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

平成　３０　年　　６　月　２１　日現在

機関番号：　３２６７５
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ００１９３

研究課題名（和文）秘匿されたデータに基づく情報処理に関する研究

研究課題名（英文）Data Processing over Concealed Data

研究代表者
尾花　賢（Obana, Satoshi）

法政大学・情報科学部・教授

研究者番号：７０６３３６００

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：情報を秘匿したまま情報処理を行う秘匿演算方式に関しては，多項目間の相関を計算するクロス集計方式，生体認証方式，および検索を暗号化したまま実現する方式を提案した．複数のユーザが自分の入力を秘匿したままで関数の計算を行うマルチパーティ計算に関しては，マルチパーティ計算において不正を防止するための基礎技術となる不正を検知，あるいは不正者を特定することが可能な秘密分散法の提案を行った．また，関数計算時にユーザ間の通信が不要となる非対話型マルチパーティ計算やd乗算可能な秘密分散に関して，理論的限界の証明や効率の良い方式の提案を行った．

研究成果の概要（英文）：With respect to secure computation over encrypted data that enables us to process encrypted data without decrypting them, we constructed protocols for cross tabulation, biometric authentication, and keyword search. With respect to secure multiparty computation (MPC) that enables multiple users to compute function without revealing inputs possessed by users, we constructed efficient cheating detectable secret sharing and cheater identifiable secret sharing which are used as building blocks to construct MPC. Moreover, we study MPC which does not require user interaction during protocol execution. Namely, we proved theoretical limitation about such protocols, and give efficient construction for them.

研究分野：　情報セキュリティ

キーワード：　マルチパーティ計算　秘密分散　秘匿生体認証

## １．研究開始当初の背景

ビッグデータ解析の普及により，インターネット上のユーザから得られる情報を入手，解析することで，世の中の動向を把握したり，企業が提供するサービスの向上が図られたりしている．しかし，データを提供するユーザのプライバシーは重視されておらず，健康情報や生体そのものの情報など，ユーザのプライバシーに関わるデータを提供することへの心理的障壁はなお大きい状況である．このような状況において，データを暗号化した状態で提供し，秘匿されたデータを復号することなくデータの解析・処理を行う秘匿演算法，およびデータを秘密分散法と呼ばれる暗号技術で秘匿して提供し，データを復元することなく，秘匿された状態のまま，提供された情報を入力とした演算を行うマルチパーティ計算などの技術に対するニーズが高まっている．

秘匿演算は，情報を暗号化したまま，その情報を復元することなく，さまざまな計算を実現する暗号技術である．通常，暗号化されたデータは，復号しない限り暗号文の元となった平文データに基づく情報処理を行うことは不可能であるが，準同型性と呼ばれる特殊な性質を有した公開鍵暗号方式を利用することにより暗号文を復号することなく元の平文に基づく演算が可能となることが知られている．ここで，公開鍵暗号の準同型性とは，平文 m1 の暗号文 E(m1)と平文 m2 の 暗号文 E(m2)との間に定義される演算を適用することにより，元の二つの平文を加算した結果の 暗号文 E(m1+m2) や乗算した結果の暗号文 E(m1×m2) を E(m1) や E(m2) を復号することなく計算することができる性質のことを意味している．クラウドコンピューティングビッグデータ解析の普及により，秘匿演算技術はユーザのプライバシーを保護しながら解析を含めた様々な情報処理を行う技術であるプライバシー保護型データマイニング(Privacy Preserving Data Mining)を実現する技術として注目を集めてきたが，暗号化したままで行える演算が非常に限定されているという課題を有している．秘匿演算で行える技術が限定されている原因は，従来知られている準同型性 を有する公開鍵暗号で平文に対して行える演算が，任意回の単純加算のみ，任意回の単純乗算のみ，あるいは一度の乗算結果の任意回の加算と，非常に限定されていた点にあった．

