第５号様式

論文審査の要旨

博士の専攻分野の名称	博　士　（　学術　）	氏名	MAHBOOB QAOSAR
学位授与の要件	学位規則第４条第[1]・２項該当		

論　文　題　目

Study on Privacy-preserving Multi-party Computation of Skyline and its Variants
（スカイライン問合せ及びその関連問合せに関する個人情報保護に配慮したマルチパーティ計算手法の研究）

論文審査担当者

主　　査	教　授	森本　康彦	印
審査委員	教　授	中西　透	印
審査委員	教　授	江口　浩二	印

〔論文審査の要旨〕

各組織が蓄積したデータベースを結合させて分析することが重要であることは広く認知されている．例えば，各病院で行われた医療情報を広く共有し，結合した巨大なデータベースには計り知れない分析価値がある．しかし，各組織がその組織が保持しているデータベースを他者と共有し分析することは個人情報保護の観点から実際には抵抗が大きくあまり進んでいない．本研究は，各組織が持つデータベースを結合させた巨大データベースから得られる知見を，実際に個々の組織のデータを共有，開示することなく得るための基礎技術で，それを利用することで価値の高いデータベースの接合と利活用が進むことが期待できる．

第１，２章では，上述の問題の背景，問題の定式化，関連研究のサーベイ及び未解決課題について述べている．

データベース中のデータの中で，何らかの属性値で他のデータに比べ良いか等しいものを含むデータを列挙する機能を「スカイライン問い合わせ」と呼び，数多くのデータ分析で利用されている．第３章では，このスカイライン問合せを，複数の組織が個々に管理・保持しているデータベースの，結合データベースに対して効率的，かつ，機密を漏洩させずに計算する手法を，完全準同形暗号技術を利用して実現する方法について述べている．

第４章では，スカイラインの関連問合せの１つである「スカイバンド問合せ」について述べている．一般的なスカイライン問合せが，他のデータに劣っていないデータ全てを取り出す問合せであるのに対して，スカイバンド問合せは，ユーザが指定した整数 K に対し，K 個以上の他のデータに劣っていないデータを全て取り出す．言い換えれば，K スカイバンド問合せで取り出されるデータは，そのデータより良いデータが最大 K-1 個

存在するかもしれない．この問い合わせは，一般のスカイライン問合せより多くの候補を取り出したい場合に使用される．スカイライン問合せと機能は似ているが，その機能を機密を漏洩せずに計算するためには独自の秘密計算プロトコルを使用する必要があり，筆者はそれをこの章で提案している．

第５章では，スカイラインの関連問合せの１つである「トップ k 支配問合せ」について，その秘密計算手法とともに述べている．あるデータ X が他のデータ Y より優れている場合，X が Y を支配していると言う．トップ k 支配問合せとは，より多くのデータを支配するデータを上位 k 個取り出す問合せである．

最後に，第５章で各提案手法の意義と今後の課題についてまとめている．

口頭試問において，審査委員から，マルチパーティとして何組織まで効率的に計算できるかなど，スケーラビリティやプロトコルの正しさに関してのいくつかの質問があり，筆者はそれぞれに対し，的確かつ丁寧に回答することができた．

以上，審査の結果，本論文の著者は博士（学術）の学位を授与されるに十分な資格があるものと認められる．

備考：審査の要旨は，1,500 字以内とする。