2022年度共同利用研究報告書

2022年12月21日

所属・職名 長崎県立大学 情報システム学部 情報セキュリティ学科・教授

星野 文学

	整理番号	2022a021		
1.研究計画題目	高度化する暗号技術と数学的技法の進展			
2.新規・継続	新規			
3.種別	一般研究			
4.種目	研究集会（Ⅱ）			
5.開催方法	ハイブリッド開催			
6.研究代表者	氏名	星野 文学		
	所属 部局名	長崎県立大学 情報システム学部 情報セキュリティ学科	職名	教授
7.研究実施期間	2022年11月07日(月曜日)～2022年11月09日(水曜日)			
8.キーワード	暗号、高機能暗号、暗号資産、耐量子計算機暗号、秘密計算			
9.参加者人数	159人			

10.本研究で得られた成果の概要

講演については，東京大学の小貫啓史特任助教の講演"Recent topics for isogeny-based cryptography"（約60分）は期待以上であった．というのも，マイクロソフト社が耐量子計算機暗号として提案し,米国立標準技術研究所(NIST)の安全性評価を凡そ5年間生き延びた同種写像暗号SIKEが本研究集会開催の3ヶ月ほど前に完全解読されたからである．他に暗号攻撃について1件，暗号設計について4件，暗号応用について3件の講演が頂けたのは，時間にして計8時間半と長くはないものの，情報と示唆の多い充実した研究集会となった．実際，いずれの講演も，内容はトップレベルの国際会議で採択されている一連の研究の一端，もしくは最先端の研究の一端であった．参加登録者については，160名弱と，講演時間計8時間半の研究集会として想定以上に興味を集めたものと考えている．参加者の内訳としては，40歳未満およそ90名と40歳以上およそ70名，また産からは40名（25%），学からは100名（63%），官からは15名（9%）その他からは4名（3%）と，学以外からの参加者が期待以上に多かった．この点も成果と考えている．（以上）

2022 年 12 月 21 日

2022 年九州大学マス・フォア・インダストリ研究所共同利用研究集会(II)

“Advances in Sophisticated Cryptography and Mathematical Techniques”

（高度化する暗号技術と数学的技法の進展）

成果報告書

組織委員

長崎県立大学情報システム学部・教授	星野 文学（代表者）
NTT 社会情報研究所・主任研究員	菊池 亮
フリーランス	大畑 幸矢
青森大学ソフトウェア情報学部・教授	穴田 啓晃
大阪大学大学院工学研究科・講師	王 イントウ
九州大学マス・フォア・インダストリ研究所・教授	縫田 光司
九州大学マス・フォア・インダストリ研究所・助教	池松 泰彦

ウェブサイト

https://joint.imi.kyushu-u.ac.jp/research-reports/year-2022/

https://joint.imi.kyushu-u.ac.jp/post-6068/

本報告書は，2022 年の共同利用研究集会(II)で採択頂いた上記の表題の研究集会を開催して得られた成果を簡潔に報告することを目的とする．

はじめに，参加者についての成果を説明する．本研究集会は 159 名の参加登録があった．参加人数の内訳を，年齢別及び産学官別でそれぞれ図 1 及び図 2 に示す．図 1 から，40 歳未満および 40 歳以上でそれぞれ 68 名および 91 名であったことが判る．また図 2 から，産からは 40 名（25%），学からは 100 名（63%），官からは 15 名（9%）であったことが判る．学からの参加者が 6 割であったが，これは大学の教員・学生が多かったためである．

