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　２ 年　 ６ 月 ２９ 日現在

機関番号：１１３０１
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ００００１

研究課題名（和文）カードベース暗号の深化

研究課題名（英文）Deepening 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・准教授

研究者番号：９０３２３０８９

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：カードベース暗号とは，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，基本演算の秘密計算やゼロ知識証明，ランキ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，計算限界の解明のための上界や下界を与えたこと，実装上の問題に対してモデル化や解決策を提案したこと等であり，これらを通してカードベース暗号の研究分野を深化させた。

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，「査読付論文」は合計24本であり，全てScopusに収録されている。本研究の直接経費の合計は350万円であるので，単純に割り算すると査読付論文1本あたりのコストは約14万5千円である。また，世界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，SciValの2016-2019のデータ（field-weighted）において対象20本のうち，5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25%である。客観的に見て，我が国の研究力向上に（低コストで）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 performs cryptographic tasks such as secure multiparty computation by using a deck of physical cards (such as playing cards). The principal investigator constructed many new efficient card-based protocols for several tasks such as elementary secure computations, zero-knowledge proofs, and secure ranking, provided upper and lower bounds on the numbers of cards, proposed implementation issues and their countermeasures, and so on. Consequently, this research project has contributed to deepening card-based cryptography.

研究分野：カードベース暗号

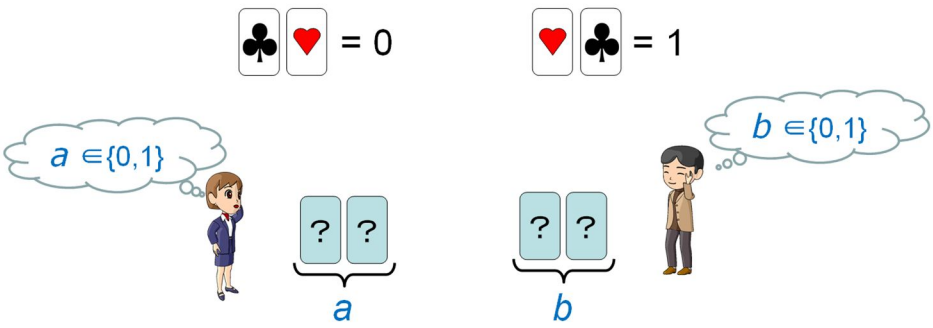
キーワード：カードベース暗号　秘密計算　物理的暗号技術

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

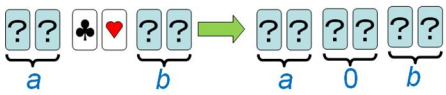
本研究課題名は「カードベース暗号の深化」である。「カードベース暗号」は，トランプカードのような物理的なカード組を用いて，秘密計算に代表される暗号機能を身近で手軽に実現するものである。まずカードベース暗号プロトコルの具体的な例を紹介する。

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。

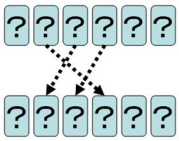


すなわち，黒と赤の並びで 1 ビットを表現している。ここで，もし 2 人とも山登りに行きたいなら $a = b = 1$ である，すなわち $a \wedge b$（論理積，AND；0 と 1 の世界の掛け算）の値は 1 となる。どちらか 1 人でも行きたくない場合には $a \wedge b = 0$ となる。したがって，論理積 $a \wedge b$ の値だけを知ることができれば，2 人は気まずくならずに次の土曜日に山登りに行くかどうかを決めることができる。実際，次のシンプルなプロトコル（研究代表者が 2009 年に国際会議 FAW 2009 にて公表）によりこのことが実現可能である。

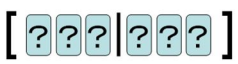
1. 初期配置:



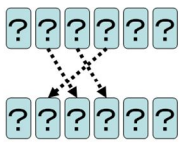
2. 並べ替え:



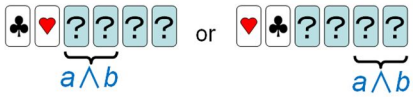
3. ランダム二等分割カット:



4. 並べ替え:



5. 左端の二枚をめくる:



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。

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」や基盤研究（C）「カードベース暗号の発展」の助成等を通して，非コミット型 AND 計算の二十数年ぶりの改良，加算器と投票プロトコルの構築，全ての三変数関数をカード 8 枚で計算できることの証明，任意の論理関数に対する汎用的なプロトコル構成法の提案，多入力 AND 計算に特化した効率的実現手法の考案，カードベース暗号プロトコルを規定する厳密な数学的計算モデルの構築等の研究成果を挙げ，国際会議や論文誌にて公表し，カードベース暗号の研究分野の開拓と発展を牽引していた。特に暗号理論のトップカンファレンスの一つである ASIACRYPT 2012 において研究成果を発表して以来，カードベース暗号に対する注目が急速に高まり，研究代表者は招待講演や招待論文の依頼を受けることが増え，それを通じて，カードベース暗号の重要性や科学的興味深さが認知され，この研究分野に参入する研究者も増えていた。

２．研究の目的

本研究の目的は，研究代表者が中心となり切り拓いてきたカードベース暗号の研究分野を格段に深化させることである。この研究分野は１．で述べた通りに急速に発展していたが，まだまだ未解決問題がたくさん残っていた。例えば，１．で説明したプロトコルはカード 6 枚でコミット型の AND 計算を実現するが，ASIACRYPT 2015 にてカード 4 枚や 5 枚のプロトコルが提案されており，枚数が削減されていた。しかし，人間が単純に実行するには難しいシャッフルを平均 8

回要する等の実装上の問題があり，よりシンプルな 5 枚プロトコルが存在するか否かについては重要な未解決課題であった。繰り返しになるが，本研究は，このカードベース暗号の研究分野を格段に深化させ，さらなる効率化・実用化や計算限界の学理的解明に取り組むものである。

３．研究の方法

本研究課題「カードベース暗号の深化」を実現するため，三つの大項目として「プロトコルの開発」,「計算限界の解明」,「実利用への適用」に取り組む。プロトコルの開発を通して計算限界の解明への要求が生まれ，計算限界の解明を通して実利用への適用による計算モデルの妥当性の検証の要求が生まれ，実利用への適用を通して新しいプロトコルの開発への要求が生まれる。このようなサイクルを効果的に回し，学理追及や応用指向研究により未解決課題を解決し，カードベース暗号の学術的重要性を定着化させる。

４．研究成果

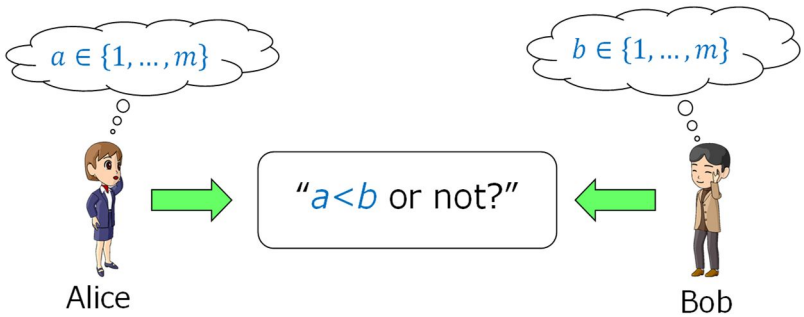
本研究課題の主な成果は次の通りである。

(1) 基本演算に対する新しいプロトコルの構築

１．で述べたように，これまで実用的なシャッフルを用いて 5 枚コミット型 AND プロトコルを構築できるかどうかは未解決問題であったが，そのようなプロトコルの存在を示すことに成功し，その成果を国際会議 APKC 2018 において発表した。また，AND 計算と並び最も重要な基本演算である XOR 計算について，ランダムカットという実用的なシャッフルのみを用いた 6 枚コミット型 XOR プロトコルを構成することに世界で初めて成功し，その成果は国際会議 APKC 2020 にて公表される。さらに，6 枚のカードで 3 変数入力がすべて等しいか否かの秘密計算を行うことのできるプロトコルを開発し，その成果を国際会議 ICISC 2018 において公表した。加えて，ハイブリットなプロトコルという概念の導入を含む成果を Soft Computing 誌に掲載している。

