2025年度共同利用研究報告書

2025年08月31日
所属・職名 電気通信大学・情報理工学研究科・助教
宮原 大輝

	整理番号	2025a036

1.研究計画題目	産学連携と数理・暗号分野連携によるカードベース暗号の深化と新境地Ⅱ			
2.新規・継続	継続			
3.種別	一般研究			
4.種目	短期共同研究			
5.開催方法	ハイブリッド開催			
6.研究代表者	氏名	宮原 大輝		
	所属	電気通信大学・情報理工学研究科	職名	助教
7.研究実施期間	2025年05月27日(火曜日)～2025年05月30日(金曜日)			
8.キーワード	カードベース暗号、秘密計算、ゼロ知識証明、有限群、アソシエーションスキーム			
9.参加者人数	65人			

10.本研究で得られた成果の概要

本研究集会「産学連携と数理・暗号分野連携によるカードベース暗号の深化と新境地Ⅱ」は、2025年5月27日(火)～5月30日(金)に実施され、カードベース暗号や現代暗号理論またはグラフ理論を専門とする研究者が一堂に会し、集中的な研究議論が実施された。本年度は、過去2回に渡って開催された同種の研究集会を融合させるような試みとして、未解決問題の更新状況を整理して共有することと、若手研究者同士での研究交流の促進を狙った。まず未解決問題について具体的には、2年前の研究集会で共有された問題「ANDプロトコルの枚数とシャッフル回数に対する不可能性」が、2024年後半から2025年初頭にかけて解決されたことを共有した。またパズルの解に対するゼロ知識証明プロトコルについても、いくつかのパズルに対する構成が提案されていることも報告した。公開研究集会でこれらを広く周知することにより、新規参入者の機会損失を低減できるとともに、カードベース暗号に関する研究分野の盛り上がりも示すことができた。次に若手研究者との研究交流については、学生を含む計8名が参加し、各講演者が準備したスライドを基に、以下の話題について白熱した議論を交わした：共役な巡回群の数え上げと円順列、ランダムカットによるランダム二等分割カットの実装とデリミタやブランチングシャッフル、差分プライバシーを考慮する関数とノイズの制約、ゼロ知識証明における検証回数削減、対称ブール関数の評価とシャッフルの種類、独立集合問題に対するゼロ知識証明の試作。どの話題についても各参加者が主体的にスライドや黒板を囲んで議論し、一部の話題については非自明な結果を得るところまで成果を挙げることができた。特に異なる専門分野の研究者が集い、集中的に議論を重ねたことで具体的な成果が得られたことは、本分野の持続的な発展に向けて非常に意義深い経験である。また、学生をはじめとする新たな研究者ネットワークを構築できた点も大きな成果である。

公開ワークショップにおける成果
未解決問題の解決状況（宮原）
　一昨年度および昨年度の研究集会で提示された未解決問題や課題に関して、現在の更新状況を共有した。具体的には、秘密計算・ゼロ知識証明プロトコルに関して未解決問題がいくつも解決されたことを示し、また派生して生まれた課題を共有した。

ランダムカットのみの4枚XORプロトコルに対する形式検証と不可能性証明（池田）
　カードベース暗号において重要とされるプロトコルとして、2色カードを用いた2入力ANDプロトコルおよびXORプロトコルが存在する。特に、実用的なシャッフル手法とされる「ランダムカット」のみを用いたプロトコルの設計は重要な課題であり、使用するカードの枚数や必要なシャッフル回数の下限を明らかにすることが期待されている。発表者は今回、ランダムカットのみを用いた4枚2入力のコミット型XORプロトコルが構成不可能であることを示し、この成果をAPKC 2025にて発表する予定である。本公開ワークショップでは、以下の内容について報告を行った：
・ランダムカットのみを用いた2入力ANDプロトコルおよびXORプロトコルに関する現状
・ランダムカットのみを用いた4枚2入力コミット型XORプロトコルの構成不可能性の証明
・不可能性を示すための形式的手法と、手証明による証明戦略について

カードを用いた差分プライバシメカニズムの視覚的表現（江利口）
　差分プライバシとは、平均値や中央値といった計算結果に対して、適切に設計された乱数（ノイズ）を加えることで、個々のデータが含まれているか推定できないようにするプライバシ保護技術である。本講演では、FUN2024で発表した、入力ビットの和に対して差分プライバシを満たすカードベースプロトコルを紹介した。将来的な課題として以下の問題を挙げた。
・任意の関数に対して差分プライバシを満たすカードベースプロトコルの構成
・提案プロトコルにおける必要カード枚数の効率化

部分開示操作を用いた効率的なカードベースプロトコル（本多）
　カードベースプロトコルには、トランプカードを使用するものがある。トランプカードの表面には、スートと数字に合わせたデザインがあり、部分開示操作はトランプカードの表面のデザインの任意の一部分のみを開示する操作である。発表者はIWSEC2024にて、部分開示操作を提案し、それを使用してANDプロトコルと4枚COPYプロトコルを有限時間かつランダムカットのみで構成した。本公開ワークショップでは、以下の内容について報告を行った：
・部分開示操作とその使用例について
・部分開示操作を使用したコミット型の4枚ANDプロトコルについて
・部分開示操作を使用した4枚COPYプロトコルについて

