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　４ 年　 ６ 月 ２１ 日現在

機関番号：１２６１２
研究種目：挑戦的研究（萌芽）
研究期間：2018～2021
課題番号：１８Ｋ１９７８０

研究課題名（和文）論理学を基にした暗号プロトコルの安全性証明と構築手法の深化

研究課題名（英文）A new look at security proofs of cryptographic primitives from logic

研究代表者
岩本　貢（Iwamoto, Mitsugu）

電気通信大学・大学院情報理工学研究科・教授

研究者番号：５０３７７０１６

交付決定額（研究期間全体）：（直接経費）　　4,900,000円

研究成果の概要（和文）：本研究では，暗号理論の安全性証明の本質を論理学の観点から再考し，シンプルで分かり易い暗号プロトコルを作成することを目指した．そのための道具として，近年盛んに研究されている物理暗号（カードなどの物理的な道具を用いて，暗号化などをシンプルにする技術）をもちいて研究を行った．通常の計算機で行われる秘密計算に近いモデルである秘匿置換ベースカードプロトコルや，安全性がシミュレーションに依らず直観的に分かり易いprivate PEZプロトコルに対して，効率や安全性を高めたいくつかのプロトコルを提案する事が出来た．それらの成果は国際論文誌や主要国際会議に採録されている．

研究成果の学術的意義や社会的意義
暗号理論の安全性証明は，安全性という曖昧な概念を数学的に書き下す，という意味で独特の論理体系を構築してきた．これは強固な安全性を保証するという利点と，その一方で分野外の研究者には困難が伴うという難点を抱えている．今後ますます重要になると予想される情報セキュリティの中核である暗号理論に対して，直観的で分かり易い理解の仕方を提供することは，暗号・情報セキュリティ技術がより社会に受け入れられるために必要なことである．論理学と暗号理論の関係をより深めていくことは，学際的な研究として重要であると考えており，得られた成果は学術的興味が実社会で役立つ良い事例になっていると考える．

研究成果の概要（英文）：In this study, we revisited the security proofs of cryptographic protocols from the viewpoint of logic and tried to understand them easily. As the tools for this purpose, we used so-called physical cryptography such as card-based protocols and private PEZ protocols, which have been studied extensively in recent years. Since the card-based protocols are based on the technique called a private permutation, the proposed protocols have a similar structure to ordinary (algebraic) multi-party computations. The security of private PEZ protocols is easier to understand compared to algebraic multi-party computations because it is free from simulation-based security. We proposed several new card-based and private PEZ protocols with higher efficiency, which contributed to understanding the security of cryptographic protocols simply. Some of these results have been published in international journals and major international conferences.

研究分野：暗号理論

キーワード：暗号理論　安全性証明　論理学　物理暗号

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

暗号理論は，情報通信における悪意のある攻撃から安全性を保証するための理論であり，暗号プロトコルの安全性証明はその最も重要な課題の一つである．安全性の証明技法は様々なものが知られているが，代表的なものとして公開鍵暗号系における「帰着技法」が挙げられる．これは「この暗号を破れる攻撃者は大きな素数の素因数分解が解ける（しかしそれは非現実的なので，その様な攻撃者は存在しない）」といった，対偶に基づく安全性証明技法である．このような問題のすり替え（例：帰着技法）や同値変形（例：ゲーム列による証明）といった考え方は，暗号理論の安全性証明全般にわたる基本的アプローチであり，非常に巧妙で強力である反面，証明が間接的になってしまうことから（用いられる数学的技巧の難しさと相俟って）暗号理論特有の分かりにくさを持っている．

一方で，これらの安全性証明で用いられる論理は対偶（背理法）や同値関係といった単純なものであり，より高度な論理的手法を導入すれば，暗号プロトコルの安全性を直接的かつ明快に理解できる可能性がある．実際に応募者らは，「カードベース暗号」と呼ばれるマルチパーティ計算（複数のプレーヤが各自の入力を秘匿しつつ，それらの関数値のみを得る暗号プロトコル）の一種において，有名な論理問題と本質的に等価な暗号プロトコルの例を明らかにし，その安全性を論理学によって直接理解することに成功した．

２．研究の目的

本研究では前節で述べた我々の成果をさらに深化させ，論理学との融合による暗号理論の新たな側面を明らかにすることを目指した．すなわち，論理学の成果を駆使して暗号プロトコルの論理構造を解析することで，その安全性を直接的に理解し，安全性証明技法および暗号プロコトルの構築技術に関する新たな方法論を確立する事が目標である．具体的には，次の二つの課題を通して研究課題にアプローチした．

課題(A) プロトコルに内在する論理の解析に基づく，安全性の理解と安全性証明技術の開発
課題(B) プロトコルの安全性が論理的に直接的で分かりやすい，暗号プロトコルの提案

