2025年度 随時応募枠共同利用研究報告書

2025年11月03日

所属・職名 東京大学大学院情報理工学系研究科・特任研究員

大橋 亮

		整理番号	2025c001	
1.研究計画題目	代数曲線やアーベル多様体に関連する数論アルゴリズム			
2.新規・継続	新規			
3.種別	随時募集枠			
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	大橋 亮		
	所属部局名	東京大学大学院情報理工学系研究科	職名	特任研究員
7.研究実施期間	2025年10月20日(月曜日)～2025年10月22日(水曜日)			
8.キーワード	代数曲線 / アーベル多様体 / 数論アルゴリズム / 同種写像暗号 / 超特別曲線			
9.参加者人数	70人			

10.本研究で得られた成果の概要

本研究集会は同種写像暗号に関連する代数幾何や数論アルゴリズムの最新成果を紹介し、分野横断的に研究課題を共有して意見交換を深めることで、新たな研究の発展を促すことを目的として開催された。初日は同種写像暗号に関するチュートリアル講演に始まり、続いて近年注目を集めるアーベル多様体を利用した同種写像暗号方式が紹介された。二日目では楕円曲線やアーベル多様体に関連するさまざまな数論アルゴリズムが取り上げられた。最終日には超特別曲線の数え上げという代数幾何的な話題として同種写像グラフを利用したアプローチと今後の研究課題が共有された。その結果、全体での参加者数はオンラインを含めると70名に達し、現地では講演後も活発に議論が交わされるなど、当初の目的は概ね達成されたと考えている。

随時募集枠-研究集会（II）
代数曲線やアーベル多様体に関連する数論アルゴリズム
成果報告書

- 研究代表者:
  大橋 亮（東京大学大学院情報理工学系研究科・特任研究員）
- 組織委員:
  相川 勇輔（東京大学大学院情報理工学系研究科・助教）
  池松 泰彦（九州大学マス・フォア・インダストリ研究所・准教授）
  内田 幸寛（東京都立大学大学院理学研究科・准教授）
  小貫 啓史（東京大学大学院情報理工学系研究科・特任講師）
  工藤 桃成（福岡工業大学情報工学部情報通信工学科・准教授）
  中川 皓平（NTT 社会情報研究所・研究員）
  吉住 崚（九州大学マス・フォア・イノベーション連係学府・博士後期課程）

1. 本研究集会の背景

耐量子計算機暗号の標準化計画が米国国立標準技術研究所(NIST)を中心に進められており、特にデジタル署名方式については 2023 年に追加公募が実施された。その候補の 1 つであった同種写像暗号方式 SQIsign が現在も選考対象として残っている。他の同種写像暗号方式についても、鍵や暗号文のサイズが小さい等の利点から注目されており、産業的なニーズも高まっている。こうした背景の下で、同種写像暗号の更なる効率化や安全性解析は極めて重要な研究課題であるが、その根幹をなす道具が代数曲線やアーベル多様体に関連する数論アルゴリズムである。実際 2022 年 7 月に従来有力と考えられていた同種写像暗号方式 SIDH に対する多項式時間攻撃が発表されたが、その際に高次元アーベル多様体の理論が中心的な役割を果たした。この出来事を契機として、アーベル多様体を利用する新たな同種写像暗号方式が数多く提案され、その効率化を目的として、アーベル多様体間の同種写像を効率的に計算するアルゴリズムも開発されている。また、こうしたアルゴリズムは超特別曲線の数え上げや同種写像グラフの構造解析といった代数幾何的な問題にも応用されており、結果として同種写像暗号の安全性解析にも寄与している。

2. 本研究集会の目的と期待される成果

以上のように代数幾何、数論アルゴリズム、同種写像暗号の三者は密接に関連しており、今後の研究の更なる進展にはこれらの分野を横断した知見の共有や連携が必要不可欠である。そこで、本研究集会ではこれらの分野に携わる研究者を幅広く招き、

最新の研究動向や成果ならびに今後の展望や課題を研究者間で共有して、活発な議論を行うことを目的とする。そのような交流を通じて、分野を越えた新たな研究課題の発見が促され、参加者間での共同研究へ繋がること等が成果として期待される。

3. 講演プログラム

開催日時: 2025 年 10 月 20 日（月）～ 2025 年 10 月 22 日（水）
開催方法: ハイブリッド開催
開催場所: 九州大学伊都キャンパス ウエスト 1 号館 コンファレンスルーム D414 号室

