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　６ 年　 ６ 月　 ７ 日現在

機関番号：１７２０１
研究種目：若手研究
研究期間：2021～2023
課題番号：２１Ｋ１７７０４

研究課題名（和文）マルチパーティ計算における大小比較アルゴリズムの効率化に関する研究

研究課題名（英文）A study on efficient comparison algorithm on multi party computation

研究代表者
岩崎　淳（Iwasaki, Atsushi）

佐賀大学・理工学部・准教授

研究者番号：７０７８９９５８

交付決定額（研究期間全体）：（直接経費）　　2,100,000円

研究成果の概要（和文）：マルチパーティ計算において二つの変数の大小を比較する大小比較アルゴリズムは，基本的なアルゴリズムであり通信コストの削減はマルチパーティ計算一般の性能向上につながる．主要な先行研究においては全体の通信コストに比較される変数のビット長をlとしたときに，通信量が$O(l)$となるアルゴリズムが提案されてきた．一方で，$O(l^2)$かかるが，現実的な通信量で実行でき，通信ラウンド数を削減したアルゴリズムも提案されている．本研究では通信量が$O(l^{3/2})$で少ないラウンド数で実行できる大小比較アルゴリズムを開発した．

研究成果の学術的意義や社会的意義
高度IT化社会において，情報を安全に処理する手法の一つにマルチパーティ計算があげられる．複数のサーバに秘匿すべき情報を分散し，分散された状態を保ったまま計算を行うことから，一部のサーバがサイバー攻撃を受けたりサーバ管理者に瑕疵があったとしても情報セキュリティを確保することができる．しかし，通常の計算に比べて計算コストは高く，特にサーバ間の通信がネックとなる．本研究成果は少ない通信コストで実行できるマルチパーティ計算における基礎的なアルゴリズムであり，マルチパーティ計算の実用化・普及に寄与する．

研究成果の概要（英文）：A comparison algorithm on multi party computation that decides which of two variables is larger is fundamental, and the communication cost affects that of the whole process. Many previous studies proposed the algorithms that requires $O(l)$ communication amount where l is the bit length of variables. On the other hand, in order to reduce the number of communication rounds, an algorithm that requires $O(l^2)$ but feasible communication amount. As our contribution, we developed a comparison algorithm requiring $O(l^{3/2})$ communication amount with less number of rounds.

研究分野：暗号　乱数

キーワード：マルチパーティ計算

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

情報化社会の進展にともない企業や行政機関が取り扱う機微な情報は増加の一途をたどり，その内容もよりセンシティブなものが増えている．一方で，内部の人間の故意・わずかな過失で機密情報が漏洩する事案は後を絶たない．従来の「情報を暗号化して保存する」という対策だけでは十分とは言えない．その解決策の一つに，秘密分散および秘密分散に基づくマルチパーティ計算があげられる．これは，複数のサーバに情報を分散して保存し，分散された状態を保ったままサーバ間で通信を行い計算・処理を行う手法である．その基礎は 1980 年代に確立していたものの，主にサーバ間の通信コストの面で実用的でなかった．近年，ハード面での進歩とマルチパーティ計算で効率的なアルゴリズムの研究が進み，徐々に社会実装されつつある．

２．研究の目的

分散された二つの値の大小を比較するマルチパーティ計算上のアルゴリズム「大小比較アルゴリズム」に着目する．大小比較は通常の（マルチパーティ計算でない）プログラムにおいて条件分岐（if 文）に相当する操作であり，より大規模で実用的な計算・処理を行う上で必須の操作である．よって，大小比較アルゴリズムの高性能化（通信量・通信ラウンド数の削減）によりマルチパーティ計算をより一層高性能化できると見込まれ，それに寄与することが本研究の目的である．

３．研究の方法

主要な先行研究においては，大小を比較される変数のビット長をlとしたときに，通信量が$O(l)$となるアルゴリズムが提案されてきた[1-4]．一方で，Morita らは通信量が$O(l^2)$かかるものの，現実的な通信量で実行でき，通信ラウンド数を削減したアルゴリズムを提案している[5]．そこで，本研究では通信量を$O(l^2)$にすることにこだわらないことで，現実的な通信量とよりいっそう少ないラウンド数で実施可能な大小比較アルゴリズムの開発を目指した．

より具体的には先行研究[3]に着目した．先行研究[3]においては大小の比較が以下の処理に帰着される：「l個の秘密分散された変数は，①すべて非零か，②一つだけ0を含む．値を復元していずれの場合となっているか確認する．」値を公開すると入力（比較される 2 つの数）の情報が漏れうる．ここでは，②の場合で，l個の変数の中における0の「位置」が問題となる．そこであらかじめl個の変数を無作為に並び替えることで問題を解決する．並び替えには自明な方法だと$O(l^2)$の通信量を要するが，Reistad-Toft においては$O(l)$で実行できる方法が提案されている．

そこで，通信量は少ないに越したことはないが$O(l^2)$を許容しつつ，よりラウンド数を抑え並べ替えについて検討した．

４．研究成果

上述の②の場合において，並べ替えの目的は0の位置を変更することにある．すなわち，並べ替え自体は無作為である必要はない．そのため，以下のような手順の並べ替えを考える：

1. 並べ替えるべき変数列を$(x_1, x_2, \ldots, x_l)$として，変数列を$\sqrt{l}$個ずつの$\sqrt{l}$ブロックに分割する．
2. 各ブロックに対して，ブロックに含まれる$\sqrt{l}$個の変数をランダムに選んだ置換により並び替える．ただし，異なるブロックで用いる置換は同一のものでよい．
3. 各ブロックを一塊として，$\sqrt{l}$個のブロックをランダムに選んだ置換により並び替える．この置換はステップ 2 の置換とは独立に選ぶ．

以上の手順により，任意の変数x_iが任意のj番目に並べ替えられる確率はiとjに依存しない．（ただし，l個の変数の置換としてはランダムにならない．）よって，並べ替えた後に秘密分散されている値を復元しその中に0が含まれていたとしても，その0が並べ替え前にどこに位置していたかの情報を完全に秘匿することができる．この手順はステップ 2 およびステップ 3 でそれぞれ$O(l^{3/2})$の通信量を要し，全体としても$O(l^{3/2})$の通信量となる．

以上の並び替えを先行研究[3]に組み込むことで，通信量が$4l^{\frac{3}{2}} + 10l + 23l^{\frac{1}{2}} + 2$で4ラウンドで実行可能な大小比較アルゴリズムを得ることができる．オンラインフェーズ（入力に依存する操作）に限ると，通信量が$l^{3/2}$，1ラウンドである．

＜引用文献＞

[1] Damgård, Ivan, et al. "Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation." Theory of Cryptography Conference. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006.

[2] Nishide, Takashi, and Kazuo Ohta. "Multiparty computation for interval, equality, and comparison without bit-decomposition protocol." Public Key Cryptography-PKC 2007: 10th International Conference on Practice and Theory in Public-Key Cryptography Beijing, China, April 16-20, 2007. Proceedings 10. Springer Berlin Heidelberg, 2007.

[3] Reistad, Tord Ingolf, and Tomas Toft. "Secret sharing comparison by transformation and rotation." International Conference on Information Theoretic Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007.

[4] Reistad, Tord Ingolf. "Multiparty comparison-an improved multiparty protocol for comparison of secret-shared values." International Conference on Security and Cryptography. Vol. 1. SCITEPRESS, 2009.

[5] Morita, Hiraku, et al. "Constant-round client-aided two-server secure comparison protocol and its applications." IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 103.1 (2020): 21-32.

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計0件

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

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0件

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