様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月 １０ 日現在

機関番号：１１３０１
研究種目：基盤研究(C)（一般）
研究期間：2021～2023
課題番号：２１Ｋ１１８８１

研究課題名（和文）カードベース暗号の継続的発展

研究課題名（英文）Continued Development of Card-based Cryptography

研究代表者
水木　敬明（Mizuki, Takaaki）

東北大学・サイバーサイエンスセンター・教授

研究者番号：９０３２３０８９

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：カードベース暗号とは，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ものである。本研究の主要な成果は，ANDやXOR等の基本演算の秘密計算やゼロ知識証明，ソーティング秘密計算等に対して新しい効率的なカードベース暗号プロトコルを構築したこと，部分開示という新しいカード操作の提案や計算モデルをリファインしたこと，積極的な論文発表とアウトリーチ活動を実施したこと等であり，これらを通してカードベース暗号の研究分野を継続的に発展させた。

研究成果の学術的意義や社会的意義
三年間の研究成果の学術的意義の根拠を示すデータとして，Scopusに収録されている「査読付論文」は合計24本である。本研究の直接経費の合計は320万円であるので，単純に割り算するとScopus収録の査読付論文1本あたりのコストは約13万3千円である。また，世界大学ランキング等の指標として重要な「トップ10%論文」について，Scopus/SciValの29 May 2024のデータによると，論文合計24本中，7本がトップ10%論文に該当している。すなわち，トップ10%論文の現在の輩出率は29.2%である。客観的に見て，我が国の研究力向上に貢献しており，社会的意義も小さくないと考えられる。

研究成果の概要（英文）：Card-based cryptography uses a physical deck of cards to achieve cryptographic functionalities such as secure computations and zero-knowledge proofs. The main achievements of this research include: the construction of new efficient card-based cryptographic protocols for elementary operations such as AND and XOR, zero-knowledge proofs, and secure sorting; the proposal of a new card operation called the half-open action and the refinement of the computational model; and the active publication of papers and outreach activities. Through these efforts, we have fostered the growth of the research field of card-based cryptography.

研究分野：カードベース暗号

キーワード：カードベース暗号　物理的暗号技術　秘密計算　ゼロ知識証明

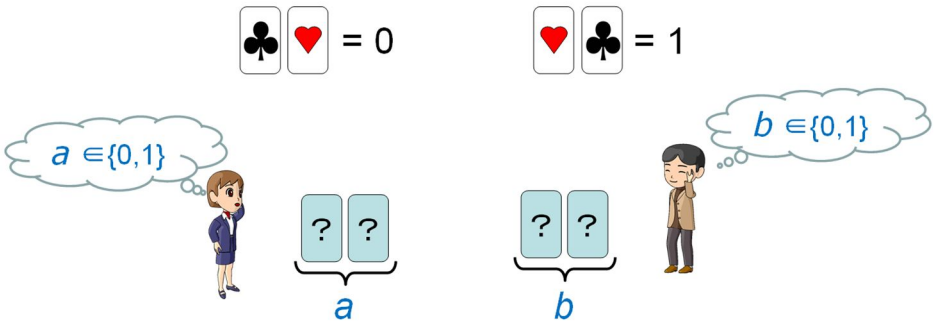
様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

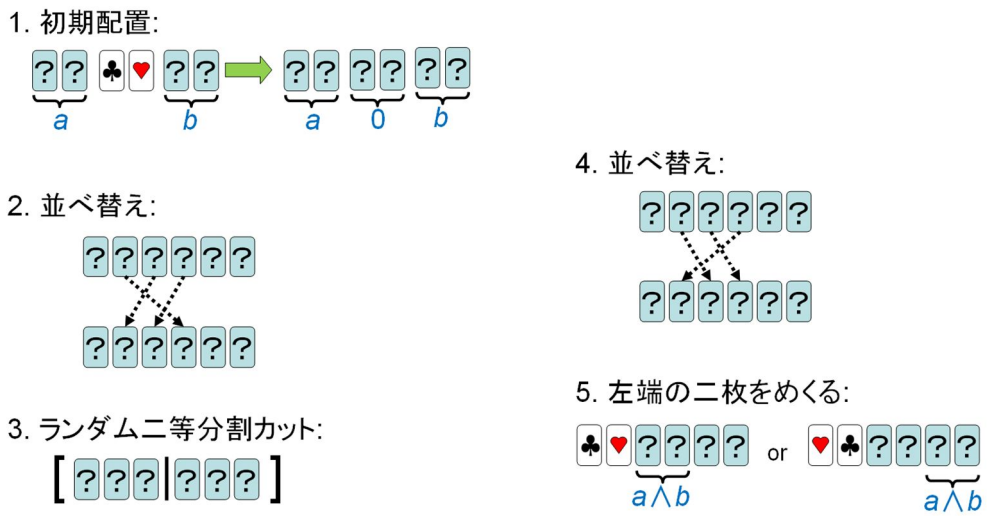
本研究課題名は「カードベース暗号の継続的発展」である。「カードベース暗号」は，トランプカードのような物理的なカード組を用いて，秘密計算やゼロ知識証明などの暗号機能を手軽に容易に実現するものである。研究代表者は，本研究開始前までに，科研費・萌芽研究「コンピュータ非依存暗号に関する研究」，基盤研究（C）「カードベース暗号の発展」，基盤研究（C）「カードベース暗号の深化」の助成等を通して，カードベース暗号の研究分野を創成し，その発展をけん引し続けていた。カードベース暗号は，我が国が世界をリードし世界のサイテーションが日本に集中する貴重な研究分野であり，我が国の研究力を支えるためにもカードベース暗号の継続的な発展を研究代表者らは望んでいた。

