マルチパーティ計算の情報理論的解析

研究代表者	岩　本　　貢	電気通信大学 大学院情報理工学研究科・准教授
共同研究者	太　田　和　夫	電気通信大学 大学院情報理工学研究科・教授
競合研究者	西　出　隆　志	筑波大学 大学院システム情報系（情報工学域)・准教授

1 はじめに

マルチパーティ計算(Multi Party Computation, MPC)とは，多人数の参加者で行う秘匿計算プロトコルの総称である．すなわち，n人の参加者がそれぞれ自身の入力値$x_i, i = 1,2,\dots,n$を秘匿したままで，多入力関数$f(x_1, x_2, \dots, x_n)$の値のみを計算することが可能となる暗号学的な手法である．

例えば，関数$f(x_1, x_2, \dots, x_n) \coloneqq \sum_{1\le i\le n} x_i, x_i \in \{0,1\}$とすれば，$x_i = 1$の時を賛成，$x_i = 0$の時を反対と定義することで，関数$f(x_1, x_2, \dots, x_n)$は（簡易な）電子投票方式となり，投票者の賛成・反対を明らかにすることなく，何人が賛成したかを計算することが出来る．また，関数$g(x_1, x_2, \dots, x_n) \coloneqq \arg\max\{x_i\}_{1\le i\le n}$と定義すれば関数$g(x_1, x_2, \dots, x_n)$はどの参加者が最大値を与えるかを示す関数になる．この関数は，マルチパーティ計算の初期の研究にみられ[6]，特に$n = 2$のときを「金持ち比べプロトコル」と呼ぶ．これは，$n = 2$のときのこの計算を，２人の金持ちがお互いの所持金を明かさずにどちらかが金持ちかを明らかにする，という論文[6]の問題設定から名付けられたものである．一般のnに対して，$g(x_1, x_2, \dots, x_n)$ は電子オークションの基本的なモデルと見ることも出来る．すなわち，封印入札を行い，第一価格を入札した入札者のみが公にされる状況である．

このようにMPCは暗号理論の基礎的部品（プリミティブ）として，また，それ自体が極めて興味深い研究対象であり，長年研究されてきた．マルチパーティ計算の実現手法には様々な方法が存在するが，その安全性は大まかに計算量的安全性と情報理論的安全性に大別される．計算量的安全性とは，攻撃者が暗号を解読するのに非常に長い時間がかかることを安全性の根拠とする安全性概念であり，情報理論的安全性とは，攻撃者が暗号を解読するのに本質的に全数探索以外の方法がないことを保証する安全性概念である．

本研究では特に，情報理論的安全性をもつ最大値関数（上記の$g(x_1, x_2, \dots, x_n)$）に注目し，その実現手法と，安全性解析を行った．その結果，国際会議発表１件，国際会議ポスター発表１件，国内発表３件の成果を得た．成果は大きく２つに大別され，

- タイブレークを考慮した$M + 1$価格封印入札方式
- カードを用いた効率的金持ち比べプロトコル

がある．以下では，これらの成果について概要を説明する．

2 研究成果

2-1 概要

（１）タイブレークを考慮した封印入札方式

本研究では，n人の参加者が電子オークションに参加する状況を考える．通常のオークションでは，それぞれの入札者が自分の入札を隠したままで，最高金額を入札した人を明らかにすることを考える．しかし，ゲーム理論的な考察によると，落札者が１名であるとき，最も高い価格を入札した人を落札者とするが，落札者が第２位の価格を入札する設定が効用関数を最大化するという意味で最適な設定であることが知られている[24]．これを拡張し，商品がM個あり，M人の落札者が第$M + 1$番目の価格を支払う「第$M + 1$価格入札方式」を本研究では取り扱う．

入札額を秘匿する必要がない，公開型のオークションにおいては，入札・開札を行うことは容易である．しかし，入札額を秘匿する場合には，通常の公開型のオークションでは特に考察する必要がなくても，電子オークションでは考察する必要が生じる場合が存在する．その一つが本研究で取り扱う，タイブレークの問題である．第$M + 1$価格入札方式においては，上位M人を決定する場合に，タイブレークが生じる可能性が十分考えられる．例えば，電子オークションにおいて上位M人を決めようとしたときにタイブレークが起こり，$M + a$人が落札価格以上の価格を入札したとしよう($a \ge 1$)．この場合，通常の公開型の電子オークションでは，これらの$M + a$人の落札者が明らかになってしまう．その中にタイになった（落札者の中で最も入札額

