2026年度共同利用研究報告書

2026年07月16日

所属・職名 マス・フォア・イノベーション連係学府数理学系・博士前期課程１年
金重 幸大

		整理番号	2026a014	
1.研究計画題目	若手研究者のための暗号周辺分野の横断的・萌芽的研究の創発			
2.新規・継続	新規			
3.種別	若手・学生研究			
4.種目	短期共同研究			
5.開催方法	対面開催			
6.研究代表者	氏名	金重 幸大		
	所属部局名	マス・フォア・イノベーション連係学府数理学系	職名	博士前期課程１年
7.研究実施期間	2026年06月22日(月曜日)～2026年06月24日(水曜日)			
8.キーワード	暗号理論，情報理論，計算量理論，量子情報理論			
9.参加者人数	36人			

10.本研究で得られた成果の概要

本研究集会では、暗号およびその周辺分野を専門とする学生・若手研究者を主な対象として、専門分野や所属を越えた交流を促進し、新たな研究の着想や共同研究のきっかけを創出することを目的に開催した。企画・運営は学生が主体となって行い、研究集会全体を通して、学生同士が主体的に学び、議論し、交流できる場となるよう構成を工夫した。

プログラムでは、秘密計算、同種写像暗号、多変数多項式暗号、署名方式、暗号解析など、暗号分野における幅広いテーマについて講演が行われた。それぞれ異なる研究分野や立場からの発表であったため、参加者は自身の専門外の研究内容や考え方に触れることができ、普段の研究活動では得られない新たな視点を得る機会となった。特定のテーマに偏ることなく、多様な分野を横断する内容で構成したことにより、暗号研究全体を俯瞰する場としても有意義な研究集会となった。

また、プログラムには第一線で活躍されている研究者によるレクチャーの時間も設けた。第一線の研究者から研究内容だけでなく、研究の背景や考え方、今後の展望などについて直接話を聞くことができたことは、学生や若手研究者にとって大きな刺激となった。基礎的な内容から最新の研究動向まで幅広く紹介していただき、参加者が今後の研究の方向性を考える上でも有益な機会となった。

さらに、講演だけでなく、参加者同士が自由に議論できるディスカッションの時間を設けた。講演内容に関する質問に加え、それぞれの研究テーマや今後の課題について活発な意見交換が行われ、専門や所属の異なる参加者同士が互いの知見を共有する場となった。学生同士が気軽に質問や議論を行える雰囲気づくりを意識したことで、講演時間だけでは生まれにくい交流が促進され、新たなつながりの形成にもつながった。

令和 8 年度九州大学マス・フォア・インダストリ研究所 若手・学生研究-短期共同研究

若手研究者のための暗号周辺分野の横断的・萌芽的研究の創発

成果報告書

研究代表者

九州大学マス・フォア・イノベーション連係学府・博士前期課程 2 年　　金重　幸大

組織委員

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・准教授　　池松　泰彦

横浜国立大学大学院環境情報学府・博士後期課程 3 年　　知久　奏斗

東京大学大学院情報理工学系研究科・博士後期課程 2 年　　瀬戸　友暁

東京大学大学院情報理工学系研究科・博士後期課程 2 年　　高寺　俊喜

ウェブサイト

https://joint.imi.kyushu-u.ac.jp/post-20855/

本研究集会の目的

暗号分野は、暗号理論のみならず、数論、代数幾何、情報理論、計算量理論、量子情報理論など、多様な学問分野を背景として発展している。一方で、若手研究者にとっては自身の専門分野以外の研究内容や理論的背景に触れる機会が限られており、分野横断的な理解や交流を深める場が十分とは言えないという課題がある。

本研究集会は、このような背景を踏まえ、暗号およびその周辺分野を専門とする学生・若手研究者が、各分野の研究課題や理論的背景、研究の動機について共有し、相互理解を深めることを目的として開催した。講演やレクチャーを通じて多様な研究分野に触れる機会を提供するとともに、ディスカッションを通じて専門や所属を越えた交流を促進し、分野横断的な視点を養う場となることを目指した。

また、本研究集会では、学生・若手研究者が互いに顔の見える関係を築き、気軽に議論や情報交換を行えるコミュニティの形成も重要な目的とした。学生が主体となって企画・運営を行うことで、参加者同士が交流しやすい雰囲気を醸成し、所属や専門分野の枠を越えた新たなつながりを生み出す契機となることを期待した。

得られた成果

本研究集会には 36 名が参加し、そのうち 29 名（約 81%）が学生であった。また、図 1 に示すように、参加者は九州大学をはじめ、全国の複数の大学・研究機関から集まり、地域や所属

