東北大学

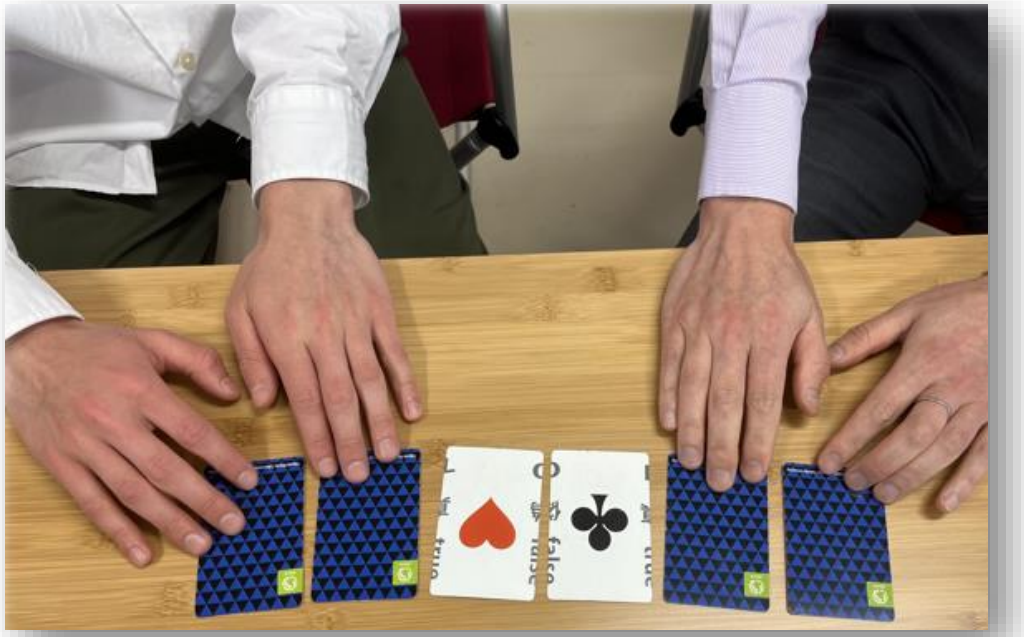
産学連携によるカードベース暗号の数理的未解決問題と新課題の整理

オープニング

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）

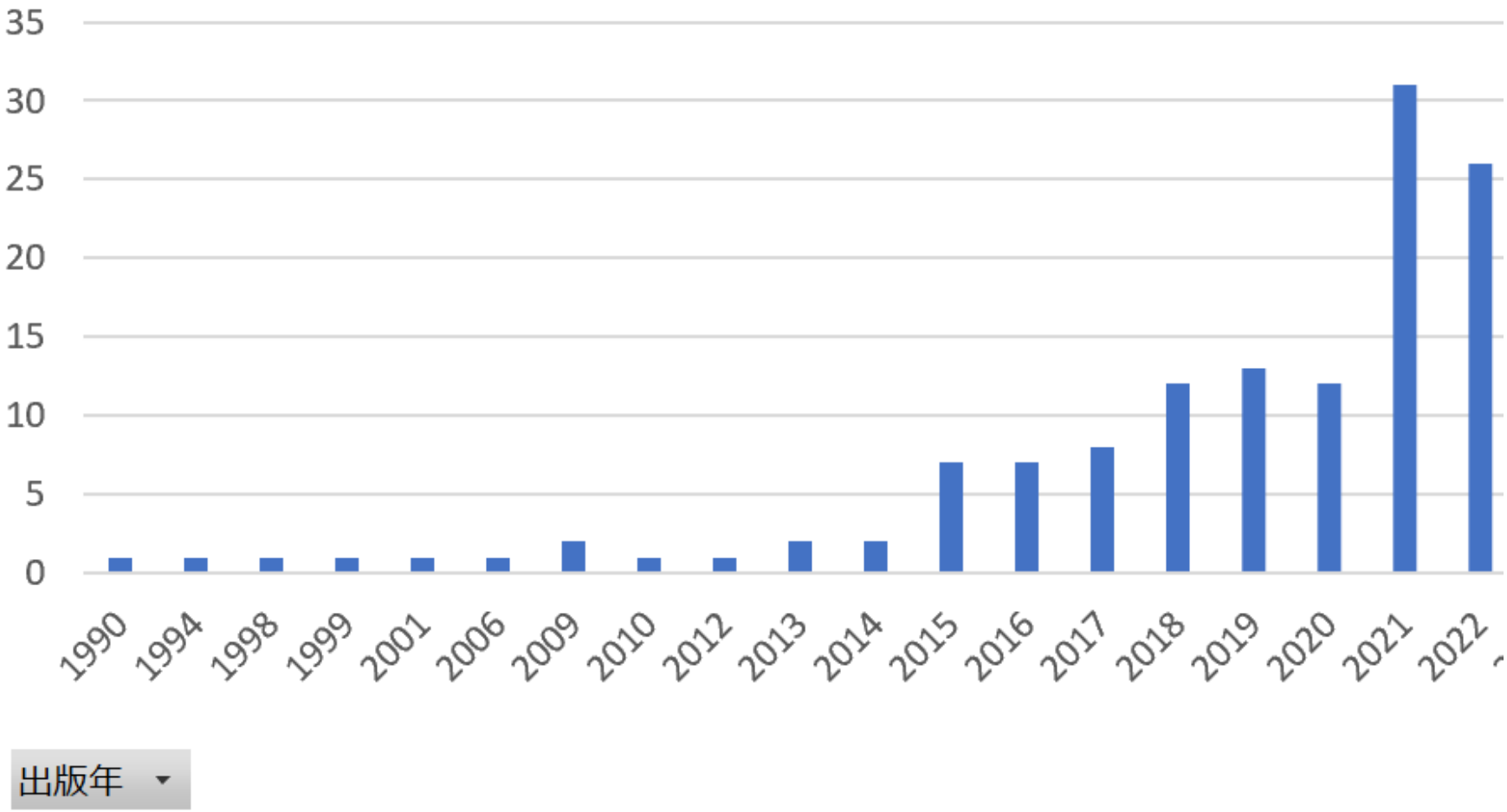
組織委員	須賀 祐治（株式会社インターネットイニシアティブ） 縫田 光司（九州大学） 品川 和雅（茨城大学）

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。

カードベース暗号分野の Scopus掲載論文数の推移



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。

組織委員（講演者）
水木 敬明（東北大学 サイバーサイエンスセンター）
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（九州大学マス・フォア・インダストリ研究所）
品川 和雅（茨城大学 理工学研究科）

講演者
真鍋 義文（工学院大学 情報学部情報科学科）
宮原 大輝（電気通信大学 情報理工学研究科）
中井 雄士（豊橋技術科学大学）

カードベース暗号の研究分野の俯瞰

カードベース暗号の計算モデル

プロトコル

抽象機械

$P = (D, U, Q, A)$

疑似コード

1 input …
2 perm …
⋮

自然言語

step1. 入力
step2. 並べ替え
⋮

計算モデルのリファイン

道具・操作を計算モデルに適用させる

計算限界の解明

カード枚数やシャッフル回数の下界の発見

・プロトコルの開発（=上界の発見）

現実世界

人間
カード組
操作

教育応用

・情報科学への興味の喚起
・暗号・セキュリティ教育
- パズルのゼロ知識証明
・抽象化の理解

実利用のプロトコルとして展開

ex.）・気まずくならない告白
・みんなで食事会を開くか決める
・金持ち比べ

（→socialな身近な問題への解決）

カードベースの計算モデル

- 標準モデル（パブリックモデル、シャッフルモデル）
  - ✓ シャッフルをベースとする

- プライベートモデル（背面処理モデル）
  - ✓ 背面での処理をベースとする

カードの種類

- 2色カード組
- 上下カード
- 正多角形カード
- …

10:00-11:30　オープニング、セッション1　（座長：縫田 光司）

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

標準モデル等

13:00-14:30　セッション2　（座長：品川 和雅）

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

プライベート
モデル

15:00-17:15　セッション3、クロージング　（座長：水木 敬明）

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

カード組と符号化

数学とのかかわり

本日のスライド資料は、後日九州大学IMIのサイトに掲載予定です。