(2) 金持ち財産比べ・ランキング秘密計算を実現するプロトコルの開発

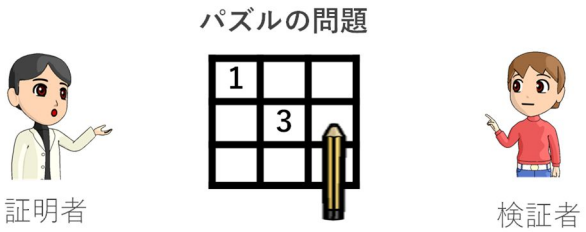
重要な秘密計算の一つに 2 入力の大小関係を求める金持ち財産比べという問題があり，その問題をカードベースで解決する，分かり易い効率的な手法を考案し，国際会議 COCOA 2018 においてその成果を公表した。



さらに，黒と赤の二色のカードではなく，（数字とスートからなる通常の）トランプカードを用いて金持ち比べを実行できるように改良を行い，その成果を Theoretical Computer Science 誌に掲載した。加えて，金持ち比べ問題の一般化として，ランキング秘密計算という問題を考え，それをカード組で解決するいくつかのプロトコルを開発し，国際会議 COCOA 2019 にてその成果を公表した。

(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。ペンシルパズルで最も有名な「数独」について，そのようなゼロ知識証明を実現する（健全性エラーのない）カードベースプロトコルを開発し，国際会議 FUN 2018 において発表した。



また，その改良を Theoretical Computer Science 誌に掲載している。その他のパズルに対するカードベースのゼロ知識証明プロトコルの開発にも力を入れ，マカロに対する成果を国際会議 SSS 2018 で，カックロに対する成果を IEICE Trans. Fundamentals 誌に，のりのりに対する成果を国際会議 COCOON 2019 で，スリザーリンクに対する成果を国際会議 ISPEC 2019 で，Takuzu

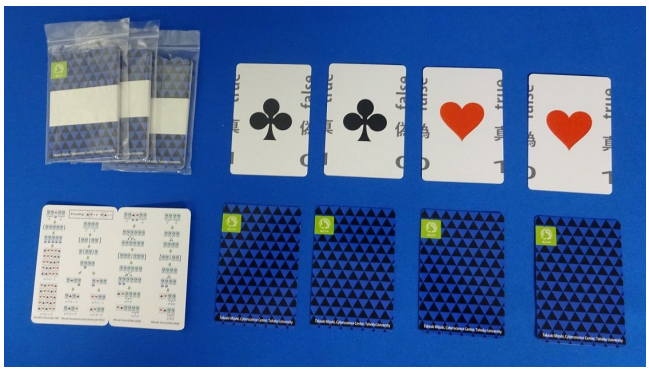
と縦横さんに対する成果を国際会議 FUN 2020 で，それぞれ公表している。

(4) 計算限界の解明に向けた解析
計算限界の解明として，コミット型 AND 計算やコピーに必要なカード枚数に関する下界について研究を進め，その成果を暗号理論のトップカンファレンスである ASIACRYPT 2017 において公表した。また，秘密計算に必要なシャッフルの回数の下界ついての解析を進めた。さらに，複雑なシャッフルの実現可能性について解析し，Pile-Shifting Scramble という手法を導入し実現可能なクラスを広げ，成果を IEICE Trans. Fundamentals 誌に掲載した。加えて，トランプカードや黒赤カードを含む，より広いクラスの様々な種類のカード組の下での計算可能性について議論を行い，得られた成果を国際会議 FAW 2019 で公表した。

(5) プロトコルの実行時間や実装に関する研究
実利用を指向した取り組みとして，プロトコルの実行時間を評価する手法の確立を進め，既存のプロトコルの詳細な比較を行い，その成果は国際会議 UCNC 2018 において発表した。また，重要なシャッフル操作の実装に関する成果が International Journal of Information Security 誌に掲載される。

(6) 他の身近な道具への展開
カードベース暗号の知見を活かし，カード組以外の身近な道具を用いたプロトコルの開発を検討し，カードの代わりにコインを用いるプロトコルを構成し，身近な道具での秘密計算の可能性をさらに広げた。この成果は国際会議 TPNC 2018 において公表している。また，光とそれを遮るシートを利用した暗号プロトコルを構築し，国際会議 WISE 2019 にて公表した。このプロトコルは中学生，あるいは小学生でも楽しんで実行できるものであり，教育的な効果が期待できる。

(7) アウトリーチ活動とフィードバック
アウトリーチ活動として，次の写真のようなカード組を製作し，定期的な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。また，一般市民向けのシンポジウムにおいて招待講演を行い，利用者や非専門家の視点からの貴重なフィードバックを得た。