を越えた交流の場を提供することができた。学生・若手研究者を主な対象として企画した研究集会として、多様なバックグラウンドを持つ参加者が一堂に会したことは、大きな成果であったと考えられる。

プログラムでは、学生・若手研究者による講演に加え、第一線で活躍する研究者によるレクチャーを実施した。また、学生講演では、秘密計算、同種写像暗号、多変数多項式暗号、量子計算、数論など、多様な研究分野に関する講演が行われ、参加者は自身の専門外の研究内容や理論的背景に触れる機会を得た。具体的な内容については、たとえば同種写像暗号に関する講演では、SIDH をはじめとする従来方式の数理構造や安全性に関する議論から、その改良方式である POKE に対する攻撃手法の紹介、さらに同種写像グラフを利用したハッシュ関数の構成など、基礎的事項から最新の研究動向まで幅広い内容が扱われた。また、レクチャーでは、同種写像暗号を専門としない学生にも理解できるよう、楕円曲線や同種写像の基礎から丁寧に解説いただくとともに、現在活発に研究が進められている最新の話題についても紹介いただいた。専門外の参加者にとっては分野への入口となる一方、専門とする学生にとっても最新の研究動向を体系的に学ぶ貴重な機会となった。

また、ディスカッションの時間を設けることで、講演内容のみならず研究上の課題や今後の展望についても活発な意見交換が行われた。初日のディスカッションでは、参加者が互いの研究分野や興味を共有する自己紹介を行った後、オープンディスカッション形式で自由な意見交換を実施した。専門分野や所属の異なる学生・若手研究者が気軽に交流できる雰囲気が生まれ、その後の講演や休憩時間における議論の活性化にもつながった。2 日目のディスカッションでは、より研究内容に踏み込んだ議論を行うことを目的とし、事前に設定したテーマについて参加者同士で意見交換を行った。また、組織委員による講演内容について改めて質疑応答や議論の時間を設けることで、講演時間内では十分に扱いきれなかった技術的な内容や今後の研究課題についても活発な議論が展開された。専門分野の異なる参加者からの視点や質問も多く寄せられ、それぞれの研究を多角的に捉え直す貴重な機会となった。

研究集会終了後に実施したアンケートでは、「新たな知り合いができた」「自身の研究に刺激を受けた」と回答した参加者が大多数を占めた（図 2、図 3）。これらの結果から、本研究集会が学生・若手研究者間の交流を促進するとともに、異なる分野の研究に触れることで新たな視点や研究への動機付けを得る機会として機能したことが示された。

以上より、本研究集会では、講演・レクチャー・ディスカッションを通じて分野横断的な相互理解を深めるとともに、学生・若手研究者を中心とした新たな研究コミュニティ形成の契機を提供するという当初の目的を十分に達成することができた。

