様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　６　月　２７　日現在

機関番号：　３２７２１
研究種目：　基盤研究(C)（一般）
研究期間：　2013～2015
課題番号：　２５３３０１６１

研究課題名（和文）検索可能暗号の機能拡張の研究

研究課題名（英文）Research for the extensions of searchable encryption schemes

研究代表者
土井　洋（DOI, Hiroshi）

情報セキュリティ大学院大学・情報セキュリティ研究科・教授

研究者番号：７０３３８６５６

交付決定額（研究期間全体）：（直接経費）　　2,900,000円

研究成果の概要（和文）：本研究では、検索可能暗号における検索可能者の指定や、検索条件を柔軟に設定可能にするための機能拡張について提案した。提案方式は複数サーバを用いるモデルであるものの有用な機能を有し、安全であり、かつ効率的である。更に、これらの方式に関連する性能向上に係る研究も行った。これらの成果により、暗号化データを利用する際の利便性とセキュリティの向上等に寄与できた。

研究成果の概要（英文）：In this research, we proposed the extensions of searchable encryption schemes that could specify the searching user and could configure several conditions. Although our extension schemes assumed the existence of multi servers, they had useful properties and were secure and efficient. Furthermore, we researched the improvement of efficiency relevant to the extension schemes. From the above results, we could contribute to the security and usefulness for using encrypted data.

研究分野：　暗号と情報セキュリティ

キーワード：　検索可能暗号　マルチパーティプロトコル

１．研究開始当初の背景

近年ではクラウドサービスを始め、インターネットを利用した、第三者が提供するサービスの利用が活発となっている。これに伴い、第三者によるデータの保存、検索、処理等のサービス提供という形態の受容性が高まっているといえる。このような環境に基づく、安全性と利便性を両立する様々な方式の研究も続けられており、検索可能暗号もこのような方式の一つである。

検索可能暗号において、暗号化の段階では、データの暗号化とともに暗号文に関連付けられた検索されるための情報（例えばキーワード等）を暗号化して付加情報（以下、タグ）として出力する。検索の段階では、復号鍵と検索したい情報を用いてトラップドアと呼ばれる情報を生成する。トラップドアとタグを所定の方法で処理すると、両者の検索に係る情報が等しいか否のみを判定できる。ここで、適切なトラップドアを用いない限り、暗号文やタグから情報は漏れない。なお、トラップドア生成者とタグを用いて判定する者は同一である必要はない。

検索可能暗号を用いると、例えばクラウド上に暗号化データを配置し、必要な暗号文のみをダウンロードする機能が実現できる。本報告では役割に応じて、暗号文作成者、検索可能者、検索サーバと呼ぶことにする。暗号文作成者が暗号文とタグをサーバ上にアップロードする。検索可能者は復号鍵を用いてトラップドアを生成し、検索サーバに送る。検索サーバはトラップドアとタグを所定の方法で処理する。最終的には検索内容が等しい暗号文を検索可能者がダウンロードした後、復号する。すなわち、検索可能暗号を用いることで、暗号文に関連付けられたタグに対して、検索サーバを介した検索の機能を実現できる。なお、クラウド上のデータはすべて暗号化されているので、セキュリティは高い。

検索可能暗号においては、検索サーバ（その管理者を含む）を完全に信頼していないことに注意が必要である。検索サーバは、例えばネットワーク上に配置されたサーバであるが、検索可能者より送られたトラップドアを用いて所定の処理を行い、検索内容が等しいかどうかを判定する。クラウド上の暗号化データの検索のシナリオでは、検索サーバは所定の処理を行うことが必須であり、この点では完全に信頼する。一方、セキュリティの観点からは、検索サーバに復号鍵は知られないこと、タグなどから不必要な情報が漏れないこと、及び蓄積されたトラップドアから別の情報に係るトラップドアを作成できないことなどが求めれらる。ただし、検索サーバは、検索の成否の履歴等を蓄積することはできる。このため、既存研究においても守る情報が何かを明確にし、安全性の議論がなされている。

