氏名（本籍）	AHMAD AKMAL AMINUDDIN BIN MOHD KAMAL（マレーシア） （アフマド アクマル アミヌディン ビン ムハンマド カマル）
学位の種類	博士（工学）
学位記番号	甲第1114号
学位授与の日付	2022年3月19日
学位授与の要件	学位規則第4条第1項該当
学位論文題目	**Secure Multi-Party Computation Based on（*k*,*n*）Threshold Secret Sharing with *n*< 2*k* - 1 and Application into Searchable Encryption** **（*n* < 2*k* - 1 における（*k*,*n*）閾値秘密分散法を用いた秘密計算法及び秘匿検索への応用）**
論文審査委員	（主査）教授　岩村　恵一 教授　浜本　隆之 教授　長谷川幹雄 教授　吉田　孝博 教授　谷口　行信 株式会社インターネットイニシアティブ シニアエンジニア 博士　須賀　祐治

論文内容の要旨

近年,ビッグデータやモノのインターネット（IoT）などのデータ収集技術の進歩に加え,情報通信技術の革新により,大量のデータの収集・分析が可能になっている.さらに,ビッグデータに埋め込まれた個人情報を活用できる技術への期待も高まっている.特に,最近では,個人データを活用することで,様々な社会問題の解決（例えば,男女間の賃金格差の問題など）や新しいサービス（より良い医療サービスなど）の開発が期待されている.

例えば,Google, Apple, Facebook, Amazon (GAFA)は現在,ユーザから収集した個人のデータを最大限に活用して,検索の速度と精度を高め,ユーザ向けのパーソナライズされた広告などの推奨機能とマッチング機能を改善している.しかし,個人情報の活用においては情報漏洩に伴うプライバシーへの悪影響が懸念される.そのため,ビッグデータ解析においては個人情報の保護と統計計算の両立が今後の実用化に向けた最大の課題である.このような課題に対し,情報の

秘匿性を担保しつつ演算を行なうことができる秘密計算技術が注目されている.

秘密計算技術は,主に鍵を用いてデータを秘匿する準同型暗号に基づく手法と,鍵を用いずにデータを秘匿する秘密分散法に基づく手法に大別できる.ただし,準同型暗号は一般的に計算量が多く,演算の処理に多大な時間がかかるという問題があり,膨大なデータを扱うビッグデータへの適用を考えた場合,計算に時間がかかる準同型暗号よりも,計算が軽く高速処理が可能な秘密分散法が適していると考えられる.秘密分散法はユーザが所持する秘密情報を複数の異なる値(分散値)に変換し,分散する手法である.

本論文では,秘密分散法の1つであるShamirの(k,n)閾値秘密分散法を用いて,安全な秘密計算法を提案する.Shamirの(k,n)閾値秘密分散法は,多項式を用いて1つの秘密情報をn個の分散値に変換し,n台のサーバに分散する.分散した分散値をk個以上集めることで元の情報を正しく復元できる一方,それ未満の情報からは一切の秘密情報を得られないという手法である.しかし,この手法を適用した従来の秘密計算においては,加算は容易に実現できるが,乗算を行なう際は多項式同士の乗算によりその次数が$k-1$から$2k-2$に変化することから,乗算結果の復元に要する分散値の数がk個から$2k-1$個に変化してしまうという問題がある.即ち,乗算を行う場合,従来はサーバ台数を$n \geq 2k-1$としなければならないため,元々$n \geq k$でよかったサーバ台数を約2倍にしなければならず,大規模な装置構成を必要とする.また,一般的にShamirの(k,n)閾値秘密分散法を用いた秘密計算では,分散値の数が$n < 2k-1$の場合,無条件での安全な計算は不可能とされている.

そこで,本論文では$n < 2k-1$の分散値でも乗算を含む秘密計算を実現できる新たなアプローチや条件を提案し,情報理論的安全性を持つ新しい秘密分散法を用いた秘密計算及びその応用である秘匿検索への適用をすることが最大の目的である.それを実現する上で本論文では以下の方式を提案する.

(第1部)

本論文の第1部では,秘密分散の情報理論的安全性を維持しながら,$n < 2k-1$の場合に条件付安全な秘密計算を実現することを目的とし,以下の秘密計算法を提案する.