特にカードベース暗号プロトコルを実際に何度も手で実行することにより，能動的攻撃についての示唆を得て，新しい攻撃モデルを確立し，対策を含めその成果を国際会議 TPNC 2019 で公表した。また，実際に何百人もの高校生にカードベースプロトコルを実行してもらったなかで，稀にカード列の並べ替え誤りが発生することがある。そこからのフィードバックとして，そのような並べ替え誤りに起因する情報漏えいについて解析を行い，この成果は国際会議 IWOCA 2018 において発表している。

(8) 研究分野の格段の発展や深化のための活動
情報理論とその応用シンポジウムの特別セッションで「カードベース暗号の最新の動向」についての招待講演を行うなどを通じて，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継続的に行った。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いる。また，Springer 社とオーム社が Co-Publisher となっている論文誌 New Generation Computing において，「Card-based Cryptography」の特集号の企画を行い，無事に受理され，研究代表者は Lead Guest Editor としてこ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有機的に連携させ，カードベース暗号の研究分野を格段に深化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査読付論文が 24 本である（全て Scopus 収録）。

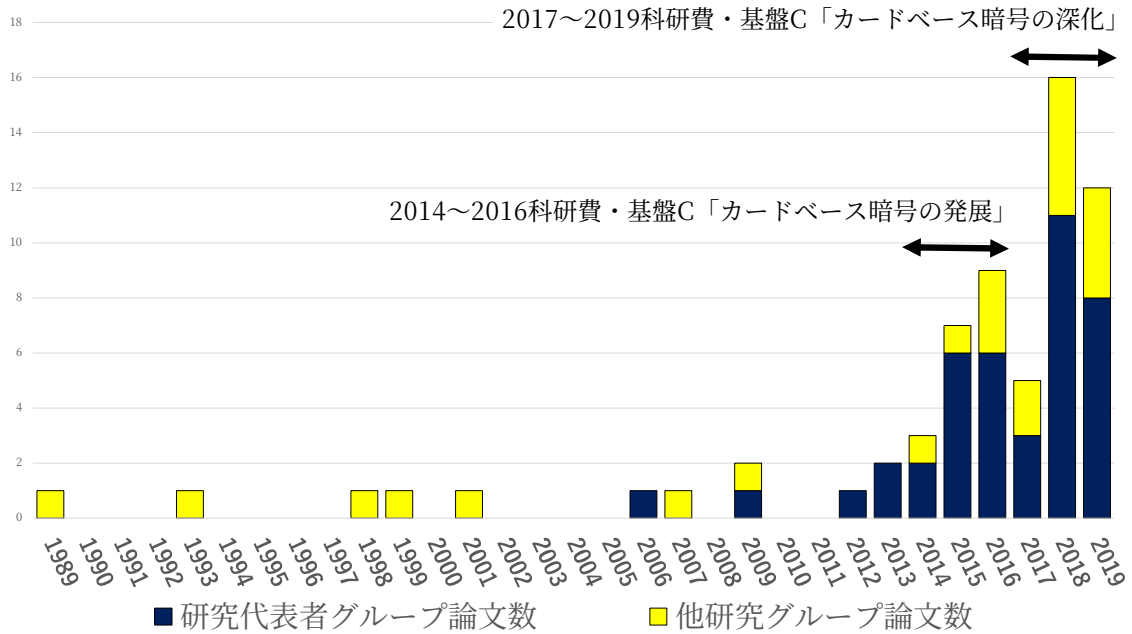
査読付論文誌（全て Scopus 収録）	掲載本数
Theoretical Computer Science	2
International Journal of Information Security	1
Soft Computing	1
IEICE Transactions on Fundamentals	2
Lecture Notes in Computer Science (LNCS)	12
Leibniz International Proceedings in Informatics (LIPIcs)	3
IFIP Advances in Information and Communication	1
ACM Conference Proceedings	2
合計	24

また，世界大学ランキングなどの指標で重要な「トップ 10%論文」について，上記の査読付論文を対象に調べてみた。SciVal を用いて 2016-2019 のデータを 2020 年 6 月 2 日に抽出したところ，研究業績の 24 本の査読付論文のうち，20 本が対象であった（研究業績には 2020 年のものや「掲載決定」を含むため)。この 20 本のうち，field-weighted でトップ 10%論文に該当するのは 5 本であった。したがって，トップ 10%論文の現在の輩出率は 25%である。

