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　５ 年　 ５ 月 ２７ 日現在

機関番号：３２６２１
研究種目：基盤研究(C)（一般）
研究期間：2020～2022
課題番号：２０Ｋ１１８１９

研究課題名（和文）加算無限個のシェアを生成可能な秘密分散法の効率化と秘匿計算への応用に関する研究

研究課題名（英文）Research on efficient secret sharing method that can generate countably infinite number of shares and its application to secure Computation

研究代表者

澁谷　智治（Shibuya, Tomoharu）

上智大学・理工学部・教授

研究者番号：２０２６２２８０

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：大規模データを活用する様々なサービスが提供されているが、これらのデータにはプライバシー情報を含むものが多い．そこで、データを暗号化してデータ解析者に提供し、暗号化されたままでデータ解析を行う技術である「秘匿計算」が注目されている．
本研究では、(1)参加者数が可算無限となる場合にも指示関数の計算が行える非対話型マルチパーティ計算アルゴリズムを構築した．また、(2)ニュートン補間多項式に基づく符号化を利用することで、従来手法より高速な符号化計算を実現した．

研究成果の学術的意義や社会的意義
機械学習やAIといった近年のデータ解析技術の飛躍的向上により、大規模データに基づく様々なサービスが提供されている．これらの活用を推進するためには、データに含まれるプライバシー情報への配慮が特に注意が必要である．本研究で得られた成果は、データを暗号化してデータ解析者に提供し、暗号化されたままでデータを解析するための基礎技術＝秘匿計算をより効率的に実現するとともに、その適用範囲を拡大する基礎技術を与えるものである．

研究成果の概要（英文）：Various services that utilize large-scale data are provided, but many of these data include privacy information. Therefore, "secret computation", which is a technique of encrypting data, providing it to a data analyst, and analyzing the data while it is encrypted, has attracted attention.
In this research, (1) we constructed a non-interactive multi-party computation algorithm that can compute indicator functions even when the number of participants is countably infinite. (2) By using encoding based on Newton's interpolating polynomials, we realized faster encoding calculation than the conventional method.

研究分野：情報理論

キーワード：秘匿計算　符号化計算　秘密分散　マルチパーティ計算　非対話型マルチパーティ計算

１．研究開始当初の背景

公開鍵暗号や電子署名の安全な運用には、秘密鍵の不正使用や盗難への対策が不可欠である．秘密鍵のような機密データから“シェア”(share)と呼ばれる n 個の分散データを生成して参加者に配布し、k 個以上のシェアが集まったときだけ機密データが復元できる(k, n)-しきい値法[1]をはじめとする秘密分散法は、鍵の不正使用や盗難に対する効果的な対策を実現する（図 1）．

(k, n)-しきい値法では、機密データの分散共有に携わる参加者数 n をシェアの生成前に確定する必要がある．また、シェアのサイズは n のみに依存して O(log n)程度である．これらの事実からは、(i)実際の参加者数が既定の n を上回るとシェアの再生成・再配布が必要となる、(ii)シェアの不足に備えて n を過大に見積もるとシェアサイズが不必要に増大する、という相反する問題が生じる．

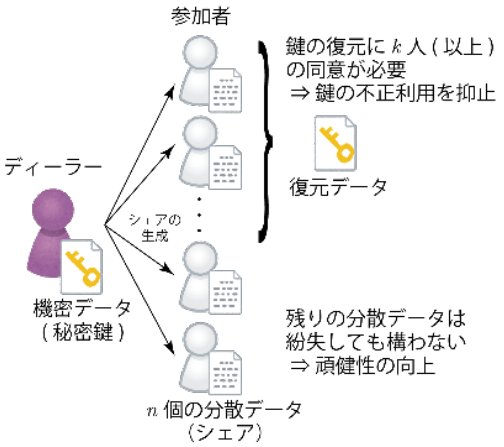

図 1 (k,n)-閾値法

これに対し Komargodski ら[2]は、参加者数が未知であっても可算無限個のシェアが生成できてシェアの不足が回避でき、さらにそれらの中の任意の k 個から機密データが復元できる秘密分散法（以後、参加者数の増加に対応可能であるという意味で発展型 k-しきい値秘密分散法とよぶ）を実現する手法を提案した．しかしながら、従来の(k, n)-しきい値法とは異なり、n 番目に生成されるシェアのサイズが、k にも依存して O(k log n)にまで増大するという深刻な問題を抱えている．

一方、機械学習や AI といった近年のデータ解析技術の飛躍的向上により、大規模データに基づく様々なサービスが提供されている．これらのデータにはプライバシー情報を含むものが多く、取扱いに注意が必要である．そこで、データを暗号化してデータ解析者に提供し、暗号化されたままでデータを解析するための基礎技術＝秘匿計算に関する研究が世界中で進められている．