(1) $n < 2k-1$において,情報理論的安全な条件付秘密計算法の提案

乗算結果の多項式の次数を変化させず,乗算を実現する一つの方法は,定数との乗算が考えられる.つまり,(多項式×多項式)というアプローチではなく,(多項式×スカラー量)という形で乗算をすることによって,多項式の次数変化を防ぐことができる.Damgårdらによって提案されたSPDZ法などの従来法もこのアプローチを使用して,乗算結果の多項式の次数を増やさず乗算を実現したが,これらの方法は,情報理論的安全性を実現できないなどの欠点がある.

そのため,本論文では,(スカラー量×多項式)という形で乗算をする情報理論的安全性を持つ秘密計算法提案する.スカラー量との乗算を実現するには,多項式で表現されている一方の分散値をスカラー値として復元する必要がある.ただし,一方の秘密情報(例えば,秘密情報a)をそのまま復元すると,その秘密情報は必ず漏洩してしまう.従って,本論文では,秘密情報をそのまま分散せず,まず,秘密情報(例えば,秘密情報a)に乱数(例えば,乱数α)とかけて,秘匿化秘密情報(例えば,αa)を計算し,Shamirの(k,n)閾値秘密分散法を用いて分散をする.乗算をする際に,秘匿化した一方の分散値を一時的に復元(例えば,αa)し,もう一方の多項式と乗算を行なうことで,次数変化を伴わない乗算を可能とする.さらに,1回の四則演算に対する秘密計算に加えて,$ab+c$のような四則演算の組合せに対しても安全な秘密計算手法を提案する.

また,前述のように,本論文では,以下の3つの条件を導入し,秘匿積和演算の組合せによって種々の演算が安全に実現できることを示す.さらに,これらの手法は,情報理論的な安全性を持つことを理論的に証明する.

条件(1):乗算の入出力に0を含まない

条件(2):攻撃者が知らない乱数とそれを構成する乱数の分散値を各サーバが持つ.

条件(3):各サーバが復元する乱数は固定される.

(第2部)

本論文の第2部では,第1部の秘密計算の応用である$n<2k-1$において安全な秘匿検索法を提案する.

(2) ドキュメントの秘匿検索への応用

秘密計算の応用の一つとして,暗号化されたデータを復号せず,暗号化したままの状態で検索ができる秘匿検索がある.例えば,アリスが自分のデータをクラウドサーバに保存をすることによって,いつでも,どこからでも,自分のデータをアクセスすることができるという利点がある.ただし,データのプライバシー及び秘匿性を保護するため,データを暗号化して保管する必要があるが,通常の暗号方式では,暗号化されたデータを復元せず,検索をすることができないという問題点がある.

そこで,本論文では,暗号化されたデータを復号することなく,正当なユーザまたは許可されたユーザだけがそのデータを取り出せる秘匿検索法を提案する.具体的には,第1部の秘密計算法を基に,条件(1)及び条件(3)を緩和した秘密計算法を利用し,登録されたドキュメントと検索したい検索クエリの各文字間の差を秘密計算し,一致するドキュメントを検索できる手法を提案する.

(第 3 部)

第1部では, 3つの前提条件のもとで, (スカラー量×多項式) のアプローチで、乗算を含む$n < 2k-1$の秘密計算法を提案した. しかし, 全ての条件を満たさないと安全性の確保ができないことは, 産業での実利用を制限する要因となる. そのため, 第3部では, (多項式×多項式) のアプローチを用いても、$N < 2k-1$ (ただし, Nはサーバ台数) の乗算ができる秘密計算法を検討し、前述の一部の条件を必要としない手法を示す.

(3) $N < 2k-1$台のサーバで$n \geq 2k-1$の設定を実現できる秘密計算の提案

ここでは, 典型的な (多項式×多項式) アプローチを使用し, $n < 2k-1$のサーバ数で乗算結果を復元できる秘密計算法を提案する. 提案法では, 乗算結果の多項式の次数を減らすために, 次数を減らす処理を導入する. 即ち, 前に述べたように, $(k-1)$次の多項式同士を乗算すると, 乗算した多項式の次数が$(2k-2)$になる. ここで, 多項式の次数を$(2k-2)$から$(k-1)$に戻す処理を導入することにより, 乗算結果を復元するために必要な分散値の数nも$n \geq k$に戻ることができる手法を提案する. Ben-Orら及びChaumらもこのアプローチを使用して, 秘密計算を提案したが, これらの手法は, 1台のサーバに 1 つの分散値を送信するため, 必要なサーバ台数は$2k-1$以上である問題点をまだ解決できない.

