

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

クロージング

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

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）

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

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

暗号の理論と技術

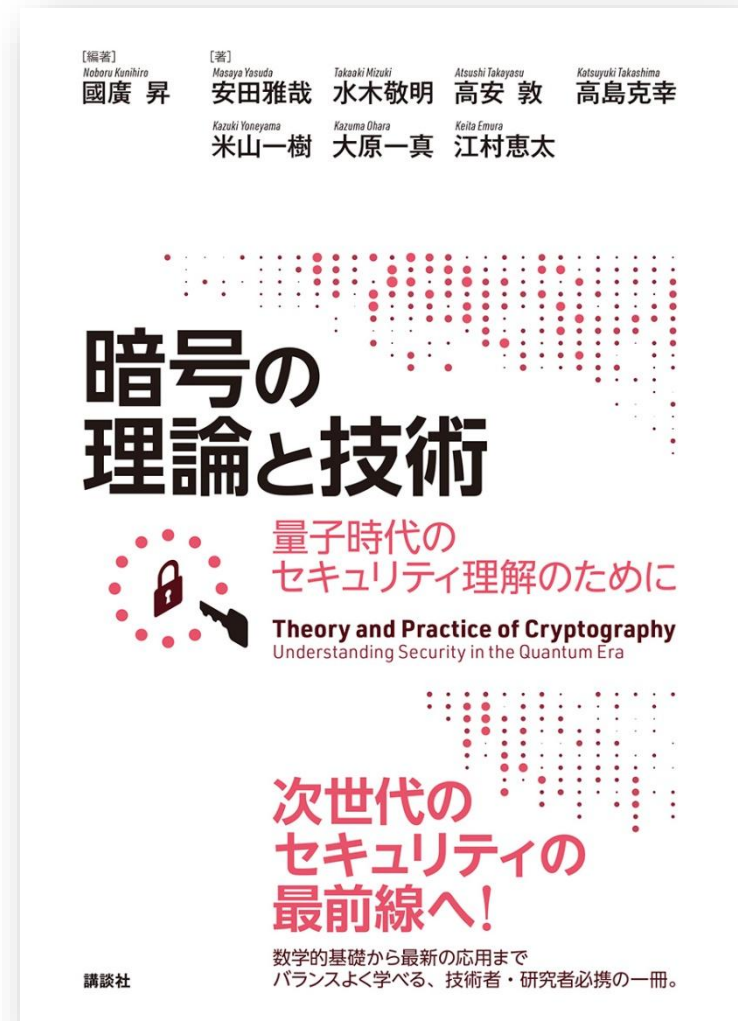
量子時代のセキュリティ理解のために

国廣昇・編著

安田雅哉／水木敬明／高安敦／
高島克幸／米山一樹／大原一真
／江村恵太・著

発行: 2024/05/22

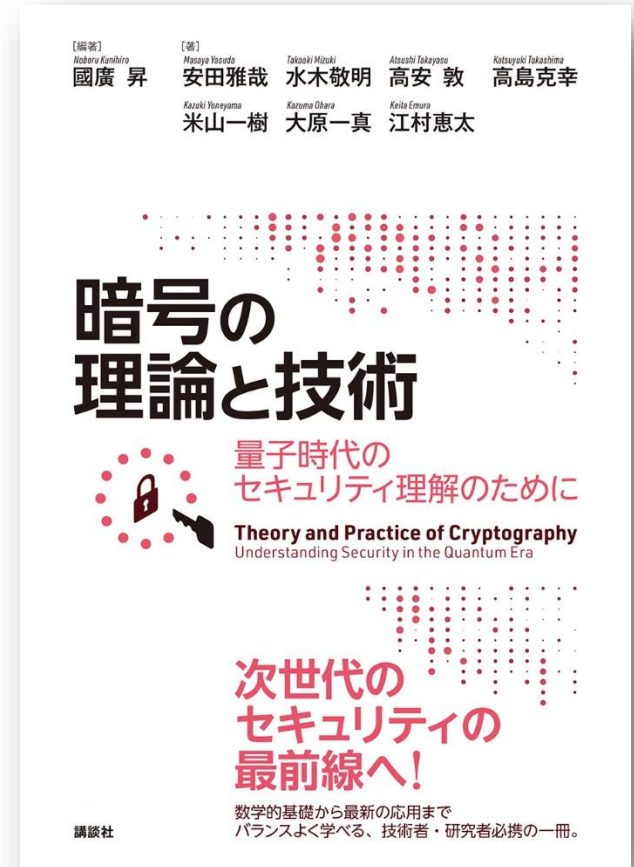
ISBN: 978-4-06-535635-7



暗号の理論と技術

量子時代のセキュリティ理解のために

- 1章 暗号技術の基礎
- 2章 現代の暗号技術を支える数学
- 3章 カードベース暗号
- 4章 格子理論を用いた暗号攻撃
- 5章 量子計算基礎とその暗号への応用
- 6章 耐量子計算機暗号
- 7章 形式手法による安全性検証
- 8章 秘密計算
- 9章 証明可能安全性と高機能暗号