研究期間全体の直接経費は 350 万円であるので，単純に割り算すると，査読付論文 1 本あたりのコストは約 14 万 5 千円であり，トップ 10%論文 1 本あたり 70 万円である。

	本数	1 本あたりコスト（単純計算）
査読付論文	24 本	145,833 円
トップ 10%論文	5 本（対象 20 本のうち）	700,000 円

最後に，2019 年までに世界中で発表された，カードベース暗号に関するすべての論文の数（学術論文誌と査読付国際会議のみ）を，各年を横軸として次のグラフにまとめた。凡例の通り，濃い青で塗りつぶしている棒グラフが研究代表者のグループによる論文数であり，2006 年に研究代表者がこの分野の研究を始める以前は，海外のグループによる研究が散発的に存在していた。近年，本研究である基盤研究(C)「カードベース暗号の深化」（2017～2019 年度）およびその一つ前の研究代表者による基盤研究(C)「カードベース暗号の発展」（2014～2016 年度）に呼応する形で飛躍的に論文数が伸びていることがわかる。注目すべきは，研究代表者のグループだけではなく，他研究グループによる論文も着実に増えていることである。このことからも，研究代表者による科研費・基盤研究(C)が先導してこの研究分野を開拓してきていることが客観的に見て取れる。



このように二つの科研費基盤研究(C)により着実に発展・深化してきたこの分野をさらに進展するべく，2020 年度の科研費基盤研究(B)に「カードベース暗号の学術的進展と分野拡大」というタイトルで応募したが，残念ながら採択には至らなかった。我が国の研究力向上に資するためにも，計画調書をしっかりと練り直し，2021 年度の応募に臨みたい。

本邦が世界を先導するこのカードベース暗号の分野を停滞することなく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。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24件（うち査読付論文　24件／うち国際共著　6件／うちオープンアクセス　20件）

１．著者名 Tatsuya Sasaki, Daiki Miyahara, Takaaki Mizuki, and Hideaki Sone	４．巻 -
２．論文標題 Efficient Card-based Zero-knowledge Proof for Sudoku	５．発行年 2020年
３．雑誌名 Theoretical Computer Science	６．最初と最後の頁 採録決定
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1016/j.tcs.2020.05.036	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 Itaru Ueda, Daiki Miyahara, Akihiro Nishimura, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone	４．巻 -
２．論文標題 Secure Implementations of a Random Bisection Cut	５．発行年 2020年
３．雑誌名 International Journal of Information Security	６．最初と最後の頁 採録決定
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10207-019-00463-w	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 Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone	４．巻 803
２．論文標題 Practical Card-based Implementations of Yao's Millionaire Protocol	５．発行年 2020年
３．雑誌名 Theoretical Computer Science	６．最初と最後の頁 207～221
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2019.11.005	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 Daiki Miyahara, Tatsuya Sasaki, Takaaki Mizuki, and Hideaki Sone	４．巻 E102.A
２．論文標題 Card-Based Physical Zero-Knowledge Proof for Kakuro	５．発行年 2019年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1072～1078
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.1072	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 Daiki Miyahara, Leo Robert, Pascal Lafourcade, So Takeshige, Takaaki Mizuki, Kazumasa Shinagawa, Atsuki Nagao, and Hideaki Sone	4．巻 -
2．論文標題 Card-Based ZKP Protocols for Takuzu and Juosan	5．発行年 2020年
3．雑誌名 FUN 2020, Leibniz International Proceedings in Informatics	6．最初と最後の頁 採録決定
掲載論文のDOI（デジタルオブジェクト識別子） -	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 Kodai Toyoda, Daiki Miyahara, Takaaki Mizuki, and Hideaki Sone	4．巻 -
2．論文標題 Six-Card Finite-Runtime XOR Protocol with Only Random Cut	5．発行年 2020年
3．雑誌名 Proceedings of the 7rd ACM International Workshop on ASIA Public-Key Cryptography	6．最初と最後の頁 採録決定
掲載論文のDOI（デジタルオブジェクト識別子） -	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 Ken Takashima, Yuta Abe, Tatsuya Sasaki, Daiki Miyahara, Kazumasa Shinagawa, Takaaki Mizuki, and Hideaki Sone	4．巻 11949
2．論文標題 Card-Based Secure Ranking Computations	5．発行年 2019年
3．雑誌名 COCOA 2019, Lecture Notes in Computer Science	6．最初と最後の頁 461～472
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-36412-0_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 －

