2022年度 随時応募枠共同利用研究報告書

2023年03月22日

所属・職名 名城大学理工学部・教授

前野 俊昭

	整理番号	2022c006

1.研究計画題目	2022年暗号及び情報セキュリティと数学の相関ワークショップ（CRISMATH 2022）			
2.新規・継続	新規			
3.種別	随時募集枠			
4.種目	研究集会（Ⅱ）オンライン型			
5.開催方法	ハイブリッド開催			
6.研究代表者	氏名	前野 俊昭		
	所属部局名	名城大学理工学部	職名	教授
7.研究実施期間	2022年12月20日(火曜日)～2022年12月21日(水曜日)			
8.キーワード	暗号、同種写像、非可換群、フィンスラー幾何学、機械学習			
9.参加者人数	65人			

10.本研究で得られた成果の概要

近年、暗号をはじめとする情報セキュリティ分野においては、従来よりも専門性の高い数学の知見に基づく様々な研究が進められており、一方で、数学分野においては、これまで以上に周辺分野との研究連携を推進する機運が高まっている。こうした傾向を鑑み、従来研究の枠組みにとらわれず、暗号分野における数学応用の幅広い可能性を模索することが双方の分野において有益であると考え、これら二つの分野の研究者・学生たちが研究的交流を行う場を提供し、両分野にわたる研究連携を推進することを目的として、両分野に関連するいくつかの研究トピックの紹介を行う研究集会を開催した。本研究集会では、幾何学的群論、フィンスラー幾何学とその暗号への応用、機械学習の暗号設計への応用、および楕円曲線の同種写像グラフとその暗号への応用を題材として、招待講演者による講演を行うとともに、講演者と参加者間での議論を行った。このように、先端的な数学理論の暗号分野への応用の事例および可能性や、暗号分野の観点からの数学分野における研究課題について、参加者間での情報共有を行ったことで、今後の両分野のさらなる連携の強化に貢献できた。

IMI 共同利用成果報告書
（随時募集枠-研究集会（II）オンライン型）
2022 年暗号及び情報セキュリティと数学の相関ワークショップ
（CRISMATH 2022）

2023 年 3 月 21 日

1　概要

近年、暗号をはじめとする情報セキュリティ分野においては、従来よりも専門性の高い数学の知見に基づく様々な研究が進められており、一方で、数学分野においては、これまで以上に周辺分野との研究連携を推進する機運が高まっている。こうした傾向を鑑み、従来研究の枠組みにとらわれず、暗号分野における数学応用の幅広い可能性を模索することが双方の分野において有益であると考え、これら二つの分野の研究者・学生たちが研究的交流を行う場を提供し、両分野にわたる研究連携を推進することを目的として、両分野に関連するいくつかの研究トピックの紹介を行う研究集会を開催した。本研究集会では、幾何学的群論、フィンスラー幾何学とその暗号への応用、機械学習の暗号設計への応用、および楕円曲線の同種写像グラフとその暗号への応用を題材として、招待講演者による講演を行うとともに、講演者と参加者間での議論を行った。このように、先端的な数学理論の暗号分野への応用の事例および可能性や、暗号分野の観点からの数学分野における研究課題について、参加者間での情報共有を行ったことで、今後の両分野のさらなる連携の強化に貢献できた。

2　開催日・会場等

日程　2022 年 12 月 20 日（火）～12 月 21 日（水）
会場　九州大学伊都キャンパス IMI オーディトリアム およびオンライン（Zoom）とのハイブリッド開催
参加登録者数　65 名
実行委員

前野 俊昭（名城大学 理工学部）（研究代表者）
縫田 光司（九州大学 マス・フォア・インダストリ研究所）

3　プログラム（敬称略）

12 月 20 日（火）

14:00-15:30　加藤 本子（琉球大学 教育学部）　「リチャード・トンプソンの群とその応用」

概要　トンプソン群は Richard Thompson によって 1960 年代に発見された非可換な無限群である．トンプソン群には F・T・V の 3 種類があり, それぞれ単位区間・単位円・カントール空間のある種の同相写像のなす群として定義される．これらの群は数学のさまざまな分野に自然に表れ, 多くの変わった性質を持つことが知られている．この講演では, 幾何学的群論の観点からトンプソン群について紹介し, これらの群を公開鍵暗号に応用する試みについて述べる。

15:40-17:10　永野 哲也（長崎県立大学 情報システム学科）　「フィンスラー暗号」

概要　この話では、フィンスラー幾何学が有する非対称性の性質に依存する公開鍵暗号系を議論する。初出は 2019 年の CSS2019 である。幾何学の背景を簡単に見た後、暗号化と復号の機能を幾何学的な直観と手順でより体系付けて捉える。次いで、暗号の強度について改良された点を説明する。また、同じ性質に依存するデジタル署名系についても言及する。