検索可能暗号において、検索可能者とは復号可能者のことである。検索可能暗号については様々な方式提案がなされているが、検索可能者は固定され、完全一致検索のみが実現されている場合が多い。ここで、暗号化時に検索可能者を指定でき、指定された検索可能者のみがトラップドアを作成できるように拡張できれば、利用範囲は拡大する。更に、検索条件を柔軟に設定可能にするような機能拡張ができれば、利便性は向上する。なお、複数の検索可能者が存在することになるので、例えば異動に伴う検索権限の失効処理に相当する機能なども望まれる。暗号化時における検索可能者の指定や、検索条件の柔軟な設定を可能とする方法については既存研究があるが、暗号文サイズが大きい、及び処理コストが大きいという問題点が存在した。クラウドサービスの普及とその受容性などを考えると、モデルの変更等（複数サーバを設ける）も視野に入れた上で上述の問題を解決可能な、既存研究とは異なる方式を提案することには意味がある。

本研究は、暗号文に関連付けられた情報を利用した検索機能に対し、利便性を向上させる安全かつ効率の良い機能拡張の提案である。

２．研究の目的

本研究では、モデルの変更も視野に入れ、検索可能暗号の機能拡張を行うことを目指す。実現すべき機能は i）検索可能者の柔軟な指定、ii）検索条件の柔軟な設定であり、特に検索可能者の指定は暗号化時のみならず、検索の実行時に可能となることも視野に入れる。なお i）が実現されれば、複数の検索可能者が存在することになるので、検索可能者の失効機能の実現も望ましい。なお、本研究ではモデルの変更も視野に入れているが、モデルを変更した場合の安全性を証明することも必要である。並行して、性能向上に寄与する研究も目標となる。

既存研究において、匿名性を有する ID ベース暗号を用いることで、検索可能暗号を実現可能であることが知られている。また、i）及び ii）を解決するアプローチとして、階層型 ID ベース暗号や属性ベース暗号などのより高機能な方式に匿名性を付加する方法が知られている。しかし、これらの手法においては、いくつか解決すべき課題がある。まず、暗号文サイズが大きいことや処理コストが大きいことである。また、設定可能なのは、検索実行時ではなく、暗号文作成時のみに限定されることである。

検索可能暗号は、性能と用途の面から、共通鍵暗号ベースの検索可能暗号と公開鍵暗号ベースの検索可能暗号の二つに大別できる。共通鍵暗号ベースの検索可能暗号は暗号文作成者と検索可能者が同一であり、用途は限定されるが処理は高速である。公開鍵暗号ベースの検索可能暗号は、性能面では共通鍵ベースのものに劣るが、誰でも暗号文作成者

となることが可能である。このため、例えばクラウド環境において、不特定多数のユーザにより作成された暗号化データを蓄積し、後日それらから必要なデータを検索する場合には都合がよい。

本研究においては、まず、共通鍵暗号ベースおよび公開鍵暗号ベースの二つの方法におけるモデルの整理、特に検索サーバに求められる機能や安全性に関する仮定等の整理を行う。そして、検索可能暗号の利便性を向上させる安全かつ効率の良い機能拡張の方向性を定める。なお、クラウドサービスを始めとする第三者が提供するサービスの利用が活発となっている状況を考慮して、本研究ではモデルの変更、例えば複数サーバを利用することも視野に入れる。研究代表者は、複数サーバの連携により、ID ベース暗号における復号権限の過度の集中を解決する方式について、一定の成果を得ている。また、このモデルにおいて、高い安全性を有することも示している。このようなモデル変更を行うことにより、利便性を高め、効率よく安全な方式を設計できる余地はある。本研究の第一段階では、検索可能者や検索条件を暗号化時に柔軟に設定可能とするための機能拡張を目指す。この際、階層型 ID ベース暗号、属性ベース暗号などの既存の研究成果の利用も視野に入れる。

