科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　　３　日現在

機関番号：　１２１０２
研究種目：　若手研究(B)
研究期間：　2011～2013
課題番号：　２３７０００２１

研究課題名（和文）分散環境に適した効率的な暗号データ共有法の研究

研究課題名（英文）Research on how to share encrypted data in a distributed setting

研究代表者
西出　隆志（Nishide, Takashi）

筑波大学・システム情報系・准教授

研究者番号：７０５７０９８５

交付決定額（研究期間全体）：（直接経費）　　2,000,000円、（間接経費）　　600,000円

研究成果の概要（和文）：クラウドコンピューティング環境はデータの共有を容易にし，高い利便性を持ったデータアクセスを実現する．しかしそのトレードオフとして，外部の管理組織へデータをアウトソースすることから，秘密情報の漏えいというデータの安全性への懸念が常に存在することになる．本研究では公開鍵暗号技術の更なる発展技術である属性ベース暗号や検索可能暗号などを利用し，更に改良することで，安全かつ実用的なクラウドコンピューティング環境の実現に取り組んだ．

研究成果の概要（英文）：Cloud computing is useful because it enables us to easily share important data. However, as its tradeoff, we are faced with the risk of information leakage because we outsource our data to a third party. In this work, we utilize and improve the advanced cryptographic techniques such as attribute-based encryption and searchable encryption to realize secure and practical cloud computing environments.

研究分野：　情報学

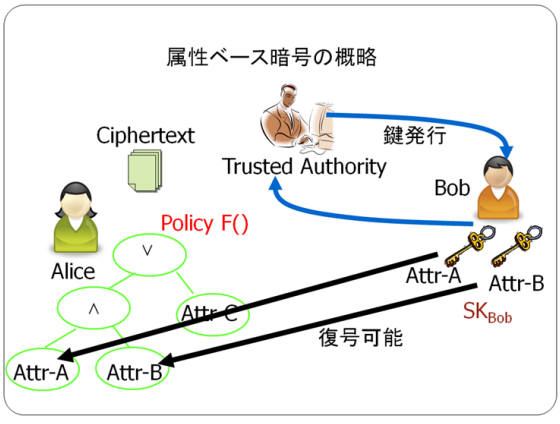
科研費の分科・細目：　情報学基礎

キーワード：　暗号技術　情報基礎　クラウド　ファイル共有

１．研究開始当初の背景

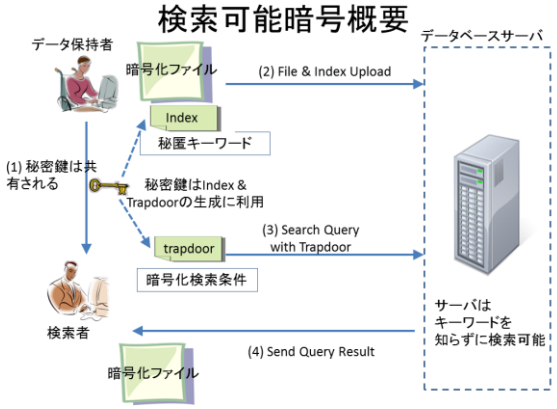
公開鍵暗号の研究において，楕円曲線上の数学構造に基づいたペアリングと呼ばれる演算を用いたペアリングベース暗号が活発に研究されている．特にペアリングベース暗号の中でも関数型暗号，述語暗号，属性ベース暗号と呼ばれる技術は，従来の公開鍵暗号では容易に実現できなかった一対多の暗号を容易な鍵管理と共に実現できる．そのため分散ネットワーク環境での暗号データの共有に適しており，今まで不可能だった様々なサービスの実現が期待されている．ここで一対多の暗号とは，ある公開鍵で暗号されたデータを復号できる秘密鍵が複数存在できることである．例えば述語暗号の一つである内積暗号では暗号文と秘密鍵にそれぞれベクトルが関連付けされて生成され，暗号文のベクトルに対し内積が 0 となるようなベクトルと関連付けられた秘密鍵であればどのようなベクトルでも復号可能ということを実現できる．

