2024年度共同利用研究報告書

2024年08月23日

所属・職名 株式会社インターネットイニシアティブ　セキュリティ情報統括室・シニアエンジニア
須賀 祐治

	整理番号	2024a035

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			
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	須賀 祐治		
	所属部局名	株式会社インターネットイニシアティブ　セキュリティ情報統括室	職名	シニアエンジニア
7.研究実施期間	2024年05月20日(月曜日)～2024年05月23日(木曜日)			
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	49人			

10.本研究で得られた成果の概要

本研究「産学連携によるカードベース暗号の数理的未解決問題と新課題の整理」は、2024年5月20日から23日にかけて実施され、カードベース暗号を専門とする研究者が再び集い、昨年度の成果を踏まえて新たな課題に取り組んだ。本年度の集会では、若手研究者の発表枠を大幅に拡大し、彼らに発表の機会を提供するとともに、工学や理学に精通したシニア研究者との対話を通じて、研究に新たな視点や解釈をもたらすことを目指した。この取り組みにより、参加者間の交流が促進され、さらなる研究の発展に寄与できたと考えられる。具体的な議論内容としては、昨年度に得られた未解決問題リストに対する進展が報告されるとともに、新たに発見された未解決問題が追加された。カードベースガーブルド回路、効率的な対称関数プロトコル、各種ペンシルパズルに対する物理的ゼロ知識証明、3Dプリンタを活用した応用事例など、幅広いかつ最新の研究成果が発表され、活発な議論が交わされた。また、代数学との関連研究として、一様巡回群分解に基づく一様閉シャッフルや、正則グラフでアクセス構造を表現する非コミットメント型プロトコルについても取り上げられ、カードベース暗号のさらなる発展に向けた重要な一歩が踏み出された。この結果、カードベース暗号の研究分野は一層の進展を遂げ、新規参入研究者の増加が期待される。

成果報告書

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
研究代表者：須賀 祐治（株式会社インターネットイニシアティブ　セキュリティ情報統括室・シニアエンジニア）
研究実施期間：2024年5月20日（月）～ 2024年5月23日（木）
公開期間：2024年5月22日（水）
研究計画詳細：https://joint1.imi.kyushu-u.ac.jp/research_chooses/view/2024a035

趣旨

カードベース暗号は、物理的なカード組を用いて秘密計算やゼロ知識証明等の暗号機能を実現する技術である。その特徴は、カードを並べることによりプロトコルを視覚的・体験的に実行できることであり、暗号技術に関する教育的効果が期待されていることに加えて、非専門家が日常生活において利用できる実用的な暗号技術であるといえる。2023年5月に開催された前回のIMI短期共同研究では、カードベース暗号における未解決問題リストを公開することにより新規参入研究者の増大を目指した。報告書に記載されている未解決リストだけでなく、広く公開されている当日の講演動画や講演資料も参照できることもあり、結果として国内外のカードベース暗号の論文数は増加に転じており、特に新規参入した研究者を含め大変好評であったことが窺える。この状況を踏まえ、以下2つの軸で短期共同研究を継続開催すべきであるという考えに至った。第1に若手研究者の招聘枠を多めに確保することで講演の機会を増やすとともに、工学、理学（特に数学）に精通したシニア研究者との対話を通して、研究の新しい解釈や気付きなどを共有することで、さらなる研究の高みを目指してもらうことを目標とする。代表者としては、若手とシニア研究者の交流の場としても機能できるよう配慮したい。第2に、昨年度得られた未解決問題に対してここ1年間で解決できた課題の共有を行うとともに、新しい視点からの研究課題を追加するなど未解決問題リストのブラッシュアップを目指すこととする。このような2つの軸を持つことで、研究領域の増大と並行してさらなる新規参入研究者の増大に資すると考える。

