科学研究費助成事業　　研究成果報告書

平成　２６　年　　５　月　２１　日現在

機関番号：　１１３０１
研究種目：　若手研究(B)
研究期間：　2011～2013
課題番号：　２３７００００７

研究課題名（和文）テンソル分解の安全な計算への応用

研究課題名（英文）Applications of Tensor Decompositions to Secure Multiparty Computations

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）　　3,200,000円、（間接経費）　　960,000円

研究成果の概要（和文）：何人かのプレーヤーがいて，各自秘密の入力を持っているとき，それぞれのプレーヤーの入力は秘密にしたままで，ある目的とする関数の出力結果だけを得ることを安全な計算と言う。目的とする関数に対して，テンソル分解の一つであるAND-XOR表現を用いて展開することで安全な計算を実現できることが知られている。本研究の主要な結果は，このようなXOR展開などを応用することにより，安全な計算を実現するプロトコルを効率化したことである。

研究成果の概要（英文）：Assume that there are players holding private inputs, and that they want to learn the output of a desired function without revealing their inputs: this is called a secure multiparty computation. It is known that tensor decompositions such as XOR expansions can be utilized for secure multiparty computations. One of the main results was to improve the efficiency of secure multiparty computations by using such XOR expansions and other representations.

研究分野：　総合領域

科研費の分科・細目：　情報学，情報学基礎

キーワード：　アルゴリズム理論

１．研究開始当初の背景

本研究は，安全な計算（Secure Multiparty Computations）を実現する暗号プロトコルの効率化を主要な目的としている。まず，この「安全な計算」の概要について言及する。歴史的には 1982 年の Yao による有名な「金持ち財産比べ」プロトコル [Y82] に始まる。このプロトコルでは，二人のプレーヤー，アリスとボブが，お互い自分の財産の額は見せずに秘密にしたままで，どちらが金持ちであるか，その事実だけを知ることができる。これを一般化すると，何人かのプレーヤーがいて，各プレーヤーは自分だけに秘密な入力を持っているとき，それぞれのプレーヤーの入力を秘密にしたままで，ある目的とする関数を計算し，その出力結果だけを所定のプレーヤーで知ることができるようにしたい。このような問題の解決をターゲットとしている安全な計算の歴史は長く，これまで非常に多くの研究者がプロトコルの開発や計算モデル・通信モデルの定式化，理論的な限界の解明，実装等に取り組んでいる。

研究代表者は，2006 年に AND-XOR 表現のひとつ，論理積（AND）項を排他的論理和（XOR）で結んで表現される ESOP（Exclusive-or Sum-of-Products）展開が，極小モデルにおける安全な計算の効率化に応用できることを示し [M06]，その成果をさらに発展させるべく，科学研究費若手研究(B)「回路設計理論の安全な計算への実用的応用」（2007～2009 年度）において，ブール行列の階段化を実行することと，ESOP 展開を最小化することが同じ意味を持つことを示した [M10]。よく知られているように，行列の階段化は多項式時間で実行できるので，先に述べた結果と合わせると，例えばガウスの消去法は，安全な計算を直ちに効率化することを意味する。

さらに，研究代表者は，上述の科研費若手研究(B)において，回路設計理論の基本演算である論理積や排他的論理和に対して，カード組を利用するという基礎的通信モデルにおいて，安全な計算のために必要なコストの削減に成功している。より具体的には，論理積については 6 枚，排他的論理和については 4 枚のカードで安全な計算を実現できることを示している [M09]。