図 1

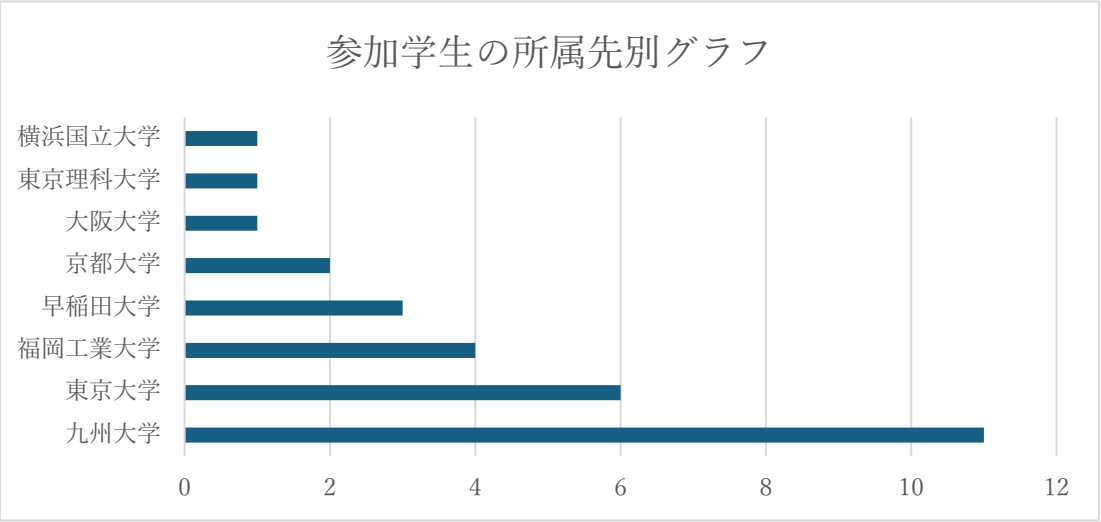

参加学生の所属先別グラフ
横浜国立大学
東京理科大学
大阪大学
京都大学
早稲田大学
福岡工業大学
東京大学
九州大学
0
2
4
6
8
10
12

図 2

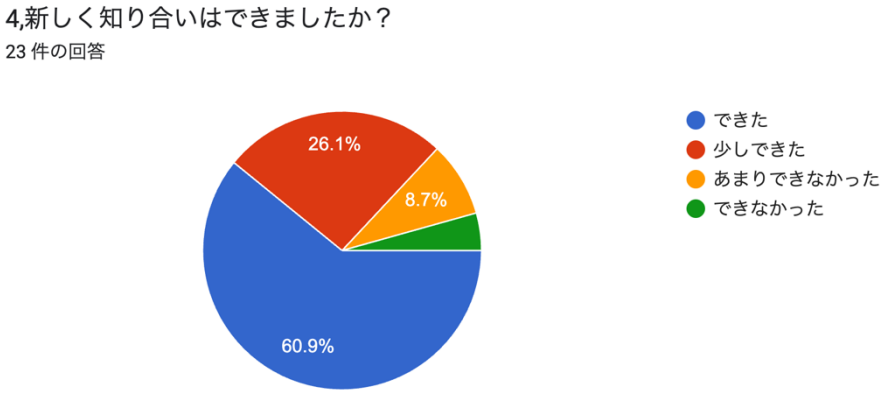
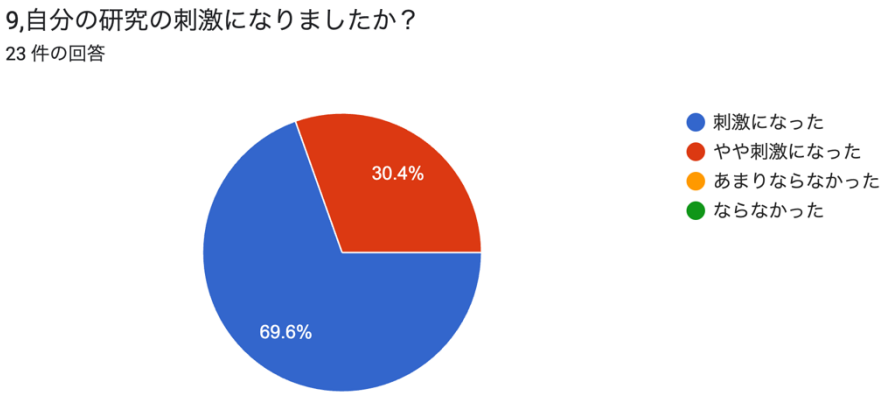

4,新しく知り合いはできましたか？
23 件の回答
26.1%
8.7%
60.9%
できた
少しできた
あまりできなかった
できなかった

図 3


9,自分の研究の刺激になりましたか？
23 件の回答
30.4%
69.6%
刺激になった
やや刺激になった
あまりならなかった
ならなかった

謝辞

本研究集会の開催にあたり、ご支援を賜りました九州大学マス・フォア・インダストリ研究所（IMI）共同利用・共同研究拠点に深く感謝申し上げます。また、ご講演・レクチャーをご担当いただいた先生方をはじめ、ご参加いただいた皆様のご協力により、本研究集会を盛会のうちに開催することができました。ここに厚く御礼申し上げます。

全体写真

九州大学 IMI 共同利用

『若手研究者のための暗号周辺分野の横断的・萌芽的研究の創発』

【日時】 2026 年 6 月 22 日(月) ～6 月 24 日(水)