暗号の理論と技術

量子時代のセキュリティ理解のために

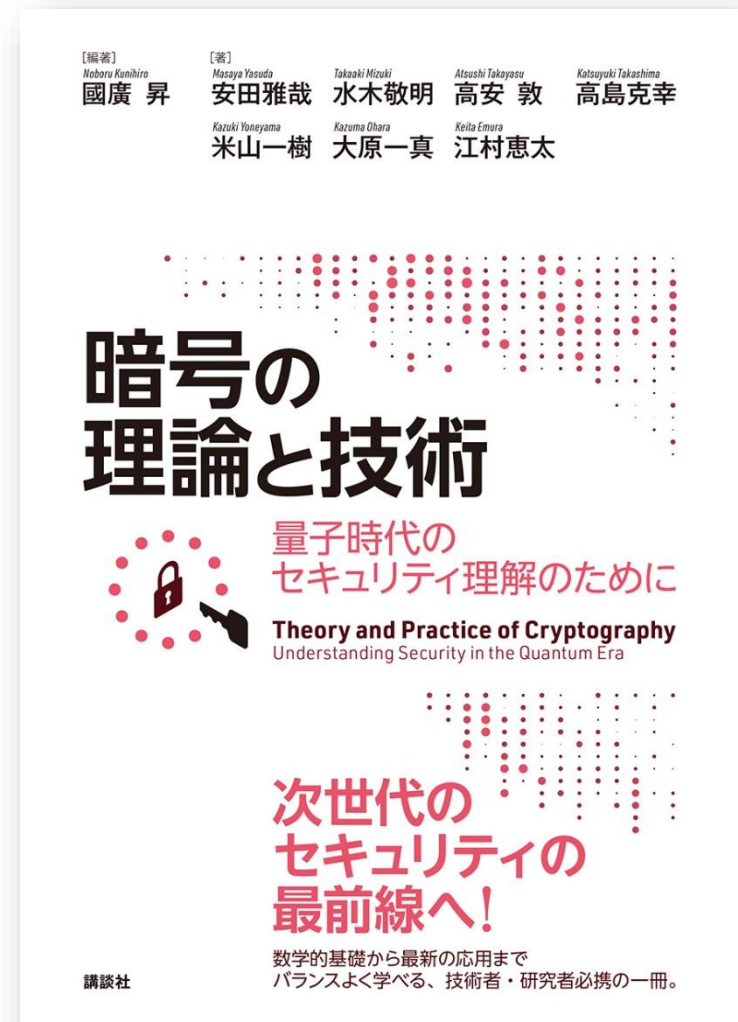
3章 カードベース暗号

3.1 カード組を用いた秘密計算

3.2 コミット型プロトコル

3.3 金持ち比べプロトコル

3.4 ゼロ知識証明プロトコル



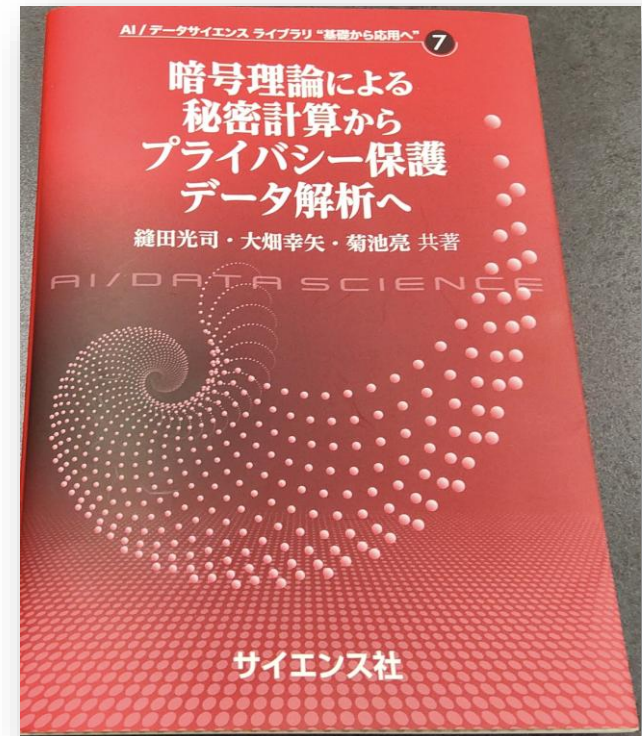
暗号理論による秘密計算からプライバシー保護データ解析へ

縫田光司、大畑幸矢、菊池 亮

第1章 秘密計算の概要と準備

- 1.1 秘密計算の状況設定の例
- 1.2 具体例：カードを用いた秘密計算
- 1.3 秘密計算に関する設定
- 1.4 秘密計算の応用
- 1.5 秘密計算プロトコルの安全性
- 1.6 本書で用いる記号について

...



第1章 群から始まる暗号理論

...

応用4：カードベース暗号

...