2009 年に Gentry が完全準同型暗号(Fully Homomorphic Encryption)と呼ばれる，任意回の乗算(AND 演算)と任意回の加算(XOR 演算)を行うことが可能な暗号方式の提案を行った(Gentry，ACM Symposium on the Theory of Computing，STOC 2009)．理論的には，任意回の AND 演算 と XOR 演算により，任意の演算が実現できるため，この結果を用いることで，任意の演算を暗号化したまま実現できることになる．しかし，現状では完全準同型暗号には次のような解決すべき課題が残されている．第一は実行速度の遅さである．2013 年に完全準同型性暗号を実装したライブラリが公開されたが，そのライブラリの実装速度は，同じ処理を暗号化せずに実現した場合と比較して 100 億倍程度遅くなるという報告もなされている．第二の課題は安全性である．完全準同型性暗号が安全性の根拠としている数学的問題はまだ歴史が浅く，その困難さが十分検証されていない状況にある．完全準同型性暗号が発表されて以来，その問題に対する関心が深まるにつれて，鍵のサイズをどの程度大きくとれば暗号の安全性が十分なものになるかが検証されてきたが，安全性を十分なものにするためには，当初想定していたよりも大きな鍵が必要になりそうであるという結果も出されている．以上の点を考慮すると，完全準同型性暗号は，理論的な重要性は十分に認められるものの，処理速度，および安全性の観点から実用化にはまだ長い時間を要する技術と考えられる．一方，従来から存在する演算の種類が限られた準同型性暗号は，完全準同型性暗号と比較して処理速度も速く，また安全性も，素因数分解や，離散対数問題など，通常の公開鍵暗号が安全性の根拠としている問題と同等の問題を安全性の根拠にしている点において，完全準同型暗号よりも十分検証がなされているものになっている．以上の観点から，近い将来利用可能な秘匿演算方式の開発に際しては，従来からの準同型性暗号に基づいた方式の開発が，より有効であると考えられる．

## ２．研究の目的

本研究では，任意回の単純加算，または単純乗算，あるいは任意回の加算と一度の乗算結果の乗算結果を行う準同型性暗号を利用した秘匿演算方式の方式提案を行っていく．完全準同型性暗号ではない準同型性暗号を用いた秘匿演算方式の方式提案としては，暗号化したままでの積集合演算（Freedman，et al.，Eurocrypt 2004)や積集合演算，和集合演算，部分集合判定(Kisser，Song，Crypto 2005)や，プライバシー保護型協調フィルタリング方式(Canny，IEEE Symposium on Security and Privacy 2002)などが知られている．これらの方式は，汎用的なものではなく，対象とする処理に特化したデータの暗号化を行うことにより，単純加算しか行えない準同型性暗号で，より複雑な処理を効率的に行うことを可能としている．本研究では，ビッグデータ解析で多く用いられると考えられるクロス集計(提供されたデータのうち，2~3 程度の項目に着目してデータの分析を行い，項目間の相関を評価する集計法)など，特定の条件を満足するデータを効率的に処理する秘匿演算の提案を目標とする．さらに，

情報を秘匿した演算の中で，近年盛んに研究が行われている，生体情報を秘匿したまま照合処理を行うテンプレート保護型の生体認証方式に関しても，安全で効率の良い方式の提案を目標とする．

本研究では，処理に特化した秘匿演算方式の研究を推進するとともに，情報を秘匿したままで情報処理を行う汎用的な手法の研究も推進する．前述の通り，汎用的な処理の実現を目的とした秘匿演算技術である完全準同型性暗号は，現時点では，処理速度，安全性ともに，実用的なレベルに達していないと考えられる．そこで，汎用的手法の開発に当たっては秘密分散法をベースとしたマルチパーティ計算による効率的な演算方式の開発を目指していく．ここで秘密分散法とは，秘匿すべき秘密情報から以下の二つの性質を満足するシェアと呼ばれる複数部分情報を生成して，生成されたシェアを個別の参加者に配布する暗号プロトコルである．

