氏　　名	TUSHAR KANTI SAHA
博士の専攻分野の名称	博士（学術）
学位記号番号	博理工甲第 1100 号
学位授与年月日	平成 30 年 9 月 21 日
学位授与の条件	学位規則第 4 条第 1 項該当
学位論文題目	Private Computation in the Cloud Using Homomorphic Encryption （準同型暗号を利用したクラウド上のプライバシー保護計算）
論文審査委員	委員長　教　授　吉浦　紀晃 委　員　教　授　吉田　紀彦 委　員　准教授　後藤　祐一 委　員　教　授　内田　淳史 委　員　早稲田大学教授 小柴　健史

論文の内容の要旨

Throughout this thesis, we considered four important problems of private computation in the cloud such as (i) private multiple queries problem, (ii) private equality tests for single and multiple equalities, (iii) private inequality tests for single and multiple in inequalities, and (iv) private database queries. For this purpose, we discussed their solutions by proposing the corresponding protocols in the cloud using the semi-honest model in which the security of the protocols is ensured by either symmetric or public-key somewhat homomorphic encryption (SwHE) based on ring learning with errors problem.

For the first problem of private multiple queries, we selected the secure pattern matching with repetitive wildcards (SPM-RW) in which a wildcard "∗" in the pattern replaces with zero or more letters in the text. Furthermore, we regarded the pattern with multiple wildcards as multiple queries for the pattern matching. To solve this multiple queries problem, we have shown an efficient SPM-RW protocol using a new packing method that helps us to pack multiple variablelength patterns (queries) in a single polynomial and sends them as a single query to the cloud. The packing method also helps us to perform the pattern matching using the squared Euclidean distance (SED) algorithm with fewer multiplications than the existing method.

In the second problem of private equality tests, we studied two sub-problems: private equality test (PET) for performing a single equality test between two messages (integers) of l bits and private batch equality test (PriBET) for performing many equality tests such as finding a single message (an integer) within a set of messages (integers). To define the PET problem, we considered the blind verification of an online auction. To solve the PET problem, we have shown a PET protocol using the existing packing method, in which the Hamming distance technique measures the equality. In addition, our protocol outperforms state-of-the-art due to using a lowdepth equality circuit. Moreover, we regard the PriBET problem as a multiple queries problem in which the lengths of the queries are equal. For example, an l-bit SSN is searched within a set of k SSNs of l bits for health insurance verification between a hospital and an

insurance company. To perform this, we have shown an efficient PriBET protocol for the blind verification of health insurance. Furthermore, we have proposed another packing method to pack multiple equal-length queries, in which the packing is derived from the packing method of multiple queries with variable-length. Besides, we have been able to perform PriBET computation using a few multiplications due to using the modified packing method.

In the third problem of private inequality tests, we considered two sub-problems: private inequality test (PIT) for performing a single inequality test of two integers of l bits and private batch inequality test (PriBIT) to perform many inequality tests such as searching a set of integers of l bits to get all values greater or less than an integer of the same size. To define the PIT problem, we regard scenario of a private online auction, in which two bids (l-bit integers) are needed to compare blindly between the auctioneer and the bidder. To solve PIT problem, we have proposed PIT protocol using a low-depth inequality circuit engaging two new packing methods along with batch technique. Furthermore, we used a packing method to measure the incremental Hamming distance calculation that required for PIT protocol. In addition, another packing method was used to find the bit difference to calculate the inequality. Moreover, the PIT protocol outperforms the existing protocol for a single inequality comparison. For the PriBIT problem, we took a real-life problem of blind health inspection between a health research institute and a hospital. To solve this problem, we have shown a PriBIT protocol to understand the batch inequalities using a low-depth batch inequality circuit with the help of two new packing methods. The packing method helps to perform PriBIT computation with a few multiplications using the double batch technique. Besides, the experiments show the practicality of the PriBIT protocol.