従来の(k, n)-しきい値法においては、シェアに対する演算によって、機密データを明かすことなくそれに対する計算処理を実現できることが知られており、秘匿計算への応用が期待されている．これに対し、Komargodski らの手法により生成されたシェアはこのような性質を備えておらず、研究開始当初においては、発展型 k-しきい値秘密分散法を用いて秘匿計算を実現する手法は見出されていなかった．

２．研究の目的

本研究では、発展型 k-しきい値秘密分散法について、シェアサイズの k への依存性が生じる原理を明らかにし、さらに、シェアサイズの削減と秘匿計算への応用を実現するための具体的な方法を開発することを目的とした．また、この目的を達成するために以下の 4 つの研究課題を設定した．

課題 1 発展型 k-しきい値秘密分散法におけるシェアサイズと k との関係の解明

Komargodski らの手法では、増え続ける参加者に対応するために、参加者を第 1 世代、第 2 世代、･･･のように世代に分割している．さらに、オリジナルの機密データから異なる世代間に配布するシェアを生成した後、このシェアを改めて機密データとして(k, n)-しきい値法によりシェアを生成して世代内の秘密分散を実現している．このような階層的なシェア生成がシェアサイズの k への依存を生じる理由であると予想した．

そこで、参加者の世代分割の必然性について検討し、発展型 k-しきい値秘密分散法におけるシェアサイズと k との関係を解明することを目指した．

課題 2 発展型 k-しきい値秘密分散法のシェアサイズの削減

課題 1 において、発展型 k-しきい値秘密分散法のシェアサイズの k への依存が回避できることが判明すれば、そのようなシェアの具体的な生成法を与えることを目的とした．一方、k への依存が不可避であれば、従来方式よりシェアサイズの小さなシェアの生成法を与えることを目的とした．なお、シェアの生成法の開発では、次の課題 3 を念頭に入れて検討を行う予定であった．

課題 3 発展型 k-しきい値秘密分散法を用いた秘匿演算の実現

課題 2 で得られたシェアに対する演算を通じて機密データに対する秘匿計算を実現するアル

ゴリズムの開発を行うことを目的とした.

課題 4 機密情報が復元できるための条件の拡張
秘密分散法の柔軟な応用を実現するために、“可算無限個の中の任意の k 個”と比較してより一般的な条件を設定し、それに対する秘密分散法を開発することを目的とした. 例えば,「シェア集合 A に対して機密データが復元できるとき、A を含むあらゆるシェア集合に対して機密データが復元できる」というような、包含関係に基づく条件の下での秘密分散法の開発などを検討する予定であった.

３. 研究の方法
前述の 4 つの研究課題を解決するために以下の計画に沿って研究をすすめることとした.

令和 2 年度（研究の初年度）においては、「世代」の概念を用いずに発展型 k-しきい値秘密分散法を実現する手法の開発に注力することとし、以下のような研究計画を立案した.

計画 1 シェアの生成に有限体の拡大体を利用した際のセキュリティ上のリスクに関する検討
機密データを含む体とは異なる体の上でシェアを生成したとき、機密データを復元する計算を行うには、それぞれの体を定義する規約多項式もシェアと併せて共有する必要がある. この規約多項式の共有を通じてシェア以外の情報が漏洩する可能性がある. そこで、このような非明示的に漏洩しうる情報を明らかにし、それらを効果的に秘匿する手法についての予備的な検討を行うこととした.

計画 2 シェアサイズに関する限界式の定式化
発展的 k-しきい値秘密分散法におけるシェアサイズの上界・下界を定式化について検討することとした. なお、k に依存しない上界が得られ場合はシェアサイズの k への依存が回避でき、k に依存する下界が得られた場合は k への依存が不可避であることが導かれる.

計画 3 シェアサイズの削減を実現するシェアの生成法の開発
計画 1 で明らかになった拡大体の利用に伴うリスクに注意し、シェアサイズの小さな発展的 k-しきい値秘密分散法の実現法を開発することとした. なお、シェアサイズが k に依存しない手法が先に得られた場合は計画 2 における上界式が得られることになるため、計画 2・計画 3 は並行して進める予定であった.

実際には COVID-19 の感染拡大の影響を受けたため、研究の初年度は思うような成果を上げることが困難であった. 特に、前述の課題 1・2 については、設定した問題の解決には至らなかった. 一方、課題 3 についてはその解決の糸口を得ることができた.
このような状況から、令和 3 年度以降については当初の研究計画を一部変更し、以下のような研究計画の下に研究を遂行した.

計画 4 秘匿計算法の開発
課題 3 の解決の糸口となった従来の秘匿計算法を拡張することより、発展的 k-しきい値秘密分散法に対する秘匿計算法を開発することとした.

計画 5 符号化計算の高速実装法の開発
これまでに知られている秘匿分散計算の中でも特に有力視されている符号化計算に関し、その高速実装法を開発することとした.

４. 研究成果
以上のような計画の下で研究を進めた結果、次の成果を得ることができた.