従来の間接的な安全性証明では，対偶や同値関係といった論理構造を前提に，数論仮定や理想機能といった数学的な仮定やモデルに安全性証明を落とし込んでいた．本研究では，公開鍵暗号といったプロトコルの構成要素（モジュール）の存在に数論仮定や一方向性の仮定を埋め込み，暗号プロトコルの構成要素同士の論理関係を明確にすることで，暗号プロトコルの安全性を論理構造として直接的に理解する．

３．研究の方法

本研究の遂行にあたっては，背景でも述べたカードベース暗号を使う方法が一つの有効な手段である．カードベース暗号では，情報の書かれたカードを裏返すことでその情報を秘匿する事が出来る．カードを裏返すことは誰にでも出来るが，カードを開けることは受信者本人しか出来ない，という意味に於いて，カードベース暗号は公開鍵暗号を分かりやすくモジュール化する格好の道具である．カードベース暗号以外にも，例えばお菓子の PEZ をデータ構造のスタックになぞらえて秘密計算を行う，private PEZ プロトコルなどの物理暗号もあわせて研究する．

４．研究成果

本節では，雑誌論文を中心に成果を概観し，その他の成果について述べる．第 5 節「雑誌論文」の項の順番に簡単に説明する．

(1)論理学に基づく安全性・健全性証明：

本研究期間の初期段階で，本研究の発端となった，カードベース暗号における大小比較プロトコルと The folk in the road の関係を扱った成果をより詳細に検討し，論文誌に投稿した．安全性証明を詳細に検討し，嘘をつくことが安全性に，嘘つきでも正直でも正しい道が分かることが健全性に完全に対応することを明らかにした．

本研究で扱うカードベース暗号は「秘匿置換」と呼ばれる，カードを処理するプレーヤ以外の人からは見えないようにする処理が重要である．従来のカードベース暗号では，全ての操作を公開で行い，シャッフル操作など，公開でもランダム化できるカード操作特有の仮定を設けることで，プレーヤの不正が（それ自体は可能だが，見つかってしまうので，現実的には）できない様

になっていた．このモデルは malicious 安全性を暗黙に仮定できるというセキュリティ上の利点がある一方で，代数的（計算機間の対話で行う一般的な）秘密計算のモデルには相性が悪かった．そこで，カードを処理するプレーヤ以外の人からは見えないようにする処理である秘匿置換を用いる事で，代数的秘密計算のモデルに近い設定にして，暗号化などの機能をうまくモジュール化することに成功している．このことによって，プロトコルが論理問題と完全に対応が付き，課題(A)がうまく解決できることを示している．

(2)不正検知の物理的取り扱い：

(1)で扱った秘匿置換ベースのカードベース暗号は，代数的な秘密計算のモデルに近く，本研究の推進には有用な手段である一方で，他のプレーヤから見えない内部乱数を用いるため，プレーヤの不正に脆弱であり，semi-honest 安全性のもとで安全であるプロトコルが多い．そこで本研究では，秘匿置換を用いたカードベース暗号で不正を検知する方法を提案した．暗号における機能をできるだけモジュール化するため，従来の代数的秘密計算とは異なり，プレーヤの（秘匿置換を含めた）プロトコル実行を全て監視するが，プレーヤの入力情報を一切明かさないような方式が実現できることを示した．

秘匿置換を用いる事の利点は，秘密計算をモジュール化できることにより，従来のカードベース暗号よりも使用するカード枚数を減らすことができ，コンパクトなプロトコルが構成できることである．Semi-honest 安全性に安全性要件を緩めることはその代償と考えていたが，プレーヤが 3 名以上である場合は，本提案によって semi-honest 安全性を満たすプロトコルを malicious 安全性に変換することができる．本論文は(5)の多数決関数についての提案であるが，一般的な状況にも拡張可能であると考えており，今後の研究課題と考えている．また，監視するプレーヤを設けたことの，代数的秘密計算における意味づけなども今後の課題である．

(3)秘密分散法の整数計画法に基づく構成法：

秘密分散法は秘密情報をいくつかの分散情報（シェア）に分散する基本的暗号プリミティブである．通常よく考えられる秘密分散法はしきい値法と呼ばれ，しきい値を定めた上でその数までシェアを集められるかが秘密情報復元の可否を決める．一方で，集めてくると秘密が復元できるシェアの組合せと，どのように解析しても秘密情報が復元できない組合せを指定できる一般アクセス構造に対する秘密分散法の研究も重要である．そこで，しきい値法をモジュール（構成要素）として，一般アクセス構造をもつ秘密分散法を実現する研究がある．本研究では，しきい値法ではなく，近年提案された階層型しきい値秘密分散法を構成要素として，一般アクセス構造をもつ秘密分散が実現できることを示し，通常のしきい値法をベースとするより効率が良くなることを示した．