Next, we considered our fourth problem of private database queries (PDBQ) in which a single value of the query needs to compare with many records of a table in the database securely. In this case, the PriBET and PriBIT protocols can be engaged along with their low-depth equality and inequality circuits. For PDBQ processing, we took four sub-problems in two settings: twoparty setting and three-party setting. In the two-party setting, we considered the traditional problems of conjunctive, disjunctive, and threshold queries with k conditions without any aggregate function. For solving conjunctive and disjunctive problems of many equalities, we have proposed private conjunctive query (PCQ) and private disjunctive query (PDQ) protocols by using the technique of the PriBET protocol and its packing method. For threshold query problem of many inequalities, we have shown private threshold query (PTQ) protocol by engaging the technique of the PriBIT protocol and its packing method. For the three-party setting, we took a special conjunctive query problem with aggregate function. To solve this problem, we have proposed special private conjunctive query (SPCQ) protocol using another packing method for encoding multi-dimensional data by modifying the packing method of the PriBET protocol. In SPCQ protocol, we have used concatenation method to realize the conjunctive property of equality appeared in the query. Moreover, theoretical analysis and practical experiments prove the practicality of the PCQ, PDQ, PTQ, and SPCQ protocols, which outperforms state-of-the-art.

For the above PriBET protocol, we have used binary encoding for the protocol's computation. Finally, we have shown an improved technique of the PriBET protocol towards big data processing using base-N fixed-length encoding rather than binary encoding in which N is the encoding size. Our practical experiments show that the base-N PriBET protocol works 8–20 faster than the PriBET protocol using binary encoding. Moreover, it can perform over 1.16 million (resp., 862 thousand) comparisons per minute for integer size of 8 bits (resp., 16 bits) with base-256 (resp., base-65536) encoding.

From the protocols of private computation along with their practicalities as mentioned above, we believe that private computation in the cloud will be an upcoming promising service that can be received by the users who want to outsource their massive computation to the cloud. We also believe that our protocols will help future researches to perform private

computation using our batch technique along with the proposed packing methods wherever they are indispensable.

論文の審査結果の要旨

学位論文審査委員会は、平成 30 年 8 月 6 日に論文発表会を開催し、論文内容の発表に続いて詳細な質疑と論文内容の審査を行った。以下に審査結果を要約する。

クラウドサービスの利用が一般的になり、多くのサービスがクラウドで運用されている。特にデータ処理をアウトソースする手段としてクラウドは有効である。クラウドで処理を行う場合には、その処理対象となる情報がクラウドからの漏洩を防ぐ必要がある。クラウドでの情報管理が十分に行われたとして、漏洩の可能性はゼロではない。クラウドで処理を行い、そして、情報の漏洩を防ぐ方法として秘密計算、また、プライバシー保護計算と呼ばれる方法がある。これは、情報を暗号化したままで処理を行うことにより、情報の漏洩を防ぐ。プライバシー保護計算を実現する方法として、準同型暗号を利用する方法があり、暗号化されたままで加算や乗算を行うことが可能である。準同型暗号としては、Partial Homomorphic Encryption(PHE) Somewhat Homomorphic Encryption(SwHE)、Fully Homomorphic Encryption(FHE) などが提案されている。準同型暗号の問題として、加算や乗算に大きな処理時間を必要とし、特に乗算の処理時間が大きい。よって、準同型暗号によるプライバシー保護計算の処理時間を減らすことは重要である。一方、Secure Pattern Match ing(SPM) など、準同型暗号を応用した様々なプライバシー保護計算が提案されている。

以上の背景から、本論文ではSwHEの一つである、SwHE Based on Ring Learning with Error (RLWE-based SwHE) を利用して、プライバシー保護計算に関する 4 つの提案を行なっている。RLWE-based SwHE を利用する理由は、処理時間が他のものに比べて短いこと、加算と回数の少ない乗算が利用できること、そして、量子コンピュータを利用した場合であっても十分な暗号強度を持っていることである。