カードベースガーブルド回路のカード枚数削減手法とその応用（戸澤）
　カードベースガーブルド回路は、任意のブール関数を一回のシャッフルで計算可能な方式である。発表者は、このカードベースガーブルド回路において必要なカード枚数を削減する手法を、国際会議 UCNC 2023 および論文誌 Natural Computing にて発表した。本公開ワークショップでは、これらの発表済みの内容に加えて、今後の課題について以下の点を中心に報告を行った：
・カードベースガーブルド回路において、ゲートごとに必要な追加カードを8枚に削減する手法
・２入力ゲートに加えて、多入力ゲートをサポートするための拡張手法
・論理ゲートに加えて、算術ゲートをサポートするための手法

・ガーブルド回路とカードベースガーブルド回路における最適化手法の関係性の考察

1回または2回のシャッフルに関する未解決問題（品川）
　まず、シャッフルの基本的な性質について述べ、シャッフル間の関係性について論じ、シャッフルの世界地図を提示した。それに基づき、秘密計算（MPC）のシャッフルに関する未解決問題と、ゼロ知識証明（ZKP）のシャッフルに関する未解決問題を提示した。前者の未解決問題は以下の通りである。
・PSS 1回のMPCプロトコルは構成可能か？
・PSS 2回のMPCプロトコルのカード枚数をゲート24枚より削減可能か？
・一様閉シャッフル1回のMPCプロトコルのカード枚数をゲート8枚より削減可能か？
・一様シャッフル1回のMPCプロトコルのカード枚数をゲート6枚より削減可能か？
・巡回群シャッフルやパイルシフティングのMPCプロトコルの最小回数は？
後者の未解決問題は以下の通りである。
・PSS1回の非対話の数独ZKPプロトコルは構成可能か？
・PSS1回の対話型の数独ZKPプロトコルの他の構成は？
・9×9数独ZKPを5分以内で実行可能な実装方法は？
・数独以外のパズルに対する定数回のZKPプロトコルは？

遷移問題とゼロ知識証明（田村）
　遷移問題とは、特定のルールに則り、初期解を段階的に変更して目的解を得ることを目的とする問題である。APKC2024では、遷移問題の代表的な問題である、15パズル、シーケンシャルトークンスワッピング、トークンスワッピングの3つに対し、カードを用いたゼロ知識証明プロトコルを与えた。本講演では、APKC2024で発表した内容に加え、遷移問題に対するカードベース暗号の今後の発展性について考察した。講演後には、遷移問題とKWHツリーとの関連性、PSPACE完全問題に対しゼロ知識証明を行う意義、独立集合問題に対するゼロ知識証明プロトコル等について議論を行った。

天秤を用いるゼロ知識証明（金子）
　物理的な天秤を用いて暗号学的な計算を行う天秤ベース暗号プロトコルを紹介した。ここではISC2024で発表した提案プロトコルに加え、天秤による比較の順番を工夫することによる発展的な話題も提供した。本講演では、セキュリティモデルの設定に関する妥当性や、枝刈りによるさらなる高速化について議論ができた。特に本講演をきっかけとして検証手順を省略する方法の理解が進み、後ろに記載するようにルールの冗長性との関連を整理できたことは特筆に値する。また参加者間による比較ソートに関する議論を通じて新たな研究者ネットワークを構築できたことも大きい。

異種カードを利用した2者間カードプロトコル（須賀）
　2者間k値入力プロトコルにおいて、UNOカードとトランプカードなど異なる種類のカードを用いたカードベース暗号についての検討結果に関して共有された。本来は「データ境目」を意味するデリミタカードという概念を導入し、RBCで実現していたシャッフルをRCのみで実現するアイデアを提示した。既存の2者間2値入力プロトコル、特にコミットメント型の従来の基本方式において、片方の入力をデリミタカードとみなすことで提案方式が適用可能であること、さらにスタンダードモデルではなく一般的に流通しているトランプカード2種類を用いた数値の入力差のみを算出するナイーブな方式を起点に議論された。
　会場からはデリミタカードと類似する概念を導入したいくつかの既存方式について指摘があり、非公開議論の場において同様の効果が得られることを確認できた。シャッフル方式としてもRBCを含む新しいシャッフル方式に関する提案がなされている。このシャッフル方式をパーツとした新しいプロトコルの構成が可能かについて問いかけが行われた。その他の