の少ない）入札者が存在した場合，改めて何らかの選択プロトコルを行い，落札者が全部でM人になるようにする．しかし，この方式では落札者できなかったにもかかわらず，最初のステップで落札者（の候補）として選ばれたa人の入札者の入札額（＝落札者の最低価格）が明らかになってしまう．電子オークションでは，落札者の入札額は明らかにしたくないので，この様な方式は明らかに問題である．

そこで本研究では，このようなタイブレークが発生しても，自動的に落札者がM人になるようなプロトコルを提案した．本プロトコルでは，上記のa人のような，タイブレークで敗れた入札者の情報は一切漏洩しない．技術詳細で述べるように，提案方式は従来手法の組み合わせに比べて効率的な方式になっている．また，提案手法は情報理論的に安全な方法で実装できる．

提案手法は国内会議[5]および国際会議[1]にて発表済みである．

（２）カードを用いた金持ち比べプロトコル

マルチパーティ計算は通常，代数的な操作と参加者間の秘密通信で行われる．しかし，それ以外の実現手法があることも知られている．代表的な例として，物理的なカードを用いて，暗号プロトコルが構成できる．本研究では，カードを用いたマルチパーティ計算として特に，金持ちプロトコルを取り上げる．カードを用いた暗号プロトコル は，一般的な計算機で実装できるプロトコルと異なり，プレイヤーの手操作で実現される．当然，手操作で 行われるプロトコルは，計算機よりも遥かに多くの実行時間を要する．そのため，カードを用いた暗号プロトコルにおいて，手順数（計算量）をどこまで小さくできるかということは重要な問題となる．

カードを用いるプロトコルだけでなく，通常のマルチパーティ計算において， NOT，AND，XOR などの基本的な論理演算プロトコルが提案されている．これによって，論理演算で構成できる（従って，離散的な任意の関数）に対してカードを用いたマルチパーティプロトコルが構成できる [28]．したがって，本研究で提案する金持ち比べプロトコル [6] もカードで実現できる．しかし，論理演算を用いての構成法は，汎用的である一方で，計算量が増えてしまうといった問題も存在する．そこで本研究では，これらの論理素子に対するプロトコルの組合せによらない，手操作数の少ないカードベースの MPC プロトコルの提案を目指した．

本研究での手操作の数は通常の MPC における計算量に相当するが，そのなかでも我々は特にシャッフル操作に着目する．既存方式のカードベース論理演算プロトコルでは，安全な秘密計算を実現するためにプレイヤー全員が納得できるまでシャッフルを行い，十分にカードが攪拌されたことを要求している．シャッフル操作は安全性を保証するための必須の手操作であるが，非常に手間がかかる．論理演算で構成されたプロトコルは，シャッフル操作を多く用いるため，効率性の面で問題がある．そこで，我々はシャッフル操作を用いることなくカードを用い金持ち比べを行う方法を考える．

カードを用いた MPC のように，計算機を用いずに実現できる暗号方式として，視覚復号型秘密分散法が知られている．視覚復号型秘密分散法は計算機を用いずに復号できるという意味で，暗号方式として非常に興味深い方式である．本研究で議論するカードベースの MPC でもカードに特有な操作を用いて金持ち比べプロトコルを実現することで，単純に基本演算の組合せで実現できるプロトコルより効率よく金持ち比べが出来ることが期待できる．

これらの方針のもと，我々は「セキュアな領域」を用いたカードベース MPC を提案した．セキュアな領域とは，例えば，裏返して受け取ったカードを自分だけが見る，といった，プレイヤー本人にのみ開示できる物理的なカード操作を指す．本研究の重要な成果として，このセキュアな領域の存在を認めると，シャッフル操作を用いずに金持ち比べプロトコルが実現できることを示したことが上げられる．その結果，プロトコルの効率が非常に良くなることを示す．提案手法は，情報理論的に安全な方式となっており，最終的に明らかになる「どちらが金持ちか」という以上の情報は一切漏洩しない．

提案手法は国内会議[3],[4]にて発表し，国際会議 IWSEC2015 にてポスター発表を行った[2]．

2-2 成果の詳細

（１）タイブレークを考慮した封印入札方式

本研究では，第$M+1$価格オークションにおいてタイが起きたときに，タイの入札者から落札者と敗者を自動的に決定する方法を提案した． タイになった入札者のうち，落札者と敗者を決定するためには次のような方式が考えられる．

- Public random priority order: 参加者に事前に順番がつけられており，タイが生じた場合はその順番

で落札できるか否かが決まる

- Random priority order: タイが生じた際にランダムに順位付けが行われ，ランダムに落札者が決定する

先行研究との比較は表１にあるとおりである．表 1 から分かるとおり，random priority order による方式は先行研究には存在しない．提案手法は public priority order，random priority order のいずれも実現でき，タイブレークが生じてもM人丁度を落札者として決定できる唯一の方式である．

