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

平成　２９　年　　５　月　２６　日現在

機関番号：　１１３０１
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３０００１

研究課題名（和文）カードベース暗号の発展

研究課題名（英文）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・准教授

研究者番号：９０３２３０８９

交付決定額（研究期間全体）：（直接経費）　　3,600,000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，様々な効率的なカードベース暗号プロトコルを構築したこと，プロトコルに必要なカード枚数の下界を与えたこと，いくつかのシャッフルの実装方法を提案したこと，カードベース暗号を教育へ応用したこと等であり，これらを通してカードベース暗号の研究分野の発展を牽引した。

研究成果の概要（英文）：Using a deck of physical cards (like playing cards), card-based cryptography performs cryptographic tasks such as secure multiparty computation. The principal investigator constructed many efficient card-based cryptographic protocols, provided lower bounds on the number of required cards, proposed implementations of shuffles, applied card-based cryptography to education, and so on. Consequently, this research project has contributed to the development of card-based cryptography.

研究分野：　暗号系

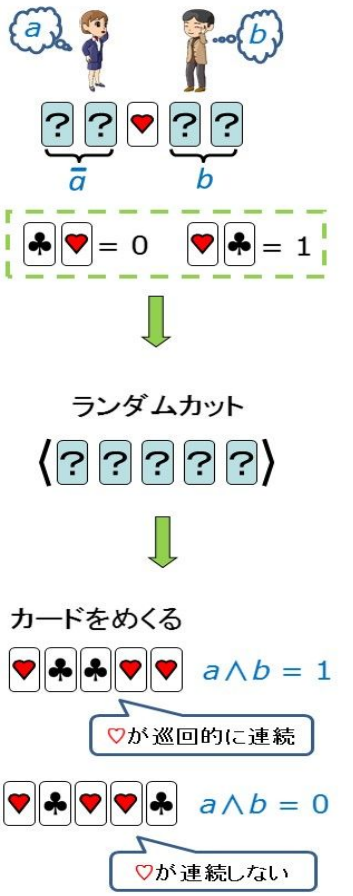
キーワード：　カードベース暗号

１．研究開始当初の背景

「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」等を身近で手軽に実現するものである。まず，カード組を用いた秘密計算とはどういうものかについて，具体的な例を挙げて説明することから始める。

友達同士の花子さんと太郎君がいて，二人がお付き合いするかどうかを決めたい場面を考えよう。ただし，告白の結果によって気まずくなるのを避けるため，交際成立か不成立かだけを知りたい。すなわち，花子さんがビット a を持ち，太郎君がビット b を持つとき，論理積（AND 演算）a∧b の結果だけを知りたい。このように，それぞれの入力の値を秘密にしたまま，目的とする関数の値だけを求めることを秘密計算と言う。

den Boer は Eurocrypt 1989 にて，5 枚のカードを用いて論理積の秘密計算を実現するプロトコル（Five-Card Trick）を提案した。



上図のように，各プレイヤーは赤と黒のカードの並びでビットを表現して入力し，ランダムカット（巡回的なシャッフル）を適用した後，全てのカードをめくり，三枚の赤いカードが連続して並ぶか否かで AND の秘密計算が実現できる。

本研究開始前まで，このようなカードベース暗号プロトコルがいくつも開発され，例えば研究代表者は Asiacrypt 2012 にて，上のような AND 計算が 4 枚のカードで実現できることを証明し，二十数年ぶりに必要なカードを 1 枚減らすことに成功していた。また，コミット型と呼ばれる AND プロトコルに関しても，研究代表者が開発したものが最高性能を有していた。また，XOR 計算に関しても，研究代表者は最適な枚数である 4 枚のカードでのプロトコルを考案していた。あるいは，秘密計算の実用上重要な応用として投票や多数決があるが，研究代表者はそれらを効率的に実現するプロトコルも与えており，例えば投票の場合，世の中で通常用いられる方法では，投票者と同じ数の投票用紙を用意するが，研究代表者の手法は投票者数の対数スケールのカード枚数で投票（秘密計算に対応した加算器）を実現していた。