1．著者名 Ken Takashima, Daiki Miyahara, Takaaki Mizuki, and Hideaki Sone	4．巻 11934
2．論文標題 Card-Based Protocol Against Actively Revealing Card Attack	5．発行年 2019年
3．雑誌名 TPNC 2019, Lecture Notes in Computer Science	6．最初と最後の頁 95～106
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-34500-6_6	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 Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Tatsuya Sasaki, and Hideaki Sone	4．巻 11879
2．論文標題 A Physical ZKP for Slitherlink: How to Perform Physical Topology-Preserving Computation	5．発行年 2019年
3．雑誌名 ISPEC 2019, Lecture Notes in Computer Science	6．最初と最後の頁 135～151
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-34339-2_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 該当する

1．著者名 Jean-Guillaume Dumas, Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Tatsuya Sasaki, and Hideaki Sone	4．巻 11653
2．論文標題 Interactive Physical Zero-Knowledge Proof for Norinori	5．発行年 2019年
3．雑誌名 COCOON 2019, Lecture Notes in Computer Science	6．最初と最後の頁 166～177
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-26176-4_14	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 Pascal Lafourcade, Takaaki Mizuki, Atsuki Nagao, and Kazumasa Shinagawa	4．巻 557
2．論文標題 Light Cryptography	5．発行年 2019年
3．雑誌名 WISE 2019, IFIP Advances in Information and Communication Technology	6．最初と最後の頁 89～101
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-23451-5_7	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 Kazumasa Shinagawa and Takaaki Mizuki	4．巻 11458
2．論文標題 Secure Computation of Any Boolean Function Based on Any Deck of Cards	5．発行年 2019年
3．雑誌名 FAW 2019, Lecture Notes in Computer Science	6．最初と最後の頁 63～75
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-18126-0_6	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 Akihiro Nishimura, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone	4．巻 E101-A
2．論文標題 Pile-Shifting Scramble for Card-Based Protocols	5．発行年 2018年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 1494-1502
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E101.A.1494	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 Kazumasa Shinagawa and Takaaki Mizuki	4．巻 11396
2．論文標題 The Six-Card Trick: Secure Computation of Three-Input Equality	5．発行年 2019年
3．雑誌名 ICISC 2018, Lecture Notes in Computer Science	6．最初と最後の頁 123-131
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-12146-4_8	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 Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone	4．巻 11346
2．論文標題 Practical and Easy-to-Understand Card-Based Implementation of Yao's Millionaire Protocol	5．発行年 2018年
3．雑誌名 COCOA 2018, Lecture Notes in Computer Science	6．最初と最後の頁 246-261
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-04651-4_17	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 Yuichi Komano and Takaaki Mizuki	4．巻 11324
2．論文標題 Multi-party Computation Based on Physical Coins	5．発行年 2018年
3．雑誌名 TPNC 2018, Lecture Notes in Computer Science	6．最初と最後の頁 87-98
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-04070-3_7	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 Xavier Bultel, Jannik Dreier, Jean-Guillaume Dumas, Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Atsuki Nagao, Tatsuya Sasaki, Kazumasa Shinagawa, and Hideaki Sone	4．巻 11201
2．論文標題 Physical Zero-Knowledge Proof for Makaro	5．発行年 2018年
3．雑誌名 SSS 2018, Lecture Notes in Computer Science	6．最初と最後の頁 111-125
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-03232-6_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 該当する