次に，研究内容の成果を説明する．次ページに実施された講演の一覧を示す．講演は次の三つのカテゴリに分類される．

カテゴリA. 暗号攻撃	: 講演 3）6）
カテゴリB. 暗号設計	: 講演 5）7）8）9）
カテゴリC. 暗号応用	: 講演 1）2）4）

このことから，本研究集会の研究題目「高度化する暗号技術と数学的技法の進展」に関し，件数及び時間の観点で攻撃から応用までをバランスよく講演頂けたものと考えている．

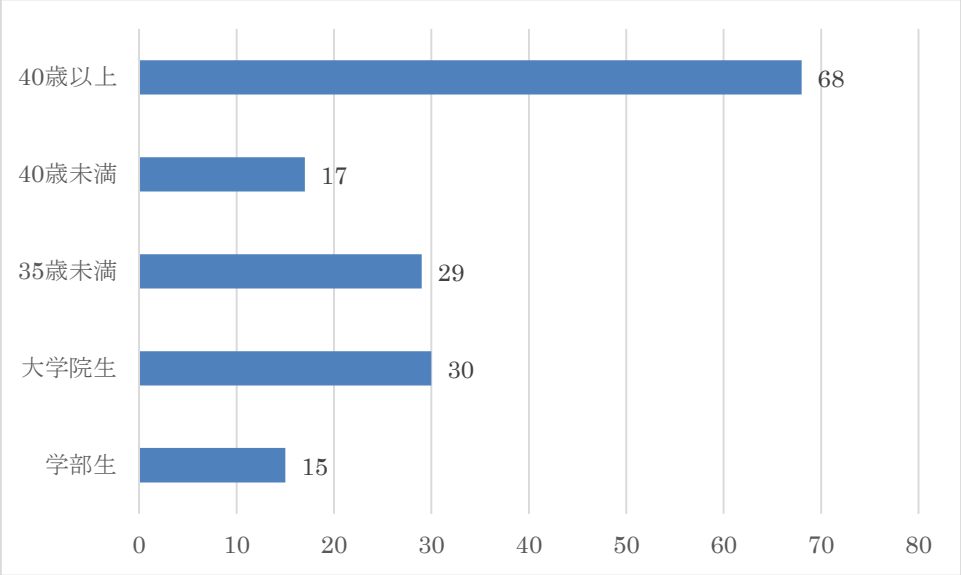

図 1　参加人数内訳．年齢別

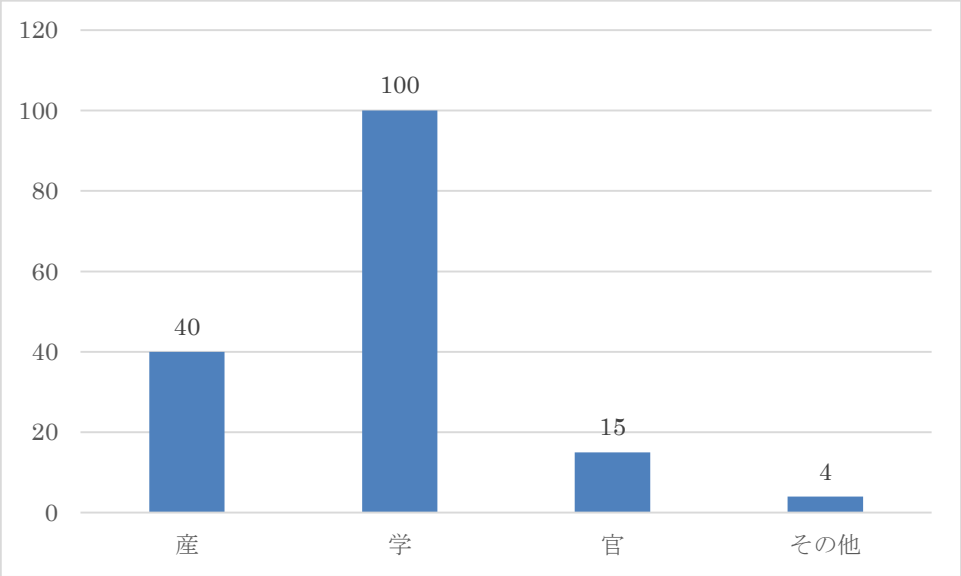

図 2　参加人数内訳．産学官別

特に本研究集会では東京大学の小貫啓史特任助教をお呼びして同種写像暗号に対する最近のトピックについて 60 分ほどの解説を頂いた．というのも，マイクロソフト社が耐量子計算機暗号として提案し，米国立標準技術研究所（NIST）の安全性評価を凡そ 5 年間生き延びた同種写像暗号 SIKE が本研究集会開催の 3 ヶ月ほど前に完全解読された為である．他に暗号設計 4 件，暗号応用 3 件などの講演も頂けており，時間にして合計 8 時間半と長くはないものの，情報と示唆の多い充実した研究集会となった．実際，いずれの講演も，内容はトップレベルの国際会議で採択されている一連の研究の一端，もしくは最先端の研究の一端であった．