以下本節の残りでは，カードベース暗号をご存知ない方のために，基盤研究（C）「カードベース暗号の深化」の研究成果報告書でも記載した，カードベース暗号プロトコルの具体的な例を紹介する。

いま Alice と Bob の 2 人がいて，0 か 1 かの 1 ビットをそれぞれ秘密に持っているとしよう。例えば，次の土曜日に 2 人で一緒に山登りに行きたいなら 1 とし，行きたくないなら 0 としよう。2 人は黒と赤のカードを使い，次のようにして自分の気持ちを相手に知られないようにテーブルの上に置くことができる。



すなわち，黒と赤の並びで 1 ビットを表現している。ここで，もし 2 人とも山登りに行きたいなら $a = b = 1$ である，すなわち $a \wedge b$（論理積，AND；0 と 1 の世界の掛け算）の値は 1 となる。どちらか 1 人でも行きたくない場合には $a \wedge b = 0$ となる。したがって，論理積 $a \wedge b$ の値だけを知ることができれば，2 人は気まずくならずに次の土曜日に山登りに行くかどうかを決めることができる。実際，次のシンプルなプロトコル（研究代表者が 2009 年に国際会議 FAW 2009 にて公表）によりこのことが実現可能である。



上図のように，並び替えやランダム二等分割カットというシャッフルの後，左の二枚をめくることで，$a \wedge b$ の値を秘匿した状態で得ることができる（このようなプロトコルはコミット型と呼ばれる）。これはカードベース暗号による秘密計算プロトコルの一例である。このプロトコルを繰り返し実行すれば，3 人以上の場合にも対応できる。

２．研究の目的

本研究では，研究代表者が先導しているカードベース暗号の分野を継続的に発展させ，さらなる改良・実用化や計算限界の理論的解明に取り組むとともに，カードベース暗号の重要性をより

定着化させるアウトリーチ活動や，魅力的な未解決問題の提示により，この分野のさらなる拡大を図る。

３．研究の方法

本研究課題「カードベース暗号の継続的発展」を実現するため，これまでの研究代表者の研究の発展を支えてきた大項目「プロトコルの開発」,「計算限界の解明」,「実利用への適用」を念頭におき，着実に研究を進める。論文発表などの積極的な成果公表や大学のオープンキャンパスなどを活用したアウトリーチ活動を実施する。

４．研究成果

本研究課題の主な成果は次の通りである。

(1) 基本演算に対する新しいプロトコルの構築

まず，カードベース暗号のメインストリームな研究テーマである AND（論理積）の秘密計算について，最小枚数を用いた 3 入力 AND プロトコルの開発に取り組み，2 回のシャッフルしか要さない効率的な新しいプロトコルを考案し，国際会議 COCOON 2021 においてその成果を公表した。1 節で説明したように 1 ビットは 2 枚のカードで表現されるため，ここで言う最小枚数とは 6 枚になる。また，多入力の AND や XOR の秘密計算について，シャッフル 1 回で実行できる，追加カードの少ない多入力プロトコルを構成し，国際会議 APKC 2022 にて成果を公表した。また，3 入力多数決関数の秘密計算の改良に取り組み，6 枚という最小枚数とシャッフル 2 回で実現できる極めてシンプルなプロトコルを発見し，その成果を国際会議 Indocrypt 2021 において公表した。さらに，Shinagawa-Nuida の Batching 技術を応用して，追加カード 2 枚を用いた多入力 AND の秘密計算のシャッフル回数の削減に網羅的に取り組み，成果を国際会議 CANS 2023 にて公表した。