1．著者名 Takaaki Mizuki and Yuichi Komano	4．巻 10979
2．論文標題 Analysis of Information Leakage Due to Operative Errors in Card-Based Protocols	5．発行年 2018年
3．雑誌名 IWOCA 2018, Lecture Notes in Computer Science	6．最初と最後の頁 250-262
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-94667-2_21	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 Daiki Miyahara, Itaru Ueda, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone	4．巻 10867
2．論文標題 Analyzing Execution Time of Card-Based Protocols	5．発行年 2018年
3．雑誌名 UCNC 2018, Lecture Notes in Computer Science	6．最初と最後の頁 145-158
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-92435-9_11	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 Tatsuya Sasaki, Takaaki Mizuki, and Hideaki Sone	4．巻 100
2．論文標題 Card-Based Zero-Knowledge Proof for Sudoku	5．発行年 2018年
3．雑誌名 FUN 2018, Leibniz International Proceedings in Informatics	6．最初と最後の頁 29:1-29:10
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.FUN.2018.29	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 Kazumasa Shinagawa and Takaaki Mizuki	4．巻 100
2．論文標題 Card-based Protocols Using Triangle Cards	5．発行年 2018年
3．雑誌名 FUN 2018, Leibniz International Proceedings in Informatics	6．最初と最後の頁 31:1-31:13
掲載論文のDOI（デジタルオブジェクト識別子） 10.4230/LIPIcs.FUN.2018.31	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 Yuta Abe, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone	4．巻 -
2．論文標題 Five-Card AND Protocol in Committed Format Using Only Practical Shuffles	5．発行年 2018年
3．雑誌名 Proceedings of the 5rd ACM International Workshop on ASIA Public-Key Cryptography	6．最初と最後の頁 3-8
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3197507.3197510	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 Akihiro Nishimura, Takuya Nishida, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone	4．巻 22
2．論文標題 Card-based Protocols Using Unequal Division Shuffles	5．発行年 2018年
3．雑誌名 Soft Computing	6．最初と最後の頁 361～371
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00500-017-2858-2	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 Julia Kastner, Alexander Koch, Stefan Walzer, Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone	4．巻 10626
2．論文標題 The Minimum Number of Cards in Practical Card-Based Protocols	5．発行年 2017年
3．雑誌名 ASIACRYPT 2017, Lecture Notes in Computer Science	6．最初と最後の頁 126～155
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-70700-6_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

〔学会発表〕　計34件（うち招待講演　5件／うち国際学会　1件）

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 ランダムカットのみを用いる6枚XORプロトコル
３．学会等名 電子情報通信学会総合大会
４．発表年 2020年

１．発表者名 村田総馬，阿部勇太，宮原大輝，水木敬明，曽根秀昭
２．発表標題 Private PEZとカードベースプロトコルの関係に関する考察
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 2020年

１．発表者名 竹茂宗，宮原大輝，水木敬明，曽根秀昭
２．発表標題 スリーブを用いた縦横さん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 2020年

１．発表者名 阿部勇太，水木敬明，曽根秀昭
２．発表標題 ランダムカットのみを用いるコミット型ANDプロトコルの改良と枚数削減不可能性
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 2019年

１．発表者名
高島健，宮原大輝，水木敬明，曽根秀昭

２．発表標題
非コミット型カードベースプロトコルと不正開示攻撃の定式化

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
2019年

１．発表者名
村田総馬，宮原大輝，水木敬明，曽根秀昭

２．発表標題
シンプルなカード入れ替え操作によるランダム置換生成の考察

３．学会等名
電子情報通信学会ソサイエティ大会

４．発表年
2019年

１．発表者名
高島健，宮原大輝，水木敬明，曽根秀昭

２．発表標題
不正開示攻撃を考慮したカードベースANDプロトコル

３．学会等名
電子情報通信学会ソサイエティ大会

４．発表年
2019年

１．発表者名
阿部勇太，水木敬明，曽根秀昭

２．発表標題
ランダムカットのみ用いる6枚コミット型ANDプロトコル

３．学会等名
電子情報通信学会ソサイエティ大会

４．発表年
2019年

１．発表者名
Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Tatsuya Sasaki, and Hideaki Sone

２．発表標題
Topology-Preserving Computation Using a Deck of Cards and Its Application (from SCIS 2019)

３．学会等名
The 14th International Workshop on Security (IWSEC 2019)（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
宮原大輝，駒野雄一，水木敬明，曽根秀昭

２．発表標題
ボールと袋を用いた秘密計算

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
2019年

１．発表者名
齋藤敬宏，千田栄幸，水木敬明

２．発表標題
シンプルなカードベース置換生成に関する一考察

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
2019年

１．発表者名
阿部勇太，林優一，水木敬明，曽根秀昭

２．発表標題
［招待講演］ Five-Card AND Protocol in Committed Format Using Only Practical Shuffles (from APKC 2018)

