

2026年度共同利用研究報告書

2026年10月08日

所属・職名 東北大学サイバーサイエンスセンター・教授

水木 敬明

		整理番号		2026a012	
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 III			
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	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	教授
7.研究実施期間		2026年07月06日(月曜日)～2026年07月10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		64人			

10.本研究で得られた成果の概要

本短期共同研究「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Ⅲ」は、2026年7月6日（月）～7月10日（金）に実施され、カードベース暗号やその周辺領域等を専門とする研究者が一堂に会し、集中的な研究議論と公開ワークショップが実施された。本年度は、過去3回にわたって開催された短期共同研究の成果と研究者ネットワークを基盤とし、プロトコル構成不可能性といった理論の深化と、カードゲームへの応用などの新境地の開拓、そして研究分野の拡大を狙った。非公開および公開ワークショップにおいて、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。まず理論面では、任意のPSMプロトコルをSSFOプロトコルに変換する方法を示し、任意関数に対する1回シャッフル全開示プロトコルの存在を初めて証明する成果があった。また不可能性証明に関して、連動操作を用いない上下カード3枚での有限時間ANDの不可能性を単位立方体を用いた視覚的表示法とともに示した報告や、連動操作を用いる上下カード n 枚しきい値関数の不可能性および $n+1$ 枚でのプロトコル構成についての報告があった。さらに、アフィン変換とランダムカットの新しい解釈から偶数-partyのequality関数の実現不可能性を示し、新たなシャッフル方式の話題も共有された。次に他分野連携・応用面では、グラフの連結成分数を数える独自のカードプロトコルが紹介され、効率化への課題が整理された。また、ハミルトン閉路問題に対するシャッフル3回の効率的なゼロ知識証明（ZKP）プロトコルや、格子グラフ上のトポロジー（連結領域や閉路など）を検証するZKPプロトコルと「ぬりめいず」への適用が報告された。さらに、近年盛んなゲーム応用として、「UNO」における仮想プレイヤー生成と手札選択プロトコルや、「ヒットアンドブロー」を一人で遊ぶためのフィードバック・コード生成プロトコルが示された。カードベース暗号の研究者が集い、プロトコルの改良やバリエーション展開、分野の方向性のブレインストーミングなど、今後の展望につながる充実した議論を展開したことは、本分野の持続的な発展に向けて意義深い。研究者ネットワークの繋がりをさらに強固にできた点も大きな成果である。加えて、産業界におけるカードベース暗号の活用に向けて議論を持ち有意義であった。

公開ワークショップにおける成果

任意の関数に対するsingle-shuffle full-openカードベースプロトコル（江利口）

Single-shuffle full-open (SSFO)プロトコルとは、シャッフル1回で、最後にカードをすべてオープンするタイプのプロトコルである。PSMプロトコルとは、通信1ラウンドの情報理論的に安全な秘密計算プロトコルである。本研究では、任意のPSMプロトコルをSSFOプロトコルに変換する方法を示し、それを用いて任意関数のSSFOプロトコルが存在することを初めて示した。また、任意の関数に対する1回のシャッフルで部分的に開示するプロトコル（Single-Shuffle Static-Openプロトコル）も提案した。質疑応答では、具体的なPSMプロトコルに関する議論が行われた。

連動操作を用いない上下カード3枚有限時間ANDプロトコルの不可能性証明（岩崎）

昨年IWSEC2025で報告した、有限時間ANDプロトコルは連動操作という特殊な操作を用いない場合に上下カード3枚では実現不可能であることを講演した。カードベース暗号において二色カード以外での計算限界の報告は貴重であり、今後の研究対象としての可能性を共有できた。会場では主に、その証明で用いられている簡約ステートの視覚的表示について質疑が行われた。この視覚的表示法は上下カード3枚のカード列を単位立方体の頂点に対応付けるものであり、直感的な理解を容易にする。このような表示法はカードベース暗号の分野では前例がなく、新たな道具立てを共有できた。