プログラム

- 5月20日（月）【非公開】13:30-17:30
- 5月21日（火）【非公開】10:00-17:30
- 5月22日（水）【公開】10:00-17:45@IMIオーディトリアム
    - 10:00-12:00 オープニング・セッション1
        - 水木 敬明(東北大学)
          昨年の研究集会からのアップデート
        - 小野 知樹(電気通信大学)
          ゲートあたり6枚で実行できるカードベースガーブルド回路
        - 高橋 由紘(茨城大学)
          多色カードを用いた効率的な対称関数プロトコル
    - 13:30-15:30　セッション2

        - 安部 芳紀(電気通信大学 <現：セコム株式会社　IS研究所>)
          数独に対する物理的ゼロ知識証明
        - 初貝 恭祐(電気通信大学)
          Sumpleteに対する物理的ゼロ知識証明
        - 宮原大輝(電気通信大学)
          月か太陽に対する物理的ゼロ知識証明
    - 15:45-17:45　セッション3・クロージング
        - 伊藤 優樹(東北大学)
          3Dプリンタのカードベース暗号への応用
        - 品川 和雅(茨城大学)
          一様巡回群分解に基づく一様閉シャッフルの実現方法とその応用
        - 須賀 祐治(株式会社インターネットイニシアティブ)
          正則グラフでアクセス構造を表現する非コミットメント型カードプロトコル
- 5月23日（木）【非公開】10:00-17:30

本プロジェクトの成果

公開ワークショップにおける成果

- 昨年の研究集会からのアップデート（水木）
  2023年度の研究集会「産学連携によるカードベース暗号の数理的未解決問題と新課題の整理」を振り返り、当時に提示された未解決問題や課題に関して現在の状況・アップデートを報告するととともに、カードベース暗号の研究分野のここ1年の発展の状況を共有した。

- ゲートあたり6枚で実行できるカードベースガーブルド回路（小野）
  ガーブルド回路は任意の論理回路を秘密計算できるプロトコルである。本公開ワークショップでは、2色カードを用いたガーブルド回路について以下の二つのプロトコルについて主に紹介した。
    - Tozawaらの1ゲートあたり8枚のプロトコル
    - Onoらの1ゲートあたり6枚のプロトコル

  また、質疑応答において、ANDゲートとXORゲートに対する操作が同じであることから論理回路を一部秘匿して秘密計算を行う応用の可能性が示された。

- 多色カードを用いた効率的な対称関数プロトコル（高橋）
  対称関数とは、入力の順序を入れ替えても出力値が変わらない関数であり、AND関数やEQ関数を含む重要な関数である。本公開ワークショップでは、通常のカードベース暗号において使用されるクラブカードとハートカードの2色カードに、スペードカードとダイヤカードを加えた合計4色のカードを用いることによって、既存の対称関数プロトコルのカード枚数を削減した。以下、本研究の成果と未解決問題を列挙する。
  成果：
    - 4色2n枚のLas Vegasプロトコルの構成
    - 3色2n+1枚の有限時間プロトコルの構成
    - シャッフル回数を削減した4色2n枚のLas Vegasプロトコルの構成

  未解決問題：
    - 2色2n+1枚の有限時間プロトコルの構成(または、不可能性の証明)
    - 2色または3色2n枚のLas Vegasプロトコルの構成(または、不可能性の証明)

- 数独に対する物理的ゼロ知識証明（安部）
  Gradwholeらの論文を皮切りに、数独に対する物理的ゼロ知識証明プロトコルが数多く提案されている。本公開ワークショップでは、既存のプロトコルを証明手法により以下の2種類に分類し、それぞれ1つずつ具体的なプロトコルを紹介した。
    - 数独の解答の盤面そのものをカードで表現する手法
    - 各数字が入るマス目の座標をカードで表現する手法

  また、物理的ゼロ知識証明における入力の作成方法について考察し、対話的な入力作成を許すことでプロトコルの効率を改善する手法を紹介した。
  さらに、新しい物理的ゼロ知識証明に関するアイデアを2つ提示した。
    - 光を用いる手法
    - 計算能力が低い検証者を仮定したモデルでの、非対話の物理的ゼロ知識証明