(4)対称関数に対する効率的 Private PEZ プロトコル

基本的なデータ構造であるスタックをお菓子の PEZ（容器に上からお菓子を詰め，上から順に食べる）に見立てて，秘匿計算を行うプロトコルを private PEZ プロトコルと呼ぶ．通常の代数的秘密計算の安全性は，プレーヤの view（確率分布）シミュレートすることで定式化されるが，private PEZ プロトコルでは view が確率分布ではなく実現値であり，それらが他のプレーヤの入力に依存せず，自分の入力のみで確定する，という分かり易さをもっている．一方で，view の実現値の同一性という分かり易さの代償として，private PEZ プロトコルは効率（例えば，事前に準備すべきお菓子の列である，初期文字列の長さ）が非常に悪く，また，構成法が組合せ的に非常に難解である．そのため，private PEZ プロトコルは 2003 年に提案されてから[Balogh et al.]，後続研究が存在しなかった．本研究では，計算対象を対称関数に限定すると，初期文字列数を従来研究の$O(2^n!)$から$O(n \cdot n!)$まで減らせることを示した（nはプレーヤ数）．提案手法の初期文字列長も指数的であるが，先行研究が二重指数であるため，大幅な改善となっている．

本研究の重要なテーマである「分かりやすさ」の意味でも本研究は重要な意義をもっている．[Balogh et al.]では安全性を二値系列の性質のみで議論しており，暗号学的な視点での理解が難しかった．本研究では，暗号学的な視点から view が分かり易くなるようなアプローチに切り替えて，数学的にも分かり易く，かつ効率的な構成法を提案している．

(5)多数決関数を最もコンパクトに実現する方法：

本研究では，3 枚のカードをもちいて 3 入力 3 出力(AND/XOR/NOR)の計算ができるプロトコルを提案した．このプロトコルを用いれば，カードの追加なしに 3 入力の多数決が実現できる．このプロトコルでは計算結果を一人のプレーヤが得て，それを他の二人に公開する必要があったが，公開手続きを経ずに 3 人で結果を共有できる方法も提案している．

提案プロトコルはすべて 3 入力プロトコルである．従来研究では 3 入力 1 出力であっても最低 6 枚のカードが必要であり，これを 3 枚で 3 出力のプロトコルが構成できる場合があることを示したことは，秘匿置換ベースのカードベース暗号の優位性を明らかにしている．さらに，秘匿置換ベースのカードベース暗号が代数的秘密計算のモジュール化に成功していることから，

このような成果を代数的秘密計算の効率化に役立てられることが期待できるが，この点は今後の課題である．

上記(1),(3)の研究を発展させたものを 2021 年度に国際論文誌 New Generation Computing に投稿し，本研究期間終了直後の 2022 年にそれぞれ採録されたことを付記する．

そのほか現在継続中の研究として，視覚型秘密分散法における改ざん検知手法，時間ドロボー（instant insanity）と呼ばれるパズルに対する物理的ゼロ知識証明，記法検出器を用いたゼロ知識非破壊検査などに関する成果を得た，これらは今後継続して発展させ，論文投稿を目指す予定である．

５．主な発表論文等

〔雑誌論文〕　計5件（うち査読付論文　5件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Nakai Takeshi、Misawa Yuto、Tokushige Yuuki、Iwamoto Mitsugu、Ohta Kazuo	４．巻 39
２．論文標題 How to Solve Millionaires' Problem with Two Kinds of Cards	５．発行年 2021年
３．雑誌名 New Generation Computing	６．最初と最後の頁 98-105
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00354-020-00118-8	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 Yoshiki Abe, Mitsugu Iwamoto, and Kazuo Ohta	４．巻 -
２．論文標題 How to Detect Malicious Behaviors in a Card-Based Majority Voting Protocol with Three Inputs	５．発行年 2020年
３．雑誌名 International Symposium on Information Theory (ISITA2020)	６．最初と最後の頁 377-381
掲載論文のDOI（デジタルオブジェクト識別子） 10.34385/proc.65.C01-9	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 Reo Eriguchi, Noboru Kunihiro, and Mitsugu Iwamoto	４．巻 2019-July
２．論文標題 Optimal Multiple Assignment Schemes Using Ideal Multipartite Secret Sharing Schemes	５．発行年 2019年
３．雑誌名 Proc. IEEE International Symposium on Information Theory (ISIT2019)	６．最初と最後の頁 3047-3051
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISIT.2019.8849591	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 Y. Abe, M. Iwamoto, and K. Ohta	４．巻 LNCS11891
２．論文標題 Efficient Private PEZ Protocols for Symmetric Functions	５．発行年 2019年
３．雑誌名 Proc. Theory of Cryptography Conference (TCC2019)	６．最初と最後の頁 372-392
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-36030-6_15	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 Yohei Watanabe, Yoshihisa Kuroki, Shinnosuke Suzuki, Yuta Koga, Mitsugu Iwamoto, Kazuo Ohta	４．巻 -
２．論文標題 Card-Based Majority Voting Protocols with Three Inputs Using Three Cards	５．発行年 2018年
３．雑誌名 Proc. International Symposium on Information Theory and Its Applications (ISITA2018)	６．最初と最後の頁 218-222
掲載論文のDOI（デジタルオブジェクト識別子） 10.23919/ISITA.2018.8664324	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 －