(1) 参加者数が可算無限となる場合にも対応できるような非対話型のマルチパーティ計算(Non-Interactive Multiparty Computation, NIMPC)を実現するための基礎理論について検討した. ここで NIMPC とは、計算に参加する n 人のパーティが個々にもつデータ x_i(i=1,2,…,n)をそれぞれが明かすことなく、指定された関数 $f(x_1, x_2, \cdots, x_n)$の値を計算するプロトコルであり、特に、参加者は自身が持つデータだけでなく、データから生成されたいかなる情報も一切交換しないようなプロトコルである. ただし、関数値の出力は計算サーバに依頼し、データ秘匿のための乱数の生成はディーラーが行う. このため、ディーラーとパーティ間、および、パーティと計算サーバ間の通信は認められている. このような NIMPC に関して以下の成果を得た.

① Beimel ら[4]により提案された NIMPC は、NIMPC への参加者が保持するデータの組$(x_1, x_2, \cdots x_n)$とディーラーの指定したデータの組$(a_1, a_2, \cdots, a_n)$が一致するときには 1、一致しないときには 0

を返す関数（指示関数と呼ばれる）の計算を実現するプロトコルに基づいている．この指示関数計算を実現する NIMPC プロトコルを拡張し、パーティ数が可算無限となった場合でも指示関数の計算を行う NIMPC の基礎的なアルゴリズムを構築した．

また、このアルゴリズムにより生成されるシェアのサイズを定式化した．その結果、新たに構築したアルゴリズムをパーティ数が有限であるときに適用すると、Beimel らの手法よりもシェアサイズを小さくできることを明らかにした．

②「指示関数の計算」を、Beimel らの手法とは異なる原理に基づく NIMPC により実現するアルゴリズムについて検討した．具体的には、従来知られている「中国の剰余定理に基づく秘密分散法[4]」を応用した手法を構築した．また、この手法を参加者数が可算無限となる場合にも適用できるような拡張について検討した．さらに、この手法により生成されるシェアのサイズや、プロトコルの実行に要する計算量などを評価した．

(2) データの処理を第三者に依頼する際、例えば暗号化などを施してデータの内容を明かさずに第三者に渡し、暗号化データを受け取った第三者はそれを復号することなく所定の処理のみを行って所望の計算結果を得る「秘匿計算」と呼ばれる技術が盛んに研究されている．特に、データを符号化して内容の漏洩を防ぎつつ、多くのサーバに符号化データの処理を依頼して分散コンピューティングによる高速な処理も実現する「符号化計算」は、秘匿計算を効率的に実現する有力な手法として注目を浴びている．

符号化計算を実現する代表的なアルゴリズムとして、Yu ら[5]により提案された「ラグランジュ符号化計算法」が知られている．この手法では、(i)ラグランジェ補間多項式の性質を利用して自身の保持するデータから符号化データを生成し、(ii)複数のサーバに送信して指示した処理を施した後、処理結果を返送してもらい、(iii)多項式補間と RS 符号の誤り訂正の原理を利用して、返送された処理結果から所望の結果を計算するものである．

Yu らの手法の符号化ステップでは、上述の(i)で述べたように、データの符号化にラグランジェ補間多項式が利用されていた．これに対し本研究では、ニュートン補間多項式に基づく符号化を利用することで、Yu らの手法よりも高速な符号化を実現するとともに、データの再符号化が効率的に行える符号化アルゴリズムを構築した．このアルゴリズムは論文としてまとめられ、電子情報通信学会英文論文誌に投稿された．

[1] A. Shamir, “How to Share a Secret,” Commun. ACM, vol.22, no.11, pp.612-613, 1979.
[2] I. Komargodski, M. Naor, and E. Yogev, “How to Share a Secret, Infinitely,” IEEE Trans. on Information Theory, vol.64, no.6, pp.4179-4190, 2018.
[3] A. Beimel, A. Gabizon, Y. Ishai, E. Kushilevitz, S. Meldgaard and A. Paskin-Cherniavsky “Non-Interactive Secure Multiparty Computation,” Advances in Cryptography - CRYPTO2014 (LNCS8617), vol.2, pp.387-404, 2014.
[4] C. Asmuth and J. Bloom, “A Modular Approach to Key Safeguarding,” IEEE Trans. on Inform. Theory, vol.29, no.2, pp.208-210, 1983.
[5] Q. Yu, S. Li, N. Raviv, S. M. M. Kalan, M. Soltanolkotabi, and S. Avestimehr, “Lagrange Coded Computing: Optimal Design for Resiliency, Security and Privacy,” arXiv:1806.00939v4, 2019.

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計1件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 Daisuke Hibino, Tomoharu Shibuya
２．発表標題 Efficient composition of encoding polynomial in distributed coded computing scheme
３．学会等名 電子情報通信学会情報理論研究会
４．発表年 2023年

〔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