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)	論文要旨
Type(English)	Summary

（博士課程）
Doctoral Program

論 文 要 旨

THESIS SUMMARY

系・コース： Department of, Graduate major in	数理・計算科学　系 数理・計算科学　コース	申請学位（専攻分野）： Academic Degree Requested	博士 Doctor of　（　理学　）
学生氏名： Student's Name	盧 儀 (Yi Lu)	審査員主査： Chief Examiner	田中　圭介

要旨（和文 2000 字程度）
Thesis Summary（approx.2000 Japanese Characters ）

昨今の IoT 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近年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、その活用に対して懸念を示す声も多い。このような現状に対して、秘密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近年注目されている。秘密計算とは、機密性の高いデータ（カルテなどの個人情報を含む医療データなど）を持つユーザ同士が協調的に計算を行うことにより、自身の持つデータを秘匿しつつ、ユーザ同士の情報を元に得られる様々な計算結果（特定の病気に関する統計情報など）を得られる技術である。近年まではその実現性を考慮すると、秘密計算は様々な効率性（通信量、通信回数、計算コストなど）の面で課題を抱えていたが、世界中の大学や企業がこの課題の解決に取りくみ、現在ではその効率が実運用に耐えうる段階まで向上してきている。

本論文では、この秘密計算技術の中でも、「Two-party exponentiation MPC」と「multi-client verifiable computation protocol」について、それぞれ秘密分散と準同型暗号という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。

まず、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これまでとは異なる二者間での指数計算用の秘密計算プロトコルの提案を行う。指数関数用の秘密計算プロトコルを効率的に設計するにあたっては、これまでシャミア型秘密分散法と呼ばれる技術に基づいて構成が行われていたが、得られる方式が既存の dishonest-majority 安全性を満たす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、この利便性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。

次に、第二の成果として、Multi-client Verifiable Computation Protocol を実現するための新たな暗号技術となる Multi-Key Verifiable Homomorphic Encryption を提案する。この技術の導入により、これまでの Multi-client Verifiable Computation Protocol が抱えていた実用上の大きな課題である Client による関数に依存した事前計算を取り除いた初めての方式を得ることができている。本成果内では、Multi-Key Verifiable Homomorphic Encryption の実現に向けて、新たな中間的な暗号技術である Multi-Key Homomorphic Encrypted Authenticator の提案も行っており、従来の Multi-Key Homomorphic Encryption とこの暗号技術を組み合わせることで、Multi-Key Verifiable Homomorphic Encryption の構成を与えている。これらの全ての暗号技術は、耐量子性を持つ代表的な困難性仮定である Learning with Errors (LWE) 仮定の下で実現可能であることを示している。

備考：論文要旨は、和文 2000 字と英文 300 語を 1 部ずつ提出するか、もしくは英文 800 語を 1 部提出してください。
Note：Thesis Summary should be submitted in either a copy of 2000 Japanese Characters and 300 Words (English) or 1copy of 800 Words (English).

注意：論文要旨は、東工大リサーチリポジトリ(T2R2)にてインターネット公表されますので、公表可能な範囲の内容で作成してください。
Attention: Thesis Summary will be published on Tokyo Tech Research Repository Website (T2R2).

（博士課程）
Doctoral Program

論 文 要 旨

THESIS SUMMARY

系・コース： Department of, Graduate major in	数理・計算科学　系 数理・計算科学　コース	申請学位（専攻分野）： Academic Degree Requested	博士（理学） Doctor of
学生氏名： Student's Name	盧 儀 (Yi Lu)	審査員主査： Chief Examiner	田中　圭介

要旨（英文 300 語程度）
Thesis Summary（approx.300 English Words ）

The advancement of computer science has led to a proliferation of data, fundamentally altering various aspects of our lives. For instance, individuals are now interconnected with vast quantities of personal information, encompassing details such as age, citizenship, and income. This flood of data has changed how businesses operate and make choices. Some companies even leverage this data abundance to offer personalized recommendations and optimize profits based on users' digital footprints. Even though there is a huge amount of data available online for these companies and organizations to use, that doesn't mean that we do not need to think about the privacy and security of data. Actually, protecting personal information is more challenging than ever before.

To solve such privacy issues in the real world, multi-party computation (MPC) protocols have gathered attentions recently. Roughly, MPC is a novel cryptographic protocol to allow participating parties to jointly compute a function over their inputs while keeping them private. In the real world, MPC has been used in many scenarios to achieve both utility and privacy, for example, privacy-preserving data mining, privacy-preserving machine learning, secure e-auctions, and private set intersection. Especially, machine learning is increasingly becoming one of the dominant research fields, with many real-world applications such as self-driving cars, healthcare, and medicine. To build a model with good utility and accuracy, machine learning needs data from various sources. In this process, MPC can provide privacy for different organizations to share datasets with others without worrying about data being revealed.

In this thesis, we focus on two research areas on constructing specific MPC: One is secret sharing based Two-party Exponentiation MPC and the other is homomorphic encryption based multi-client verifiable computation.

Specifically, as the first result, we propose a new public base exponentiation protocol without bit-decomposition based on additive secret sharing. Our protocol is based on a new simple but efficient approach involving quotient transfer that allows the parties to perform the most expensive part of the computation locally. Our protocol requires 3 rounds and 4 invocations of multiplication.

Then, as the second result, as a core cryptographic primitive for private and verifiable delegating computations in the multi-user setting, we propose multi-key verifiable homomorphic encryption (MVHE). In order to obtain an MVHE scheme, we also propose a new notion of multi-key homomorphic encrypted authenticator (MHEA), which is a multi-key variant of homomorphic encrypted authenticator (HEA). We show that an MVHE scheme can be constructed by combining a multi-key homomorphic encryption (MHE) scheme and an MHEA scheme.

備考 ： 論文要旨は、和文 2000 字と英文 300 語を 1 部ずつ提出するか、もしくは英文 800 語を 1 部提出してください。
Note : Thesis Summary should be submitted in either a copy of 2000 Japanese Characters and 300 Words (English) or 1copy of 800 Words (English).

注意：論文要旨は、東工大リサーチリポジトリ(T2R2)にてインターネット公表されますので、公表可能な範囲の内容で作成してください。
Attention: Thesis Summary will be published on Tokyo Tech Research Repository Website (T2R2).