特に本研究で扱った属性ベース暗号は，従来オペレーティングシステムのような仕組みで実現されてきたロールベースアクセス制御を，ソフトウェアに頼ることなく，暗号技術そのもので実現する技術であり，クラウド/インターネット分散環境のような単一のクライアント環境を想定できない状況で有用な技術である．また属性ベース暗号はアメリカ国立標準技術研究所(NIST)でも標準化が検討されており，次世代の新暗号技術として実用化に向けた動きが活発になりつつある．また検索可能暗号と呼ばれる技術はクラウドストレージに暗号化したデータを置いた際に困難となる検索処理を，データを復号することなく，実現しようとする試みであり，安全性と利便性の共存が求められる環境において必須の技術である．



２．研究の目的

クラウドコンピューティング環境はデータの共有を容易にし，高い利便性を持ったデータアクセスを実現する．しかしそのトレードオフとして，外部の管理組織へデータをアウトソースするということから，秘密情報の漏



えいというデータの安全性への懸念が常に存在することになる．またクラウド環境への攻撃者の侵入事例をゼロにすることは現実では困難であり，こういった攻撃は起きうるという前提で安全なシステム構築をしていくことが求められている．

これまでに属性ベース暗号や検索可能暗号に関する研究が活発に進められているが，より柔軟な現実のシステムを設計するには既存の技術にはまだ課題が多く残されている．そこで本研究では公開鍵暗号技術の更なる発展技術である属性ベース暗号や検索可能暗号などを利用し，更に改良することで，安全かつ実用的なクラウドコンピューティング環境を実現することを目的としている．

３．研究の方法

安全性を高めたクラウドストレージの実用化に向けて，既存研究で不足している点として以下の内容に注目し，研究を促進していく．

(1) 暗号データに対するアクセス制御と検索機能の同時実現
暗号化にはアクセス制御を意識した属性ベース暗号によるものを想定し，この事実を利用することで暗号データへの検索処理の効率化ができないか検討する．

(2) 検索機能の拡張
指定したキーワードに完全に一致しない場合でも，検索ヒットが求められる場合もありうる．そのためキーワードの完全一致以外にも対応した検索可能暗号について検討する．

(3) 属性ベース暗号における鍵失効機能
実世界でのクラウドストレージの運用を考えた場合，鍵失効機能が必須と考えられる．特に複数鍵発行機関が存在する属性ベース暗号において，鍵失効機能を実現する手法について検討する．

４．研究成果

本研究活動では属性ベース暗号や検索可能暗号の実用化による安全なクラウドコンピューティング環境の実現に向けて，更に求め

られる機能性，安全性，効率性の向上を行った．

(1)まず暗号データに対するアクセス制御と検索機能の同時実現について述べる．
クラウドコンピューティング環境においてデータをクラウドストレージに保存する場合，機密データを含む場合には暗号化が必須となる．また企業内などでのデータの共有を考えると，複雑な鍵管理をできるだけ排除した形でのアクセス制御も必須となる．既存研究においては暗号データへの検索手法と，効率的な鍵管理を含めたアクセス制御手法は独立して検討されることが多かったが，本研究成果の一つではこれら検索とアクセス制御を同時に考慮した暗号クラウドストレージの検討を行った．また実社会での利用を考えたとき，一度アクセス権限を得た利用者の異動などによる権限の失効も対応しておく必要がある．本提案では利用者の権限失効の必要性にも注目し，失効時にも膨大なデータの再暗号化を必要とせず，また暗号データに対する検索とアクセス制御を効率的に達成する方式を実現した．
効率化におけるアイディアとして，アクセス制御情報をクラウドサーバ側で活用し，データ検索者が復号可能な暗号データのみを検索対象暗号データとすることで，処理が実用的なレベルまで効率化できうることを示した．ここでは暗号基礎技術の個々の独立した検討だけでなく，実システム運用を考慮したうえで，それらをどのように適切に組み合わせ，利便性と効率を同時に実現するかに焦点を置いた．またこの提案によって，実用化において必要と考えられる Read 権限と Write 権限を持つ利用者が混在するクラウドストレージ環境を容易に扱うことができる．ここではそのような環境において，属性ベース暗号と，更に属性ベース署名と呼ばれる(属性ベース暗号の署名版)技術を用いて認証を行い，Write 権限のある利用者のみがファイルの更新をできる仕組みを提案している．