- 予め定められた参加者集合が各自のシェアを公開することにより秘密は一意に復元される
- 上記で定められた参加者以外が秘密の復元を試みても，秘密に関するいかなる部分情報も得ることはできない

秘密分散をベースにしたマルチパーティ計算は，計算に参加する参加者がそれぞれ秘密 si に対するシェアを保持し，シェアから秘密を復元することなく秘密を入力とした任意の関数 f(s1，s2，...，sN) の値を計算する暗号プロトコルである．秘密分散をベースにしたマルチパーティ計算に関しては，Ben-Or，Goldwasser，Wigderson により，n 人の参加者の全てが正直にプロトコルに従う場合は，n/2 人以上の参加者が結託しない限り，任意の関数 f に対する安全なマルチパーティ計算が実現可能であること，および参加者がプロトコルに従わない場合でも，n/3 人以上の参加者が結託しない 限り安全なマルチパーティ計算が実現可能であることを示している(Ben-Or，Goldwasser，Wigderson，ACM Symposium on the Theory of Computing，STOC 1988)．この研究以後，秘密分散をベースとしたマルチパーティ計算に関して非常に多くの成果が得られており，特に，閾値型構造と呼ばれる全参加者のうちで結託する(不正を行う可能性のある)参加者の人数をあらかじめ想定し，それ以下の不正者の存在の下で安全性を保証する方式については，既に効率的な方式が提案されている．しかし，一般不正者構造(General Adversary Structure)と呼ばれる不正を行う可能性のある参加者の集合が，単純に参加者の人数で特徴づけできない方式に関しては，安全なプロトコルを実現するために必要なデータ通信量が非常に多いという課題が残されている．これは，不正者の構造が閾値構造の場合は，Shamir の閾値型秘密分散というマルチパーティ計算と親和性の高い秘密分散が利用できるのに対し，一般不正者構造に関しては，適した秘密分散が存在しないことが原因となっている．一般不正者構造に関する秘密分散をベースとしたマルチパーティ計算に関しては，Maurer (SCN2002), Hirt, Maurer，Zikas (Asiacrypt 2008)，Hirt，Tschudi (Asiacrypt 2013)らが方式を提案しているが，現在最も効率の良い方式においても，プロトコルで一度乗算を行うたびに一般不正者構造の集合要素数に比例したデータ通信量が必要となり，プロトコル実行時の大きなオーバーヘッドとなっている．本研究では，この状況に鑑み，一般不正者構造においても効率のよい秘密分散法をベースとしたマルチパーティ計算のベースとなる秘密分散法の提案，およびその秘密分散法をベースとした安全なマルチパーティ計算のプロトコル提案を目指していく．

## ３．研究の方法

情報を暗号化したまま処理を行う秘匿演算方式に関しては，データ解析における多くの場面で利用される 2 項目間のクロス集計を実現する．従来のクロス集計を行う秘匿演算では，暗号文のサイズが一方のデータが取り得る値の候補数に比例してしまい，効率が悪かった．本研究では，従来方式よりも小さいオーダーの暗号文サイズでクロス集計を実現するために，2014 年に Hayashi，Obana が提案した特定の条件を満たすデータを集計する秘匿演算方式をベースに検討を行った(Hayashi，Obana，ISITA 2014)．この方式は，(1)指定した 条件に合致する集計値のみが求まり，(2)条件に合致しないデータの集計値については全く情報を漏らさず，また，(3)従来方式と比較して暗号文のサイズが小さい(条件判断を行う集合のサイズに比例しない)という三つの望ましい性質を有した秘匿演算方式である．この方式で提案されているアイデアを，条件付き集計よりも複雑な処理であるクロス集計に適用する方法を検討することにより従来よりも効率の良い方式の構成を行った．

情報を秘匿したまま，生体情報の照合を行う，テンプレート保護型生体認証方式に関しては，生体情報の照合に適した生体情報の符号化法について検討を行った．生体情報の照合を行う際の課題は，生体情報は常に安定したデータを取ることができず，データ取得の度にデータに揺らぎが生じる点にある．暗号化したままでデータの完全マッチングを行う方式はいくつか提案されている(例えば，Curtmola，ACM conference on Computer and communications security，CCS 2006 等)．しかし，前述の通り生体情報のマッチングにおいては，データ取得時に揺らぎが生じるた