(2) 新しい汎用的プロトコルの構築

8 入力以上の対称関数を追加カードなしで秘密計算できることを発見し，国際会議 ICTAC 2022 においてその汎用プロトコルを公表した。また，トランプカードを用いた 3 入力プロトコルを追加カードなしで開発し，国際会議 AFRICACRYPT 2022 において公表した。また，Shinagawa-Nuida のガーブル回路の手法を改良し，ゲート当たり 8 枚の手法を国際会議 UCNC 2023 にて公表した。また，対称関数の部分クラスに対して効率的なプロトコルを構成し，国際会議 APKC 2023 にて公表した。

(3) パズルに対するゼロ知識証明

ゼロ知識証明とは，答えを知っている証明者が答えを知らない検証者に，その答えを見せずに答えを知っていることを納得させる暗号技術である。パズルに対するゼロ知識証明プロトコルは，パズルの答えを知っている証明者と答えを知らない検証者の間で実行される。

カードベースのゼロ知識証明プロトコルの構築として，Slitherlink と Masyu に対するものを論文誌 Theoretical Computer Science に掲載し，Nurikabe と Hitori に対するものを国際会議 CiE 2021 にて公表し，Cryptarithmetic（覆面算）に対するものを国際会議 UCNC 2021 にて公表した。また，Usowan に対するものを国際会議 TAMC 2022 にて公表し，Nurimisaki に対するものを国際会議 SSS 2022 にて公表し，国際会議 CiE 2021 のジャーナル版として Nurikabe と Hitori

に加え Heyawake に対するものを論文誌 New Generation Computing に掲載し，Suguru に対するものをその NP 完全性の証明とともに論文誌 Information and Computation にジャーナル版として掲載した。また，UNO を用いた数独に対するものを国際会議 FCT 2023 にて公表した。これは，UNO を 2 セットしか要せず，シャッフル回数も少なく，人間が実際に実行できるという意味で非常に効率的なものである。さらに，国際会議 SSS 2022 のジャーナル版として Nurimisaki に加え Kurodoko に対するものを論文誌 Theoretical Computer Science に掲載した。

(4) 新しいアプリケーションの開拓

前項からも分かるように，これまで数独をはじめとしてパズルに関するカードベースのゼロ知識証明プロトコルが数多く構成されている（研究代表者以外の研究グループからの発表も多い）。パズル以外にもゼロ知識証明プロトコルの構築の展開を図ることを考え，カードゲームや組み合わせ遷移問題を検討した。具体的には，一人カードゲームである Topswops に対してゼロ知識証明プロトコルを考案し国際会議 ISPEC 2022 にて公表し，またパンケーキソートという組合せ遷移問題に対するものを国際会議 SecITC 2022 にて公表した。

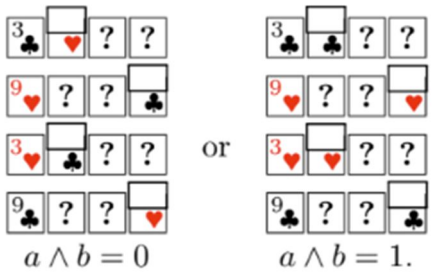
さらに，計算機科学の分野で最も基本的なものの一つと言えるソーティングに着目し，カードベースの汎用的なソーティングプロトコルを初めて構築し，国際会議 IWSEC 2022 にて公表した。

(5) 計算限界の解明に向けた取り組み

物理的なカード組を用いたゼロ知識証明プロトコルの枠組みを確立するため，その定式化に取り組み，既存の抽象機械をリファインして数理的に計算モデルを構築した。そして，グラフ同型問題やグラフ 3 彩色問題に対するゼロ知識証明プロトコルをそのフレームワーク内で構成した。これらの成果を国際会議 ProvSec 2021 において公表した。

(6) 新しいカード操作や実装に関する研究

カードベースプロトコルの実行における操作誤りの影響や対策について研究を進展させ，その成果を論文誌 Information and Computation に掲載した。また，部分開示という新しい操作方法を考案し，トランプカードの効率的な AND プロトコルを国際会議 FAW 2022 で公表した。この新しい操作は，既存のカードベース暗号の計算モデルを超えるものであり，効率化に寄与していることから，今後の新展開が期待される。



(7) 他の身近な道具への展開

これまで培ってきたカードベース暗号の知見やテクニックを活用し，新しい物理的な道具としてボールと袋の利用を考え，それらを用いた効率的な秘密計算プロトコルを考案し，その成果を国際会議 IEEE Computer Security Foundations Symposium (CSF 2021)において公表した。