〔学会発表〕　計12件（うち招待講演　2件／うち国際学会　1件）

１．発表者名 根岸 奎人，渡邉 洋平，岩本 貢
２．発表標題 視覚復号型秘密分散法における任意の改ざんを検知する手法
３．学会等名 暗号と情報セキュリティシンポジウム（SCIS2021）
４．発表年 2021年

１．発表者名 初貝 恭祐，安部 芳紀，中井 雄士，品川 和雅，渡邉 洋平，岩本 貢
２．発表標題 時間ドロボー問題に対する健全性誤りのない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（SCIS2021）
４．発表年 2021年

１．発表者名 中井 雄士，徳重 佑樹，岩本 貢，太田 和夫
２．発表標題 秘匿置換を用いたカードベースしきい値関数プロトコル
３．学会等名 暗号と情報セキュリティシンポジウム（SCIS2021）
４．発表年 2021年

１．発表者名
安部 芳紀，岩本 貢，太田 和夫

２．発表標題
対称関数を効率的に計算するPrivate PEZ プロトコル（from TCC 2019）

３．学会等名
電子情報通信学会ISEC研究会（招待講演）

４．発表年
2021年

１．発表者名
品川和雅，三浦典之，岩本貢，崎山一男，太田和夫

２．発表標題
気泡検出器を用いたゼロ知識非破壊検査

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
安部芳紀，岩本貢，太田和夫

２．発表標題
任意の始集合を持つ関数を計算するprivate PEZ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（SCIS）2020

４．発表年
2020年

１．発表者名
安部芳紀，岩本貢，太田和夫

２．発表標題
任意の関数を計算するprivate PEZプロトコルの改善

３．学会等名
コンピューターセキュリティシンポジウム（CSS）2019

４．発表年
2019年

１．発表者名
Yoshiki Abe, Mitsugu Iwamoto, Kazuo Ohta

２．発表標題
How to improve the private PEZ protocol for general functions

３．学会等名
The 14th International Workshop on Security (IWSEC2019), poster session（国際学会）

４．発表年
2019年

１．発表者名
岩本貢

２．発表標題
秘密計算の安全性～プライバシーを保ちつつどこまで計算できるか

３．学会等名
第8回バイオメトリクスと認識・認証シンポジウム(SBRA)（招待講演）

４．発表年
2018年

１．発表者名
安部 芳紀, 山本 翔太, 岩本 貢, 太田 和夫

２．発表標題
初期文字列が29 文字の4 入力多数決Private PEZプロトコル

３．学会等名
情報理論・情報セキュリティ・ワイドバンドシステム合同研究会

４．発表年
2019年

１．発表者名
安部 芳紀, 山本 翔太, 岩本 貢, 太田 和夫

２．発表標題
不正検知可能な3入力多数決カードプロトコル

３．学会等名
暗号と情報セキュリティシンポジウム (SCIS2019)

４．発表年
2019年

１．発表者名
山本 翔太，安部 芳紀，岩本 貢，太田 和夫

２．発表標題
4入力多数決を計算する効率的なPrivate PEZ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（SCIS2019）

４．発表年
2019年

〔図書〕　計2件

１．著者名 太田和夫、岩本貢、渡邉洋平（取材協力）	４．発行年 2021年
２．出版社 ニュートンプレス	５．総ページ数 176
３．書名 Newton別冊　数学の世界　現代編　増補第2版（暗号 個人情報を守る数学，pp.98-115）	

１．著者名 Takeshi Nakai	４．発行年 2021年
２．出版社 The University of Electro-Communications	５．総ページ数 96
３．書名 PRIVATE PERMUTATIONS IN CARD-BASED CRYPTOGRAPHY	

〔産業財産権〕

〔その他〕

電気通信大学　教員総覧
http://kjk.office.uec.ac.jp/Profiles/11/0001044/profile.html
岩本・渡邉研究室ホームページ
https://iw-lab.jp/
岩本貢のホームページ
https://www.iw-lab.jp/users/mitsugu/

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1件

国際研究集会	開催年
Workshop on Cryptography Using Physical Tools	2019年～2019年

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