未解決問題としては、異種カードでの4枚COPYを実現できるかについて失敗事例の紹介とともに共有された。

==========
非公開ワークショップにおける成果

5月27日（火曜）【非公開】10:00-17:30
参加者：宮原大輝、水木敬明、須賀祐治、品川和雅、池田 昇太、江利口 礼央、本多 由昂、金子 尚平
　代表者の宮原から本ワークショップの開催主旨を説明し、8名によるディスカッションを開始した。各講演者が準備してきた発表スライドを元にひとつひとつのテーマについて集中的に議論を行い、翌日の公開ワークショップに向けて準備を進めた。
　池田氏からは巡回的なシャッフル操作のみを用いる際の不可能性証明に関して紹介があり、数学的な知見から共役な巡回群の数え上げが話題に挙がり、ネックレスやブレスレットおよびオイラー数との関連について持ち帰りで検討することとなった。本多氏からはトランプカードプロトコルの実装方法に関して紹介があり、特にカード列の一部にマーキングを施す方法とUedaらの既存手法との関連や、Kochらの定式化上での扱いについて議論が交わされ、興味深い検討事項となった。江利口氏からは差分プライバシの視覚的表現について紹介がなされ、これに対しカードベース暗号の専門家から必要なカード枚数や手順数の評価、出力変換方法などについて多様なフィードバックが寄せられ、異なる専門領域を横断する活発な議論が生じた。

5月29日（木曜）【非公開】10:00-17:30
参加者：宮原大輝、水木敬明、須賀祐治、品川和雅、田村 祐馬、戸澤 一成、金子 尚平
　前日の公開ワークショップを振り返り、特に質疑の時間におけるさまざまなコメントやディスカッションについてレビューを行い、本共同研究のアウトプットの一つであるスライド資料のさらなるブラッシュアップにつなげた。また、カードベース暗号の研究分野を含め、今後の展望や展開について充実した議論を持つことができた。特にゼロ知識証明の効率化に繋がる重要な成果として、パズルのルールの冗長性から検証の一部を省略できることが成果として得られ、組織委員の代表者3名により論文としてアウトプットすることとなった。

5月30日（金）【非公開】10:00-17:30
参加者：宮原大輝、水木敬明、須賀祐治、品川和雅
　組織委員の発表について中心的にディスカッションを行った。品川氏から、追加カードのBatchingによるシャッフル操作回数の効率化に関する最新結果が紹介された。これについて参加者より、追加カード枚数と効率化の関係式に関していくつか質問があり、ディスカッションが行われた。関連して須賀氏から、カードを表にしてBatchingした場合の効率化やシャッフル操作の指標について話題提供があり、初日の本多氏の検討事項とも関連させて実装方法に関する理解が進んだ。また須賀氏より関連して、2色カード組とトランプカード組を組み合わせたプロトコルやデリミタに関する紹介があり、関連するカードベース暗号の既存研究についてディスカッションが行われた。

受付中

…開催日：2025/05/28〜2025/05/28

産学連携と数理・暗号分野連携によるカードベース暗号の深化と新境地Ⅱ｜2025a036

カテゴリー：イベント　タグ：一般研究 短期共同研究

開催概要

- **開催方法**：九州大学 伊都キャンパス及びZoomミーティングによるハイブリッド開催
- **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オーディトリアム（W1-D-413）
- **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**：一般研究-短期共同研究
- **研究計画題目**：産学連携と数理・暗号分野連携によるカードベース暗号の深化と新境地Ⅱ
- **研究代表者**：宮原 大輝（電気通信大学・情報理工学研究科・助教）
- **研究実施期間**：2025年5月27日（火）〜 2024年5月30日（金）
- **公開期間**：2025年5月28日（水）
- **研究計画詳細**：https://joint2.imi.kyushu-u.ac.jp/research_chooses/view/2025a036

プログラム

5月27日（火）【非公開】10:00~17:30

5月28日（水）【公開】

10:00-12:00　オープニング、セッション1

10:00-10:10

宮原 大輝（電気通信大学）
オープニング

10:10-10:40

宮原 大輝（電気通信大学）
未解決問題の解決状況

10:40-11:20

池田 昇太（茨城大学）
ランダムカットのみの4枚XORプロトコルに対する形式検証と不可能性証明

11:20-12:00

江利口 礼央（産業技術総合研究所）
カードを用いた差分プライバシメカニズムの視覚的表現

13:30-15:30　セッション2

13:30-14:10

戸澤 一成（東京大学）
カードベースガーブルド回路のカード枚数削減手法とその応用

14:10-14:50

品川 和雅（筑波大学）
1回または2回のシャッフルに関する未解決問題

14:50-15:30

本多 由昂（茨城大学）

部分開示操作を用いた効率的なカードベースプロトコル

15:45-17:45　セッション3、クロージング

- **15:45-16:25**

須賀 祐治（株式会社インターネットイニシアティブ）
異種カードを利用した2者間カードプロトコル

- **16:25-17:05**

金子 尚平（電気通信大学）
天秤を用いるゼロ知識証明

- **17:05-17:45**

田村 祐馬（東北大学）
遷移問題とゼロ知識証明

- **17:45-17:50**

水木 敬明（東北大学）
クロージング

5月29日（木）【非公開】10:00~17:30

5月30日（金）【非公開】10:00~17:30