(8) アウトリーチ活動

カードベース暗号は人間が実際にカード組を操作することで暗号機能を手軽に容易に実現するという特徴を有している。残念ながらパンデミックの影響で本研究課題の研究期間の 1 年目と 2 年目にはカードベース暗号プロトコルの一般市民の皆様への対面実演を行うことはできなかった。しかし，3 年目にはアウトリーチ活動として，写真のようなカード組を製作し，本学のオープンキャンパスにて高校生をはじめとする一般市民の方々にカードベース暗号の実演を行い，カードベース暗号が日常生活で役に立つことを実感していただいた。

さらに，株式会社 NTT ドコモの秘匿クロス統計技術に関する展示（docomo OpenHouse ’24）の準備の際に技術支援･監修を行い，展示説明の一部にカードベース暗号プロトコルが用いられた。展示会の来場者に大変好評であったとのフィードバックを得ており，カードベース暗号が秘匿クロス統計技術などの新しい暗号技術のアピールに大きな力を発揮することが確認できた。企業にカードベース暗号を活用いただけたことは今後のこの研究分野の発展の継続にとって非常に心強い。

加えて，カードベース暗号の教育への応用として，2023 年度の東北大学全学教育科目「学問論演習」という授業において，15 コマすべてを使い，カードベース暗号を題材とした授業・演習を実施した。過去にもカードベース暗号の授業での活用は内外で行われているが，改めてその効果や価値の高さを確認することができた。

(9) 研究分野の発展のための活動

前項の最後に書いた企業による活用にも関連して，「高機能暗号の社会展開を促進する物理・視覚暗号」という観点からカードベース暗号を捉え，同名の招待論文を他の研究者とともに執筆し電子情報通信学会論文誌 A に掲載している。当該論文は，カードベース暗号だけでなく，視覚暗号，PEZ プロトコル，影絵プロトコル，非専門家向けの説明ツールや初学者向けの教育ツールが高機能暗号の社会普及に資することを論じている。

また，国際会議 IEEE International Symposium on Multiple-Valued Logic (ISMVL 2023)においてカードベース暗号に関する招待講演を行い，この研究分野の認知度を高め，重要性を広くアピールする活動を行った。

暗号と情報セキュリティシンポジウムやコンピュータセキュリティシンポジウムにおいては，カードベース暗号のセッションが組まれており，セッション数は年々増加しており，カードベース暗号の研究分野の発展が確認できる。また，国際会議 ICIAM 2023 においてカードベース暗号の他の研究者たちとともにミニシンポジウムを企画し，カードベース暗号の若手研究者に招待講演を依頼しエンカレッジし，業界のさらなる発展に資することができた。

さらに，Springer 社の論文誌 New Generation Computing において，「Card-based Cryptography」の特集号の企画し，2021 年 4 月発行の第一回の特集号に続き，研究代表者は Lead Guest Editor として編集を行い，2022 年 4 月に第二回の特集号が発行された。現在は第三回の特集号の編集を行っているところである。

以上，主な研究成果を各項目に分けて記載した。三年間の研究期間を通して，研究計画に記載していた通り，プロトコルの開発，計算限界の解明，実利用への適用という三本柱をベースとして，カードベース暗号の研究分野を継続的に発展させることができたと考えている。

本研究課題の学術的な意義の客観的なデータとして，三年間の研究業績は Scopus 収録の査読付論文が 24 本である。

査読付論文誌（全て Scopus 収録）	掲載本数
Theoretical Computer Science	2
Information and Computation	2
New Generation Computing	1
Lecture Notes in Computer Science (LNCS)	16
Proceedings IEEE	1
ACM Conference Proceedings	2
合計	**24**

なお，この表に掲載したものの他に，上の項目(9)で述べたように， 電子情報通信学会論文誌 A に招待論文（和文）を 1 本掲載している。また，数多くの口頭発表を行った。

科研費の助成によりカードベース暗号の研究分野を継続的に発展させることができ，すべての関係者の皆様のご理解とサポートに深く感謝する次第である。さらに有難いことに，2024 年度からは，基盤研究(B)「カードベース暗号の学術的推進」をスタートしており，引き続きしっかりと研究を進めてゆく所存である。

我が国が世界をリードするカードベース暗号の分野を引き続き発展させるためにも，みなさまのご支援を願う次第である。基盤研究（C）「カードベース暗号の深化」の研究成果報告書でも記載したが，日常生活で，例えば次の土曜日に山登りに行くかどうかを気まずくならずに決めたいときには，カードベース暗号をご活用いただけると幸甚である。

