2023年度共同利用研究報告書

2023年09月01日

所属・職名 東北大学サイバーサイエンスセンター・准教授
水木 敬明

	整理番号	2023a020		
1.研究計画題目	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			
2.新規・継続	新規			
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	水木 敬明		
	所属部局名	東北大学サイバーサイエンスセンター	職名	准教授
7.研究実施期間	2023年05月29日(月曜日)～2023年06月01日(木曜日)			
8.キーワード	カードベース暗号、秘密計算、有限群、アソシエーションスキーム			
9.参加者人数	62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、2023年5月29日～6月1日に実施され、カードベース暗号を専門とする研究者が一同に集い、それぞれ得意とする分野の現状や未解決問題を整理して持ち寄り、集中的に議論を行った。具体的には、ANDプロトコルにまつわる未解決問題、カードベースZKPプロトコル、無開示性を持つカードベース暗号プロトコルについて、カードベース暗号に登場するさまざまなカード組と符号化、デッキ分割法とアソシエーションスキーム、カードベース暗号に現れる数学、プライベートモデルにおける秘匿置換を用いたカードベース暗号それぞれについて、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、計算モデルの分類をはじめ、多くの点においてコンセンサスを形成した。そのようにしてブラッシュアップした未解決問題と新課題の整理を公開ワークショップにおいて広く周知することができ、カードベース暗号の研究分野の発展に資することができた。

成果報告書

開催概要

開催方法：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
研究代表者：水木 敬明（東北大学サイバーサイエンスセンター・准教授）
研究実施期間：2023年5月29日（月）～ 2023年6月1日（木）
公開期間：2023年5月31日（水）
研究計画詳細：https://joint1.imi.kyushu-u.ac.jp/research_chooses/view/2023a020

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。カードベース暗号は1990年代に萌芽的研究が提案されたが、2010年代に本研究代表者らのグループが計算モデルを抽象機械によって数理的に定式化したことを皮切りに、複数の研究グループが活発に論文成果を発表するようになり、特にここ数年論文数が急増している。また同分野の近年の研究には、有限群論、アソシエーションスキーム、形式検証系などの数理科学的な題材との関連についての新しい研究テーマも現れてきており、研究分野として急成長を遂げる転換点にあると考えられる。このようにカードベース暗号分野が急速に拡大する状況において、この分野の未解決問題を把握すること自体のコストが高くなっており、新規参入のハードルは年々上がっている。本共同研究では、さらなる分野の発展のため、新規に参入する研究者の増加を目標とし、この分野を先導する産業界と学術界の研究者が集中的に議論し、潜在的な研究者の参入のガイドになるような、未解決問題や新課題の整理を行う。そして、得られた整理の結果を未解決問題リストのような形で公表することにより、新規参入研究者の増大に資する。

プログラム

- 5月29日（月）10:00−16:30 非公開
- 5月30日（火）10:00−16:30 非公開
- 5月31日（水）【公開】@IMIオーディトリアム
    - 10:00-11:30　オープニング、セッション1
        - 水木 敬明（東北大学 サイバーサイエンスセンター）
          ANDプロトコルにまつわる未解決問題
        - 宮原 大輝（電気通信大学 情報理工学研究科）
          カードベースZKPプロトコル
    - 13:00-14:30　セッション2
        - 中井 雄士（豊橋技術科学大学）
          秘匿置換を用いたカードベース暗号
        - 真鍋 義文（工学院大学 情報学部情報科学科）
          無開示性を持つカードベース暗号プロトコルについて
    - 15:00-17:15　セッション3、クロージング

        - 品川 和雅（茨城大学 理工学研究科）
          カードベース暗号に登場するさまざまなカード組と符号化
        - 須賀 祐治（株式会社インターネットイニシアティブ）
          デッキ分割法とアソシエーションスキーム
        - 縫田 光司（九州大学マス・フォア・インダストリ研究所）
          カードベース暗号に現れる数学
- 6月1日（木）10:00−12:00, 16:00-19:00 非公開

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

- ANDプロトコルにまつわる未解決問題
  標準モデルにおけるANDプロトコルの考案・開発と計算限界の解明は、カードベース暗号の研究分野で最も歴史のあるテーマであり、これに関する数多くの論文がこれまで発表されている。本公開ワークショップでは、2色カード組を用いるという前提のもと、次のぞれぞれのプロトコルについて、現時点で分かっていることをサーベイとして示し、また多くの未解決問題や課題を提示した。
    - 非コミット型2入力ANDプロトコル
    - コミット型2入力ANDプロトコル
    - 多入力ANDプロトコル
    - 汎用プロトコル