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
2019年

１．発表者名
水木敬明

２．発表標題
気まずくならない告白って？～カード組を用いた秘密計算

３．学会等名
東北大学大学院情報科学研究科シンポジウム～「情報科学」から「コミュニケーション」を考える（招待講演）

４．発表年
2019年

１．発表者名
Pascal Lafourcade，宮原大輝，水木敬明，佐々木達也，曽根秀昭

２．発表標題
物理的トポロジカル秘匿計算とその応用

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
2019年

１．発表者名
宮原大輝，水木敬明，曽根秀昭

２．発表標題
カードベース安定マッチング

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
2019年

１．発表者名
水木敬明

２．発表標題
カードベース暗号の最近の動向

３．学会等名
情報理論とその応用シンポジウム・特別セッション（招待講演）

４．発表年
2018年

１．発表者名
品川和雅，佐々木達也，水木敬明

２．発表標題
二人で楽しくババ抜きをプレイする方法

３．学会等名
情報理論とその応用シンポジウム

４．発表年
2018年

１．発表者名
宮原大輝，水木敬明，曽根秀昭

２．発表標題
トランプカードを用いた金持ち比べプロトコル

３．学会等名
電子情報通信学会コンピュテーション研究会

４．発表年
2018年

１．発表者名
齋藤敬宏，千田栄幸，水木敬明

２．発表標題
プレゼント交換に適したシンプルなカードベース置換生成

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
2018年

１．発表者名
駒野雄一，水木敬明

２．発表標題
情報セキュリティアンプラグド～計算機を用いない情報セキュリティ教育～

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
2018年

１．発表者名
高島健，阿部勇太，佐々木達也，宮原大輝，品川和雅，水木敬明，曽根秀昭

２．発表標題
カード組を用いた秘匿ランキング計算

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
2018年

１．発表者名
駒野雄一，水木敬明

２．発表標題
コインを用いる新たなマルチパーティ計算

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
2018年

１．発表者名
宮原大輝，佐々木達也，水木敬明，曽根秀昭

２．発表標題
カックロに対する物理的ゼロ知識証明の効率化

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
2018年

１．発表者名
宮原大輝，林優一，水木敬明，曽根秀昭

２．発表標題
［招待講演］ The Minimum Number of Cards in Practical Card-Based Protocols（ASIACRYPT 2017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
2018年

１．発表者名
阿部勇太，水木敬明，曽根秀昭

２．発表標題
5枚コミット型ANDプロトコルの改良

３．学会等名
電子情報通信学会総合大会

４．発表年
2018年

１．発表者名
高島健，水木敬明，曽根秀昭

２．発表標題
カード組を用いた安全なランキング計算

３．学会等名
電子情報通信学会総合大会

４．発表年
2018年

１．発表者名
佐々木達也，水木敬明，曽根秀昭

２．発表標題
数独の物理的ゼロ知識証明の効率化

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
2018年

１．発表者名
宮原大輝，林優一，水木敬明，曽根秀昭

２．発表標題
カード組の上下非対称性に基づくランダム二等分割カットの実装

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
2018年

１．発表者名
水木敬明，駒野雄一

２．発表標題
カードベースプロトコルにおける並べ替え誤りに関する考察

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
2017年

１．発表者名
阿部勇太，林優一，水木敬明，曽根秀昭

２．発表標題
単純なシャッフルを用いた5枚コミット型ANDプロトコル

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
2017年

１．発表者名
上田格，林優一，水木敬明，曽根秀昭

２．発表標題
実行時間に基づいたカードベースプロトコルの評価手法

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
2017年

１．発表者名
宮原大輝，林優一，水木敬明，曽根秀昭

２．発表標題
Private Permutation を用いない金持ち比べカードベースプロトコルの効率化

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
2017年

１．発表者名 上田格，林優一，水木敬明，曽根秀昭
２．発表標題 カードベースプロトコルの実行時間の評価に関する一提案
３．学会等名 電子情報通信学会ソサイエティ大会
４．発表年 2017年

１．発表者名 宮原大輝，林優一，水木敬明，曽根秀昭
２．発表標題 コミット型ANDプロトコルのシャッフル回数の下界について
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 2017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