５．主な発表論文等

〔雑誌論文〕　計25件（うち査読付論文　25件／うち国際共著　7件／うちオープンアクセス　24件）

１．著者名 Robert Leo、Miyahara Daiki、Lafourcade Pascal、Mizuki Takaaki	４．巻 972
２．論文標題 Physical ZKP protocols for Nurimisaki and Kurodoko	５．発行年 2023年
３．雑誌名 Theoretical Computer Science	６．最初と最後の頁 114071～114071
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2023.114071	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Komano Yuichi、Mizuki Takaaki	４．巻 13809
２．論文標題 Card-Based Zero-Knowledge Proof Protocol for Pancake Sorting	５．発行年 2023年
３．雑誌名 SecITC 2022, Lecture Notes in Computer Science	６．最初と最後の頁 222～239
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-32636-3_13	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Tozawa Kazunari、Morita Hiraku、Mizuki Takaaki	４．巻 14003
２．論文標題 Single-Shuffle Card-Based Protocol with Eight Cards per Gate	５．発行年 2023年
３．雑誌名 UCNC 2023, Lecture Notes in Computer Science	６．最初と最後の頁 171～185
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-34034-5_12	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Shikata Hayato、Miyahara Daiki、Mizuki Takaaki	４．巻 －
２．論文標題 Few-helping-card Protocols for Some Wider Class of Symmetric Boolean Functions with Arbitrary Ranges	５．発行年 2023年
３．雑誌名 APKC '23, ACM Conference Proceedings	６．最初と最後の頁 33-41
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3591866.3593073	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Tanaka Kodai、Mizuki Takaaki	4．巻 14292
2．論文標題 Two UNO Decks Efficiently Perform Zero-Knowledge Proof for Sudoku	5．発行年 2023年
3．雑誌名 FCT 2023, Lecture Notes in Computer Science	6．最初と最後の頁 406～420
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-43587-4_29	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Yoshida Takuto、Tanaka Kodai、Nakabayashi Keisuke、Chida Eikoh、Mizuki Takaaki	4．巻 14342
2．論文標題 Upper Bounds on the Number of Shuffles for Two-Helping-Card Multi-Input AND Protocols	5．発行年 2023年
3．雑誌名 CANS 2023, Lecture Notes in Computer Science	6．最初と最後の頁 211～231
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-981-99-7563-1_10	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 [招待論文] 花岡 悟一郎、岩本 貢、渡邉 洋平、水木 敬明、安部 芳紀、品川 和雅、新井 美音、矢内 直人	4．巻 J106-A
2．論文標題 高機能暗号の社会展開を促進する物理・視覚暗号	5．発行年 2023年
3．雑誌名 電子電子情報通信学会論文誌A	6．最初と最後の頁 214～228
掲載論文のDOI（デジタルオブジェクト識別子） 10.14923/transfunj.2022JAI0002	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Robert Leo、Miyahara Daiki、Lafourcade Pascal、Mizuki Takaaki	4．巻 40
2．論文標題 Card-Based ZKP for Connectivity: Applications to Nurikabe, Hitori, and Heyawake	5．発行年 2022年
3．雑誌名 New Generation Computing	6．最初と最後の頁 149～171
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00354-022-00155-5	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Mizuki Takaaki、Komano Yuichi	4．巻 285
2．論文標題 Information leakage due to operative errors in card-based protocols	5．発行年 2022年
3．雑誌名 Information and Computation	6．最初と最後の頁 104910～104910
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.ic.2022.104910	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Robert Leo、Miyahara Daiki、Lafourcade Pascal、Libralesso Luc、Mizuki Takaaki	4．巻 285
2．論文標題 Physical zero-knowledge proof and NP-completeness proof of Suguru puzzle	5．発行年 2022年
3．雑誌名 Information and Computation	6．最初と最後の頁 104858～104858
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.ic.2021.104858	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

