論文 / 著書情報
Article / Book Information

題目(和文)	
Title(English)	Constructions for Multi-Party Computation Based on Secret Sharing and Homomorphic Encryption
著者(和文)	盧儀
Author(English)	Yi Lu
出典(和文)	学位:博士(理学), 学位授与機関:東京工業大学, 報告番号:甲第12833号, 授与年月日:2024年9月20日, 学位の種別:課程博士, 審査員:田中 圭介,伊東 利哉,尾形 わかは,鹿島 亮,安永 憲司
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第12833号, Conferred date:2024/9/20, Degree Type:Course doctor, Examiner:,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	審査の要旨
Type(English)	Exam Summary

（博士課程）

論文審査の要旨及び審査員

報告番号	甲第　　号		学位申請者氏名		盧　儀（Yi Lu）	
論文審査 審査員		氏　名	職　名		氏　名	職　名
	主査	田中　圭介	教授	審査員	安永　憲司	准教授
	審査員	伊東　利哉	教授			
		尾形　わかは	教授			
		鹿島　亮	准教授			

論文審査の要旨（2000字程度）

本論文は、「Constructions for Multi-Party Computation Based on Secret Sharing and Homomorphic Encryption」（秘密分散と完全準同型暗号に基づく秘匿計算）と題し、英文で全４章から構成されている。

近年のIoTの研究や社会実装の流れに伴い、ユーザの位置情報や生体情報などのライフログを利用したビッグデータに基づくクラウドサービスが提案されてきている。しかし、これらの個人データはプライバシー性が高いため、その活用にあたっては個人情報流出等の懸念も少なくない。このような現状に対して、秘匿計算と呼ばれる暗号技術が、プライバシー保護とデータの利活用を両立できる技術として注目されている。本論文では、この秘匿計算技術の中でも、「二者間の秘匿指数計算」と「マルチクライアント検証付き計算プロトコル」のそれぞれに対して、秘密分散と完全準同型暗号の構成要素に基づいた新たな構成を提案しており、効率性や利便性の観点において重要な改良に成功している。

第１章「Introduction」では、本論文の導入として、論文全体の概要として秘匿計算一般について述べるとともに、研究対象とする二つの秘匿計算技術、「二者間の秘匿指数計算」と「マルチクライアント検証付き計算プロトコル」に関するこれまでの研究を紹介している。さらに本論文で示される二つの成果について、それらの背景を説明するとともに研究動機を述べている。

第２章「Efficient Two-Party Exponentiation from Quotient Transfer」では、本章で用いられる表記や暗号技術の導入に始まり、第一の成果として、Quotient Transferと加法型秘密分散法の組み合わせに基づく、既存方式とは設計方針の異なる二者間での指数計算用の秘匿計算プロトコルの提案を行なっている。指数関数用の秘匿計算プロトコルを設計するにあたっては、これまでShamir型秘密分散法と呼ばれる技術に基づいた構成が知られていたが、得られる方式が既存の攻撃者が過半数を超える状況においても安全性を満たすような秘密計算プロトコルとの組み合わせが困難であるという欠点があった。提案方式は、この組み合わせの課題を解決するとともに、既存のどの方式よりも効率的であるという特徴をもつ。

第３章「Multi-Key Verifiable Homomorphic Encryption」では、本章で用いられる表記や暗号技術の導入に始まり、第二の成果として、マルチクライアント検証付き計算プロトコルを実現するための新たな暗号技術となる複数鍵による検証付き完全準同型暗号を提案している。この技術の導入により、これまでのマルチクライアント検証付き計算プロトコルが抱えていた実用上の大きな課題であるクライアントが行わなくてはならなかった計算を省略できる初めての構成を実現している。

第４章「Conclusion and Future Work」では、本論文のまとめと今後の課題について述べている。

以上のように、本論文は二つの秘匿計算技術、二者間の秘匿指数計算およびマルチクライアント検証付き計算プロトコルに対して、効率性や利便性の向上などを達成した新たな方式の提案、さらにはそれらの提案方式に対する安全性モデルにおける安全性証明を与えるなど多くの知見を与えており、理学上貢献するところ大である。よって、本論文は博士（理学）の学位論文として十分価値があるものと認める。