- カードベースZKPプロトコル
  タイトルに現れるZKPはzero-knowledge proof（ゼロ知識証明）の略語であり、証明者と検証者による対話証明の一種である。本発表では、カード組を含む身近な道具立てを活用したZKPプロトコルに関する研究を整理し、以下の未解決課題を提示した。
    - ペンシルパズルの解に対するZKPプロトコルを、現実的な時間内で実行する方法、または効率化手法
    - これまでに国内会議等で検討されていないペンシルパズルに対するZKPプロトコルの構成

- 秘匿置換を用いたカードベース暗号
  標準的なカードベ―ス暗号は、すべての操作をテーブル上などで公開して行うモデルを採用している. 一方で、カードベース暗号にプライベートな操作（秘匿置換）を導入したモデルも存在する. 本発表ではプライベートな操作に基づくカードベース暗号に関する導入を行い、研究の現状整理を行った. また、以下の未解決問題を提出した.
    - 金持ち比べプロトコル以外で, 計算機ベースからカードベースへ変換可能なプロトコルの発見
    - 秘匿置換以外のプライベートな操作を導入することによるプロトコルの効率化
    - 秘匿置換に基づくカードベースZKPプロトコルの構築

- 無開示性を持つカードベース暗号プロトコルについて
  プライベート処理を行うカードベース暗号では、プロトコル実行中にカードの開示処理を行わないという無開示性を持つプロトコルを構成することができる。無開示性を持つプロトコルに関する既存の成果を発表し、以下の未解決問題を提出した。
    - 任意の関数を無開示性を持って計算する、効率のよいプロトコルの考案
    - 無開示性を持つプロトコルで計算可能な関数族の同定

- 開示処理を行うプロトコルの無開示性を持つプロトコルへの変換手法

- カードベース暗号に登場するさまざまなカード組と符号化
  カードベース暗号ではこれまで二色カードとトランプカードが伝統的に用いられてきたが、近年、上下カードや正多角形カードなどの新しい種類のカードが用いられるようになった。これらの新しいカード組の研究の現状を整理し、それらにまつわる未解決問題を提示した。具体的には、以下の未解決問題を提出した。
  - 上下カードを用いたn変数ANDプロトコルがn枚で構成できないことを示せ。(あるいは、n枚のANDプロトコルを構成せよ。)
  - 上下カードを用いた任意対称関数に対する最適なプロトコルを構成せよ。
  - 上下カードを用いた任意関数に対する最適なプロトコルを構成せよ。
  - 正多角形カードを用いたn枚以下の乗算プロトコルを構成せよ。
  - 100～1000程度の整数値までの実用的な加算プロトコルを構成せよ。
  - 1枚符号化のNiemi-Renvallのコピープロトコルについて、カード枚数や失敗確率の改善をせよ。
  - 1枚符号化のある関数のプロトコルについて、カード枚数や失敗確率の改善をせよ。

- デッキ分割法とアソシエーションスキーム
  扱うカードの種類として標準モデルで利用される2色カードではなく主に上下カードと呼ばれるカード束を用いた方式で，かつ非コミットメント型(結果開示の際にはすべてもしくは一部のカードを開示することで結果を得る方法)における最新の研究結果と未解決問題を提示した．非公開ワークショップでは有益な意見を参加者より得ることができ，新たな未解決問題についても最終講演資料に追記した．また質疑応答で板書を使い説明した内容については，講演時には提示しなかったスライドとして事後講演資料の中に提示している．
  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

- カードベース暗号に現れる数学
  カードベース暗号の既存研究の中で、数学分野および(カードベースではない)暗号分野との関連が特に強い題材について、既存の研究成果を整理するとともに今後の研究課題として未解決問題の紹介を行った。具体的には以下の題材について紹介した。
  - 出力の確率的生成を行うカードプロトコルの使用カード枚数の下界:
    不動点のない置換の一様ランダム生成を行うプロトコルを中心として、一様シャッフルを用いた有限時間プロトコルに必要なカード枚数の下界の解析を取り扱っ