以上が研究開始当初の背景であり，おおまかには，これらの既存成果をさらに発展させることが，本研究の重要な目標となっていたと言える。

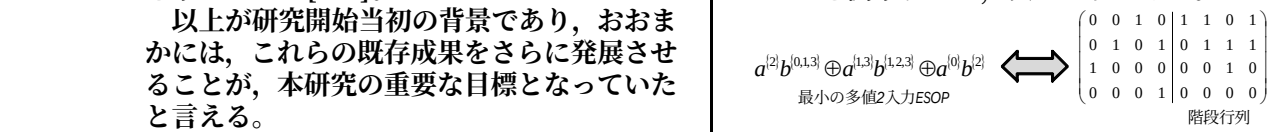
[Y82] A. C. Yao, Protocols for secure computations, Annual Symposium on Foundations of Computer Science (FOCS 1982), pp.160-164, 1982.
[M06] T. Mizuki, T. Otagiri, and H. Sone, Secure computations in a minimal model using multiple-valued ESOP expressions, Theory and Applications of Models of Computation (TAMC 2006), Lecture Notes in Computer Science, vol.3959, Springer-Verlag, pp.547-554, 2006.
[M10] T. Mizuki, H. Tsubata, and T. Nishizeki, Minimizing AND-EXOR expressions for two-variable multiple-valued input binary output functions, Journal of Multiple-Valued Logic and Soft Computing, vol.16, pp.197-208, 2010.
[M09] T. Mizuki and H. Sone, Six-card secure AND and four-card secure XOR, Frontiers in Algorithmics (FAW 2009), Lecture Notes in Computer Science, Springer-Verlag, vol.5598, pp.358-369, 2009.

２．研究の目的

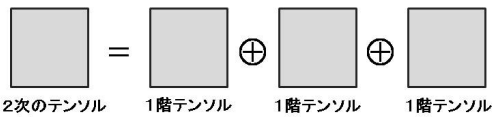
本研究は，研究代表者による既存の成果をさらに発展させることに主眼を置き，それまでに得られている安全な計算を実現するプロトコルの効率化を狙っている。特に，テンソル分解についての既知の知見をうまく活用し，安全な計算を実現する暗号プロトコルの効率化に応用を図ることなどを目的としている。前述の通り，リテラルの論理積を排他的論理和で結んで得られる ESOP 展開が安全な計算に応用できることと，ESOP 展開の最小化が行列の階段化と同等の意味を持つこと，すなわち，行列の階数が安全な計算のコストに直結するという知見を既に得ているので，行列の階数の一般化がテンソルの階数であると捉え，テンソル分解と ESOP 展開の関係を明らかにし，安全な計算を効率化することを目指している。さらには，より広いクラスの安全な計算を実現するプロトコルの改良やモデル化にも取り組む。

３．研究の方法

既に上で述べているように，研究代表者の既存知見として，ESOP 展開の最小化とブール行列の階段化が同じ意味を持つということがある。もう少し詳しく説明すると，2 変数多値入力 2 値出力関数の ESOP 展開をブール行列とみなすことで，ESOP 展開に対する変形ルールの適用と，ブール行列における基本変形が同等の意味を持つことを示している。このことを例示すると，次のようになる。

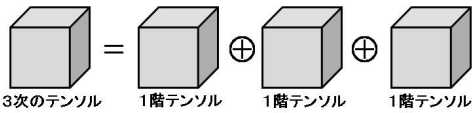


ここで，階段行列は，2 次のテンソルに対する 1 階テンソルへの分解（正準分解；Canonical Decomposition）と見なすことができる。



これを自然に拡張すると，例えば，3 変数多値入力 2 値出力関数の ESOP 展開は，3 次のテンソルに対する 1 階テンソル分解と捉えられ

ることが期待される。



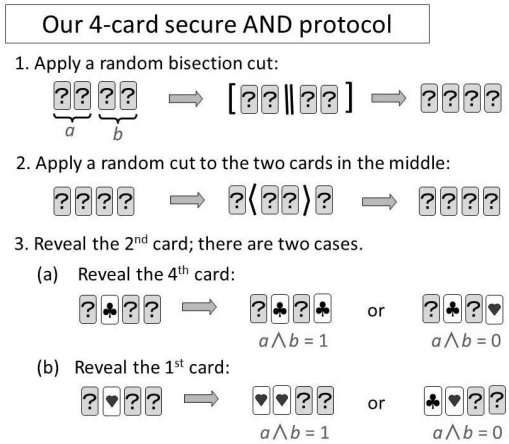
このような洞察を踏まえ，安全な計算の問題を，linear algebra な問題に帰着させ，効率の良いプロトコル開発を目指す。例えば，ESOP 展開の一般化である ESCT (Exclusive-or Sum of Complex Terms)展開を考えると，やはり安全な計算に応用できることが過去に知られている一方，ESCT 展開の最小化については未踏の領域である。このような最小化アルゴリズムの開発に成功すれば，効率の良い安全な計算に応用できるため，ESCT 展開の最小化に関する問題に取り組む。また，計算したい目的とする関数のさまざまな展開を試みることにより，他のモデルにおけるプロトコルの改良も視野に入れる。