(2)次に暗号データに対する検索機能の拡張について述べる．
通常，データが暗号化された場合，クラウドストレージサーバにデータ検索させることは困難となる．その解決策として本研究では暗号化されたデータに対してもキーワード検索可能な検索可能暗号の提案を行った．特にここでは共通鍵暗号に基づく検索可能暗号を扱った．提案方式では暗号化されたファイルと共にファイルの内容に関連する複数のキーワードを添付してクラウドストレージに保存する手法を用いている．この保存の際に暗号化ファイルに関連付けられるキーワードは，Bloom Filter と呼ばれるデータ構造を用いて文字毎に区切った形で Bloom Filter に格納する．また Bloom Filter で用いるハッシュ関数として，暗号データを共有する利用者らの間で共有されている秘密鍵を用いた鍵付ハッシュ関数を使用する．暗号データに対するキーワード検索を行う利用者は，キーワードに対応する Bloom Filter のデータを作成し，クラウドストレージサーバに送信することで，クラウドストレージサーバは指定されたキーワードの中身を知らずに検索し，検索ヒットした暗号データを検索者へ返すことが可能となる．また提案方式の安全性解析では検索キーワードを推測しようとする攻撃者の挙動をモデル化し，そのモデルにおいて鍵付ハッシュ関数がランダム関数と識別困難であるとの仮定の下で提案方式の安全性を示した．既存方式の多くが固定キーワード検索のみをサポートしていたことに対し，暗号データに対する類似キーワード検索も可能とした点が既存研究との違いとして挙げられる．また提案手法をタブレットなどのモバイルデバイス上でウェブアプリケーションとして実装し，性能測定も行い，それらの測定結果から提案手法が実用上，問題ないレベルで実行可能であることを確認した．
また検索可能暗号の安全性評価をさらに確実なものとするために，検索可能暗号への攻撃手法についても検討を進めた．特に検索可能暗号の既存の安全性モデルを超えた攻撃手法の可能性について検討を行った．従来の検索可能暗号の複数の安全性モデル(例 IND-CKA モデル)の中では，頻度解析と呼ばれる攻撃手法は考慮範囲外であった．頻度解析とは攻撃者が，キーワードがどのような頻度で文書に存在するかを事前に知っているという前提で，検索結果から，秘密にされているキーワードを推測する攻撃のことである．より強力な攻撃者を想定したとき，このような頻度解析が現実の脅威となりうることは十分に考えられる．そこで既存の検索可能暗号方式が我々の想定する頻度解析攻撃に対して，どの程度耐性を持ちうるか実装実験などを通して評価を行った．またこの攻撃手法を，Bloom Filter を用いた我々の提案方式にも適用し，どの程度攻撃が成功するのか，またどのようにすれば攻撃を回避できるのかについても検討を行った．調査の結果，ある程度の偽陽性を許容することで頻度攻撃を回避できることが分かった．ここで偽陽性とは本来，指定したキーワードの検索結果として含まれるべきでないものまでもが検索結果に(ある種のノイズとして)含まれてしまうことである．これは通常は望ましくはないが，検索結果に少量の余分なノイズが入ることは実際の利用の中では許容可能範囲であると考えられるため，安全性と性能のトレードオフとして捉えることができる．