連動操作を用いる上下カード n 枚しきい値関数プロトコルの不可能性証明（飯野）

本講演では、IEEE CCWC2026にて発表した、 n 枚 n 入力閾値プロトコルの不可能性を紹介した。これは2023年の研究集会（2023a020）でも一部触れられていた未解決問題（有限時間コミット型 n 枚 n 入力論理積の不可能性）であり、本研究はさらに広い範囲での不可能性を得ている。加えて、追加カード1枚を用いるコミット型の閾値プロトコルも構築し、 $n+1$ 枚が必要十分条件であることを示した。会場では、提案プロトコルの物理的な実装方法に関して、トルネードシャッフルを想定する、カードを裏面のまま順序の入れ替えと上下反転を同時に行うことのできる既存の手法を少し改良したシャッフル方法の提案があった。また、より広義の対称関数についても提案プロトコルがカバーできているとの指摘があり、新しい発見へと繋がった。

Six-Card Trickの別解釈と 10-Card Trickへの道（須賀）

3-party equality 関数を実現する Six-Card Trick [Shinagawa-Mizuki ICISC2018] を基点に、 ϕ 関数（左シフトとビット反転を融合したアフィン変換）が、ある値を配置する際にランダムカットと同一視できるという新しい解釈が説明された。ビット列における周期と軌道に関するLemmaを与えることで、この解釈を用いると同じアプローチでは 偶数-party の equality 関数を実現不可能であるということが示された。

会場からは提案方式が同値類間に推移させるダブルシフティング技法の適用において、同非均衡である、つまり偏った同値類間の推移では十分に安全な方式でなくパーフェクトな方式であることが理想的であるとのコメントが得られた。その後のローカルな議論において $RC \rightarrow$ ダブルシフティング適用 $RC \rightarrow RC$ と3回行う必要がある点について合意された一方で、やはりパーフェクトな方式については難しいという見解を得ている。本来の意味としての一致関数となる10-Card Trickの実現ができていないが、一致関数以外は1) 4人一致、2) 隣り合う3人一致、3) 隣り合わない3人一致という3つの出力に分散されることを許せばRC1回で安全に実現できることも示された。今後、より正確な推移確率の導出と $(4n+2)$ -Card trickへの一般化が今後望まれるなど研究の余地がまだ残されている。

グラフの連結成分を数えるカードプロトコル（縫田）

カードベース暗号の分野における主要な研究課題として、ペンシルパズルの解の存在に対するゼロ知識証明プロトコルの構成が挙げられる。その際、検証すべき解の条件として、何らかの意味での「連結性」が課されることが少なくない。本発表では、より一般的な問題である「グラフの連結成分の個数を数える」という問題に対して、話者の研究（CSS 2024、New Generation Computing 2025）で構成したカードプロトコルの紹介を行った。

なお、今回発表したカードプロトコルは、カードプロトコルとしての実装しやすさを考慮しつつ話者が一から構成した連結成分数え上げアルゴリズムに基づいているが、会場からは、カードプロトコルへの変換しやすさと性能の良さを両立させる既存アルゴリズムの存在の可能性について質問が寄せられた。そうした従来手法の存在の調査を含め、本手法の効率性のさらなる向上は今後の研究課題である。

ハミルトン閉路問題に対するカードベースゼロ知識証明とその応用（猪狩）

ハミルトン閉路問題とは、与えられたグラフに対してすべての頂点を一度ずつ通る閉路（ハミルトン閉路）が存在するかどうかを問うNP完全な問題である。本講演では、既存のハミルトン閉路問題に対するゼロ知識証明（ZKP）プロトコルを効率化し、シャッフル3回のプロトコルを提案したことが説明された。具体的には、辺に着目したプロトコルと、隣接行列に基づくプロトコルを提案した。また、巡回セールスマン問題に対するZKPプロトコルも説明した。

格子グラフ上のトポロジーに対するカードベースプロトコル（宮原）

ペンシルパズルの解に対するゼロ知識証明プロトコルに関する研究として、本講演では、解がグリッド上において「連結領域、木、道、閉路」を構成するという、パズルに頻出する条件を満たすか検証するカードベースプロトコルを紹介した。さらにこれを「ぬりめいず」に適用したゼロ知識証明プロトコルを紹介した。これはFUN2026において発表した成果である。質疑応答では、言葉のパズルに分類されるクロスワードなどに対するゼロ知識証明プロトコルを研究する意義を議論した。