め，単純な完全マッチングでは情報の照合を行うことができない．そこで本研究では，ある程度の揺らぎを許容したマッチングを，情報を秘匿したままで行ういくつかの符号化法について検討を行った．方式の検討に当たっては，誤り訂正符号と適切な情報秘匿を組み合わせる方式および準同型性を有する公開鍵暗号をベースにした方式の検討を行った．

秘密分散をベースにしたマルチパーティ計算に関しては，まず，一般不正者構造に対して安全なマルチパーティ計算に適した秘密分散法の方式検討を行った．一般不正者構造に対して安全なマルチパーティ計算において，現状最も大きな課題になっている点は，乗算を行う際に，不正なデータを送信する不正者を検出し，プロトコルから除外する箇所にある．本研究では，まずこの不正者検出，および不正者の除外を効率的に行うための秘密分散法の検討を行った．さらに本研究では，従来のマルチパーティ計算で課題となっていた，計算過程での参加者間の通信を削減する方法の検討を行った．具体的には，Beimel らが 2014 年に提案した，計算過程にユーザ間の通信が不要な Non-Interactive Secure Multiparty Computation と呼ばれる方式のさらなる改善を目指し，理論的限界の解明や効率の良い方式の検討を行った．

## ４．研究成果

情報を暗号化したまま処理を行う秘匿演算方式に関しては，まず効率の良い 2 項目間のクロス集計を実現した．従来，M 個の要素と N 個の要素の要素間のクロス集計を暗号化したまま行う場合，暗号文が MN に比例するサイズとなってしまい効率が悪かったが，本研究で提案した方式は，情報を特別な多項式に埋め込むことにより，暗号文のサイズを MN の平方根に比例するサイズまで削減することに成功している． また，この方式をさらに一般化し，3 項目以上のクロス集計を実現する方式を構成した．クロス集計を行う対象となる項目数を N とし，各項目の取り得る値の個数を a_i (i=1, 2,..., N)とした時，提案方式は暗号文のサイズが a_1 x a_2 x ... x a_n の c+1 乗根となる効率的な方式となっている(ここで c は暗号化したまま行える乗算の回数)．

テンプレート保護型の生体認証に関しては，まずはじめに生体情報の照合に適した生体情報の符号化法について検討を行い，誤り訂正符号に基づく方式 1 種類と，準同型性を有する公開鍵暗号を用いた方式を 2 種類提案した．従来，公開鍵暗号を用いたテンプレート保護型生体認証方式は，認証時に利用した生体情報と，登録した生体情報との間の距離が漏れるという問題を有していたが，公開鍵暗号に基づく 2 種類の方式は，認証時に利用した生体情報と登録した生体情報が同じ人物から取得されたと推定されるか否かしか漏らさない利点を有しており，距離を漏らす従来方式に対して有効であったヒル・クライミング攻撃と呼ばれる攻撃に耐性を持たせることに成功している．準同型暗号を用いた方式に関しては，はじめに提案した方式よりも認証時の通信量を大幅に削減した方式の提案も行い，ソフトウェアによる実装を通じてその有効性の確認も行った．より具体的には，準同型暗号を用いた秘匿生体認証方式と，Eigenface などのよく知られた生体認証方式を組み合わせることで，認証性能 HTER(Half Total Error Rate)が 0．05 程度となる秘匿生体認証を 50ms 弱の時間で行えることを示した．さらに，生体情報が二値ベクトルで表現される状況に対応できるよう，登録情報と認証時の生体情報のハミング距離をメトリックとして生体認証を行う新たな方式の提案を行った．二値ベクトルで表現された生体情報を扱うことのできる既存のテンプレート保護型生体認証としては，Bringer らの方式が知られているが，提案方式は Bringer らの方式の課題であったリプレイ攻撃への耐性と，パラメータ選択の自由度向上を共に実現することに成功している．

