Secure Cloud Computing via Fully Homomorphic Encryption

著者	陸 文杰
発行年	2019
その他のタイトル	完全準同型暗号によるセキュアクラウドコンピューティング
学位授与大学	筑波大学 (University of Tsukuba)
学位授与年度	2018
報告番号	12102甲第8999号
URL	http://hdl.handle.net/2241/00156986

氏　名	陸　文杰
学位の種類	博　士（　工学　）
学位記番号	博　甲　第　８９９９　号
学位授与年月日	平成　３１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	Secure Cloud Computing via Fully Homomorphic Encryption (完全準同型暗号によるセキュアクラウドコンピューティング)

主　査	筑波大学　教授	博士（工学）	佐久間 淳
副　査	筑波大学　教授	博士（工学）	天笠 俊之
副　査	筑波大学　教授	理学博士	北川 博之
副　査	筑波大学　准教授	博士（情報科学）	面 和成
副　査	筑波大学　准教授	博士（工学）	西出　隆志
副　査	東京大学　准教授	博士（工学）	國廣 昇

論　文　の　要　旨

審査対象論文は、準同型暗号を用いた内積計算をベースとした様々な統計解析・機械学習の非対話的な秘密計算について、その計算・空間・帯域の効率性を向上させるための暗号理論上の手法やアルゴリズムについて検討している。

第１章では、準同型暗号を用いた秘密計算の背景と対象論文の貢献を説明している。

第２章では、対象論文に必要となる技術的背景を説明している。

第３章では、準同型暗号を用いた高次元ベクトル同士の内積計算の高速化と、そのゲノム疫学への応用について記述している。

第４章では、準同型暗号を用いた行列同士の積計算の高速化と、その記述統計・予測統計への応用について記述している。

第５章では、準同型暗号を用いた行列同士の積計算について、低帯域なネットワークにおける高速化と並行実行時の効率性の改善について記述し、準同型暗号を用いたニューラルネットワークによる推論への応用について記述している。

第６章では、準同型暗号を用いた値同士の非対話的な比較演算とその応用について記述している。

第７章では、準同型暗号を用いた内積計算について、条件に応じた計算の効率化について、これまでの議論を総括している。

審査対象論文は、特に準同型暗号を用いた内積計算について、様々な計算条件に適した、平文の暗号文への詰め込み方（パッキング手法）を考案しその効率性を実験的に評価している。

審　査　の　要　旨

【批評】

審査対象論文は、信頼できないクラウドサーバ上での安全な計算、特にデータ解析を行う上で重要な内積計算を効率化する３つのプロトコルの設計と開発を行っている。

一つ目は、高次元ベクトルの内積の効率化に関する工夫であり、定数レベルでの改善であるが、数千次元のベクトル同士の場合には数千倍の高速化が達成され、実用上のメリットは大きいと評価できる。特に、ゲノム疫学における統計的検定の秘密計算では、実用規模のゲノムワイド関連性解析の秘密計算を現実的な計算時間で達成できることを示したことは高く評価できる。

二つ目は、繰り返しの行列計算を可能にする準同型暗号のパッキングに関する工夫である。従来法では一度しか実行できなかった暗号文同士の行列計算を繰り返し可能にした。またこのような工夫を用いて、様々なタイプの記述統計や予測統計の安全なアウトソーシングを実現した。高次元な線形回帰の非対話的なアウトソーシングは世界初であり、その有用性は高く評価できる。

三つ目は、多数の計算能力の低いクライアントとサーバの間の準同型暗号を用いた内積計算のアウトソーシングの効率的な実行方法を提案している。深層学習など計算負荷の高い機械学習の予測サービスにおける秘密計算の導入可能性を示唆しており、その有用性は高く評価できる。

審査対象論文は、内積計算という統計解析・機械学習においてファンダメンタルな計算に着目し、様々な条件下で準同型暗号を用いた内積計算を効率的に実現する方法について提案し、実用規模の統計解析・機械学習の秘密計算を非対話的なアウトソーシングにより実現する手段を見出しているという意味において、学術的に高く評価できる。

【最終試験の結果】

平成 31 年 1 月 30 日、システム情報工学研究科において、学位論文審査委員の全員出席のもと、著者に論文について説明を求め、関連事項につき質疑応答を行った。その結果、学位論文審査委員全員によって、合格と判定された。

【結論】

上記の学位論文審査ならびに最終試験の結果に基づき、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。