様式 C-19

科学研究費補助金研究成果報告書

平成 22 年　5 月 17 日現在

研究種目：若手研究（B）
研究期間：2007～2009
課題番号：19700002
研究課題名（和文）　回路設計理論の安全な計算への実用的応用

研究課題名（英文）　Application of Logic Circuit Design to Secure Computation

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

研究成果の概要（和文）：安全な計算とは，各プレーヤーが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は秘密にしたままで，ある目的とする関数を計算し，その出力結果だけを知ることである。一方，与えられた関数に対して，論理積項を排他的論理和で結んで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，そのような展開の最小化アルゴリズムを与え，安全な計算を効率化したことである。

研究成果の概要（英文）：Secure computation allows players to learn the output of a desired function without revealing their inputs when each player has a private input. On the other hand, it has been known that exclusive-or sum-of-products forms of a given function can be utilized for secure computation. One of the main results was to give an algorithm for minimizing such forms and enhance the performance of secure computation.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	800,000	0	800,000
2008 年度	800,000	240,000	1,040,000
2009 年度	900,000	270,000	1,170,000
年度			
年度			
総　計	2,500,000	510,000	3,010,000

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，暗号・認証等，ネットワーク

１．研究開始当初の背景

1982 年の Yao による有名な「金持ち財産比べ」プロトコル［Y82］に始まり，今日に至るまで，安全な計算（Secure Multiparty Computations）に関して，多数の研究者により数百という論文が世に出ており，現在も数多くの研究者による活発な研究が続いている。「金持ち財産比べ」とは，花子さんと太郎君の二人がいるとき，お互い自分の財産の額は秘密にしたままで，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ような暗号プロトコルを設計する問題である。この問題を一般化したものが本研究もターゲットにしている「安全な計算」である。すなわち，n 人のプレーヤーがいて，各プレーヤー P_i は自分だけに秘密な入力 x_i 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 $f(x_1, x_2, \cdots, x_n)$ を計算し，その出力結果だけを全員のプレーヤーで知ることができるようなプロトコルを設計する問題である。

本研究課題は，この「安全な計算」に関する問題に焦点を絞り，回路設計理論における優れた既知の結果・手法を適用することにより，効率的な暗号プロトコルを開発することを目標としていた。すなわち，本研究は，研究課題名が示す通り，回路設計理論の安全な計算への実用的応用を目指すものである。

本研究課題の開始よりも以前に，研究代表者は，本研究課題を思い立ったベースとなる研究成果を既に得ていた。すなわち，研究代表者は，論理積（AND）項を排他的論理和（EXOR）で結んで表現される ESOP (Exclusive-or Sum-of-Products) 展開が論理設計理論の分野において古くから盛んに研究されていることに着目し，ある特別なモデルにおける安全な計算に対して，それらの既存研究を応用することが可能な暗号プロトコルを開発し，ESOP 展開に関する既知のヒューリスティックなアルゴリズムや手法を応用することにより，効率的に安全な計算を実現できる可能性を指摘していた。この成果は，研究代表者らにより，2006 年 5 月に公表されている[M06]。本研究課題は，ファーストステップとも言うべきこの既存の研究成果を更に発展させることを目指して提案したものであり，幸いにして科学研究費・若手研究 (B) に採択された。

以下では，研究開始当初の背景として，もう少し過去の既存研究について述べる。本節の冒頭で述べた通り，安全な計算に関する既存の研究は，多数存在する。その理由の一つは，扱うモデルの多様性にある。一例を挙げると，通信モデルとしてどのような通信路を仮定するか，プレーヤーは正直であるか否か，不正を行うプレーヤーは何人でどのように選ばれるのか，それらのプレーヤーの能力をどのように仮定するか，などである。これら多くの条件・仮定の組み合わせの数だけ，研究ストリームがあると言ってもよいほどである。その中で，計算量理論の意味での回路の複雑さとの関連性に着目している研究として，例えば Feige ら[F94]は，ある通信モデルにおいて，NL というクラスに属する関数は多項式の通信量で安全に計算できることを示した（その後，より広いクラスについても同様のことが証明されている）。

[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.