1．著者名 Kuzuma Tomoki、Isuzugawa Raimu、Toyoda Kodai、Miyahara Daiki、Mizuki Takaaki	4．巻 -
2．論文標題 Card-based Single-shuffle Protocols for Secure Multiple-input AND and XOR Computations	5．発行年 2022年
3．雑誌名 APKC '22, ACM Conference Proceedings	6．最初と最後の頁 51-58
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3494105.3526236	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Haga Rikuo、Toyoda Kodai、Shinoda Yuto、Miyahara Daiki、Shinagawa Kazumasa、Hayashi Yuichi、Mizuki Takaaki	4．巻 13504
2．論文標題 Card-Based Secure Sorting Protocol	5．発行年 2022年
3．雑誌名 IWSEC 2022, Lecture Notes in Computer Science	6．最初と最後の頁 224～240
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-15255-9_12	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Shikata Hayato、Toyoda Kodai、Miyahara Daiki、Mizuki Takaaki	４．巻 13572
２．論文標題 Card-Minimal Protocols for Symmetric Boolean Functions of More than Seven Inputs	５．発行年 2022年
３．雑誌名 ICTAC 2022, Lecture Notes in Computer Science	６．最初と最後の頁 388～406
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-17715-6_25	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Haga Rikuo、Hayashi Yuichi、Miyahara Daiki、Mizuki Takaaki	４．巻 13503
２．論文標題 Card-Minimal Protocols for Three-Input Functions with Standard Playing Cards	５．発行年 2022年
３．雑誌名 AFRICACRYPT 2022, Lecture Notes in Computer Science	６．最初と最後の頁 448～468
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-17433-9_19	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Robert Leo、Miyahara Daiki、Lafourcade Pascal、Mizuki Takaaki	４．巻 13751
２．論文標題 Card-Based ZKP Protocol for Nurimisaki	５．発行年 2022年
３．雑誌名 SSS 2022, Lecture Notes in Computer Science	６．最初と最後の頁 285～298
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-21017-4_19	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Komano Yuichi、Mizuki Takaaki	４．巻 13620
２．論文標題 Physical Zero-Knowledge Proof Protocol for Topswops	５．発行年 2022年
３．雑誌名 ISPEC 2022, Lecture Notes in Computer Science	６．最初と最後の頁 537～553
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-21280-2_30	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Miyahara Daiki、Mizuki Takaaki	４．巻 13461
２．論文標題 Secure Computations Through Checking Suits of Playing Cards	５．発行年 2023年
３．雑誌名 FAW 2022, Lecture Notes in Computer Science	６．最初と最後の頁 110～128
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-20796-9_9	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Robert Leo、Miyahara Daiki、Lafourcade Pascal、Mizuki Takaaki	４．巻 13571
２．論文標題 Hide a Liar: Card-Based ZKP Protocol for Usowan	５．発行年 2023年
３．雑誌名 TAMC 2022, Lecture Notes in Computer Science	６．最初と最後の頁 201～217
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-20350-3_17	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Lafourcade Pascal、Miyahara Daiki、Mizuki Takaaki、Robert Leo、Sasaki Tatsuya、Sone Hideaki	４．巻 888
２．論文標題 How to construct physical zero-knowledge proofs for puzzles with a “single loop” condition	５．発行年 2021年
３．雑誌名 Theoretical Computer Science	６．最初と最後の頁 41～55
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2021.07.019	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Toyoda Kodai、Miyahara Daiki、Mizuki Takaaki	４．巻 13143
２．論文標題 Another Use of the Five-Card Trick: Card-Minimal Secure Three-Input Majority Function Evaluation	５．発行年 2021年
３．雑誌名 INDOCRYPT 2021, Lecture Notes in Computer Science	６．最初と最後の頁 536～555
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-92518-5_24	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Miyahara Daiki、Haneda Hiromichi、Mizuki Takaaki	4．巻 13059
2．論文標題 Card-Based Zero-Knowledge Proof Protocols for Graph Problems and Their Computational Model	5．発行年 2021年
3．雑誌名 ProvSec 2021, Lecture Notes in Computer Science	6．最初と最後の頁 136～152
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-90402-9_8	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Isuzugawa Raimu、Toyoda Kodai、Sasaki Yu、Miyahara Daiki、Mizuki Takaaki	4．巻 13025
2．論文標題 A Card-Minimal Three-Input AND Protocol Using Two Shuffles	5．発行年 2021年
3．雑誌名 COCOON 2021, Lecture Notes in Computer Science	6．最初と最後の頁 668～679
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-89543-3_55	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Isuzugawa Raimu、Miyahara Daiki、Mizuki Takaaki	4．巻 12984
2．論文標題 Zero-Knowledge Proof Protocol for Cryptarithmetic Using Dihedral Cards	5．発行年 2021年
3．雑誌名 UCNC 2021, Lecture Notes in Computer Science	6．最初と最後の頁 51～67
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-87993-8_4	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Miyahara Daiki、Komano Yuichi、Mizuki Takaaki、Sone Hideaki	4．巻 -
2．論文標題 Cooking Cryptographers: Secure Multiparty Computation Based on Balls and Bags	5．発行年 2021年
3．雑誌名 IEEE Computer Security Foundations Symposium (CSF 2021)	6．最初と最後の頁 1-16
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CSF51468.2021.00034	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Robert Leo、Miyahara Daiki、Lafourcade Pascal、Mizuki Takaaki	4．巻 12813
2．論文標題 Interactive Physical ZKP for Connectivity: Applications to Nurikabe and Hitori	5．発行年 2021年
3．雑誌名 CiE 2021, Lecture Notes in Computer Science	6．最初と最後の頁 373～384
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-80049-9_37	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