- Sumpleteに対する物理的ゼロ知識証明（初貝）
  2023年3月にChatGPTはSumpleteというパズルを生成した。発表者はSumpleteのNP完全性の証明・物理的ZKPの考案を行い、昨年開催されたCOCOON2023で両成果を発表した。本公開ワークショップでは、COCOONで発表した内容に加え、その後の進捗について報告した。（■はCOCOONの内容を、□はその後の進捗を表す）

  ■部分和問題からに帰着による、マスの数字に制限のないSumpleteのNP完全性証明
  □XSATからの帰着による、マスの数字に制限のあるSumpleteのNP完全性証明
  ■整数コミットメントを用いた、Sumpleteに対する物理的ZKPの提案
  □2の補数表現を用いた、Sumpleteに対する物理的ZKP

  非公開日での議論や発表後の質疑応答から、プロトコルの評価・改良のアイディアについて、以下のコメントを頂いた。

  ◎2つの物理的ZKPの比較
  - 目指す指針によって、プロトコルの優劣が変わるとご指摘を頂いた
  - 操作の分かりやすさ・操作の容易さ：整数コミットメントを用いる手法が適切
  - 厳密な定義の追究：2の補数表現を用いる手法が適切

  ◎整数コミットメントに用いるカードの削減
  - 目標値近傍でなければ、整数コミットメントへの加算で生じる数字のオーバーフローは無視できるため、最小値や最大値を表すカードを削減できるのでは？

  ◎複数マスに対する並列的な加算操作
  - 数字が同じマスの加算操作を並列して一度に行うことで、検証に必要なシャッフル回数（またはステップ数）を削減できるのでは？

  ◎ダミーカウンターの削除
  - 高橋さん（茨城大学）の提案プロトコル2：ランダム二等分割カットによって、入力カード列の恒等置換と逆順のいずれかを出力するプロトコルを考案
  - マスに置かれたカードペアの値によって、カウンターの恒等置換（＝何も足さない）または数字を足したカウンターを出力するプロトコルを作成できるのでは？
  - 切り替えのためにダミーカウンターを用いる必要がなくなる

- 月か太陽に対する物理的ゼロ知識証明（宮原）
  本発表では、まず昨年の研究集会で提示したカードベースゼロ知識証明プロトコルにおける未解決問題に関して、進捗状況を示した。特に数独に対するプロトコルは、ここ1年の研究によって、極限に近いところまで効率性が明らかになっていることを述べた。そして、ペンシルパズルの一つである「月か太陽」の解に対して、カード組を用いるゼロ知識

証明プロトコルの構成を示した。質疑応答を通じて、解に関する一部の情報とパズルのNP困難性の関係について議論できた。

- 3Dプリンタのカードベース暗号への応用（伊藤）
  カードベース暗号の主要な目的の1つは、物理的なカード組等の身近な道具を使って暗号機能を実現することであり、人間が扱い易い、あるいは作成し易い道具を検討することはこの研究分野において非常に重要である。本公開ワークショップでは、3Dプリンタを用いてカードベース暗号に有用な装置・道具を作成したことを報告した。特に、複雑なシャッフルの実装のための特殊なカードケースは、対称関数の秘密計算の効率化に寄与することが学術的にも興味深いことを共有した。3Dプリンタで具体的に作成した装置は次の通りである。
  - Five-Card Trick用オープン装置
  - 特殊カードケース
  - カードを取り出すのための補助装置
  - 特殊カードケースのシャッフル器

- 一様巡回群分解に基づく一様閉シャッフルの実現方法とその応用（品川）
  本講演では、一様巡回群分解という有限群の分解の一種を定義し、その基本性質を示し、そのカードベース暗号への応用について報告した。一様巡回群分解の基本事実として、任意の可解群は一様巡回群分解を持つことを示した。任意の群が一様巡回群分解を持つかどうかはまだ解明されていないが、その探索範囲を限定するための補題も証明した。この理論のカードベース暗号への応用として、以下の二つの具体的な応用を与えた。
  - もしある群Gが一様巡回群分解を持てば、群Gに対応する一様閉シャッフルを巡回群シャッフルの列に分解することを示した。
  - 15パズルとルービックキューブに対して、秘匿した状態で一様ランダムなインスタンスを生成する方法（秘匿ランダムインスタンス生成）を示した。