４．研究成果

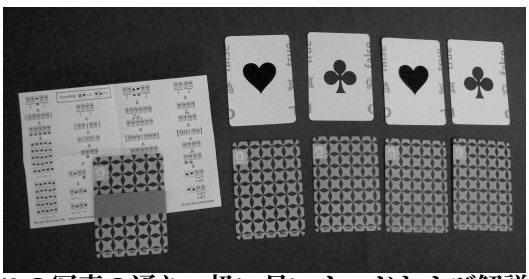
まずテンソル分解の一つ ESOP 展開の一般化である ESCT 展開に着目し，2 変数多値入力 2 値出力関数に対して，その最小化に関する問題に取り組んだ。その結果，最小 ESOP 展開と最小 ESCT 展開の関係・性質を明らかにし，最小な ESCT 展開を求める効率的なアルゴリズムを考案し，Discrete Applied Mathematics 誌にて成果を公表するこができた（５．主な発表論文等〔雑誌論文〕の②）。すなわち，任意の 2 変数多値入力 2 値出力関数に対して，その最小 ESOP/ESCT 展開の項数の差は高々1 であることを示すとともに，差が 1 であるか 0 であるかの完全な特徴付けを与え，最小展開を求めるアルゴリズムも構成的に示している。ESCT 展開を使うと ESOP 展開から高々1 つの項数を減らすことができるというこの結果は，一見，暗号プロトコルの効率化という観点からはネガティブに思われるかもしれないが，そのようなことはなく，特に項数が小さいときに効果がある。例えば，最小 ESOP 展開の項数が 3 である 5 値入力関数を考え，その最小 ESCT 展開の項数が 2 であるとき，安全な計算に必要な通信コストは，19 ビットから 13 ビットへ減らすことができ，約 32%のコストを削減できる。

また，多変数多値入力 2 値出力関数の ESOP 展開と正準テンソル分解との関連性の解析を進め，既存のテンソル分解に関する成果を ESOP 展開へ応用できることを明らかにしている。したがって，例えば，3 変数多値入力 2 値出力関数の ESOP 展開は，3 次のテンソルに対する正準分解と同じ意味を持つことになり，これまで 3 変数以上の多値 ESOP 展開に関して最小化アルゴリズムや計算困難性は知られていなかったが，テンソル分解における種々の既存の結果をそのまま適用できることになった。

次に別なモデルとして取り組んだ，カード組を用いた安全な計算に関する成果を述べる。まず安全な計算を実現するプロトコルの効率化に取り組んだ。具体的には，これまで論理積を計算する最も優れたものは 1989 年に den Boer が開発した暗号プロトコルであったが，その効率化に成功し，20 数年ぶりの改良を実現した。すなわち，非コミット型の論理積計算に必要なカード枚数を 5 枚から 4 枚に減らすことができ，2 変数の入力の表現に 4 枚のカードが必要であることから，その意味で開発したプロトコルは最適である。プロトコルの詳細は次の通りである。



この成果は，暗号理論に関する世界最高峰の国際会議のひとつである ASIACRYPT 2012 に受理され，開発したプロトコルを広く公表することができた（〔雑誌論文〕の⑥）とともに，この成果に基づく 2 件の招待講演を行った（〔学会発表〕の①および④）。また，単純な論理積だけにとどまらず，より応用範囲の広い半加算器や全加算器を実現する効率の良い暗号プロトコルを開発し，〔雑誌論文〕の⑤の通りに成果を公表した。加えて，これもまた応用範囲の広い多数決関数に注目し，暗号プロトコルへの応用に適したその関数の展開を考案し，安全な多数決計算の効率化を実現することができた。これらの成果は，〔雑誌論文〕の④および〔学会発表〕の③に対応する。さらに，計算モデルの精密化・定式化にも取り組み，その成果を International Journal of Information Security 誌に公表した（〔雑誌論文〕の③）。これらの学術的な成果発表に加えて，アウトリーチ活動の一つとして，実際にカードを試作し，本学のオープンキャンパスや高校での出前授業を通じて，広く一般の方々に開発したプロトコルを試してもらっている。



この写真の通り，扱い易いカードおよび解説書を作成し，安全な計算とは何か，暗号とは何かについて，できるだけ分かり易く一般の方々に伝えており，多くの方々からのご意

見・コメントをもとに，物理的な材質などの意味でカード組そのものの改良や，新しいプロトコルの考案，あるいはその応用を検討する一助としている。実際，プロトコルを実行することを通して，物理的なカードの形状に起因する情報漏えいや，プレーヤーの攻撃を検討する必要性を認識し，それらを解決する手法を見付けることができ，その成果は〔雑誌論文〕の①および〔学会発表〕の②に対応している。