た。特に、abc予想、素数定理、グラフ理論のKőnigの補題を用いた既存の下界証明技法を紹介し、関連する整数論の未解決問題を提示した。

- ○ 一様群シャッフルのより単純なシャッフルへの分解：
  カードベースプロトコルのシャッフル操作は、置換の集合上の確率分布の実現とも表現できる。この分布が対称群の部分群上の一様分布である場合（一様群シャッフル）は比較的実装しやすいとされているが、具体的な実装方法を与えるには、この部分群をより簡単な構造の部分群に（シャッフル操作と相性良く）分解できることが望ましい。この問題について既存の研究成果を紹介し、関連する有限群論の未解決問題を提示した。
- ○ カードベースゼロ知識証明に現れる秘密計算の問題：
  ある種のパズルの解のゼロ知識証明を行うカードプロトコルの構成には、カードベースに限定しない秘密計算として考えても面白い機能の実現が求められることがある。そうしたカードベース暗号と秘密計算の関係および関連する未解決問題を提示した。

非公開ワークショップにおける成果

- 5月29日（月）10:00−16:30 非公開
  参加者：水木敬明、須賀祐治、縫田光司、品川和雅、真鍋義文、宮原大輝
  代表者の水木から本ワークショップの開催主旨を説明し、各参加者の自己紹介を行なった。
  そののち、6人によるディスカッションを開始し、具体的には、ANDプロトコルにまつわる未解決問題、カードベースZKPプロトコル、無開示性を持つカードベース暗号プロトコルについて、カードベース暗号に登場するさまざまなカード組と符号化、デッキ分割法とアソシエーションスキーム、カードベース暗号に現れる数学それぞれについて、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、計算モデルの分類をはじめ、多くの点においてコンセンサスを形成し、各自持ち寄った未解決問題や課題をブラッシュアップするとともに、新しい未解決問題や課題もうまれた。
- 5月30日（火）10:00−16:30 非公開
  参加者：水木敬明、須賀祐治、縫田光司、品川和雅、真鍋義文、宮原大輝、中井雄士
  この日から参加の中井雄士氏の発表スライドを元に集中的に議論を行い、プライベートモデルにおける秘匿置換を用いたカードベース暗号に関してさまざまな角度から実りあるディスカッションを行うことができた。また、前日の議論を元に各自アップデートした発表スライドを共有して再度議論を深め、翌日の公開ワークショップに向けて準備を進めた。

- 6月1日（木）10:00−12:00, 16:00-19:00 非公開
  参加者：水木敬明、須賀祐治、縫田光司、品川和雅、真鍋義文、宮原大輝、中井雄士
  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。

開催中

…開催日：2023/05/29〜2023/06/01

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｜共2023a020

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**：Zoomミーティングによるハイブリッド開催
- **開催場所**：公開日2023年5月31日（水）は下記にて行います
  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
- **研究代表者**：水木 敬明（東北大学サイバーサイエンスセンター・准教授）
- **研究実施期間**：2023年5月29日（月）〜 2023年6月1日（木）
- **公開期間**：2023年5月31日（水）
- **研究計画詳細**：https://joint1.imi.kyushu-u.ac.jp/research_chooses/view/2023a020

プログラム

5月29日（月）10:00−16:30 非公開

5月30日（火）10:00−16:30 非公開

5月31日（水）【公開】@IMIオーディトリアム

10:00-11:30　オープニング、セッション1

水木 敬明（東北大学 サイバーサイエンスセンター）
ANDプロトコルにまつわる未解決問題

宮原 大輝（電気通信大学 情報理工学研究科）
カードベースZKPプロトコル

13:00-14:30　セッション2

中井 雄士（豊橋技術科学大学）
秘匿置換を用いたカードベース暗号

真鍋 義文（工学院大学 情報学部情報科学科）
無開示性を持つカードベース暗号プロトコルについて

15:00-17:15　セッション3、クロージング

品川 和雅（茨城大学 理工学研究科）
カードベース暗号に登場するさまざまなカード組と符号化

須賀 祐治（株式会社インターネットイニシアティブ）
デッキ分割法とアソシエーションスキーム

縫田 光司（九州大学マス・フォア・インダストリ研究所）
カードベース暗号に現れる数学

6月1日（木）10:00−12:00, 16:00-19:00 非公開