そこで, 本論文では実際に用いるサーバ台数をNとし, 秘密分散法におけるパラメータnと分けて$k \leq N < 2k-1$, $n \geq 2k-1$として秘匿乗算を実現する. 即ち, 1 台のサーバに同じ秘密情報に対する分散値を乱数で秘匿化して複数送信することにより, サーバ台数Nを$k \leq N < 2k-1$としたままでも, $n \geq 2k-1$の分散値を計算することができるため, 秘匿乗算を実現できることを示す. また, 次数を減らす処理を導入することにより, 最終的にk個の分散値から乗算した結果を復元できることを示す. さらに、提案手法では、秘密計算を行なうサーバのみの攻撃($k-1$台まで)を考える場合、条件(1)を必要としない秘密計算法を実現できることを示す. これによって, 本論文ではサーバ台数を$k \leq N < 2k-1$とし, 1 つの前提条件のみで$n < 2k-1$の秘匿乗算を実現できるようにする.

論文審査の結果の要旨

本論文では、学長からの審査付託を受けて、標記６名の審査委員で構成する審査委員会を組織し、提出された学位論文について審査を行った。

審査委員会においては、学位申請者から、学位論文の内容や前回審査における指摘事項の対応結果について説明させ、その後、質疑応答を実施することで、博士論文として満たすべき条件や必要な修正点を確認するという形式で進めた。

本論文では、ビッグデータ解析において個人情報の保護と統計計算の両立を可能とする秘密計算技術について研究を行っている。秘密計算技術は、主に鍵を用いてデータを秘匿する準同型暗号に基づく手法と、鍵を用いずにデータを秘匿する秘密分散法に基づく手法に大別できるが、本論文では計算が軽く高速処理が可能な秘密分散法を用いた秘匿計算を研究している。しかし,秘密分散法を用いる従来の秘密計算において、乗算を行なう場合、必要な分散値の数がk個から$2k-1$個に変化してしまうという問題が発生する。即ち、乗算を行う場合サーバ台数を約2倍にしなければならず、大規模な装置構成を必要とする。また、k人の当事者間で秘密計算できないという問題もある。そこで、本論文では$n<2k-1$個の分散値でも乗算を含む秘密計算を実現できる新たなアプローチや条件を提案し、情報理論的安全性を持つ新しい秘密分散法を用いた秘密計算及びその応用である秘匿検索への適用を行っている。これによって、従来方式の問題であったサーバ資源の増大や、当事者間の秘密計算を可能とする。

第1回審査では、学位申請者から学位論文の内容について説明があり、各審査委員から主に以下の指摘があった。

(1) 提案方式と従来方式の違いをわかりやすくするために1つの表にまとめること
(2) 秘密分散法を用いた方式のデメリットも明確にすること
(3) 秘密計算の歴史や応用例などは少なくてもよいこと
(4) 処理時間を含めた実装結果も示すこと

第2回審査では、第1回審査における指摘事項を反映させた発表があった。改善は確認されたが、以下の点について審査委員から指摘があった。

(1) 提案方式に条件が必要であることを明確にすること
(2) 提案方式の位置づけや強みを含めた貢献を明確にすること
(3) 提案した秘密計算の定量的な評価も入れること

第3回審査では、公聴会を兼ねて実施し、これまでの審査の指摘事項を踏まえて修正した内容の発表があった。指摘事項はほぼ改善され、わかりやすい発表であったという評価であったが、審査委員及び公聴会出席者から以下のような質問があった。

(1) 検索は検索速度が命だが、無暗号化より処理速度が一桁以上遅いのは大丈夫か？
(2) 情報理論的安全性を計算量的安全性に落とすことによって効率が向上するか？
(3) 研究がずいぶん進んでいるようだが、実用化には何が必要か？

学位論文申請者はこれらの質問に適切に回答し、質問者および審査委員からの了解が得られた。

以上により、本論文は、博士（工学）の学位論文として十分に価値あるものと認められる。