氏　名（本籍）	ハサン アブドウレラ サレー カーデム（バーレーン）
学位の種類	博　士（工　学）
学位記番号	博 甲 第 5679 号
学位授与年月日	平成 23 年 3 月 25 日
学位授与の要件	学位規則第 4 条第 1 項該当
審査研究科	システム情報工学研究科
学位論文題目	**A Study on Privacy Preserving Query Processing for Relational Databases on the Internet** （インターネット上のリレーショナルデータベースに対するプライバシを保護した問合せ処理に関する研究）

主　査	筑波大学教授	理学博士	北 川 博 之
副　査	筑波大学教授	博士（理学）	加 藤 和 彦
副　査	筑波大学教授	博士（工学）	李　　頡
副　査	筑波大学教授	工学博士	岡 本 栄 司
副　査	筑波大学准教授	博士（工学）	天 笠 俊 之

論 文 の 内 容 の 要 旨

インターネットの普及と情報化社会の浸透に伴い、情報セキュリティ、情報プライバシの重要性が急速に増している。特に、近年注目されているクラウド環境では、データベースがインターネット上に配置されるため、セキュリティやプライバシの確保が一層困難になる。

このような背景を受け、本研究ではインターネットからアクセス可能なリレーショナルデータベースを対象としたプライバシ保護検索に関する研究を行った。主な貢献は以下の通りである。

1. 複数のクライアントが存在するインターネット上のリレーショナルデータベースを対象とした新たなセキュリティモデル（MCDB：Mixed-Cryptography Database）を提案した。このモデルでは、複数のクライアントが存在する状況において、データベースの各カラムをクライアントが独自の秘密鍵で暗号化することを許す。これによって、データベースサーバが攻撃者によって攻撃されたとしても、各クライアントの持つカラムは安全である。また、信頼できる第三者のコーディネイトによって、複数のクライアントが協調動作することにより問合せ処理が可能となる。
2. リレーショナルデータベースの数値属性を対象とした新たな暗号化方式 MV-OPES（Multivalued Order-Preserving Encryption Scheme）を提案した。既存の暗号化方式である順序保存暗号化法（OPES；Order-Preserving Encryption Scheme）は、数値の大小関係を保存したまま数値を別の分布に写像することにより、暗号のまま問合せ処理が可能な技術である。しかしながら、一つの値が必ず別の一つの値に写像されるため、頻度に基づく攻撃により容易にセキュリティを破られるという問題があった。このため、本研究では、一つの値をある一定の範囲内の任意の値にランダムに写像する手法を提案した。値の大小関係は保存されているものの、一つの値が複数の値に写像されるため、オリジナルの OPES の欠点は克服される。さらに、MV-OPES では、複数の関係表の結合演算やその他の多くの関係演算を実現可能である点が特徴である。

3. MV-OPES は OPES に比べて安全ではあるものの、暗号文の大域的な順序が保存されているため、統計量に対する攻撃では、セキュリティが破られる可能性がある。このため、数値属性の定義域をいくつかのパーティションに分割し、そのパーティションの順序を入れ替えることにより、さらに安全性を高めた MV-POPES (Multivalued-Partial Order Preserving Encryption Scheme) を提案した。パーティションの順序がランダムになるため、問合せ性能が従来手法 (MV-OPES) に比べて落ちてしまうが、パーティションの順序入れ替えを制御することにより、性能が改善することを示している。

審 査 の 結 果 の 要 旨

情報セキュリティおよび情報プライバシは、今日の情報システムにおいて最も重要な要素である。本研究は、インターネット上に配置されたリレーショナルデータベースにおける、プライバシを考慮した新たな分散問合せモデルと暗号化法を提案しており、その有用性は極めて高いと言える。また、MV-OPES、MV-POPES について詳細なセキュリティの分析を行っており、当該分野における大きな貢献が認められる。今後は、数値以外の属性への対応など、残された課題への取組みが期待される。

よって、著者は博士（工学）の学位を受けるに十分な資格を有するものと認める。