[F94] U. Feige, J. Kilian, and M. Naor, A minimal model for secure computation, Annual ACM symposium on Theory of computing (STOC 1994), pp.554-563, 1994.

２．研究の目的

各プレーヤー P_i が秘密の入力 x_i を持っているとき，ある関数 $f(x_1, x_2, \cdots, x_n)$ を安全に計算したいとする。ある関数 $f(x_1, x_2, \cdots, x_n)$ とそれを表す論理回路との間には密接な関係があるため，安全な計算に関する問題においても，これまで多くの研究者により，プロトコルの効率性や安全性と，回路における種々の性質との関連性が明らかにされている。それらの研究のほとんどは，計算量理論的な意味での“回路の複雑さ”との関係に着目しており，そこで得られている数々のプロトコルは，どちらかと言うと，理論的な興味によるものが多いと言えるかもしれない。

一方，本研究課題では，計算量理論的な意味での“回路”に関する性質ではなく，「回路設計理論」が言うところの“回路”に関する既知の成果に注目する。回路設計理論（あるいはスイッチング回路理論）の歴史は古く，スイッチ，リレー，真空管，ダイオード，トランジスタ，パラメトロン，PLA (Programmable Logic Array)，FPGA (Field Programmable Gate Array) などといった論理素子の登場の歴史とともに発展が続いている。この回路設計理論の分野では，素子数削減のための論理回路の簡単化アルゴリズムや，実装や設定変更が容易な論理回路設計法が，極めて多くの研究者により数多く提案されており，これらの成果は実用的に世の中で広く用いられている。本研究課題では，このような回路設計理論における優れたアルゴリズムや回路設計法を利用し，安全な計算への応用を行う。同時に，得られた知見を活かして他の暗号プロトコルの設計・安全性証明に役立てるとともに，安全な計算という問題が内包する本質的な難しさについても探る。

３．研究の方法

本研究の計画・方法を一言で表すと，回路設計理論における手法を，安全な計算を実現する暗号プロトコルの効率化に応用することである。具体的には次の通りである。

n 人のプレーヤーがそれぞれ秘密の入力を持っているとき，ある関数 $f(x_1, x_2, \cdots, x_n)$ を安全に計算したいとしよう。このとき，関数 $f(x_1, x_2, \cdots, x_n)$ を何らかの論理回路で表現

し，その回路にしたがって何らかのプロトコルで計算を行うという手法を取ることは，汎用的で適切な方法であることは直感的にも明らかである。そこで問題は，

・どのような回路に表現すれば，安全な計算のプロトコルに応用できるか？

・表現する回路をどのようにして短くできるか（簡単化できるか）？

という二つに集約できる。

後者については，より短い（簡単な）論理回路で関数 $f(x_1, x_2, \cdots, x_n)$ を表現すればするほど，プロトコルの計算時間や通信量が小さくなるということは直感的にも理解できる。回路設計理論における論理関数の表現法には，有名なところでは，論理積（AND）項を論理和（OR）で結んだ SOP（Sum-of-Products）展開や，論理積項を排他的論理和（EXOR）で結んだ ESOP（Exclusive-or Sum-of-Products）展開などがあり，簡単化のための優れたアルゴリズムが数多く知られている。