次に，計算量に関する比較を表 2 に示す．ここでk: 入札者数，p: MPC を実行するときの法，ℓ: 入札金額のビット長，n: MPC を実行する人数，M: オークションにかけられる品物の数，COM: 1 回の比較演算に要する通信回数，である．ラウンド数・通信回数共に提案手法の効率が良いことが分かる．

表 1　先行研究との設定の比較［1］

プロトコル	形式	タイブレーク	備考
[20] [13]	任意	可能	Yao の Garbled circuit が必要．2-party プロトコル（金持ち比べプロトコル）に限る
[16]	1st	不可能	タイの場合，２人以上の勝者が明らかになる
[18]	2nd	不可能	
[17]	$(M+1)$	不可能	タイの場合，２人以上の勝者が明らかになる
[14] [7] [19]	$(M+1)$	不可能	タイが存在する場合，M 人未満の勝者が明らかになる．M 人全員が同じ入札額の場合，勝者が特定できない．
[23]	GVA	不可能	タイの場合，全員がタイであることは分かる．
[8]	1st	部分的に可能	敗者には勝者も落札者も分からない方式．Public priority order のみ可能．
	2nd		
	$(M+1)$	不可能	タイの場合，２人以上の勝者が明らかになる
[10]	1st	不可能	2-party プロトコル（金持ち比べプロトコル）に限るオンラインプロトコル
[15]	1st	部分的に可能	改良された Yao の garbled circuits を用いて最小値とその入札者のみが分かる方式．Public priority order による
[21]	1st	不可能	タイの場合，２人以上の勝者が明らかになる
本研究	$(M+1)$	可能	厳密にM人の落札者を決定できる Public/random priority order が可能

表 2 先行研究との計算量・通信量の比較［1］

プロトコル	ラウンド数	通信回数（乗算回数）	備考
Selection network [25]	$O(\log_2 k)$	$O(COM\, k \log_2(M+1))$	Based on garbled circuit Limited to 2-party case
Oblivious keyword sort	$O(1)$	$O(COM\ k\text{^}2)$	honest & dishonest majority
Modified quicksort &shuffle [11]	$O\left(\frac{2^n}{\sqrt{n}}+\log_2\frac{k}{M}\right)$	$O\left(k\frac{2^n}{\sqrt{n}}+COM\, k\right)$	w/ honest majority
	$O\left(n+\log_2\frac{k}{M}\right)$	$O\left(nk^2+COM\, k\right)$	w/ dishonest majority
Radix sort & shuffle [12]	$O\left(\frac{2^n}{\sqrt{n}}\left(\ell+\log_2\frac{k}{M}\right)\right)$	$O\left(\frac{2^n}{\sqrt{n}}\left(\ell+\log_2\frac{k}{M}\right)^2\right)$	w/ honest majority
	$O(n(\ell+\log_2 k))$	$O\left(nk^2(\log_2 k)^2\right)$	w/ dishonest majority
本研究	$O(\ell+\log_2 k)$	$O(k(\ell+\log_2 k))$	honest & dishonest majority

（２）カードを用いた金持ち比べプロトコル

カードベース暗号プロトコルの計算量を評価する（提案手法は論文[2]-[4]を参照されたい）．既存方式は，安全に演算結果を出力するためにランダム二等分割カット[28]などのシャッフルを用いている．安全にシャッフルを適用するための方法は幾つかある．例えば，セキュアな領域を仮定するのであれば，プレイヤーがそれぞれセキュアな領域内で他プレイヤーに見られないように，ランダムな回数シャッフルを適用する．常にpublicな領域であることを仮定するのであれば，回数が分からなくなるまで，シャッフルを適用する．シャッフルは，プレイヤー同士が協力して行う確率的なカードの並び替え操作であり，プレイヤー全員が納得できるまでシャッフルを行うことが求められる．一方で，シャッフル以外の操作は，決められた手順通りのカード操作を行うだけなので，シャッフルと比較して短い時間で行うことが可能である．したがって，プロトコルの計算コストの多くは，このシャッフル操作が占めている．そのため，カードベース暗号プロトコルにおいて，計算量はシャッフル適用回数で評価する．

AliceとBobが金持ち比べプロトコルを論理演算に基づいて行う場合，図のアルゴリズムで実現できることが知られている．以降，図のように出力を$a \geq b$，$a < b$ の2通りとした金持ち比べプロトコルで比較を行う．ここでa_iはAlice，b_iはBobが扱うビット列であるとする