〔学会発表〕　計39件（うち招待講演　4件／うち国際学会　1件）

1．発表者名 Takaaki Mizuki
2．発表標題 Card-based Cryptography: How to Securely Compute Multiple-valued Functions Using a Deck of Cards
3．学会等名 IEEE International Symposium on Multiple-Valued Logic (ISMVL 2023)（招待講演）（国際学会）
4．発表年 2023年

1．発表者名 葛馬知紀，五十鈴川頼宗，豊田航大，宮原大輝，水木敬明
2．発表標題 ［招待講演］Card-Based Single-Shuffle Protocols for Secure Multiple-Input AND and XOR Computations (from APKC 2022)
3．学会等名 電子情報通信学会情報セキュリティ研究会（招待講演）
4．発表年 2023年

1．発表者名 四方隼人，水木敬明
2．発表標題 トランプカードを用いた対称関数に対する追加カード2枚の秘密計算
3．学会等名 情報処理学会コンピュータセキュリティ研究会
4．発表年 2023年

１．発表者名
吉田拓叶，中林佳祐，田中滉大，千田栄幸，水木敬明

２．発表標題
2枚の追加カードを用いた多入力AND秘密計算におけるシャッフル回数の削減

３．学会等名
電子情報通信学会情報セキュリティ研究会

４．発表年
2023年

１．発表者名
田中滉大，水木敬明

２．発表標題
ABC End Viewに対するもう１つの物理的ゼロ知識証明

３．学会等名
LAシンポジウム

４．発表年
2023年

１．発表者名
伊藤優樹，四方隼人，葛馬知紀，水木敬明，菅沼拓夫

２．発表標題
3Dプリンタのカードベース暗号実装への活用

３．学会等名
情報処理学会コンピュータセキュリティ研究会

４．発表年
2023年

１．発表者名
葛馬知紀，水木敬明

２．発表標題
カードの部分開示を用いたプロトコルにおけるエラーの解析

３．学会等名
コンピュータセキュリティシンポジウム

４．発表年
2023年

１．発表者名
伊藤優樹，四方隼人，水木敬明，菅沼拓夫

２．発表標題
3Dプリンタによるオープン装置や特殊カードケースの作成と対称関数の秘密計算への適用

３．学会等名
コンピュータセキュリティシンポジウム

４．発表年
2023年

１．発表者名
田中滉大，水木敬明

２．発表標題
2回あるいは1回のシャッフルを用いた数独に対する物理的ゼロ知識証明

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2024年

１．発表者名
木村佳和，水木敬明，駒野雄一

２．発表標題
ルービックキューブの解法の物理的ゼロ知識証明

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2024年

１．発表者名
小泉康一，大槻正伸，水木敬明，花岡悟一郎

２．発表標題
視覚復号型秘密分散暗号シートを用いた多値多入力秘密計算プロトコル

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2024年

１．発表者名
四方隼人，水木敬明

２．発表標題
効率的なコミット型閾値関数カードベースプロトコル

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2024年

１．発表者名
葛馬知紀，平野智也，大島莉凜，安田百福，水木敬明

２．発表標題
ガムロ：新しいトランプゲームと秘密計算の応用

３．学会等名
情報処理学会コンピュータセキュリティ研究会

４．発表年
2024年

１．発表者名
田中滉大，黒田真那，志摩邑那，水木敬明

２．発表標題
不等号ナンプレに対する物理的ゼロ知識証明

３．学会等名
情報処理学会全国大会

４．発表年
2024年

１．発表者名
五十鈴川頼宗，豊田航大，佐々木優，宮原大輝，水木敬明

２．発表標題
［招待講演］A Card-Minimal Three-Input AND Protocol Using Two Shuffles (COCOON 2021より)