その解決の後、検索可能者を暗号化時ではなく、検索の実行時に指定可能な方式の検討を進める。例えば、動的に検索可能者を変更できる特別なサーバ等を新たに設け、暗号文またはトラップドアを適切に処理する方式も可能性として考えられるが、モデルに沿った適切な解決方法を探る。その実現と並行して、検索可能者の失効機能の実現も目指す。ここでは、代理再暗号等を用いることも視野に入れる。

これらの目的の達成は一見容易であるようだが、セキュリティを確保するのは簡単ではない。例えば、モデルの変更が生じた場合、モデルに沿ったセキュリティの定義と、それに基づく安全性証明を行う必要がある。一連の研究では、秘密分散共有法を利用する可能性が高いが、システム全体としては複雑になり、データサイズや処理コストとのトレードオフが発生することが予想される。そこで、並行して提案方式の性能向上へ寄与する研究も行う。

３．研究の方法

本研究では、検索可能暗号の機能拡張のための研究を推進する。具体的にはモデルの整理を行った後、検索可能者（すなわち復号可能者）の指定や検索条件を柔軟に設定可能とするための方式の検討を行い、あわせて安全性証明と性能向上等の研究を推進する。前者については、検索可能者の動的変更等も視野に入れている。ここでは階層型 ID ベース暗号、属性ベース暗号などの高機能暗号を使うことも視野に入れている。

研究初年度である平成 25 年度は、共通鍵暗号ベース、および公開鍵暗号ベースの検索可能暗号の既存の研究成果を調査し、それを基にモデルの検討を行う。共通鍵暗号ベースの方式については、完全一致検索以外の検索に関する既存研究等を主な対象とし、様々な拡張に関して調査研究を進める。一方、公開鍵暗号ベースの方式については、検索条件を柔軟に設定可能とするために有益な属性ベース暗号、述語暗号等を中心に調査研究を行う。

これらの調査研究を通して、モデルの検討を進める。モデルの検討は、安全性要件を定義すること、すなわちセキュリティモデルの検討にも大きな影響を与える。検索可能暗号のモデルに関する様々な角度からの検討を行い、現時点のクラウドサービスの進展や、ニーズ、性能面について検討し、適切なモデルを定める。

平成 26 年度は、平成 25 年度に得られた知見をもとに、検索可能者の指定が可能な検索可能暗号の研究を継続・推進する。検索可能者は検索可能者でもあるが、それを暗号文作成時に指定可能とすることを実現する。これが実現されれば、暗号文作成者の指定に基づき、検索サーバが検索可能者の認証を行うことになる。既存研究として、匿名性を有する階層型 ID ベース暗号を基に構成する方式が知られている。本研究では、モデルの変更、例えば複数のサーバの利用なども視野に入れる。最近のクラウド環境を考えると、複数のサーバが協力することで検索を実現するというモデルはコスト面や受容性という点でも妥当と考えられる。並行して、より詳細な検索条件を設定できる方式についても、同一モデルの上で検討する。具体的には、属性ベース暗号等を用いた実現可能性を検討する。

この際、検索時にサーバに漏れる情報を十分評価する必要がある。共通鍵暗号ベース、および公開鍵暗号ベースの検索可能暗号の安全性に関する考え方などを参考にし、検討を進める。なお、クラウド上の暗号化データの検索のシナリオでは、検索サーバはクラウドが担当することになる。クラウドの処理能力は高いので、それ以外、すなわち暗号文作成者、検索可能者に要する処理コスト等について評価を行う。

最終年度である平成 27 年度は、これまでの成果に基づき、検索可能者を指定可能な検索可能暗号等の構成法に対し、一般化とその安全性の評価についての研究を進める。一般化とその安全性の評価がなされれば、既存の様々な方式への安全な適用が容易になる。