1ビット目の計算は1回の AND 演算で終わる．2ビット 目以降は1ビット 毎に2回の AND 演算と2回のOR 演算を要する．また ，a_i, b_iがそれぞれ 2 箇所の演算に用いられているため,コピー演算を 2回要する．表 1 のシャッフル回数より ，各 ビット 毎に 6 回のシャッフル操作が発生するため、図のアルゴリズムをカードで実現した場合のシャッフル回数は $6n-5$ である．一方で ，提案方式において，シャッフル操作は用いられていない．提案方式のシャッフル回数は0である．プロトコル中，Aliceの確率的な選択操作があるが，これはAliceのみが納得すればよい操作であり,決められた手順操作とほぼ同様の計算時間で行うことが可能である．また， Bobには確率的な操作が一切無く，全て決められた手順操作である ．

カードベースの AND 演算プロトコルとコピープロトコルを組み合わせることで ,AND 演算とコピー演算を同時に実現するプロトコルが知られている[29]. このプロトコルを利用することで ，図のプロトコルは $4n+2$ 枚のカードで実現可能である.提案方式において，用いるカードの枚数は $4n+2$ 枚である．入力値に関するカードと記録 card 組以外に ，プロトコル中で追加されるカードは存在しない．しかし，プロトコル手順を見て分かる通り，Bob は常に各ビットの値を表現する 2 枚のカード組のうち，左のカードしか用いていない．そのため，Aliceの入力値の定義をとし ,Bob の入力値の定義をとしても，プロトコルは実現できる．したがって ，提案方式を実現するために実質必要なカード枚数は $3n+2$ 枚である．また ，提案方式ではセキュアな領域をうまく用いることで ，出力を 3通りとした場合でも ，計算量や利用カード枚数を増やすことなく ，金持ち比べプロトコルが実現できる．

また，提案手法[2],[3]は非コミット型のプロトコルであるが，これをコミット型プロトコルに変更する方法も文献[3],[4]で提案している．ただし，こちらのほうが効率は悪くなる．

図 論理演算に基づく，大小比較プロトコル

---

input: $a = (a_n, ..., a_2, a_1)_2$, $b = (b_n, ..., b_2, b_1)_2$;
$f_1 = \bar{a}_1 \wedge b_1$;
for(i : 2 to n) {
　$f_i = \bar{a}_i \wedge b_i \vee (\bar{a}_i \vee b_i) \wedge f_{i-1}$;
}
output: f_n ;
　if $f_n = 0$ then $a \geq b$
　if $f_n = 1$ then $a < b$

【参考文献】

[1] T. Nishide, M. Iwamoto, A. Iwasaki, and K. Ohta, “Secure $(M+1)$st-Price Auction with Automatic Tie-Break,” 6th International Conference on Trustworthy Systems (InTrust2014), pp.422-436, LNCS9473, 2015.