(3)次に属性ベース暗号における鍵失効機能について述べる．
通常の属性ベース暗号では単一の鍵発行機関が存在し，利用者の所有する属性集合に基

づき，鍵生成を行う．しかし実際の運用では，利用者の属性を管理する機関は複数存在することが多いため，単一の鍵生成機関では実利用に適していないという問題がある．これを解決する属性ベース暗号として複数の鍵発行機関が存在可能な方式が提案されている．これらの方式に鍵失効機能を追加することでより実用的なシステムの構成が可能と考えられる．鍵の失効とは一度，属性に対応する鍵を鍵発行機関から与えられた利用者がある時点で，その属性を所有する権限を無くしたため，それ以降の鍵の利用を無効化することである(つまり暗号ファイルを復号するために鍵を利用できなくすることである)．このような問題に対する解決策として，複数の鍵発行機関が存在する環境での属性ベース暗号の利用を想定し，クラウドストレージ利用者の権限の失効手法を提案した．暗号に関する鍵を所有していても失効処理を行うことで復号機能を停止する機能は企業などでの利用者の異動や一時的な権限の付与に有用であり，提案方式ではクラウドストレージでの再暗号不要な方式を実現した．提案方式では時刻情報もファイル暗号の際に用いる属性情報として利用し，さらに二分木のデータ構造で管理することで鍵の失効機能を実現できることを検証した．また時刻情報に基づく鍵の失効だけでなく，利用者の名前に基づく鍵の失効機能も取り入れて設計を行った．しかし提案方式には安全性の検証や，公開鍵情報量の削減など，更なる改善の余地があるため，今後も研究を続ける計画である．

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　6 件）

① Fangming Zhao, Takashi Nishide, and Kouichi Sakurai, ``Fine-Grained Access Control Aware Multi-User Data Sharing with Secure Keyword Search,'' IEICE Transactions on Information and Systems, 査読有, 2014, (掲載決定).

② Takanori Suga, Takashi Nishide, and Kouichi Sakurai, ``Character-based Symmetric Searchable Encryption and Its Implementation and Experiment on Mobile Devices,'' Wiley Security and Communication Networks, DOI: 10.1002/sec.876, 査読有, 2013.

③ Takanori Suga, Takashi Nishide, and Kouichi Sakurai, ``Secure Keyword Search Using Bloom Filter with Specified Character Positions,'' 6th International Conference on Provable Security (ProvSec), LNCS 7496, pp.235-252, Springer-Verlag, 査読有, 2012.

④ Fangming Zhao, Takashi Nishide, and Kouichi Sakurai, ``Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control,'' 14th Annual International Conference on Information Security and Cryptology (ICISC'11), LNCS 7259, pp.406-418, Springer-Verlag, 査読有, 2012.

⑤ Fangming Zhao, Takashi Nishide, and Kouichi Sakurai, ``Realizing Fine-grained and Flexible Access Control to Outsourced Data with Attribute-based Cryptosystems,'' 7th Information Security Practice and Experience Conference (ISPEC), LNCS 6672, pp.83-97, Springer-Verlag, 査読有, 2011.

〔学会発表〕（計　9　件）

① Takashi Nishide, ``Toward Revocation Mechanism for Multi-Authority CP-ABE,'' 暗号と情報セキュリティシンポジウム(SCIS), 5pages, 京都, 1 月 24 日, 2013.

② 菅孝徳, 西出隆志, 櫻井幸一, ``検索可能暗号に対する頻度分析攻撃実験,'' 暗号と情報セキュリティシンポジウム(SCIS), 5pages, 石川, 2 月 1 日, 2012.

③ Fangming Zhao, Takashi Nishide, Kouich Sakurai, ``Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control,'' コンピュータセキュリティシンポジウム(CSS), 6pages, 新潟, 10 月 20 日, 2011.

④ 菅孝徳, 西出隆志, 櫻井幸一, ``ブルームフィルタを用いた検索自由度の高い検索可能暗号の設計と実装評価,'' 第 53 回コンピュータセキュリティ研究発表会(CSEC), 6pages, 福岡, 5 月 13 日, 2011.

⑤ Fangming Zhao, Takashi Nishide, and Kouichi Sakurai, ``Achieving Fine-grained and Flexible Access Control to Outsourced Data with Attribute-based Cryptosystems,'' 暗号と情報セキュリティシンポジウム(SCIS), 8pages, 福岡, 1 月 27 日, 2011.

６．研究組織
(1)研究代表者

西出 隆志 (NISHIDE TAKASHI)
筑波大学・システム情報系・准教授
研究者番号：70570985