

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

オープニング

水木 敬明

東北大学サイバーサイエンスセンター

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

九州大学 伊都キャンパス ウエスト1号館 D棟 4階 IMIカンファレンスルーム (W1-D-414)

7月9日(木)【公開】10:00-16:40

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）

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・シニアエンジニア）

宮原 大輝（電気通信大学・助教）

縫田 光司（九州大学・教授）

品川 和雅（筑波大学・助教）

カードベース暗号は、**物理的なカードと操作のみ**で秘密計算などを実現する研究分野であり、近年、理論的及び実用的観点からの研究進展とともに研究コミュニティが着実に拡大している。



本研究は、**2023年度以降のIMI短期共同研究**によって形成されたコミュニティを基盤とし、分野全体の課題構造の再整理と、持続的な発展に向けた研究基盤の整備を主たる目的とする。

2023年：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

2024年：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

2025年：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

2026年：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

具体的には、**拡大しつつある研究人口**が継続的に成果を挙げられるよう、参加者による集中的な議論を通じて既存の研究成果や未解決問題を体系化する。特に、カード枚数、シャッフル回数、モデル制約といった評価指標の整理を行い、研究の位置づけをさらに明確化する。これにより、新規参入者を含む研究者間での共通理解を深め、分野外からの視点も取り入れた新たな研究展開の土台を築く。

2026年 暗号と情報セキュリティシンポジウム



東北大学

● 2日目：1/27 (火)

時間	会場A	会場B	会場C	会場D	会場E	会場F	会場G	会場Z
09:30 - 10:50	2A1 サイドチャネル攻撃 (3)	2B1 耐量子計算機暗号 (1)	2C1 秘密計算 (1)	2D1 フォーマルメソッド	2E1 セキュリティ評価 (1)	2F1 組み込みセキュリティ	2G1 Webセキュリティ	2Z1 AIへの攻撃と対策 (2)
10:50 - 11:10	コーヒーブレイク							
11:10 - 12:30	2A2 サイドチャネル攻撃 (4)	2B2 耐量子計算機暗号 (2)	2C2 秘密計算 (2)	2D2 署名・証明書プロトコル	2E2 セキュリティ評価 (2)	2F2 自動車セキュリティ (1)	2G2 クラウドセキュリティ	2Z2 AIへの攻撃と対策 (3)
12:30 - 13:50	ランチ&企業紹介							
13:50 - 15:10	2A3 カードベース暗号・物理暗号 (1)	2B3 耐量子計算機暗号 (3)	2C3 秘密計算 (3)	2D3 MPC-in-the-headによる署名・証明	2E3 セキュリティ評価 (3)	2F3 自動車セキュリティ (2)	2G3 SNSとディープフェイク	

● 3日目：1/28 (水)

時間	会場A	会場B	会場C	会場D	会場E	会場F	会場G	会場Z
09:30 - 10:50	3A1 カードベース暗号・物理暗号 (2)	3B1 耐量子計算機暗号 (4)	3C1 匿名化・合成データ	3D1 共通鍵暗号 (3)	3E1 量子暗号プロトコル	3F1 自動車セキュリティ (3)	3G1 バイオメトリクス (1)	3Z1 AIへの攻撃と対策 (4)
10:50 - 11:10	コーヒーブレイク							
11:10 - 12:30	3A2 カードベース暗号・物理暗号 (3)	3B2 楕円曲線	3C2 デジタルアイデンティティ・VC (1)	3D2 共通鍵暗号 (4)	3E2 量子アルゴリズム	3F2 自動車セキュリティ (4)	3G2 バイオメトリクス (2)	3Z2 AIへの攻撃と対策 (5)
12:30 - 13:50	ランチ&企業紹介							
13:50 - 15:10	3A3 カードベース暗号・物理暗号 (4)	3B3 耐量子計算機暗号 (5)	3C3 デジタルアイデンティティ・VC (2)	3D3 共通鍵暗号 (5)	3E3 暗号プロトコルとセキュリティモデル	3F3 自動車セキュリティ (5)	3G3 サイバーセキュリティとAI	

● 5日目：1/30 (金)

時間	会場A	会場B	会場C	会場D	会場E	会場F	会場G	会場Z
09:30 - 10:50	5A1 カードベース暗号・物理暗号 (5)	5B1 情報理論的安全性	5C1 差分プライバシー・連合学習	5D1 認証	5E1 公開鍵暗号	5F1 E2EE・鍵交換	5G1 サプライチェーンセキュリティ	5Z1 AI活用とリスク
10:50 - 11:10	コーヒーブレイク							
11:10 - 12:50	5A2 カードベース暗号・物理暗号 (6)	5B2 同種写像	5C2 分散機械学習	5D2 予備発表枠	5E2 プロキシ再暗号化・登録ベース暗号	5F2 予備発表枠	5G2 ランサムウェア対策	5Z2 AIを用いた攻撃と対策

6セッション！

期待される成果は、分野全体の見通しを改善する「研究課題構造の明確化」である。これは、研究テーマの重複を防ぎ、個々の研究の理論的位置づけを整理するだけでなく、将来的な論文化や新規共同研究の創出に向けた強固な基盤となる。技術的成果の個別の創出にとどまらず、人的リソースの増加という近年の変化を踏まえ、分野を持続的かつ安定的に発展させるための環境整備を行う点に、本研究の学術的・社会的意義がある。



講演プログラム(1)

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

COCOON 2026

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

IWSEC 2025

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

CCWC 2026

講演プログラム(2)

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

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

New Generation
Computing

IEICE Trans. A

講演プログラム(3)

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

FUN 2026

13:40-14:10

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

UCNC 2025

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

TAMC 2025

10:00-10:10

水木 敬明（東北大学）

オープニング

10:10-10:40

座長：品川

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

座長：宮原

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）

Six-Card Trickの別解釈と 10-Card
Trickへの道

**※各講演の開始時刻は
前後することがあります**

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

座長：須賀

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