前者については，前々節において既に記述しているように，研究代表者は，本研究課題の開始より以前に，ESOP 展開を応用した暗号プロトコルの開発に成功していた[M06]。その暗号プロトコルについて，もう少し詳しくその仕様・性能を述べる。Alice，Bob および Carol の 3 人がいるとしよう。Alice は秘密の入力 a を持ち，Bob は秘密の入力 b を持っているとき，ある関数 f の出力結果 f(a,b) だけを Carol に知らせたい，そのようなモデルにおける安全な計算の問題を考える（このようなモデルにおける問題は Feige ら[F94]によって提起された）。研究代表者は，関数 f(a,b)の ESOP 展開における積項数に比例した性能をもつ，安全な計算を実現する暗号プロトコルを開発した。すなわち，関数 f(a,b)の ESOP 展開の積項数を t で表すと，Alice と Bob が 3t ビットの乱数を共有しているとき，Alice から Carol へ 2t ビット，Bob から Carol へ t+1 ビットの通信を行うことで，目的とする安全な計算が実現できることを示した。

以上を要するに，ESOP 展開の積項数 t を小さくすることができれば，開発済の暗号プロトコルは自動的に効率化されることになる。したがって，回路設計理論の優れた手法を見極めつつ，ESOP 展開の最小化アルゴリズムを開発していく。なお，当該問題に対応する ESOP 展開は，より具体的には，多値 2 入力論理関数に対応するものとなり，残念ながら長い回路設計理論における歴史の中で，このようなクラスの論理関数に対する ESOP 展開の効率の良い最小化アルゴリズムを求めた研究者はいない。よって，研究代表者自身の手によって，既存の手法を見極めつつ，多値 2 入力関数に対する ESOP 展開最小化アルゴリズムを独創的に開発する必要がある。

また，得られた排他的論理和にかかわる知見を活かして他の暗号プロトコルの安全性の厳密な証明に役立てるとともに，論理積や排他的論理和といった基本演算について，安全な計算という問題が持つ本質的な難しさについて，簡易なモデルの下でその可能性や限界について解析を進めていく。

４．研究成果

前節で述べたように，本研究で主に取り上げている安全な計算のモデルとしては，3 人のプレーヤーがいて，そのうちの 2 人が秘密の入力を持っており，残りの 1 人にだけある目的とする関数の出力結果を安全に計算させるというものである。また，この問題に対して，ESOP 展開の積項数が性能を決定するような暗号プロトコルが知られており，具体的には，多値 2 入力論理関数の ESOP 展開を最小化することが重要であることは既に述べた通りである。そのため，まず，そのような論理関数と ESOP 展開にかかわる性質を研究した。その結果，ブール行列の階段化を実行することと，ESOP 表現を簡単化することとの関連性を見出すことに成功した。具体的には次に示す通りである。

ESOP 展開の簡単化に対する既知のアルゴリズムで最も有名なものは，EXMIN2 [T93]である。EXMIN2 における変形ルールの 1 つを多値 2 入力論理関数に適用することを考えるとき，多値 2 入力論理関数の 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発見した。すなわち，任意の ESOP 展開をあるブール行列に一対一に対応させることができ，ESOP 展開における変形ルールの適用を，ブール行列における基本変形に対応させることができる。したがって，ブール行列の上で基本変形を考えるだけで，ESOP 展開の変形を完全にシミュレートすることが可能となった。このことは，ブール行列を階段化することが，直ちに ESOP 展開を最初化することに対応することを意味する。

行列の階段化については，ガウスの消去法など，既知の有名なアルゴリズムを適用するだけでその高速化が実現できるため，本成果により，ESOP 表現の最小化を実現する効率の良いアルゴリズムがただちに得られる。

以上により，ESOP 展開の最小化を実現する多項式時間アルゴリズムを開発することに成功し，先に述べているように，暗号プロトコルの効率性は，ESOP 展開の積項数に依存するので，この開発した ESOP 表現の最小化アルゴリズムにより，効率的な安全計算プロトコルがただちに得られる。これらの成果を国際会議で公表し，その論文を Journal of Multiple-Valued Logic and Soft Computing