【場所】九州大学 伊都キャンパス ウエスト 1 号館 D 棟 4 階 IMI カンファレンス

ルーム（W1-D-414）

【組織委員】

・九州大学マス・フォア・イノベーション連係学府・博士前期課程 2 年　金重　幸大

・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・准教授　池松　泰彦

・横浜国立大学大学院環境情報学府・博士後期課程 3 年　知久　奏斗

・東京大学大学院情報理工学系研究科・博士後期課程 2 年　瀬戸　友暁

・東京大学大学院情報理工学系研究科・博士後期課程 2 年　高寺　俊喜

【プログラム】

6 月 22 日（月）

・13:00-13:10

オープニング

・13:10-14:10

講演者：縫田 光司

講演題目：「秘密計算および関連する話題について」

・14:20-14:50

講演者：瀬戸 友暁

講演題目：「データ符号化の秘密計算」

・14:50-15:20

講演者：藤田 祐輝

講演題目：「検証者指定署名とその拡張」

・15:20-15:50

講演者：知久 奏斗

講演題目：「登録型高機能暗号について」

・15:50-

ディスカッション

6 月 23 日（火）

・10:00-11:00

講演者：小貫 啓史

講演題目：「同種写像暗号への招待：基礎・主要方式・応用」

・11:10-11:40

講演者：高寺 俊喜

講演題目：「POKE に対する送信側一時鍵再利用攻撃」

・11:40-12:10

講演者：谷地 啓輔

講演題目：「同種写像から見る SIDH 鍵共有」

・12:10-12:40

講演者：杉本 貴美

講演題目：「同種写像に基づくハッシュ関数」

・14:20-14:50

講演者：金重 幸大

講演題目：「同種写像暗号における代数幾何学の基礎」

・14:50-15:20

講演者：肖 懐遠

講演題目：「バイナリ ECDLP を解く Shor アルゴリズムの量子回路設計から考えるポスト量子時代の暗号解析」

・15:20-15:50

講演者：髙 和真

講演題目：「数理ソルバーを用いた共通鍵暗号の自動安全性評価」

・15:50-

ディスカッション

6 月 24 日（水）

・10:00-11:00

講演者：池松 泰彦

講演題目：「多変数多項式暗号の紹介」

・11:10-11:40

講演者：荒井 秀斗

講演題目：「Wedge を用いた UOV に対する攻撃の検討」

・11:40-12:10

講演者：朝重 菜音

講演題目：「完全準同型暗号方式 FINAL について」

・12:10-12:40

講演者：今村 浩二

講演題目：「局所環上の加群におけるマトロイドの表現について」

受付中

開催日：2026/06/22〜2026/06/24

若手研究者のための暗号周辺分野の横断的・萌芽的研究の創発｜2026a014

カテゴリー：イベント　タグ：若手研究 短期共同研究

開催概要

- **開催方法**：対面開催
- **開催場所**：九州大学 伊都キャンパス ウエスト1号館 D棟 4階 IMIカンファレンスルーム（W1-D-414）
- **主要言語**：日本語
- **主催**：九州大学マス・フォア・インダストリ研究所
- **種別・種目**：若手・学生研究-短期共同研究
- **研究計画題目**：若手研究者のための暗号周辺分野の横断的・萌芽的研究の創発
- **研究代表者**：金重 幸大（九州大学　マス・フォア・イノベーション連係学府数理学系・博士前期課程1年）
- **研究実施期間**：2026年6月22日(月)〜2026年6月24日(水)
- **公開期間**：2026年6月22日(月)〜2026年6月24日(水)
- **研究計画詳細**：https://joint2.imi.kyushu-u.ac.jp/research_chooses/view/2026a014

プログラム

6月22日（月）

13:00-13:10

オープニング

13:10-14:10

縫田 光司（九州大学IMI）
「秘密計算および関連する話題について

14:20-14:50

瀬戸 友暁（東京大学・博士2年）
「データ符号化の秘密計算」

14:50-15:20

藤田 祐輝（京都大学・博士1年）
「検証者指定署名とその拡張」

15:20-15:50

知久 奏斗（横浜国立大学・博士3年）
「登録型高機能暗号について」

15:50-

ディスカッション

6月23日（火）

10:00-11:00

小貫 啓史（東京大学）
「同種写像暗号への招待：基礎・主要方式・応用」

11:10-11:40

高寺 俊喜（東京大学・博士2年）
「POKEに対する送信側一時鍵再利用攻撃」

- **11:40-12:10**

  谷地 啓輔（東京大学・修士1年）
  「同種写像から見るSIDH鍵共有」

- **12:10-12:40**

  杉本 貴美（東京大学・修士1年）
  「同種写像に基づくハッシュ関数」

- **14:20-14:50**

  金重 幸大（九州大学・修士2年）
  「同種写像暗号における代数幾何学の基礎」

- **14:50-15:20**

  肖 懐遠（東京大学・修士2年）
  「バイナリECDLPを解くShorアルゴリズムの量子回路設計から考えるポスト量子時代の暗号解析」

- **15:20-15:50**

  髙 和真（NICT/大阪大学・博士1年）
  「数理ソルバーを用いた共通鍵暗号の自動安全性評価」

- **15:50-**

  ディスカッション

6月24日（水）

- **10:00-11:00**

  池松 泰彦（九州大学IMI）
  「多変数多項式暗号の紹介」

- **11:10-11:40**

  荒井 秀斗（東京理科大学・修士2年）
  「Wedgeを用いたUOVに対する攻撃の検討」

- **11:40-12:10**

  朝重 菜音（九州大学・博士1年）
  「完全準同型暗号方式FINALについて」

- **12:10-12:40**

  今村 浩二（九州大学IMI）
  「局所環上の加群におけるマトロイドの表現について」