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

オープニング

電気通信大学　宮原大輝

研究集会の概要

崎山・李・宮原 研究室

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

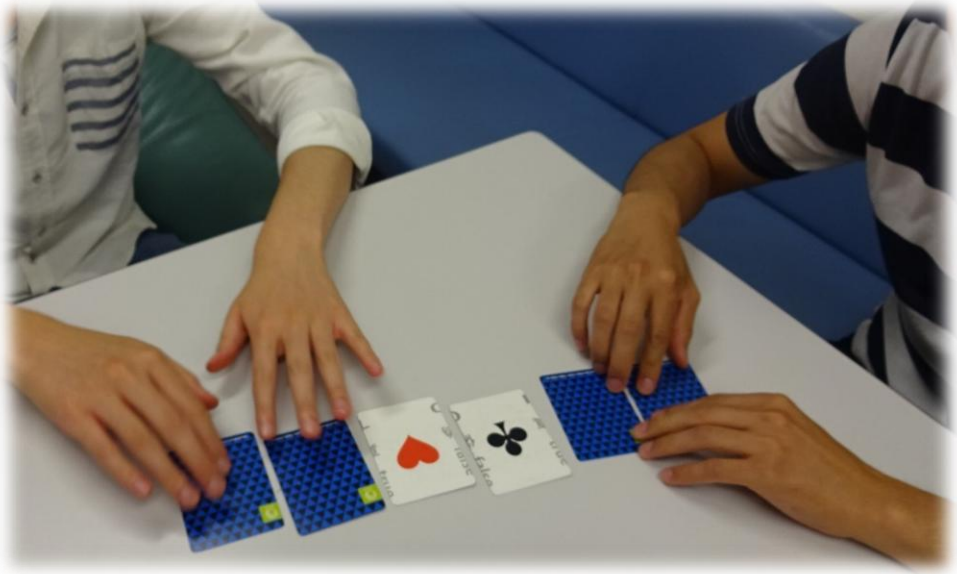
研究代表者：宮原 大輝（電気通信大学）

組織委員	水木　敬明（東北大学） 須賀　祐治（株式会社インターネットイニシアティブ） 縫田　光司（九州大学） 品川　和雅（茨城大学）

2024年度：https://joint.imi.kyushu-u.ac.jp/post-15010/
2023年度：https://joint.imi.kyushu-u.ac.jp/post-9009/

研究集会の目的（Webサイト記載）

カードベース暗号は、物理的なカード組の特徴を利用して暗号機能を実現する技術である。カードベース暗号には、実際にカード組を操作して暗号プロトコルを視覚的に体験できる特徴があるため、高校生などの非専門家に対する教育にも応用でき、実際に模擬講義などで活用されている事例もある。



研究集会の目的（Webサイト記載）

IMI短期共同研究としてこれまで過去2年に渡り、以下の2つを軸としてカードベース暗号に関する研究集会を開いた。

研究資料

1. 分野内での数理的な未解決問題をリストとして整理して広く周知することにより、新規参入者の増大を目指した。これにより、多くの研究者による研究発表が国内で観測され、大きな効果があったと言える。

2. 学生を含む若手研究者による講演の機会を多く設け、多様なバックグランドを持つシニア研究者との議論を通じ、研究をさらに深めるきっかけとなることを狙った。その結果、講演を行った学生による新規の学術論文が発表され、本分野のさらなる活性化に寄与した。

交流機会

研究集会の目的(Webサイト記載)

しかし、1つ目の軸として掲げていた未解決問題リストについては、その一部が2024年の後半から2025年初頭にかけて解決されてきている。すでに解決されている問題に新規参入者が挑戦することは機会損失であり、未解決問題リストのアップデートは緊喫の課題である。そこで最新の研究動向を把握して共有するべく短期共同研究を継続開催する判断に至った。本開催により、国内の潜在的な研究者に最新の研究資料および未解決問題のリストを提供することで、新規参入者の増大に寄与し、学術論文数の増大および研究領域の拡大が期待できる。

講演タイトル	発表者	解決(進展)個数
ANDプロトコルにまつわる未解決問題	水木　敬明	2
カードベースZKPプロトコル	宮原　大輝	4
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	品川　和雅	2
カードベース暗号に現れる数学	縫田　光司	1

*プライベートモデルでは市販のトランプカードを用いるプロトコルの構成が2023年以降よく研究されている

プログラムの概要（セッション1）

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

未解決問題の整理

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

カードベース暗号×形式検証

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

カードベース暗号×差分プライバシ

プログラムの概要（セッション2）

崎山・李・宮原 研究室

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

カードベース暗号
×ガーブルド回路

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

ガーブルド回路・
ゼロ知識証明

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

IWSEC 2024
Best Paper

プログラムの概要（セッション3）

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

上下非対称カード
でのシャッフル実装

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

カードベースゼロ知識
証明プロトコルの発展

17:45–17:50
水木 敬明（東北大学）
クロージング

まとめ・展望

録画について

- 発表内容は後日にオンデマンド配信されます
  - 発表自体：YouTube
  - スライド：研究集会のWebページ
- ただし、発表中の質疑応答にあたる部分はYouTubeで公開されません
  - 積極的に議論いただけますと幸いです