カードゲームUNOにおける仮想プレイヤー生成（品川）

カードベース暗号をカードゲームに応用する研究が2025年頃から盛んに行われている。本研究はカードゲームUNOに対する仮想プレイヤーをカードベース暗号的に生成する研究である。具体的には、仮想プレイヤーの手札のプレイ可能なカードの中から、1枚のカードを一様ランダムに選択するプロトコルを提案する。このプロトコルを用いることで、「特定の種類のカードを所有しているかどうか」等も秘密計算することができ、ワイルドドロー4のルールを適用することも可能である。質疑応答では、「仮想プレイヤーがワイルドドロー4を持っていない」という情報が完全に漏洩してしまうことに対する対策や、3回のプロトコル実行を2回に削減する方法などが議論された。

カードベース暗号を用いたヒットアンドブローの遊び方（池田）

カードベース暗号のゲームへの応用の研究が近年研究されてきている。その中で本研究ではヒット&ブローというゲームを扱う。ヒット&ブローは出題者が持っている秘密の数字（コード）を解答者が推測するゲームである。本公開ワークショップでは、本研究の内容について以下の報告を行った：

- ・コードと推測値を入力として、それに対応するヒント（HitとBlow）を出力するフィードバックプロトコルの提案
- ・出題者のコードを複数個生成するコード生成プロトコル（コードの値はランダム）の提案
- ・これらのプロトコルを用いることで、ヒット&ブローを一人で遊ぶことができることを示した

=====

非公開ワークショップにおける成果

7月6日（月）【非公開】14:00-15:30

参加者：水木敬明、宮原大輝、縫田光司

代表者の水木から都合により現地参加が出来ずオンラインでの参加となる旨のお詫びがあったのち、各参加者のスケジュール予定の確認や、公開日の研究集会の進め方などについて議論を行った。また、オープニングやクロージングのスライド資料について確認を行い、修正や改善などを行った。

7月7日（火）【非公開】10:00-17:00

参加者：水木敬明、須賀祐治、宮原大輝、縫田光司、品川和雅、池田昇太、飯野静流、猪狩紫雲

組織委員および講演者によるディスカッションを行った。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、翌々日の公開ワークショップに向けて準備を進めた。

品川氏からはUNOに対する仮想プレイヤーの生成方法についての紹介があり、カードベース暗号のカードゲーム・ボードゲームへの応用の研究の分類や、プレイヤーの戦略に関する拡張についての議論があった。猪狩氏からはハミルトン閉路問題に対するゼロ知識証明の紹介があり、プロトコルの動きの確認や、理解促進するスライド構成などについて熱心な議論があった。池田氏からはゲームとカードベース暗号の融合について議論のたたき台の提示がありディスカッションを行ったとともに、ヒットアンドブローに関するプロトコルについての説明があり、バリエーションなどについて活発な議論を行った。

7月8日（水）【非公開】10:00-17:00

参加者：水木敬明、須賀祐治、宮原大輝、縫田光司、品川和雅、岩崎淳、江利口礼央、池田昇太、飯野静流、猪狩紫雲

代表者から改めて趣旨説明や期間中の予定の説明があったのち、前日に引き続き、組織委員および講演者によるディスカッションを行った。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。

飯野氏からは連動操作を許す場合の上下カードの n 枚 n 入力の不可能性証明と $n+1$ 枚プロトコル考案について紹介があり、証明の概要の箇所や考案プロトコルの仕組みについて議論を交わした。岩崎氏からは上下カード3枚有限時間ANDプロトコルの不可能性証明について紹介があり、証明の詳細や上下カード特有のシャッフル操作について議論があった。江利口氏からはsingle-shuffle full-openプロトコルの構成について紹介があり、Uniform Selectionの構成について議論を行なった。宮原氏からはグリッド上の連結領域といったトポロジーに対するゼロ知識証明プロトコルについて紹介があり、関連研究としてごく最近提案された絵のパズルに対するプロトコルについて議論した。

7月10日（金）【非公開】9:30-16:30

参加者：水木敬明、須賀祐治、宮原大輝、縫田光司、品川和雅、池田昇太

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。特に産業界でのカードベース暗号の活用に向けて様々な議論を行った。

