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９）　　審　査　要　旨

専攻　情報科学専攻　　学籍番号　５５９４５０１２　　学生氏名　　松田　規

論文題目　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

クラウドサービスの活用が広まりつつあるが、その情報漏洩対策としてデータ暗号化が注目されている。特に、暗号化の際に復号できるユーザの条件を所属などの属性で指定できる関数型暗号や、多くの暗号化データから目的のデータを検索できる検索可能暗号の活用が期待されている。しかし、その実用化のためには、復号鍵失効や検索性能向上が必要となる。具体的には、関数型暗号では、復号鍵に復号条件を設定するため復号条件が変化した際に復号鍵を削除（失効）する必要があり、また、検索可能暗号では、暗号化したタグ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処理が低速であることから、データ件数に比例して増加する処理時間を削減する必要がある。

本研究では、プロキシーサーバとユーザが連携して暗号化データを復号する仕組みをとることで、プロキシーサーバ側の鍵を消去することで鍵失効を実現するとともに、既存研究よりも高い安全性モデルである adaptive 状況下で安全性の証明を実施している。また、検索可能暗号については、k-匿名化のアイデアを活用し、安全性と高速性のバランスをユーザ自身がコントロールできる仕組みを提案するとともに、検索権限の複数ユーザでの共有や、リレーショナルデータベースへの組み込み方式を提案している。

第１章は序論であり、本研究の背景と目的について述べている。

第２章では、関連研究および既存研究を、関数型暗号の高機能化や安全性証明の発展、検索可能暗号の高機能化や高速化などの観点から説明している。

第３章では、鍵ポリシー型および暗号文ポリシー型の関数型暗号に関して、復号鍵失効を実現するアルゴリズムを提案し、システム上でのデータフローを提示している。提案方式は、既存研究よりも高い安全性モデルである adaptive 状況下で安全性が付与可能であるとともに、システム全体の計算量が増加しない効率性も達成したことが示されている。

第４章では、検索可能暗号の高速化、検索権限のグループ共有、リレーショナルデータベースへの組み込み方法について提案している。既存研究では実現できていなかった、安全性と高速性のバランスをユーザ自身がコントロールすることを可能としている。また、検索性能の評価を通じ、提案方式の効果も示されている。

第５章では、本研究をまとめるとともに、本研究の研究成果を活かした今後の展望について述べている。

以上のように、本論文は、クラウド活用におけるデータの機密性を関数型暗号や検索可能暗号を用いて保護する先進的かつ実用的なアルゴリズムやシステム構成を提案するとともに、性能評価による有効性を実証しており、情報工学の発展に寄与するところが大きい。よって、本論文は博士（工学）の学位論文としてふさわしいものと認められる。

（１，０００字程度）