離散フーリエ変換や GAPN 関数による符号への応用や、群論を用いた完全準同型暗号の構成などの新しい研究の芽を共有でき、今後の研究の方向性・可能性を見つけることができた。また本研究集会では、産官学のそれぞれで著名な研究者に数多く参加して頂け、暗号と数学の両分野における長期的かつ永続的な研究交流を促進するための研究集会とすることができた。