また須賀氏から、今回公開日での議論は時間の関係でなされていなかったが、非対称なアソシエーションスキームの構造を持つカードプロトコルの構成方法について共有された。具体的にはカード入力の際のエンコーディングルールを非対称にするように方式拡張を行うことでこれまで実現できなかった位数7の平方剰余 Quadratic residueに該当する非対称アソシエーションスキームが構成可能である。本方式は当日のディスカッション内容を踏まえ、今後の研究会などで公開される見込みである。



開催日:2026/07/09~2026/07/09

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Ⅲ | 2026a012

カテゴリ: 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 ウェスト1号館 D棟 4階 IMIカンファレンスルーム (W1-D-414)
- 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Ⅲ
- 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・教授)
- 研究実施期間:2026年7月6日(月)~ 2026年7月10日(金)
- 公開期間:2026年7月9日(木)
- 研究計画詳細:https://joint2.imi.kyushu-u.ac.jp/research_chooses/view/2026a012

プログラム

7月6日(月)【非公開】

7月7日(火)【非公開】

7月8日(水)【非公開】

7月9日(木)【公開】

10:00-10:10

水木 敬明(東北大学)

オープニング

10:10-10:40

江利口 礼央(産業技術総合研究所)

任意の関数に対するsingle-shuffle full-openカードベースプロトコル

10:40-11:10

岩崎 淳(佐賀大学)

連動操作を用いない上下カード3枚有限時間ANDプロトコルの不可能性証明

11:10-11:40

飯野 静流(電気通信大学)

連動操作を用いる上下カードn枚しきい値関数プロトコルの不可能性証明

13:10-13:40

須賀 祐治(株式会社インターネットイニシアティブ)

13:40-14:10

縫田 光司 (九州大学)

グラフの連結成分を数えるカードプロトコル

14:10-14:40

猪狩 紫雲 (千葉工業大学)

ハミルトン閉路問題に対するカードベースゼロ知識証明とその応用

15:00-15:30

宮原 大輝 (電気通信大学)

格子グラフ上のトポロジーに対するカードベースプロトコル

15:30-16:00

品川 和雅 (筑波大学)

カードゲームUNOにおける仮想プレイヤー生成

16:00-16:30

池田 昇太 (茨城大学)

カードベース暗号を用いたヒットアンドブローの遊び方

16:30-16:40

水木 敬明 (東北大学)

クロージング

7月10日 (金)【非公開】

申込方法

事前申込制 (組織委員, 講演者のかたも登録が必要です)

参加無料

定員になり次第, 参加登録を締め切らせていただく場合がございます。

＼下記URLより参加登録をお願いいたします／

[参加登録フォーム](#)

Zoom (オンライン) からご参加の方

Zoomを使ったオンライン開催, ハイブリッド開催の場合

参加登録後に件名 **[九大IMIより] Zoom用URLのお知らせ** というメールがimikyoten@gmail.comから自動配信されます。

届いていない方は, お手数をおかけしますがもう一度ご登録いただくか下記にメールにてご連絡をお願い申し上げます。

(迷惑メールフォルダもご確認お願いいたします)

<九州大学マス・フォア・インダストリ研究所 共同利用・共同研究拠点事務局>

imikyoten(at)jimu.kyushu-u.ac.jp

(at)を@に変更してください

Zoomについて

開催日までにZoomアプリをインストールしてください。

Zoomアプリは無料版で問題なくご視聴いただけます。

ミーティング用Zoomクライアントのダウンロードは下記からお願いします。
すでにインストールされている方は最新版にアップデートをお願いいたします。
https://zoom.us/download#client_4meeting
パソコンやスマホへのインストール方法は下記をご参照ください。
<https://zoom.nissho-ele.co.jp/blog/manual/zoom-install.html>

概要	運営	2026年度公募	アクセス・お問合せ
概要	運営委員会	採択研究・報告書一覧	学内専用(トップページ)
活動報告	共同利用・共同研究委員会	イベント情報	委員専用
	国際プロジェクト委員会	会場設備	研究代表者専用
		Q&A	メールマガジン