[2] T.Nakai, Y.Tokushige, M.Iwamoto, and K.Ohta, “Toward Reducing Shuffling in Card-based Cryptographic Protocol for Millionaire Problem, ” International Workshop on Information Security (IWSEC2015), (poster session), August, 2015.
[3] 中井雄士,徳重佑樹,岩本貢,太田和夫, “カードを用いた効率的な金持ち比べプロトコル,” 暗号と情報セキュリティシンポジウム (SCIS2015) 予稿集, 3F4-2, 2015.
[4] 徳重佑樹, 中井雄士,岩本貢,太田和夫, “カードベース暗号プロトコルにおける安全な選択処理,” 暗号と情報セキュリティシンポジウム (SCIS2015) 予稿集, 3F4-4, 2015.
[5] 西出隆志, 岩本貢, 岩崎敦, 太田和夫, “自動タイブレークの仕組みを持つ第$M+1$価格暗号オークション方式” 暗号と情報セキュリティシンポジウム (SCIS2015) 予稿集,
[6] A.Yao, “Protocols for secure computations,” Proceedings of the 23th IEEE Symposium on FOCS 1982, pages 160–164, 1982.
[7] M. Abe and K. Suzuki, “M+1-st price auction using homomorphic encryption,” PKC, LNCS 2274, pp.115–124, Springer, 2002
[8] F. Brandt, “How to obtain full privacy in auctions,” Int. J. Inf. Sec., vol.5, no.4, pp.201–216, 2006.
[9] F. Brandt and T. Sandholm, “Efficient privacy-preserving protocols for multi- Unit auctions,” Financial Cryptography, LNCS 3570, pp.298–312, Springer, 2005.
[10] I. Damgaard, M. Geisler, and M. Krøigaard, “Homomorphic encryption and secure comparison,” International Journal of Applied Cryptography, 1(1), pp.22– 31, 2008.
[11] K. Hamada, R. Kikuchi, D. Ikarashi, K. Chida, and K. Takahashi, “Practically efficient multi-party sorting protocols from comparison sort algorithms,” ICISC’12, LNCS 7839, pp.202–216, Springer, 2013.
[12] K. Hamada, D. Ikarashi, K. Chida, and K. Takahashi, “Oblivious radix sort: an efficient sorting algorithm for practical secure multi-party computation,” Cryptology ePrint Archive 2014/121, 2014.
[13] A. Juels and M. Szydlo, “A two-server, sealed-bid auction protocol,” Financial Cryptography, LNCS 2357, pp.72–86, Springer, 2002.
[14] H. Kikuchi, “$(M+1)$st-Price Auction Protocol,” Financial Cryptography, LNCS 2339, pp.341–353, Springer, 2001.
[15] V. Kolesnikov, A-R. Sadeghi, and T. Schneider, “Improved garbled circuit building blocks and applications to auctions and computing minima,” Proc. Cryptology and Network Security (CANS), LNCS 5888, pp.1–20, 2009.
[16] K. Kurosawa and W. Ogata, Bit-slice auction circuit,” ESORICS, LNCS 2502, pp.24–38, Springer, 2002.
[17] H. Lipmaa, N. Asokan, and V. Niemi, “Secure Vickrey auctions without threshold trust,” Financial Cryptography, LNCS 2357, pp.87–101, Springer, 2002.
[18] T. Mitsunaga, Y. Manabe, and T. Okamoto, “Efficient secure auction protocols based on the Boneh-Goh-Nissim encryption,” IWSEC, LNCS 6434, pp.149– 163, Springer, 2010
[19] T. Mitsunaga, Y. Manabe, and T. Okamoto, “A secure M+1st price auction protocol based on ビット slice circuits,” IWSEC, LNCS 7038, pp.51–64, Springer, 2011.
[20] M. Naor, B. Pinkas, and R. Sumner, “Privacy preserving auctions and mechanism design,” ACM Conference on Electronic Commerce, pp.129–139, 1999.
[21] M. Nojoumian and D. R. Stinson, “Unconditionally secure first-price auction protocols using a multicomponent commitment scheme,” ICICS, LNCS 6476, pp.266–280, Springer, 2010.
[22] A. Shamir, “How to share a secret,” Communications of ACM, vol.22, no.11, pp.612–613, 1979.
[23] K. Suzuki and M. Yokoo, “Secure generalized vickrey auction using homomorphic encryption,” Financial Cryptography, LNCS 2742, pp.239–249, Springer, 2003.
[24] W. Vickrey, “Counter speculation, auctions, and competitive sealed tenders, ” The Journal of Finance, vo.16(1), pp.8–37, 1961.
[25] G. Wang, T. Luo, M. T. Goodrich, W. Du, and Z. Zhu, “Bureaucratic protocols for secure two-party sorting, selection, and permuting,” ASIACCS, pp.226– 237, ACM, 2010.
[26] B. Zhang, “Generic constant-round oblivious sorting algorithm for MPC,” ProvSec, LNCS 6980, pp.240–256, Springer, 2011.

[27] B. den Boer, More efficient match-making and satisfiability: the five card trick , EUROCRYPT 1989, LNCS, Springer-Verlag, vol.773, pages 208–217, 1990.
[28] T. Mizuki and H. Sone, “Six-card secure AND and four card secure XOR,” FAW 2009, LNCS, Springer-Verlag, vol.5598, pages 358–369, 2009.
[29] 西田拓也 , 林優一 , 水木敬明 , 曽根秀昭, “カード組を用いた任意の論理関数の安全な計算について,” CSS2014, 2014.

〈発 表 資 料〉

題　　名	掲載誌・学会名等	発表年月
Secure $(M + 1)$st-Price Auction with Automatic Tie-Break	The 6th International Conference on Trustworthy Systems (InTrust 2014)	2014.12
Toward Reducing Shuffling in Card-based Cryptographic Protocol for Millionaire Problem	International Workshop on Information Security and Cryptography (IWSEC2015), poster session	2015.08
カードベース暗号プロトコルにおける安全な選択処理	暗号と情報セキュリティシンポジウム(SCIS2015)	2015.1
自動タイブレークの仕組みを持つ第$M+1$価格暗号オークション方式	暗号と情報セキュリティシンポジウム(SCIS2014)	2014.1