4つの提案の1つ目は、SPM における問い合わせ内容の拡張である。従来の SPM では、問い合わせのパターンにおいてワイルドカードを一つしか利用できなかったが、複数個のワイルドカードを 1 つの問い合わせに用いて SPM を実現できるようになった。この拡張により、従来の SPM では複数回問い合わせを行う必要のあったパターンマッチを 1 つの問い合わせにより実現することが可能となり、パターンマッチを行う際の問い合わせ回数を減少させることが可能となった。また、準同型暗号の処理時間を減少させることにも成功した。

2 つ目は、等式の判定する Private Equality Test(PET) の提案である。従来から等式の判定方法は提案されていたが、本論文で処理時間を減少させることに成功させるとともに、単一の値と複数の値との等価性を一度に判定する方法 (PriBET) を提案した。

3 つ目は、不等式の判定する Private Inequality Test(PIT) の提案である。従来から不等式の判定方法は提案されていたが、PET と同様に、処理時間を減少させることに成功した。また、単一の値と複数の値との不等式の真偽を一度に判定する方法 (PriBIT) を提案した。

4 つ目は、データベースへの問い合わせ方法の提案である。提案方法は従来の方法より効率がよいことを目指している。

本論文の構成と内容は次のとおりである。

第 1 章では、本論文の背景、プライバシー保護計算のための基本技術（準同型暗号など）の説明、プライバシー保護計算の重要性、本論文の構成について述べている。

第 2 章では、従来のプライバシー保護計算を述べている。具体的には、プライバシー保護計算での複数回のパターンマッチング、2 つの値の等式の判定、2 つの値の不等式の判定、データベースへの問い合わせに

関する従来の研究を述べている。

第３章では、プライバシー保護計算に利用される準同型暗号の説明を行なっている。具体的には、準同型暗号 SwHE、そして、RLWE の説明を行なっている。

第４章では、本論文で必要となる諸定義、そして、データをエンコードする Packing Method の説明を行っている。

第５章では、SPM における複数回のパターンマッチとその問題点を説明している。そして、その問題点を解決するために、複数個のワイルドカードを一つのパターンマッチで実施する方法を提案し、提案方法が従来の方法によるパターンマッチよりも効率がよいことを実験的に示している。

第６章では、従来の PET の説明とその問題点を説明している。その問題点を解決するために、新しい PET の手法を提案し、従来の PET よりも効率がよいことを実験的に示している。また、PriBET を提案している。

第７章では、従来の PIT の説明とその問題点を説明している。その問題点を解決するために、SwHE を利用して新しい PIT の手法を提案し、従来の PIT よりも効率が良いことを実験的に示している。また、複数の不等式をバッチ処理で行う PriBIT を提案しており、これは従来にはない新しい方法である。

第８章では、プライバシー保護計算でのデータベースへの問い合わせを説明し、新しい方法を提案している。そして、その性能を理論的に分析し、実験的に性能が従来のものよりも良いことを示している。

第９章では、提案している PriBET の応用例をいくつか示し、実験的に PriBET が有効であることを示している。

最後に第１０章では、本論文で得られた成果をまとめるとともに、今後の課題を述べている。

以上、要するに、本論文では、プライバシー保護計算において、従来の手法よりもより効率的な計算手法を提案し、その提案手法の有効性を実験的に示している。本論文で得られた知見は、プライバシーを確保した上でのクラウドの利用可能性を広げるものであり、重要な意義があり応用上でも有用である。

本論文の主な内容は、査読付き学術雑誌論文５編（数理電子情報コースにおいて学術雑誌論文相当と見なす査読付き国際会議論文を含む）で公表ないしは受理されている。

以上を総合し、本学位論文審査委員会は、本論文が、博士（学術）の学位を授与するに十分に値するものと認め、「合格」と判定した。