  重要な未解決問題としては、任意の群が一様巡回群分解を持つかどうかを示すことである。別の問題として、他のパズルに対する秘匿ランダムインスタンス生成プロトコルを構成することも挙げられる。

- 正則グラフでアクセス構造を表現する非コミットメント型カードプロトコル（須賀）
  前回の研究集会にて提示したJohnson scheme J(v,k) に関連するカードプロトコルのナイーブな構成から派生して、入力を制限させることにより得られるいくつかの方式について提示した。具体的には与えられたデッキ（カード束）をランダムカットのみから得られるように制限することで、入力をv_C_k通りからv通りに限定する。このようにカード入力を限定することで、プロトコル出力のアクセス構造を表現する正則グラフの頂点とカード入力を同一視し、2点の連結性や2点間の距離に応じて、プロトコル出力が表現されるケースを扱った。このとき、アクセス構造を表現する正則グラフは位数vの巡回群の元と考えられることから、一般的な有限群の場合にカードプロトコルとしてどのような制約を与えているのかについても議論した。
  以下本講演で提示した未解決問題について列挙する:
  - 2-party多値入力の一致関数の実現（ナイーブな手法については講演中に板書で、また最終講演資料には細く資料として提示）
  - （Hamming schemes での構成事例を提示した上で）Johnson scheme J(v,k) に関連するカードプロトコルの構成（もしくは既存のカードプロトコルがJohnson schemeと関連している事例の例示）
  - 位数4,6のアソシエーションスキームと関連するカードプロトコルの構成

- 2枚入力 3-valued n-party 一致関数の構成（緩い条件：上下カード・非コミットメント型）
- カードプロトコルにおいてカード入力を制限する一般的な構成
- （ひとつ前の未解決問題を受けて）カード入力として1枚カードを追加することによる新しいプロトコルを構成できるが、この拡張方式に呼応する一般的拡張方式の提示

非公開ワークショップにおける成果

- 5月20日（月）【非公開】13:30-17:30
  参加者：須賀祐治、水木敬明、縫田光司、品川和雅、宮原大輝、初貝 恭祐、小野 知樹、高橋 由紘
  代表者の須賀から本ワークショップの開催主旨を説明し、遠隔参加者含め8名によるディスカッションを開始した。品川氏より3Dプリンタを用いたシャッフル補助器具のプロトタイプである暗号コマ等の紹介がなされた。Five card trick などで用いられる一般的なシャッフル方式であるランダムカットを、高速で回転させることにより人間が目視するだけでは識別できないためプロトコルの安全性と高めることができる効果を示している。議論においてはランダム2等分割カットなどでの安全な適用方法や、コマ自体の改良方式について複数のアイデアが共有されるなど、論理的な安全性だけでなく、物理的にも安全性を確保する方向に向けた方式に関して議論が行われた。
  宮原氏からは、まず昨年の研究集会で提示した未解決問題の進捗状況が共有された。特に数独の解に対するゼロ知識証明プロトコルについて、シャッフル回数削減の劇的な改善が行われ、それに伴い、シャッフル回数の下限に関する新しい未解決問題が生じていることが述べられた。また1つの輪を描くペンシルパズルに対するゼロ知識証明プロトコルに関する最新成果が紹介され、アルゴリズムの正当性や安全性について深く議論した。その過程で、より効率的なアルゴリズムの糸口を発見することができた。