最後に，本研究集会の開催に当たっては，九州大学マス・フォア・インダストリ研究所から支給頂いた予算を用いた．ここに深謝申し上げる．

（以上）

2022 年 12 月 21 日

実施された講演の一覧

第 1 日：11 月 07 日（月）

1) 13:10-14:10
Kazumasa Omote (University of Tsukuba)
Blockchain and its applied research

2) 14:30-15:30
Masayuki Yoshino/Kyohei Yamamoto (Hitachi, Ltd.)
On research of cryptography for secure SaaS: attacks, security requirements and practical solutions

3) 15:50-16:10 Student lecture slot
Tomoka Takahashi (Osaka University)
On the Weakness of Ring-LWE mod Prime ideal by Trace Map

第 2 日：11 月 08 日（火）

4) 10:00-11:00
Takenobu Seito (Deloitte Touche Tohmatsu LLC)
Recent Trends on Zero-Knowledge Proof: Theory and its Applications

5) 11:20-12:20
Kotaro Matsuoka (Kyoto University)
Evaluating Boolean circuits over ciphertexts using Fully Homomorphic Encryption over the Torus

6) 14:00-15:00
Hiroshi Onuki (The University of Tokyo)
Recent topics for isogeny-based cryptography

7) 15:20-16:20
Yohei Watanabe (The University of Electro-Communications)
Recent Progress in Searchable Encryption

第 3 日：11 月 09 日（水）

8) 10:00-11:00
Takanori Yasuda (Okayama University of Science)
Construction of pairing using elliptic curves

9) 11:20-12:20
Dung Hoang Duong (University of Wollongong)
Cryptography from group actions

開催日：2022/11/07～2022/11/09

高度化する暗号技術と数学的技法の進展｜共2022a021

カテゴリー：イベント　　タグ：一般研究 研究集会II

開催概要

- **開催方法：**会場とZoomウェビナーによるハイブリッド開催
- **場所：**JR博多シティ９階会議室（１）
- **主要言語：**日本語/英語
- **主催：**九州大学マス・フォア・インダストリ研究所

- **種別・種目**：一般研究-研究集会(II)
- **研究計画題目**：高度化する暗号技術と数学的技法の進展
- **研究代表者**：星野 文学（長崎県立大学 情報システム学部 情報セキュリティ学科・教授）
- **研究実施期間**：2022年11月7日（月）～ 2022年11月9日（水）
- **研究計画詳細**：https://joint1.imi.kyushu-u.ac.jp/research_chooses/view/2022a021

プログラム (*はオンライン発表予定)

11月7日（月）

13:00-13:10

オープニング

13:10-14:10

面 和成（筑波大学）*
Blockchain and its applied research

14:30-15:30

吉野 雅之/山本 恭平（日立製作所）
On research of cryptography for secure SaaS: attacks, security requirements and practical solutions

15:50-16:10 学生講演枠

髙橋 朋伽（大阪大学）
On the Weakness of Ring-LWE mod Prime ideal by Trace Map

11月8日（火）

10:00-11:00

清藤 武暢（有限責任監査法人トーマツ）*
Recent Trends on Zero-Knowledge Proof: Theory and its Applications

11:20-12:20

松岡 航太郎（京都大学）
Evaluating Boolean circuits over ciphertexts using Fully Homomorphic Encryption over the Torus

14:00-15:00

小貫 啓史（東京大学）
Recent topics for isogeny-based cryptography

15:20-16:20

渡邉 洋平（電気通信大学）
Recent Progress in Searchable Encryption

11月9日（水）

10:00-11:00

安田 貴徳（岡山理科大学）
Construction of pairing using elliptic curves

11:20-12:20

Dung Hoang Duong（University of Wollongong）
Cryptography from group actions

12:20-12:30

クロージング