更に、検索可能者を検索時に動的に変更可能な方式についても検討する。この方式においては、検索可能者は暗号化時ではなく検索

時に事前に定められたサーバが決定できる。しかし、サーバに不要な情報は漏れないように設計する必要がある。そこで、複数の検索可能者が存在することによる課題である、検索可能者の失効機能の実現も検討する。並行してこれらの方式の高速化に寄与する研究も進める。

3 年の研究期間で、検索可能暗号における既存のモデルの整理の後、検索可能者（すなわち復号可能者）や検索条件を柔軟に設定可能にするための機能拡張に関する研究を推進する。同様の方式はいくつか知られているが、クラウドサービスの進展などによるモデルの変更も視野に入れ、機能拡張を行う。ここで、暗号文サイズや処理性能等についても考察した提案を行うことを目指す。更に、これらの方式に関連し、高速化に寄与する方式等（例えば、秘密分散共有法の高速化）についての研究も行う。これらにより、暗号化データをクラウド上に配置するというサービスの利便性とセキュリティの向上等に寄与できると考えている。

なお、本研究においては、研究代表者が拡張方式の着想や具体的な提案、更に安全性証明などを行う。ただし、情報セキュリティ大学院大学や他大学の博士前期・後期課程学生や修了生にも必要に応じて研究の一部に協力してもらう。この際、方式検討グループ、安全性証明グループを設け、相互に情報を共有しながら研究を進める。

４．研究成果

本研究では、暗号化対象に関連付けられた情報を利用した検索機能に対し、利便性を向上させる拡張方式の提案や安全性の確立に関する研究等を推進した。具体的には、検索可能暗号に対して様々な条件を柔軟に設定可能とするための機能付加、性能向上、および安全性の確立に関する研究を行った。

初年度にあたる平成 25 年度は、まず検索可能暗号の既存の研究成果を調査し、それを基にモデルの検討を行った。検索可能暗号は、共通鍵暗号ベースの検索可能暗号と公開鍵暗号ベースの検索可能暗号の二つに大別できる。モデルも異なるが、検索を行う第三者（検索サーバ）が知ることができる情報も異なる。初年度は、機能、セキュリティ、およびシステム（検索サーバを含む）に対する仮定など、様々な角度からの検討を行った。この際、クラウドの普及と第三者（サーバ）利用に対する受容性なども考慮した。検討の結果、多くのモデルとそれに基づく方式提案がなされているものの、現時点のクラウドサービスの進展、ニーズの反映や性能面等を考えると、他のモデルでの検討の余地があることがわかった。この結果を受けて、本研究では、複数の第三者（サーバ）の利用も視野に入れることとした。その際、どのような種類の第三者機関を設けるか、また第三者機関に対しどのような安全性仮定を置くか、言いかえるとどの程度の信頼を置く必要があるか、などの要件を含めた検討も行い、モデルを定めた。以後、公開鍵暗号ベースの検索可能暗号の機能拡張に注力することとした。

平成 26 年度は、平成 25 年度に得られた知見をもとに、複数サーバモデルで、検索可能者の指定等を含む検索に関する条件の柔軟な設定に関する研究を推進した。検索可能者は復号鍵を使いトラップドアを作成できる者でもあるが、それを暗号文作成時に指定できることを実現した。指定されなかったユーザは、検索のための適切なトラップドアを生成することができないため、検索実行ができない。言いかえると、検索可能者の認証を、暗号文作成者の指定に基づき、検索サーバが行えることになる。

この機能は、既存研究では ID ベース検索可能暗号として知られている技術であるが、それは匿名性を有する階層型 ID ベース暗号を基に構成される場合が多い。本研究では、複数のサーバ（例えばクラウド事業者）を用いることにより、匿名性を有さない階層型 ID ベース暗号を基に構成することを可能とした。最近のクラウド環境を考えると、複数のサーバが協力して検索を行うというモデルはコスト面でも妥当と考えられる。まずは、サーバを 2 台とした構成を検討し、モデル、セキュリティ要件を明確化した。通常、階層型 ID ベース暗号においては、全ての復号鍵を生成できる管理者が存在し、それを完全に信頼しなくてはならない。しかし、複数サーバモデルの下で、この問題も同時に解決した。