研究代表者の研究グループ以外による研究としては，冒頭に紹介した 1989 年の den Boer による Five-Card Trick に引き続き，2001 年頃まで，欧米のいくつかの研究者グループによりいくつかのカードベース暗号プロトコルが提案されている。2001 年以降から本研究開始前までの期間においては，カードベース暗号の研究に取り組んでいたのは，研究代表者のグループだけのようであった。

２．研究の目的

前節で述べたように，カードベース暗号は，身近にある物理的なカード組を用いて秘密計算を実現するものであり，プロトコルの正当性や安全性は高校生でも理解することができるとともに，実際に自分の手でプロトコルを容易に動かすことができる非常に魅力的なものである。本研究では，既存の成果をさらに学理的に進展させ，秘密計算を効率的に実現する汎用的手法や本質的限界を解明するとともに，人間フレンドリーな分かり易いプロトコルの開発を追及する。また，カードベース暗号が一般市民にも理解が容易であるという特徴を活かし，開発するプロトコルを実際に使って心の底から「安全を実感」してもらうことを目指している。

既存の成果を学理的に発展させるという目標について，もう少し詳しく述べる。カードベース暗号の研究分野は上で述べた通りに着実に進んでいるが，まだまだ未解決問題がたくさん残されていた。例えば，コミット型の AND 計算では，6 枚のカードを用いたものが本研究開始前時点においては最良であったが，この 6 枚より減らせるか，あるいは原理的に不可能なのかについて解明することが望まれていた（なお，この未解決問題は，ドイツの研究者 Koch らによって，Asiacrypt 2015 において，肯定的に解決された）。また，3 変数以上の関数に対する秘密計算について，汎用的な効率的手法が検討されておらず，普遍的な学理追及が必要とされていた。

研究代表者が Asiacrypt 2012 において 4 枚の AND 計算プロトコルを発表して以降，その分かり易さも相まって，カードベース暗号への注目度が急速に高まりつつあった。この追い風を受けて，カードベース暗号の研究分

野に参入する研究者が増え，本研究課題の題目通り「カードベース暗号の発展」を実現することも大きな目的である。

３．研究の方法

研究代表者はこれまで既に数多くのカードベース暗号プロトコルを開発してきているので，そこで得られている知見や経験を活かすとともに，注目度が高まっているカードベース暗号をさらに研究集会や国際会議において発表することによりアピールし，他の研究者とのディスカッション等を通して，新しいプロトコルの開発や計算限界の解明にフィードバックする。また本学のオープンキャンパスや高校での出前授業等において開発したプロトコルを一般市民の方々に試してもらい，そこでのフィードバックも次への開発へ活かし，本研究の目的を達成する。

４．研究成果

本研究の成果は次の各項目に示す通りである。

(1) 3 変数関数に対する秘密計算

これまで対称な 3 変数関数は高々6 枚のカードで計算できることが知られているのに対して，本研究では，対称関数に限定せず，すべての 3 変数関数が 6 枚以内のカードで計算できることを証明した。この成果は IEICE Trans. Fundamentals 誌に掲載されている（５．主な発表論文等の〔雑誌論文〕の⑬）。

(2) 任意の関数に対する汎用的プロトコル

4 変数以上のすべての関数に対応した汎用的なプロトコル構築法を AND-EXOR 表現を用いることにより確立し，どんな関数であっても高々6 枚の追加カードがあれば秘密計算を実現するプロトコルを構成できることを示した。また，対称関数に限定した場合には高々 2 枚の追加カードで十分であることを証明した。これらの成果はカードベース暗号の本質的限界を探る上で重要な上界となるものであり，国際会議 TAMC 2015 においてその内容を公表した（〔雑誌論文〕の⑭）。

(3) 効率的な多入力 AND 秘密計算

秘密計算の応用として多人数の問題に効率的に対応することは極めて重要であるが，その代表とも言える多入力の AND 秘密計算について，既存のコミット型 AND プロトコルを組み合せて構成される単純な方法よりも効率的なプロトコルを開発し，その成果を Theoretical Computer Science 誌に掲載した（〔雑誌論文〕の⑦）。