第9章 カードを用いた手品暗号

正五角形の幾何学（←大げさ？）

「コミット型」と「非コミット型」

別の道具と数学の利用

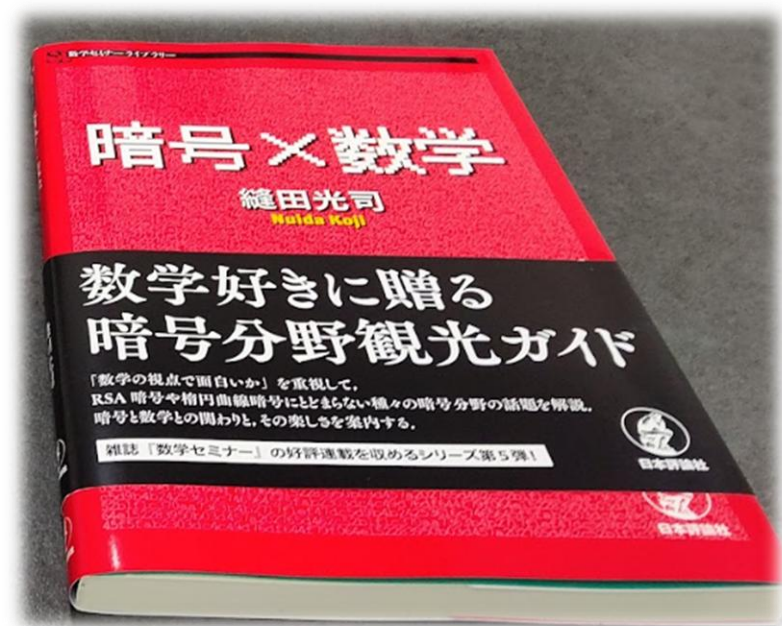