［第 1 日目］

13:30-14:30
守谷 共起（三菱電機株式会社情報技術総合研究所）
同種写像暗号の導入

15:00-16:00
小貫 啓史（東京大学）
Isogeny-based public key encryption schemes using 2-dimensional isogenies

16:30-17:30
中川 皓平（NTT 社会情報研究所）
On signature schemes using 2-dimensional isogeny

［第 2 日目］

09:30-10:30
相川 勇輔（東京大学）
Isogeny Expanders

11:00-12:00
吉住 崚（九州大学）
アーベル多様体上のテータ座標による効率的な同種写像計算

13:30-14:30
片山 瑛（NTT 社会情報研究所）
有限体上の楕円曲線の自己準同型環と同種写像のなす群の数論アルゴリズム

15:00-16:00
石塚 裕大（九州大学）
数論統計のアルゴリズム的な側面について

［第 3 日目］

09:30-10:30
工藤 桃成（福岡工業大学）
Introduction to superspecial curves: History and recent developments

11:00-12:00

大橋 亮（東京大学）

同種写像グラフを利用した超特別曲線の列挙アルゴリズム

4. 本研究集会で得られた成果の概要

本研究集会は同種写像暗号に関連する代数幾何や数論アルゴリズムの最新成果を紹介し、分野横断的に研究課題を共有して意見交換を深めることで、新たな研究の発展を促すことを目的として開催された。初日は同種写像暗号に関するチュートリアル講演に始まり、続いて近年注目を集めるアーベル多様体を利用した同種写像暗号方式が紹介された。二日目では楕円曲線やアーベル多様体に関連するさまざまな数論アルゴリズムが取り上げられた。最終日には超特別曲線の数え上げという代数幾何的な話題として同種写像グラフを利用したアプローチと今後の研究課題が共有された。その結果、全体での参加者数はオンラインを含めると 70 名に達し、現地では講演後も活発に議論が交わされるなど、当初の目的は概ね達成されたと考えている。

以上

開催日：2025/10/20〜2025/10/22

代数曲線やアーベル多様体に関連する数論アルゴリズム｜2025c001

カテゴリー：イベント　タグ：随時募集　研究集会II

開催概要

- **開催方法**：ハイブリッド開催
- **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**：随時募集枠-研究集会（Ⅱ）
- **研究計画題目**：代数曲線やアーベル多様体に関連する数論アルゴリズム
- **研究代表者**：大橋 亮 (東京大学大学院情報理工学系研究科・特任研究員)
- **研究実施期間**：2025年10月20日（月）〜 2025年10月22日（水）
- **公開期間**：2025年10月20日（月）〜 2025年10月22日（水）
- **研究計画詳細**：https://joint2.imi.kyushu-u.ac.jp/research_chooses/view/2025c001

プログラム

10月20日（月）

13:00-13:20

研究集会の趣旨説明

13:30-14:30

守谷 共起 (三菱電機株式会社情報技術総合研究所)

同種写像暗号の導入

15:00-16:00

小貫 啓史 (東京大学)

Isogeny-based public key encryption schemes using 2-dimensional isogenies

16:30-17:30

中川 皓平 (NTT社会情報研究所)

On signature schemes using 2-dimensional isogeny

10月21日(火)

09:30-10:30

相川 勇輔 (東京大学)

Isogeny Expanders

11:00-12:00

吉住 崚 (九州大学)

アーベル多様体上のテータ座標による効率的な同種写像計算

13:30-14:30

片山 瑛 (NTT社会情報研究所)

有限体上の楕円曲線の自己準同型環と同種写像のなす群の数論アルゴリズム

15:00-16:00

石塚 裕大 (九州大学)

数論統計のアルゴリズム的な側面について

16:30-17:30

ディスカッション

18:30

懇親会

10月22日(水)

09:30-10:30

工藤 桃成 (福岡工業大学)

Introduction to superspecial curves: History and recent developments

11:00-12:00

大橋 亮 (東京大学)

同種写像グラフを利用した超特別曲線の列挙アルゴリズム

申込方法

事前申込制（組織委員，講演者のかたも登録が必要です）
参加無料
定員になり次第，参加登録を締め切らせていただく場合がございます．

＼下記URLより参加登録をお願いいたします／

参加登録フォーム