(4) 市販トランプカードの利用

既存研究で提案されてきたカードベース暗号プロトコルのほとんどすべては，表面が同一の模様のカードを複数枚必要とするため，基本的に市販トランプカードでは実行できない。そこで本研究では，市販トランプカードでも実行可能なプロトコルの開発に取り組み，効率的な AND/XOR/COPY プロトコルを考案し，これらを組み合わせることで任意の関数を秘密計算できることを示した。この成果を国際会議 CANS 2016 等において公表している（〔雑誌論文〕の⑤，〔学会発表〕の⑦）。

(5) 変則的なシャッフル

近年注目されている「変則的なシャッフル」の本質的な限界を探るべくそれを用いた新しいカードベース暗号を考案し，既存プロトコルより優れた AND 計算やコピープロトコルを構成するとともに，変則シャッフルの具体的な実装方法も与え，その成果を国際会議 TPNC 2015 や AsiaPKC 2016 等において公表した（〔雑誌論文〕の⑨，〔学会発表〕の①④⑤⑥）。

(6) 必要なカード枚数に関する下界

カードベース暗号プロトコルの計算限界を解明する上で，必要なカード枚数の下界を求めることは極めて重要である。本研究では，2 ビット出力関数に焦点を当て，それらを秘密計算するために必要なカード枚数の下界を与え，その枚数で動作するプロトコルも構築することにより，カード枚数に関する必要十分条件を明らかにした。この成果は，国際会議 Mycrypt 2016 にて公表した（〔雑誌論文〕の②）。

(7) シャッフルの実装法

カードベース暗号の重要なプリミティブであるランダム二等分割カットは，与えられたカード列を二等分割し，それらをランダムに入れ替えるシャッフルであり，結果として得られるカード列は 2 通りしかない。そのため，しばしば，このようなシャッフルをどのように実装するのが適切か議論になっていた。本研究では，この問題を解決するいくつかの実装方法を提案し，基礎実験を通して，提案手法の安全性を示した。この成果は国際会議 TPNC 2016 等において公表している（〔雑誌論文〕の④，〔学会発表〕の③）。

(8) 効率的な不動点のない置換生成

よりアプリケーションを指向し，クリスマスの時期に典型的な「プレゼント交換」を適切に実施できるようにするため，不動点を持たない置換の生成という問題に取り組み，既存のプロトコルの大幅な効率化に成功した。この成果は国際会議 UCNC 2015 等にて公表した（〔雑誌論文〕の⑪，〔学会発表〕の⑨）。

(9) 様々な形状のカード組の利用

本研究では，様々な形状のカード組の活用を検討した。まず，偏光板カードを用いたプロトコルを国際会議 IWSEC 2015 や IEICE Trans. Fundamentals 誌で公表している（〔雑誌論文〕の⑥⑫）。また，正多角形の形状をした回転可能なカードを用いると効率的に秘密計算

が実現できることを ProvSec 2015 や IEICE Trans. Fundamentals 誌等において公表している（〔雑誌論文〕の①⑩,〔学会発表〕の⑧）。

(10) 研究分野の格段な発展のための活動
電子情報通信学会 Fundamentals Review 誌から依頼を受け,「カード組を用いた秘密計算」という解説記事を掲載している（〔雑誌論文〕の⑧）。更に,カードベース暗号の計算モデルに関するサーベイと汎用的な枠組みの確立を与える招待論文を IEICE Trans. Fundamentals 誌に掲載している（〔雑誌論文〕の③）。

(11) アウトリーチ活動と教育への応用
カードベース暗号に適したカード組を作成し，オープンキャンパスや高校での出前授業において開発したプロトコルを一般市民の方々に試してもらい，カードベース暗号の普及・発展に努めている。