- 5月21日（火）【非公開】10:00-17:30
  参加者：須賀祐治、水木敬明、縫田光司、品川和雅、宮原大輝、初貝 恭祐、小野 知樹、伊藤 優樹、高橋 由紘
  午前中は、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った。前日の議論も踏まえ各自アップデートした発表スライドを再度共有して議論を深め、翌日の公開ワークショップに向けて準備を進めた。午後は、未解決問題や課題をブラッシュアップ、また新しい未解決問題や課題についてのディスカッションを行った。

- 5月23日（木）【非公開】10:00-17:30
  参加者：須賀祐治、水木敬明、縫田光司、品川和雅、宮原大輝
  前日の公開ワークショップをふりかえり、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。
  午前中は宮原氏によるペンシルパズルに対するゼロ知識証明プロトコルの既存方式に関する解説を中心に議論を深めた。午後は品川氏によるSCIS2022論文をベースに巡回群分解に関わる話題，また須賀より新しいシャッフルと有限群の関係性など、群論に関わる議論を行った。

開催日：2024/05/20～2024/05/23

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｜2024a035

Deepening and new frontiers in card-based cryptography through industry-academia collaboration and cooperation in the fields of mathematics and cryptography

5 月 20 日（月）13:30−17:30 非公開

5 月 21 日（火）10:00−17:30 非公開

5 月 22 日（水）10:00−17:45【公開】@IMI オーディトリアム

10:00-12:00　オープニング・セッション 1

10:00-10:10 須賀 祐治(株式会社インターネットイニシアティブ)

オープニング

10:10-10:40 水木 敬明(東北大学)

昨年の研究集会からのアップデート

10:40-11:20 小野 知樹(電気通信大学)

ゲートあたり 6 枚で実行できるカードベースガーブルド回路

11:20-12:00 高橋由紘(茨城大学)

多色カードを用いた効率的な対称関数プロトコル

13:30-15:30　セッション２

13:30-14:10 安部 芳紀(電気通信大学 <現：セコム IS 研究所>)

数独に対する物理的ゼロ知識証明

14:10-14:50 初貝 恭祐(電気通信大学)

Sumplete に対する物理的ゼロ知識証明

14:50-15:30 宮原大輝(電気通信大学)

月か太陽に対する物理的ゼロ知識証明

15:45-17:45　セッション３・クロージング

15:45-16:25 伊藤 優樹(東北大学)

3D プリンタのカードベース暗号への応用

16:25-17:05 品川 和雅(茨城大学)

一様巡回群分解に基づく一様閉シャッフルの実現方法とその応用

17:05-17:35 須賀 祐治(株式会社インターネットイニシアティブ)

正則グラフでアクセス構造を表現する非コミットメント型カードプロトコル

17:35-17:45 須賀 祐治(株式会社インターネットイニシアティブ)

クロージング

10:00-12:00 Opening, Session1

10:00-10:10 Yuji Suga
Opening Remarks

10:10-10:40 Takaaki Mizuki
Updates from the Last IMI Short-term Joint Research

10:40-11:20 Tomoki Ono
Card-based Garbled Circuits with Six Cards per Gate

11:20-12:00 Yoshihiro Takahashi
Efficient Card-Based Protocols for Symmetric Functions Using Four-Colored Decks

13:30-15:30 Session2

13:30-14:10 Yoshiki Abe
Physical Zero-Knowledge Proofs for Sudoku

14:10-14:50 Kyosuke Hatsugai
A Physical Zero-knowledge Proof for Sumplete

14:50-15:30 Daiki Miyahara
A Physical Zero-knowledge Proof for Moon-or-Sun

15:45-17:45 Session3, Closing

15:45-16:25 Yuki Ito
Applications of 3D Printer to Card-Based Cryptography

16:25-17:05 Kazumasa Shinagawa
How to Implement Uniform Closed Shuffles Based on Uniform Cyclic Group Factorization and Its Applications

17:05-17:35 Yuji Suga
Non-committed Card Protocols that Represent the Access Structure in Given Regular Graphs

17:35-17:45 Yuji Suga
Closing Remarks

5 月 **23** 日（木）**10:00–17:30** 非公開