12 月 21 日（水）

9:30-11:00　Ishak Meraouche（九州大学 大学院システム情報科学府）　“Advances in Neural networks based Cryptography”

概要　Artificial Intelligence (AI) and cryptography have always been separate disciplines in the past. Early AI models were not able to learn the simplest and most primitive mathematical functions or operations such as the XOR operation. Due to this fact, interest in building AI models that can learn cryptographic techniques have decreased significantly until the late 90s and early 2000s where some models were introduced. However, with the advances in AI, especially with deep learning, things are starting to change. Multiple models based on Generative Adversarial Networks (GANs) have been introduced since late 2016 and have shown significant performance and security in encryption. In this talk, we will start by seeing how AI based cryptography has evolved since the early 2000s. Next, we will survey the most prominent GANs models that have been proposed in recent years and were able to learn strong cryptographic techniques. After that, we will see the security of these models and how their security can be evaluated. Lastly, we will introduce our contributions to this topic.

11:10-12:40　相川 勇輔（三菱電機）　「Isogeny Graphs and Cryptography」

概要　Charles らはエクスパンダーグラフ上のランダムウォークから暗学的なハッシュ関数を構成しました。そこで利用されたグラフの一つが、頂点を超特異楕円曲線とし、辺がそれらの間の同種写像から成るグラフです。このようなグラフは同種写像グラフと呼ばれます。この構成をアーベル多様体に一般化することによって、近年超特別アーベル多様体の同種写像グラフの組み合わせ論的および代数的性質の研究が進展しています。そこで、今回はこれらの進展を紹介します。また、田中亮吉氏（京都大学）と山内卓也氏（東北大）との共同研究で得られた、超特別アーベル多様体の同種写像グラフのスペクトラルギャップに関する成果 (arXiv:2201.04293) についても紹介したいと思います。

プログラム

12月20日（火）

14:00-15:30

加藤 本子 （琉球大学 教育学部）
リチャード・トンプソンの群とその応用

概要 : トンプソン群はRichard Thompsonによって1960年代に発見された非可換な無限群である. トンプソン群にはF・T・Vの3種類があり, それぞれ単位区間・単位円・カントール空間のある種の同相写像のなす群として定義される. これらの群は数学のさまざまな分野に自然に表れ, 多くの変わった性質を持つことが知られている. この講演では, 幾何学的群論の観点からトンプソン群について紹介し, これらの群を公開鍵暗号に応用する試みについて述べる。

15:40-17:10

永野 哲也 （長崎県立大学 情報システム学科）
フィンスラー暗号

概要 : この話では、フィンスラー幾何学が有する非対称性の性質に依存する公開鍵暗号系を議論する。初出は2019年のCSS2019である。幾何学の背景を簡単に見た後、暗号化と復号の機能を幾何学的な直観と手順でより体系付けて捉える。次いで、暗号の強度について改良された点を説明する。また、同じ性質に依存するデジタル署名系についても言及する。

12月21日（水）

9:30-11:00

Ishak Meraouche （九州大学 大学院システム情報科学府）
Advances in Neural networks based Cryptography

Abstract : Artificial Intelligence (AI) and cryptography have always been separate disciplines in the past. Early AI models were not able to learn the simplest and most primitive mathematical functions or operations such as the XOR operation. Due to this fact, interest in building AI models that can learn cryptographic techniques have decreased significantly until the late 90s and early 2000s where some models were introduced. However, with the advances in AI, especially with deep learning, things are starting to change. Multiple models based on Generative Adversarial Networks (GANs) have been introduced since late 2016 and have shown significant performance and security in encryption. In this talk, we will start by seeing how AI based cryptography has evolved since the early 2000s. Next, we will survey the most prominent GANs models that have been proposed in recent years and were able to learn strong cryptographic techniques. After that, we will see the security of these models and how their security can be evaluated. Lastly, we will introduce our contributions to this topic.

11:10-12:40

相川 勇輔 （三菱電機）
Isogeny Graphs and Cryptography

概要 : Charlesらはエクスパンダーグラフ上のランダムウォークから暗学的なハッシュ関数を構成しました。そこで利用されたグラフの一つが、頂点を超特異楕円曲線とし、辺がそれらの間の同種写像から成るグラフです。このようなグラフは同種写像グラフと呼ばれます。この構成をアーベル多様体に一般化することによって、近年超特別アーベル多様体の同種写像グラフの組み合わせ論的および代数的性質の研究が進展しています。そこで、今回はこれらの進展を紹介します。また、田中亮吉氏（京都大学）と山内卓也氏（東北大）との共同研究で得られた、超特別アーベル多様体の同種写像グラフのスペクトラルギャップに関する成果(arXiv:2201.04293)についても紹介したいと思います。