具体的な構成法として、Boney、 Boyen が 2004 年に提案した、RFC5091 で取り上げられている ID ベース暗号（BB1 方式と呼ばれる）と密接な関係がある、階層型 ID ベース暗号を基にした構成法を示した。安全性の証明では、2 台のうちの 1 台からの情報漏えいがなければ、暗号文とタグから平文に関する情報が漏れないことをフォーマルに証明した。なお、この構成では匿名性を有さない階層型 ID ベース暗号を本モデルに適用している。しかし、匿名性を有する階層型 ID ベース暗号を用いて構成する場合と比較し、暗号文サイズや処理コストの点で遜色ないことを理論的評価により示した。

更に、より詳細な検索条件を利用できる属性ベース暗号の適用についても検討を進めた。階層型 ID ベース暗号と同様、匿名性を有する属性ベース暗号を基に、属性ベースの検索可能暗号を構成できることが知られている。しかし、複数サーバモデルを採用することにより、匿名性を有さない属性ベース暗号を基に、属性ベースの検索を実現できる可能性を示した。本提案も、既存方式と比較し、暗号文サイズや処理コストの点で遜色ない可能性がある。安全性の証明も、同一モデル上で与えた。

最終年度にあたる平成 27 年度は、本研究

成果として既に提案した複数サーバモデルの匿名性を有する階層型 ID ベース暗号及び検索可能者を指定可能な検索可能暗号に関し、構成法の一般化と安全性についての研究を進め、情報処理学会の英文論文誌にて発表した。

モデルと安全性の定義は前年度までの研究でほぼ完了している。しかし、ベースとする階層型 ID ベース暗号毎に安全性証明を構成する必要がないように、一般的な構成法を示し、それに対する安全性証明を付与した。これは、ベースとする階層型 ID ベース暗号が双線形群上で構成されている場合の安全性証明に適用可能であることを示したことになる。すなわち、前年度に示した具体的な構成法以外についても、安全性を証明する手間を小さくできる。並行して、Boneh、Boyen、Goh が 2005 年に提案した階層型 ID ベース暗号に基づく構成法も示した。

ここまでの成果により、検索可能者や条件を暗号文作成時に指定可能とすることを達成した。しかし、指定可能なのは暗号文作成時のみであり、その後、動的に検索可能者を変更することはできない。そこで、別途信頼がおけるサーバを設け、トラップドアを変換可能とする方式の構築も行った。これにより、暗号文作成時ではなく、検索の実行時に動的に検索可能者を変更可能となる。第三者（サーバ）を複数用いるという点では前年度までの研究と同じだが、サーバごとに役割を異なるものとするアプローチを採用した。具体的には、トラップドアを得て変換を行うサーバと、検索を実行するサーバを設けた。ここで、各サーバの結託可能性などを検討し、現実的な状況で考慮すべき結託に対して安全性を有することを目的とし、モデルと安全性要件を明確化した。

構成においては、代理再暗号の技術を利用した。代理再暗号では一般に暗号文を変換する。代理再暗号と組みあわせた検索可能暗号はいくつか知られているが、検索可能者を変更する場合はサーバに蓄積された全てのタグを変換する必要がある。提案法では、トラップドアのみを変換することとし、タグを変換しないアプローチを採用した。この結果、システム全体での計算量の抑制が期待できる。そして Boneh、Di Crescenzo、Ostrovsky、Persiano が 2004 年に提案した、RFC5091 で取り上げられている ID ベース暗号（BF 方式）と密接な関連がある、検索可能暗号に基づく具体的な構成方法を示した。なお、検索可能者の変更を許可するサーバにより動的に検索可能者を変更できる方式であるので、同サーバにより検索可能者の失効管理も実現できることに本方式の特徴がある。