加えて,東北大学全学教育科目・基礎ゼミにおいて「カード組を用いた暗号プロトコル」というテーマで授業を行い,人間フレンドリーな研究成果の教育への応用も進めている（〔学会発表〕の②）。

以上が本研究で得られた成果である。研究期間全体を通して，積極的な成果の公表や，解説論文・招待論文の執筆等により，カードベース暗号の分野に参入する研究者がここ数年で急増しており，暗号と情報セキュリティシンポジウム（SCIS）においてカードプロトコルのセッションが組まれるなど，研究課題名「カードベース暗号の発展」の通り，分野の発展を牽引することができた。
研究代表者はこれらの成果を踏まえ，2017 年度より，科学研究費基盤研究(C)「カードベース暗号の深化」(2017～2019 年度)にて，当該分野のさらなる深化を進めている。

５．主な発表論文等

〔雑誌論文〕（計 14 件）

① Kazumasa Shinagawa, Takaaki Mizuki, Jacob C.N. Schuldt, Koji Nuida, Naoki Kanayama, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto, Card-Based Protocols Using Regular Polygon Cards, IEICE Trans. Fundamentals, 査読有, vol.E100-A, 2017, 掲載決定.

② Danny Francis, Syarifah Ruqayyah Aljunid, Takuya Nishida, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone, Necessary and Sufficient Numbers of Cards for Securely Computing Two-Bit Output Functions, Mycrypt 2016, Lecture Notes in Computer Science, Springer-Verlag, 査読有, 2017, 掲載決定.

③ Takaaki Mizuki and Hiroki Shizuya, [Invited Paper] Computational Model of Card-Based Cryptographic Protocols and Its Applications, IEICE Trans. Fundamentals, 査読有, vol.E100-A, no.1, 2017, pp.3-11.
DOI: 10.1587/transfun.E100.A.3

④ Itaru Ueda, Akihiro Nishimura, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone, How to Implement a Random Bisection Cut, Theory and Practice of Natural Computing (TPNC 2016), Lecture Notes in Computer Science, Springer-Verlag, 査読有, vol. 10071, 2016, pp. 58-69.
DOI: 10.1007/978-3-319-49001-4_5

⑤ Takaaki Mizuki, Efficient and Secure Multiparty Computations Using a Standard Deck of Playing Cards, Cryptology and Network Security (CANS 2016), Lecture Notes in Computer Science, Springer-Verlag, 査読有, vol.10052, 2016, pp.484-499.
DOI: 10.1007/978-3-319-48965-0_29

⑥ Kazumasa Shinagawa, Takaaki Mizuki, Jacob C.N. Schuldt, Koji Nuida, Naoki Kanayama, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto, Secure Computation Protocols Using Polarizing Cards, IEICE Trans. Fundamentals, 査読有, vol.E99-A, no.6, 2016, pp. 1122-1131.
DOI: 10.1587/transfun.E99.A.1122

⑦ Takaaki Mizuki, Card-Based Protocols for Securely Computing the Conjunction of Multiple Variables, Theoretical Computer Science, 査読有, vol.622, 2016, pp.34-44.
DOI: 10.1016/j.tcs.2016.01.039

⑧ 水木敬明, 解説論文：カード組を用いた秘密計算, 電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review, 査読無, vol. 9, no.3, 2016, pp. 179-187.
DOI: 10.1587/essfr.9.3_179

⑨ Akihiro Nishimura, Takuya Nishida, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone, Five-Card Secure Computations Using Unequal Division Shuffle, Theory and Practice of Natural

Computing (TPNC 2015), Lecture Notes in Computer Science, Springer-Verlag, 査読有, vol. 9477, 2015, pp. 109-120.
DOI: 10.1007/978-3-319-26841-5_9

⑩ Kazumasa Shinagawa, Takaaki Mizuki, Jacob C. N. Schuldt, Koji Nuida, Naoki Kanayama, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto, Multi-party Computation with Small Shuffle Complexity Using Regular Polygon Cards, International Conference on Provable Security (ProvSec 2015), Lecture Notes in Computer Science, Springer-Verlag, 査読有, vol. 9451, 2015, pp. 127-146.
DOI: 10.1007/978-3-319-26059-4_7