プロトコルの複雑度の下界とabc予想

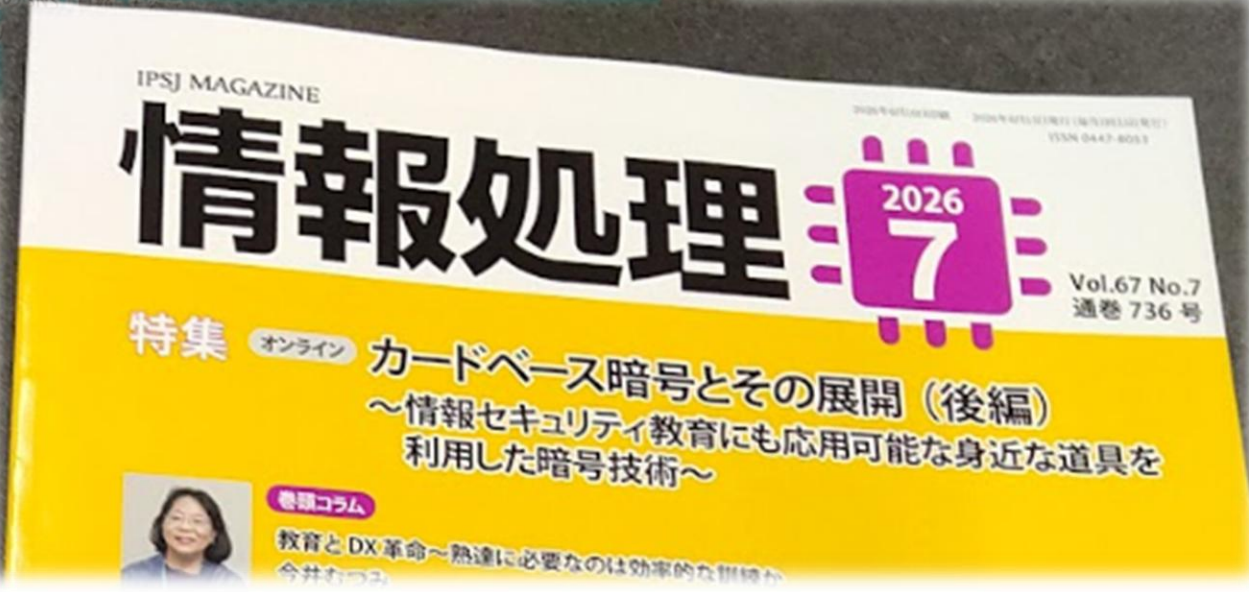
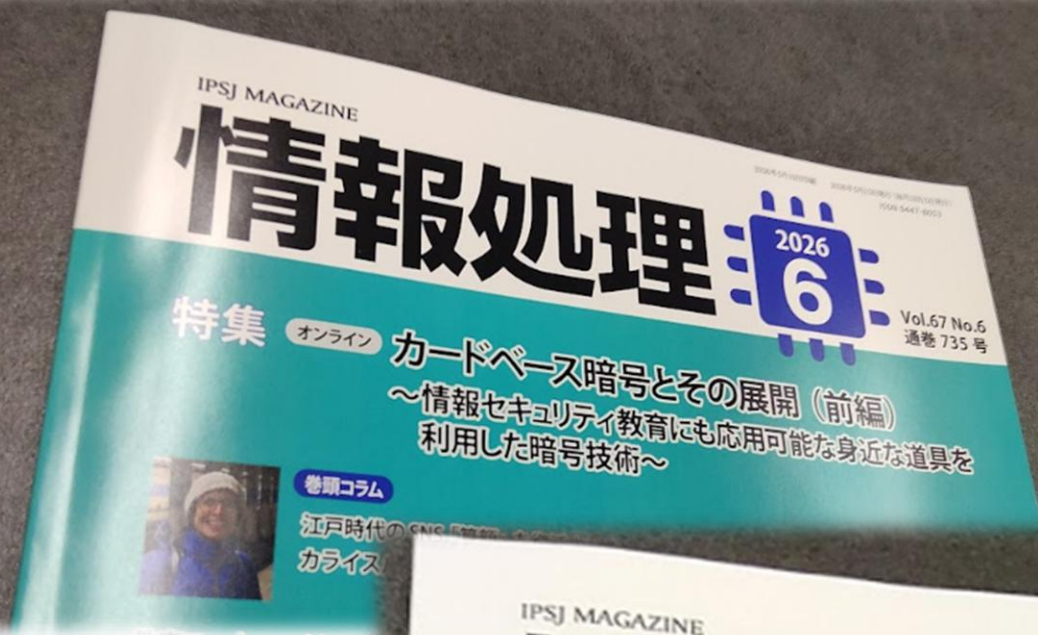
追記／