誌に掲載することができた。

また，回路設計理論の基本的な演算である排他的論理和の別な応用として，他人数のプレーヤー間での安全な情報共有プロトコルが存在するが，既存のプロトコルでは，そのラウンド数が与えられた鍵共有状態の形状に依存していた。具体的には，その形状をグラフの木とみなしたとき，その木の高さに比例したラウンド数が必要であった。研究代表者は，この問題の改良に取り組み，１ラウンドで安全な情報共有が終了するような，非インタラクティブなプロトコルの開発に対して，その安全性の証明を行った。したがって，この開発したプロトコルは，どんな形状の鍵共有状態に対しても 1 ラウンドで終了する。この成果については，論文誌 Information Processing Letters に掲載された。

さらに，回路設計理論の基本演算とも言うべき論理和や排他的論理和に対して，基礎的通信モデルにおいて，安全な計算という問題が持つ本質的な難しさや実現可能性を解析した。具体的には，その通信モデルの下で，論理和や排他的論理和に対する安全な計算のために必要なコストについて，過去の既存研究と比較して，そのコストの削減に成功している。特に，排他的論理和の方に関しては，そのモデルの下で最適なコストとなっている。これらの成果を国際会議において公表した。

最後に今後の展望について言及する。本研究課題は，ESOP 展開が安全な計算に応用できること[M06]に基づきスタートし，成果を得たものであるが，最近，国外の研究グループが，研究代表者の暗号プロトコル[M06]を引用しつつ，ESCT (Exclusive-or Sum of Complex Terms)と呼ばれる展開も安全な計算に応用できることを発見している。その preliminary な内容は文献[S08]で公表されている。文献[S08]は，文献[M06]のプロトコルの ESOP 展開を ESCT 展開に置き換えたものであり，プロトコルの性能評価等については今後の研究の進展が期待されるところであるが，ESCT 展開は ESOP 展開よりもより広いクラスであり，今後ますます回路設計理論が安全な計算へ応用されていく可能性が高まり，両分野の知見を融合して，さらなる効率的なプロトコルの開発が期待される。もちろん，研究代表者自身も，本研究課題で得られた成果をますます発展させていく所存である。

[T93] T. Sasao, EXMIN2: a simplification algorithm for exclusive-or sum-of-products expressions for multiple-valued-input two-valued-output functions, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol.12, pp.621-632, 1993.

[S08] M. Sampson, D. Voudouris, and G. Papakonstantinou, Secure computations in minimal model using simple ESCT decomposition, 16th International Conference on Software, Telecommunications and Computer Networks, pp.380-383, 2008.

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 4 件）

①Takaaki Mizuki, Hitoshi Tsubata, and Takao Nishizeki, Minimizing AND-EXOR Expressions for Two-Variable Multiple-Valued Input Binary Output Functions, Journal of Multiple-Valued Logic and Soft Computing, 査読有, vol.16, 2010, pp.197-208.

②Takaaki Mizuki, Takuya Sato, and Hideaki Sone, A One-Round Secure Message Broadcasting Protocol through a Key Sharing Tree, Information Processing Letters, 査読有, vol.109, 2009, pp.842-845.

③ Takaaki Mizuki and Hideaki Sone, Six-Card Secure AND and Four-Card Secure XOR, Frontiers in Algorithmics (FAW 2009), Lecture Notes in Computer Science, Springer-Verlag, 査読有, vol.5598, 2009, pp.358-369.

④Takaaki Mizuki, Hitoshi Tsubata, and Takao Nishizeki, Minimizing AND-EXOR Expressions for Multiple-Valued Two-Input Logic Functions (Extended Abstract), Theory and Applications of Models of Computation (TAMC 2009), Lecture Notes in Computer Science, Springer-Verlag, 査読有, vol.5532, 2009, pp.301-310.

〔学会発表〕（計 2 件）

①津幡斉，水木敬明，西関隆夫，多値 2 入力論理関数のAND-EXOR論理式の最小化，電子情報通信学会回路とシステム研究会，2008 年 3 月 7 日，山口大学常盤キャンパス.

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