⑪ Rie Ishikawa, Eikoh Chida, and Takaaki Mizuki, Efficient Card-based Protocols for Generating a Hidden Random Permutation without Fixed Points, Unconventional Computation and Natural Computation (UCNC 2015), Lecture Notes in Computer Science, Springer-Verlag, 査読有, vol.9252, 2015, pp. 215-226.
DOI: 10.1007/978-3-319-21819-9_16

⑫ Kazumasa Shinagawa, Takaaki Mizuki, Jacob Schuldt, Koji Nuida, Naoki Kanayama, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto, Secure Multi-Party Computation Using Polarizing Cards, Advances in Information and Computer Security (IWSEC 2015), Lecture Notes in Computer Science, Springer-Verlag, 査読有, vol. 9241, 2015, pp. 281-297.
DOI: 10.1007/978-3-319-22425-1_17

⑬ Takuya Nishida, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone, Securely Computing Three-input Functions with Eight Cards, IEICE Trans. Fundamentals, 査読有, vol.E98-A, no.6, 2015, pp. 1145-1152.
DOI: 10.1587/transfun.E98.A.1145

⑭ Takuya Nishida, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone, Efficient Card-Based Protocols for Any Boolean Function, Theory and Applications of Models of Computation (TAMC 2015), Lecture Notes in Computer Science, Springer-Verlag, 査読有, vol. 9076, 2015, pp. 110-121.
DOI: 10.1007/978-3-319-17142-5_11

〔学会発表〕(計9件)

① 西村明紘, 林優一, 水木敬明, 曽根秀昭, Pile-Shifting Scrambleで実現可能な二状態不均一シャッフルに関する考察, 2017年暗号と情報セキュリティシンポジウム, 2017年1月24日, ロワジールホテル那覇(沖縄県那覇市).

② 水木敬明, カードベース暗号の教育への応用, 電子情報通信学会情報セキュリティ研究会, 2016年11月7日, 福井市地域交流プラザAOSSA(福井県福井市).

③ 上田格, 西村明紘, 林優一, 水木敬明, 曽根秀昭, ランダム二等分割カットの安全な実行に関する考察, 電子情報通信学会情報セキュリティ研究会, 2016年9月2日, 機械振興会館(東京都港区).

④ Akihiro Nishimura, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone, An Implementation of Non-Uniform Shuffle for Secure Multi-Party Computation, 3rd ACM International Workshop on ASIA Public-Key Cryptography (AsiaPKC '16), 2016年5月30日, 西安(中国).

⑤ 西村明紘, 林優一, 水木敬明, 曽根秀昭, 不均一な確率分布のシャッフル操作の実現に関する一考察, 2016年暗号と情報セキュリティシンポジウム, 2016年1月22日, ANAクラウンプラザホテル熊本ニュースカイ(熊本県熊本市).

⑥ 西村明紘, 西田拓也, 林優一, 水木敬明, 曽根秀昭, 2015年電子情報通信学会ソサイエティ大会, 変則的シャッフルを用いたカードベース暗号プロトコル, 2015年9月10日, 東北大学川内北キャンパス(宮城県仙台市).

⑦ 水木敬明, 市販トランプカードを用いた安全な計算について, 電子情報通信学会情報セキュリティ研究会, 2015年3月3日, 北九州市立大学(福岡県北九州市).

⑧ 品川和雅, 水木敬明, 縫田光司, 金山直樹, 西出隆志, 岡本栄司, 正多角形カードを用いた秘密計算プロトコル, 2015年暗号と情報セキュリティシンポジウム, 2015年1月20日, リーガロイヤルホテル小倉(福岡県北九州市).

⑨ 石川理恵, 千田栄幸, 水木敬明, カード組を用いた不動点のない置換のランダム生成, 電子情報通信学会情報セキュリティ研究会, 2014年11月21日, 兵庫県立大学(兵庫県神戸市).

6. 研究組織

(1)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