シャッフルの実現方法と有限群の分解

パズルの配置のランダム生成への応用

その他の組合せ論的・離散数学的対象との関連





2号連続
で特集

カードベース暗号とその展開(前編)～情報セキュリティ教育にも応用可能な身近な道具を利用した暗号技術～:編集にあたって／概要

駒野雄一

1. カードベース暗号の歴史と概要

水木敬明

2. カードベース暗号と算術計算 -アンケートやレクリエーションへの応用に向けて-
小高駿；駒野雄一

3. カードを用いた物理的ゼロ知識証明

品川和雅

4. カードベース暗号の計算モデル

真鍋義文

5. カードベース暗号の数学的解析

縫田光司

カードベース暗号とその展開(後編)～情報セキュリティ教育にも応用可能な身近な道具を利用した暗号技術～:編集にあたって／概要

駒野雄一

6. 新たな道具を用いる物理的暗号

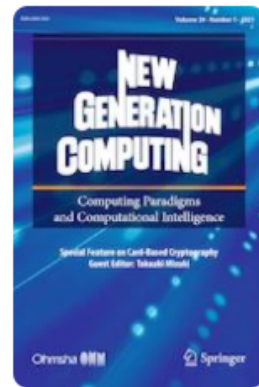
宮原大輝

7. 物理的暗号と情報理論 -物理仮定と情報理論的安全性-

岩本貢

8. 高機能暗号の社会展開に向けた物理的暗号技術の活用の取り組み

花岡悟一郎



Volume 39, Issue 1

April 2021

Special Feature on Card-Based Cryptography (pp. 1-158)

Issue Editor:

Takaaki Mizuki

第一回: Volume 39, issue 1, April 2021

<https://link.springer.com/journal/354/volumes-and-issues/39-1>

第二回: Volume 40, issue 1, April 2022

<https://link.springer.com/journal/354/volumes-and-issues/40-1>

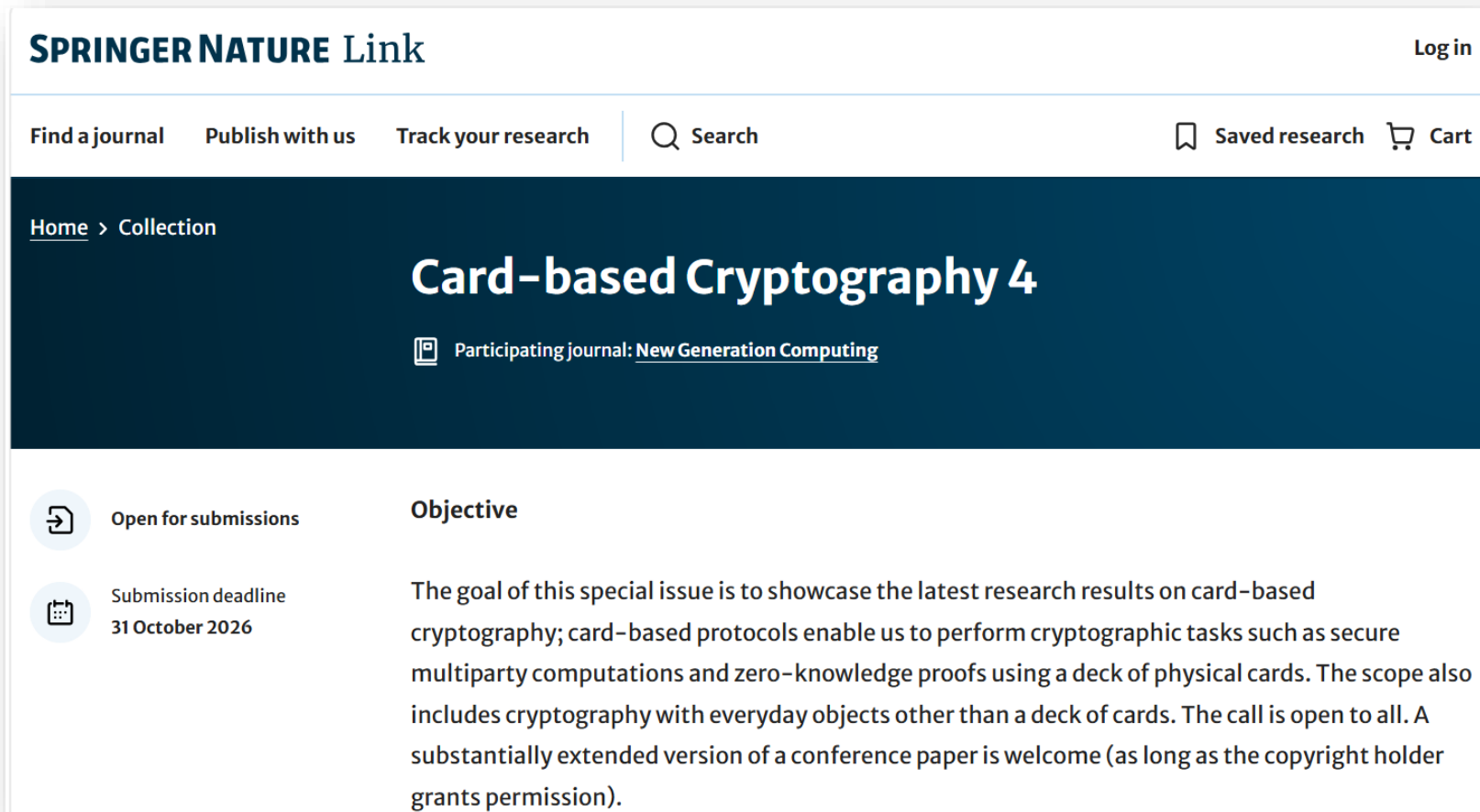
第三回: Volume 42, issue 3, April 2024

<https://link.springer.com/journal/354/volumes-and-issues/42-3>

第四回：投稿受付中！

<https://link.springer.com/collections/dcgghgaai>

Submission deadline: 31 October 2026



SPRINGER NATURE Link Log in

Find a journal Publish with us Track your research Search 🔖 Saved research 🛒 Cart

[Home](#) > Collection

Card-based Cryptography 4

 Participating journal: [New Generation Computing](#)

 Open for submissions

 Submission deadline
31 October 2026

Objective

The goal of this special issue is to showcase the latest research results on card-based cryptography; card-based protocols enable us to perform cryptographic tasks such as secure multiparty computations and zero-knowledge proofs using a deck of physical cards. The scope also includes cryptography with everyday objects other than a deck of cards. The call is open to all. A substantially extended version of a conference paper is welcome (as long as the copyright holder grants permission).

研究集会のコンテンツ(IMIサイト)

2023:

<https://joint.imi.kyushu-u.ac.jp/post-9009/>



2024:

<https://joint.imi.kyushu-u.ac.jp/post-15010/>



2025:

<https://joint.imi.kyushu-u.ac.jp/post-18086/>



2026:

<https://joint.imi.kyushu-u.ac.jp/post-20867/>



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。

カードベース暗号の研究に取り組んでみませんか？

今回の講演内容(未解決問題や今後の課題等)を基にして論文を出版される場合、この研究集会がきっかけであることを謝辞にご記載いただけると嬉しいです。

本研究は九州大学マス・フォア・インダストリ研究所 共同利用・共同研究拠点の支援を受けた。(2026年度短期共同研究「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」(2026a012))

This work was supported by Institute of Mathematics for Industry, Joint Usage/Research Center in Kyushu University. (FY2026 Short-term Joint Research “Deepening and new frontiers in card-based cryptography through industry-academia collaboration and cooperation in the fields of mathematics and cryptography III” (2026a012).)

ご質問などありましたら、代表者の水木@東北大までお願いします。(内容に応じて、適切な講演者等に転送します。)

mizuki+imicard[AT]tohoku.ac.jp