さて、本研究で提案した方式においては、秘密分散共有法が重要な要素技術となる。本研究においていくつかの提案を行ったが、いずれも何らかの形で秘密分散共有法を利用している。本研究では、広く知られている Shamir の秘密分散法（(k、n) 閾値法）を拡張した、Tassa の階層型秘密分散法に対しての高速化も検討した。Tassa の方式は有限体上で機能するが、標数が小さい場合は階層に関する制限が生じる場合がある。本研究では、高速化を視野に入れて、標数が小さい場合の有限体上での高速化に関する研究を行い、特定の階層構造に適用可能な方式を提案するとともに、実装し、その性能評価結果を示した。

以上、3 年間の研究において、検索可能暗号における既存のモデルの整理の後、検索可能者（すなわち復号可能者）や検索条件を柔軟に設定可能にするための機能付加に関する成果を得た。同様の方式はいくつか知られているが、提案方式は複数サーバを用いるモデルであるものの様々な機能拡張を達成し、暗号文サイズや処理性能等についても遜色ない。また、検索可能者を動的に変更可能とする方式、及び失効機能についても提案した。更に、これらの方式に関連する秘密分散共有法の高速化についての一定の成果も得た。これらの成果により、暗号化データをクラウド上に配置するというサービスの利便性とセキュリティの向上等に寄与できたと考えている。

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 Koji Tomida, Hiroshi Doi, Masami Mohri, Yoshiaki Shiraishi, Ciphertext Divided Anonymous HIBE and Its Transformation to Identity-Based Encryption with Keyword Search, Journal of Information Processing, 査読あり, Vol.23, No.5, pp.562-569 (2015). DOI:10.2197/ipsjjip.23.562

〔学会発表〕（計５件）

① 島幸司, 土井洋, 標数 2 の有限体上の ({1,k},n)階層的秘密分散法の研究, 情報処理学会 コンピュータセキュリティ研究会, 2016.3.2, 明治大学 駿河台キャンパス(東京都・千代田区). http://id.nii.ac.jp/1001/00157806/

② Ryo Fujita, Takeo Mizuno, Hiroshi Doi, Shigeo Tsujii, Proxy Trapdoor-Re-Generation Scheme in Public Key Encryption with Keyword Search - Realization of Provably Secure Organizational Cryptosystem, 2016 年暗号と情報セキュリティシンポジウム SCIS2016, 2016.1.20, ANA クラウンプラザホテル熊本ニュースカイ(熊本県・熊本市).

③ 島幸司, 土井洋, 階層的秘密分散法の高速化に関する研究, コンピュータセ

キュリティシンポジウム CSS2015, 2015.10.23, 長崎ブリックホール(長崎県・長崎市).
http://id.nii.ac.jp/1001/00146934/

④ Koji Tomida, Hiroshi Doi, Masami Mohri, Yoshiaki Shiraishi, A Transformation from Attribute-based Encryption to Associative Searchable Encryption by Using Hash Function, 電子情報通信学会 情報通信システムセキュリティ研究会, 2015.3.4, 名桜大学(沖縄県・名護市).

⑤ 冨田幸嗣, 土井洋, 毛利公美, 白石善明, 暗号文分割型の ID ベース検索可能暗号の構成, コンピュータセキュリティシンポジウム CSS2014, 2014.10.23, 札幌コンベンションセンター(北海道・札幌市).
http://id.nii.ac.jp/1001/00106571/

〔図書〕(計　　件)

〔産業財産権〕
○出願状況(計　　件)

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況(計　　件)

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
土井　洋　(DOI, Hiroshi)
情報セキュリティ大学院大学・情報セキュリティ研究科・教授
研究者番号：７０３３８６５６

(2)研究分担者
(　　)

研究者番号：

(3)連携研究者
(　　)

研究者番号：