加えて，多人数での安全な計算におけるセキュアなチャネルを確保するために，鍵共有グラフにおける鍵選択に関する研究（〔学会発表〕の⑤）や鍵共有グラフを用いた秘密伝送に関する研究（〔雑誌論文〕の⑦）を行った。

以上が本研究で得られた成果である。研究代表者はこれらの成果を踏まえ，2014 年度より，科学研究費基盤研究(C)「カードベース暗号の発展」（2014～2016 年度）にて，当該分野のさらなる発展を目指している。

５．主な発表論文等
（研究代表者，研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 7 件）

① Takaaki Mizuki and Hiroki Shizuya, Practical Card-based Cryptography, Fun with Algorithms 2014, Lecture Notes in Computer Science, Springer-Verlag, 査読有, vol.8496, 2014, pp.318-329, 掲載決定.

② Takaaki Mizuki, Daizo Mikami, and Hideaki Sone, Minimizing ESCT Forms for Two-Variable Multiple-Valued Input Binary Output Functions, Discrete Applied Mathematics, 査読有, vol.169, 2014, pp.186-194.
DOI: 10.1016/j.dam.2013.12.023

③Takaaki Mizuki and Hiroki Shizuya, A Formalization of Card-Based Cryptographic Protocols via Abstract Machine, International Journal of Information Security, 査読有, vol. 13, 2014, pp. 15-23.
DOI: 10.1007/s10207-013-0219-4

④ Takuya Nishida, Takaaki Mizuki, and Hideaki Sone, Securely Computing the Three-Input Majority Function with Eight Cards, Theory and Practice of Natural Computing 2013, Lecture Notes in Computer Science, Springer-Verlag, 査読有, vol. 8273, 2013, pp. 193-204.
DOI: 10.1007/978-3-642-45008-2_16

⑤Takaaki Mizuki, Isaac Kobina Asiedu, and Hideaki Sone, Voting with a Logarithmic Number of Cards, Unconventional Computation and Natural Computation 2013, Lecture Notes in Computer Science, Springer-Verlag, 査読有, vol. 7956, 2013, pp. 162-173.
DOI: 10.1007/978-3-642-39074-6_16

⑥Takaaki Mizuki, Michihito Kumamoto, and Hideaki Sone, The Five-Card Trick Can Be Done with Four Cards, Advances in Cryptology -- ASIACRYPT 2012, Lecture Notes in Computer Science, Springer-Verlag, 査読有, vol. 7658, 2012, pp. 598-606.
DOI: 10.1007/978-3-642-34961-4_36

⑦ Yoshihiro Indo, Takaaki Mizuki, and Takao Nishizeki, Absolutely Secure Message Transmission Using a Key Sharing Graph, Discrete Mathematics, Algorithms and Applications, 査読有, vol.4, 2012, 1250053 (15 pages).
DOI: 10.1142/S179383091250053X

〔学会発表〕（計 5 件）

①水木敬明，［招待講演］カード組を用いた秘匿計算プロトコルについて，第 7 回公開鍵暗号の安全な構成とその応用ワークショップ，2014 年 3 月 20 日，産業技術総合研究所臨海副都心センター別館.

②水木敬明，静谷啓樹，カードベース暗号プロトコルに対する攻撃に関する考察，電子情報通信学会情報セキュリティ研究会，2013 年 11 月 28 日，東北大学.

③西田拓也，林優一，水木敬明，曽根秀昭，カードを用いた安全な三入力多数決の計算について，コンピュータセキュリティシンポジウム 2013，2013 年 10 月 22 日，かがわ国際会議場・サンポートホール高松.

④水木敬明，［招待講演］The Five-Card Trick Can Be Done with Four Cards（ASIACRYPT 2012 より），電子情報通信学会情報セキュリティ研究会，2013 年 5 月 23 日，機械振興会館.

⑤松田重裕，林優一，水木敬明，曽根秀昭，部分的漏えい鍵共有グラフにおける鍵選択に関する一考察，2012 年電子情報通信学会総合大会，2012 年 3 月 20 日，岡山大学.

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