情報を暗号化したまま処理を行う秘匿演算方式に関しては，研究計画当初に予定していたクロス集計と秘匿生体認証の実現に加え，データベースを暗号化したままキーワード検索を行うことの可能な二種類の新しい検索可能暗号の提案も行った．第一の提案方式は，従来同様な技術を実現するために利用されていたデータ構造を根本的に見直し，非常に単純なデータ構造で検索インデックスを作成することで，従来効率的に実現することが困難であったデータベースの情報更新や，データの削除を効率的に実現することに成功している．また，第二の提案方式では，従来検索可能暗号で利用実績のあるデータ構造であるブルーム・フィルタを拡張したカウンティング・フィルタと呼ばれるデータ構造に基づく方式を提案した．ブルーム・フィルタを用いた従来方式ではデータベースで管理する情報の更新や削除が困難であるという課題があったが，カウンティング・フィルタを用いることにより，更新や削除が容易に行えることが示された．提案した二種類の方式に関しては，方式の実装も行い，実用的な処理速度でデータベースの情報更新や削除を行うことが可能であることを確認した．

マルチパーティ計算に関しては，まずはじめに任意の線形秘密分散法に対して適用可能な，不正を検知可能な準最適秘密分散法の提案を行った．従来の準最適な方式は，秘密がランダムなビット列である場合に安全でないことが問題となっていたが，本研究で提案した方式は，秘密が(ランダムなビット列を含む)どのような体の要素であっても安全性を証明可能であり，さらに，各ユーザが保

持する情報のサイズも理論的下界と１ビットしか差がない準最適な方式となっている．また，マルチパーティ計算において Rushing adversary と呼ばれる，強力な敵に対しても安全性を保証可能な秘密分散の提案も行った．Rushing Adversary とはマルチパーティ計算において他のユーザが送信する情報を観測した後に不正を行うことができるユーザであり，このタイプの敵に対する効率的な不正防止可能な秘密分散を構築することは大きな課題であった．本研究では，不正者の数 t が全パーティ数 n に対して t<n/3 を満たす場合，t<n/2 を満たす場合それぞれについて，従来よりも効率の良いいくつかの方式を提案した．

ユーザ間のインタラクションが不要なマルチパーティ計算である Non-Interactive Secure Multiparty Computation (NIMPC)に関しても検討を行い，通信量の理論的下界を導出するとともに，従来方式と比較して通信量が10の20乗分の１ となる効率的な方式の提案を行った． NIMPC に関しては，さらに検討を進め，はじめに提案した方式をベースに，効率の良い多ビット出力の任意の関数の NIMPC の提案を行った．関数の出力が L ビットとなるとき，提案方式の通信量ははじめに提案した方式の通信量の 1/L となることが示された．

マルチパーティ計算に関しては，計算可能な関数のクラスは制限されるものの，ユーザ間の通信を全く行うことなく複数の秘密の乗算結果のシェアを計算することが可能な d 乗算可能秘密分散法における不正防止技術の検討も行った．具体的には，不正な乗算結果の部分情報を出力する不正者を検知することが可能な検証乗算可能な秘密分散法のモデルの構築，および構築したモデルにおける方式の構成可能性の検討を行った．また，検証乗算可能な秘密分散に関しては，任意に小さい不正成功確率を許容した場合に，秘密の部分情報が３つの有限体要素からなる非常に効率的な方式の構成も行った．

## 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１件）


① Haruna Higo, Toshiyuki Isshiki, Kengo Mori, Satoshi Obana, Privacy-Preserving Fingerprint Authentication Resistant to Hill-Climbing Attacks, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 査読有, E101-A, 2018, 138-148, DOI:10.1587/transfun.E101.A.138


〔学会発表〕（計 17 件）


① Satoshi Obana, Cheating Prevention in Secret Sharing Schemes, International Workshop on Secret Sharing and Security(招待講演), 査読無, 2018

