検索可能暗号を適用したデータベースに対する鍵失効方式と検索性能向上方式の研究

（課程博士・様式７）（Doctoral qualification by coursework,Form 7）

学 位 論 文 要 旨

Abstract of Doctoral Thesis

専　　攻：　情報科学専攻　　氏　名：　松田 規
Course：　　Name：

論文題目：
Title of　Thesis：
検索可能暗号を適用したデータベースに対する鍵失効方式と検索性能向上方式の研究

論文要旨：
Abstract：

近年、サービスの早期立ち上げのため、また企業の IT コスト低減のため、クラウドサービスを活用することが当たり前になりつつある。このような状況はさらに広がりを見せつつあり、これまでは一企業がクラウドを活用するケースが主流であったが、複数企業でクラウド上のデータを共同利用するケースへとニーズが拡大しつつある。このようなユースケースにおいて、情報漏洩などのリスクを低減するためには高安全なクラウドサービスの実現が必要となるが、その解決策の一つがデータ暗号化である。

この用途に適した暗号方式として、関数型暗号や検索可能暗号が挙げられる。関数型暗号は、データ暗号化の際に「A 部 and (部長 or 課長)」のように所属などの属性による論理式で復号できるユーザの条件を指定でき、その属性に合致する復号鍵を持ったユーザだけが復号可能となる暗号方式である。そのため、機密度や公開範囲の異なる様々なデータを扱う企業がクラウドサービスを利用する際に都合が良く、さらに暗号化データ自身がアクセス制御の仕組みを持つため、情報漏洩のリスクを大きく低減できる技術として期待されている。また、検索可能暗号は、暗号化によりキーワードを秘匿して保護するとともに、復号を行うことなくキーワードの一致・不一致の判定ができる暗号方式である。多くの暗号化データが蓄積されると目的のデータがどれかが分からなくなるという状況を解決することができるため、セキュリティの確保に加えて利便性も確保できる。

ここで１番目の課題は、関数型暗号において、ユーザの属性が変わったときに、すでに発行している復号鍵を確実に消去しないと復号権限を削除（失効）できないという点が挙げられる。既存研究でも様々な解決方式が提案されているが、失効に伴うクラウド側の処理量が多い方式や、暗号として理想的な adaptive-secure な安全性証明が付与されていない方式などが多く、効率と安全性の両立に関して課題が残されている。２番目の課題は、検

索可能暗号において暗号化キーワードからは一般のデータベースが実施しているような索引生成ができないため、検索時にすべての暗号化キーワードに対して一致判定処理を行う必要が生じてしまい、データ件数に比例した処理時間を要する点が挙げられる。同時に、グループ共有やデータベースへの組み込み方式の確立も課題となる。既存研究では、誰でも検索ができるという現実的でない安全性の緩和を行うことで実現を図った方式が提案されているのみであり、十分な安全性と実用性を持った方式は提案されていない。

そこで本研究では、企業間での情報共有に適した検索可能暗号データベースの実現のため、上記にて示したユーザ秘密鍵失効と検索性能という課題の解決を行った。具体的には、下記の２つの実現方式を提案し、安全性評価、プロト実装や性能評価を実施した。

1. ユーザ秘密鍵失効方式

既存の失効方式として、①有効期限を付与して自然失効させる方式、②復号鍵や暗号文を更新して復号権限を削除する方式、③プロキシーを活用してユーザ秘密鍵の失効を管理する方式、を比較し、方式③のアプローチが最もシステム適用時の負荷が少ないことを示した。方式③を実現するため、高島らによって提案された関数型暗号をベースとして、プロキシー鍵を持ったプロキシーサーバ と、ユーザ秘密鍵を持ったユーザによる協調処理によって復号処理を実施するアルゴリズムを実現した。さらに、提案方式に対して、既存研究よりもさらに高い adaptive な状況下で安全性証明を付与した。

2. 検索性能向上方式

k 匿名性のアイデアを検索可能暗号に融合することで、暗号化キーワードからユーザが指定したビット数の索引値をサーバが取得できるアルゴリズムを実現した。この索引値で索引を生成することで、検索の高速化を実現した。また、既存の識別不可能性の定義を緩和し、ユーザが指定した索引値以上の情報が漏れないことを定式化した安全性モデルを定義し、そのモデルにおいて提案方式の安全性を証明した。同時に、内積述語暗号を用いて階層型 ID に基づく検索可能暗号を実現することで、任意の ID にマッチするワイルドカードを実現できることも示した。この仕組みにより、検索できるユーザが一人ではなく、同じグループに属するユーザが誰でも検索できるグループ共有機能の実現を行った。さらに、実現した索引生成の仕組みを一般的なデータベース上にて実装し、性能評価によって索引値のビット数に応じて検索性能が向上することを明らかにした。

上記の成果により、企業機密や個人情報をクラウドサービスに保管する場合でも、情報漏洩のリスクを大きく低減することができ、さらに検索性という利便性を確保することができるクラウドベースのファイル共有サービスが実現できる。そのため、これまでクラウド活用を躊躇していた医療情報や金融情報などの機密度の高い情報を扱う分野でもクラウド活用が広く進められるようになると考えている。