３．学会等名
電子情報通信学会情報セキュリティ研究会（招待講演）

４．発表年
2022年

１．発表者名
駒野雄一，水木敬明

２．発表標題
Topswopsの物理的ゼロ知識証明プロトコル

３．学会等名
マルチメディア、分散、協調とモバイルシンポジウム

４．発表年
2022年

１．発表者名
四方隼人，水木敬明，宮原大輝

２．発表標題
対称関数に対するカードベースプロトコルについて

３．学会等名
LAシンポジウム

４．発表年
2022年

１．発表者名
葛馬知紀，宮原大輝，水木敬明

２．発表標題
多入力ANDプロトコルとシャッフルについて

３．学会等名
LAシンポジウム

４．発表年
2022年

１．発表者名
芳賀陸雄，林優一，宮原大輝，水木敬明

２．発表標題
ランダムカット1回の6枚XORプロトコルの不可能性について

３．学会等名
情報処理学会コンピュータセキュリティ研究会

４．発表年
2022年

１．発表者名
田中滉大，水木敬明

２．発表標題
UNOを用いた数独に対するゼロ知識証明について

３．学会等名
情報処理学会アルゴリズム研究会

４．発表年
2022年

１．発表者名
駒野雄一，水木敬明

２．発表標題
Pancakeソーティングに対する物理的ゼロ知識証明

３．学会等名
コンピュータセキュリティシンポジウム

４．発表年
2022年

１．発表者名
四方隼人，水木敬明

２．発表標題
4種カード組を用いた対称関数の秘密計算

３．学会等名
電子情報通信学会情報セキュリティ研究会

４．発表年
2022年

１．発表者名
田中滉大，水木敬明

２．発表標題
番号付きスリーブを活用した数独のゼロ知識証明

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2023年

１．発表者名
四方隼人，水木敬明

２．発表標題
4種カードを用いた効率的な対称関数秘密計算

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2023年

１．発表者名
葛馬知紀，水木敬明

２．発表標題
シャッフル1回の多入力ANDプロトコルのカード枚数削減

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2023年

１．発表者名
五十鈴川頼宗，水木敬明

２．発表標題
カードベースプロトコルの部分開示操作におけるエラーと対策に関する考察

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2023年

１．発表者名
吉田拓叶，千田栄幸，水木敬明

２．発表標題
説明動画再生時間に基づくカードベースプロトコルの評価

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2023年

１．発表者名
田中滉大，水木敬明

２．発表標題
両面不透明スリーブを用いた数独のゼロ知識証明

３．学会等名
情報処理学会全国大会

４．発表年
2023年

１．発表者名
豊田航大，宮原大輝，水木敬明，曽根秀昭

２．発表標題
［招待講演］Six-Card Finite-Runtime XOR Protocol with Only Random Cut (from APKC 2020)

３．学会等名
電子情報通信学会情報セキュリティ研究会（招待講演）

４．発表年
2021年

１．発表者名
小山寛人，宮原大輝，水木 敬明

２．発表標題
部分開示を用いるトランプカードプロトコルとその発展

３．学会等名
情報処理学会コンピュータセキュリティ研究会

４．発表年
2021年

１．発表者名
五十鈴川頼宗，宮原大輝，水木敬明

２．発表標題
最小枚数の非コミット型６入力ANDプロトコルのシャッフル回数の改善

３．学会等名
コンピュータセキュリティシンポジウム

４．発表年
2021年

１．発表者名
中林佳祐，宮原大輝，水木敬明

２．発表標題
2枚の追加カードを用いた多入力ANDプロトコルのシャッフル回数の削減

３．学会等名
コンピュータセキュリティシンポジウム

４．発表年
2021年

１．発表者名
豊田航大，宮原大輝，水木 敬明

２．発表標題
ランダム二等分割カットのみを用いる5枚コミット型ANDプロトコル

３．学会等名
情報処理学会コンピュータセキュリティ研究会

４．発表年
2021年

１．発表者名
四方隼人，豊田航大，宮原大輝，水木敬明

２．発表標題
最小のカード枚数による対称関数の秘密計算について

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2022年

１．発表者名
葛馬知紀，五十鈴川頼宗，豊田航大，宮原大輝，水木敬明

２．発表標題
シャッフル1回のみの秘密計算に必要なカード枚数について

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2022年

１．発表者名
宮原大輝，水木敬明

２．発表標題
部分開示を用いるトランプカード金持ち比べプロトコル

３．学会等名
情報処理学会アルゴリズム研究会

４．発表年
2022年

１．発表者名
四方隼人，豊田航大，宮原大輝，水木 敬明

２．発表標題
対称論理関数に対する最小枚数プロトコルの改良

３．学会等名
情報処理学会コンピュータセキュリティ研究会

４．発表年
2022年

１．発表者名
芳賀陸雄，林優一，宮原大輝，水木敬明

２．発表標題
トランプカードによる3入力論理関数の秘密計算プロトコル

３．学会等名
情報処理学会コンピュータセキュリティ研究会

４．発表年
2022年

１．発表者名
吉田拓叶，千田栄幸，水木敬明

２．発表標題
カードベース3入力ANDプロトコルの比較

３．学会等名
電子情報通信学会総合大会

４．発表年
2022年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関