② 吉田真紀, 尾花賢, 検証乗算可能な秘密分散, 2018 年暗号と情報セキュリティシンポジウム, SCIS2018, 査読無, 2018

③ Maki Yoshida, Satoshi Obana, Verifiably Multiplicative Secret Sharing, Information Theoretic Security - 10th International Conference, ICITS 2017, 査読有, 2017

④ 尾花賢, 秘密分散法における不正防止技術, 2017 年電子情報通信学会総合大会(招待講演), 査読無, 2017

⑤ 大木哲史, 一色寿幸, 肥後春菜, 森健吾, 尾花賢, 秘匿生体認証に適した特徴量抽出法に関する考察, 2017 年暗号と情報セキュリティシンポジウム, SCIS 2017, 査読無, 2017

⑥ 一色寿幸, 肥後春菜, 森健吾, 尾花賢, 大木哲史, ヒルクライミング攻撃に耐性を持つ効率的な秘匿生体認証方式, 2017 年暗号と情報セキュリティシンポジウム, SCIS 2017, 査読無, 2017

⑦ 佐野僚哉, 尾花賢, リプレイ攻撃や不正なサーバによる攻撃に耐性のある秘匿生体認証方式, 2017 年暗号と情報セキュリティシンポジウム, SCIS 2017, 査読無, 2017

⑧ Satoshi Obana, Maki Yoshida, An Efficient Construction of Non-Interactive Secure Multiparty Computation, Cryptology and Network Security - 15th International Conference, CANS 2016, 査読有, 2016

⑨ Hidetaka Hoshino, Satoshi Obana, Cheating Detectable Secret Sharing Scheme Suitable for Implementation, Third International Workshop on Information and Communication Security, 査読有, 2016

⑩ Shunta Nozoe, Satoshi Obana, Searchable symmetric encryption supporting update, 2016 International Symposium on Information Theory and Its Applications, ISITA 2016, 査読有, 2016

⑪ Avishek Adhikari, Kirill Morozov, Satoshi Obana, Partha Sarathi Roy, Kouichi Sakurai, Rui Xu, Efficient Threshold Secret Sharing Schemes Secure Against Rushing Cheaters, Information Theoretic Security - 9th International Conference, ICITS 2016, 査読有, 2016

⑫ 肥後春菜, 一色寿幸, 森健吾, 尾花賢, リプレイ攻撃に対して安全な秘匿生体認証方式, 2016 年暗号と情報セキュリティ

シンポジウム，SCIS 2016，査読無，2016
⑬ 肥後春菜，一色寿幸，森健吾，尾花賢，秘匿生体認証における生体情報の秘匿性に関する定義，2016 年暗号と情報セキュリティシンポジウム，SCIS 2016，査読無，2016
⑭ 肥後春菜，一色寿幸，森健吾，尾花賢，認証時の情報開示の少ない秘匿生体認証方式，2016 年暗号と情報セキュリティシンポジウム，SCIS 2016，査読無，2016
⑮ Maki Yoshida，Satoshi Obana，On the (In)Efficiency of Non-Interactive Secure Multiparty Computation，Information Security and Cryptology - ICISC 2015 - 18th International Conference，査読有，2015
⑯ Hidetaka Hoshino，Satoshi Obana，Almost Optimum Secret Sharing Schemes with Cheating Detection for Random Bit Strings，10th International Workshop on Security，IWSEC 2015，査読有，2015
⑰ Haruna Higo，Toshiyuki Isshiki，Kengo Mori，Satoshi Obana，Privacy -Preserving Fingerprint Authentication Resistant to Hill-Climbing Attacks，Selected Areas in Cryptography - SAC 2015 - 22nd International Conference，査読有，2015

６．研究組織

(1)研究代表者

尾花　賢（Obana，Satoshi）
法政大学・情報科学部・教授
研究者番号：70633600

(4)研究協力者

星野　英貴（Hoshino，Hidetaka）
野副　俊太（Nozoe，Shunta）