様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　元 年　 ６ 月 １５ 日現在

機関番号：１４５０１
研究種目：基盤研究(C)（一般）
研究期間：2015～2018
課題番号：１５Ｋ００００２８

研究課題名（和文）安全なクラウドコンピューティングに向けた代理計算に関する研究開発

研究課題名（英文）R&D on privacy-preserving outsourced computing in cloud computing

研究代表者
王　立華（Wang, Lihua）

神戸大学・工学研究科・特命准教授

研究者番号：００４４７２２８

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：本研究では、安全なクラウドコンピューティングに向けた代理計算に関する研究開発を行った。安全な代理計算のプリミティブとして、内積計算、行列積、整数の大小比較を暗号化したまま効率的に行う方式を設計し、実装による速度評価を行った。いずれも量子コンピュータに対しても安全である。また、安全な代理計算の応用として、データを開示せずに機械学習の計算を行うプライバシー保護データマイニングについて研究開発を行い、プライバシー保護Naive Bayes分類や三層ニューラルネットワークにおける効率的な秘匿推論処理などの研究開発を行った。一連の研究成果は７件の国際会議や論文誌で採択されたほか、特許出願も行った。

研究成果の学術的意義や社会的意義
クラウドコンピューティングに代表される、計算処理をサーバに委任する「代理計算」においては、計算対象データのサーバへの開示が必要なため、データ漏えい等の対策が必須である。本研究ではこの課題の解決策として、暗号技術を応用した安全な代理計算技術の研究開発を行っており、データを暗号化したまま計算を行うことができる「準同型暗号」において、ベクトル内積などの計算プリミティブの効率的な方式の開発や、応用例としてニューラルネットワーク推論処理などの機械学習アルゴリズムの安全な代理計算を構築した。これらの結果は、特定の処理に特化した代理計算については、データを安全に保ちつつ効率良く計算ができることを示している。

研究成果の概要（英文）：In this research, we studied the privacy-preserving outsourced computation in cloud computing and its applications in machine learning. In particular, we proposed several protocols for the inner product, matrix product, and integer comparison on ciphertexts. All the proposed protocols are secure against attacks by quantum computers, and they are also efficient according to the extensive experimental results. Based on these protocols, we also proposed several privacy-preserving outsourced machine learning schemes, including Naive Bayes classification and 3-layer neural networks. The detailed security analyses showed that these schemes would not reveal any information to the cloud or others during the process, and the experimental results also demonstrated that they are relatively efficient. With the above research results, we have published seven papers in international conferences and journals, and have applied for a patent.

研究分野：情報学基礎

キーワード：クラウドセキュリティ　代理再暗号　準同型暗号　秘密計算　プライバシー保護データマイニング

様　式　C－１９、F－１９－１、Z－１９、CK－１９（共通）

1. 研究開始当初の背景

ネットワーク技術や分散処理技術の発達により、ネットワーク構成等の物理環境を意識することなくネットワーク上の多数の計算機を活用できる「クラウドコンピューティング」が急速に発展しており、コスト削減や運用安定化などを理由に企業でも利用が進んでいる。クラウドコンピューティングに代表される、サーバに処理を委任する「代理計算」では、処理するデータを外部のサーバに保存する必要があるため、データ漏えい等の対策が必須である。さらにクラウドコンピューティングでは、ネットワーク上のどのサーバを利用しているか特定が困難であるため、攻撃者によって乗っ取られたサーバを知らずに利用してしまう等、セキュリティの対策が複雑化する。これらの問題を背景として、近年、暗号技術を応用した安全な代理計算技術の研究が活発に行われている。

【代理計算が満たすべき要素】
安全なクラウドコンピューティングに向けた代理計算において、考慮すべき要素を以下に示す。(a)クラウド環境に適した安全性モデルクラウドコンピューティングは、クラウドに対して処理を委任するクライアントが複数存在し、クラウド上に存在する複数のサーバは互いに協調しながら処理を行う「複数クライアント・複数サーバモデル」である。さらに、クライアント・サーバの中に複数の攻撃者が存在し、協調・結託して攻撃を行う（結託攻撃）ことも想定した安全性モデルを構築する必要がある。(b) RSA 暗号や楕円曲線暗号などの現在利用されている暗号のほとんどは、量子コンピュータによって容易に解読できる。米 NASA がカナダ D-Wave 社から量子コンピュータを購入、米 Google が量子コンピュータの設計・開発に乗り出すなど、実用化が現実になりつつあり、データの安全性を長期間保つためには、量子コンピュータによる攻撃に対しても安全である必要がある。

【代理計算の現状】
代理計算の研究は、様々な用途に利用可能な「汎用」代理計算と用途を限定することで安全性・効率を向上させた「専用」代理計算に分けることができる。代表的な既存研究（汎用では[1,2,3]、専用では[4,5,6,7]などの安全性モデルは、単一クライアントあるいは単一サーバであり、クラウド環境全体を考慮したモデルとはなっておらず、また結託攻撃に対してもほとんどが対応できていない。攻撃者の特定・追跡機能を備えた代理計算方式は、[8]で Libert らによって提案されているが、ペアリング暗号ベースであるため、量子コンピュータの攻撃に対して安全ではない。また、[9]では格子理論を応用して、量子コンピュータの攻撃に対して安全な代理計算方式が提案されているが、この方式は攻撃者の特定機能を備えていない。このように、既存研究では、前項で述べた安全なクラウドコンピューティングに向けた代理計算が備えるべき機能について、全てを満足する方式は提案されていない。

2. 研究の目的

クラウドコンピューティングに代表される、サーバに処理を委任する「代理計算」では、処理するデータをサーバに保存する必要があるため、データのセキュリティが重要な問題である。これを解決するためにいくつかの手法が研究されているが、代理計算に関わるクライアント・サーバによる結託攻撃に対して安全ではない、量子計算機の攻撃に対して安全ではない、など未だ多くの課題が残っている。
本研究では、主に以下の 3 つの課題に取り組む。

課題1.　クラウド環境を考慮した「複数クライアント・複数サーバモデル」における安全性の定義とその安全性を満たすための暗号学的要素の導出
課題2.　結託攻撃耐性、量子計算機による攻撃に対する安全性などのクラウド環境に必要な機能を備えた代理計算システムの設計
課題3.　提案方式の高速実装と実証実験による実用性の検証

3. 研究の方法

代表者含む当該分野の研究者計 7 名（研究分担者 1 名、連携研究者 1 名、研究協力者 4 名）のチーム体制で、平成 27 年度から平成 30 年度までの 4 年間で 3 つの課題に取り組む。文献調査からスタートし、学会参加によって最新情報収集と研究交流や、メールベースと対面研究打ち合わせなどの手段で当分野の研究協力者と共同研究によって、計画を遂行した。各課題のスケジュール・研究体制は以下のとおり。

下記図 1 の計画にそって、安全なクラウドコンピューティングに向けた代理計算に関する研究開発として、(1)準同型暗号を用いた秘密計算、(2)代理再暗号、(3)クラウド/フォグコンピューティング、(4)プライバシー保護データマイニングについて研究開発を行った。

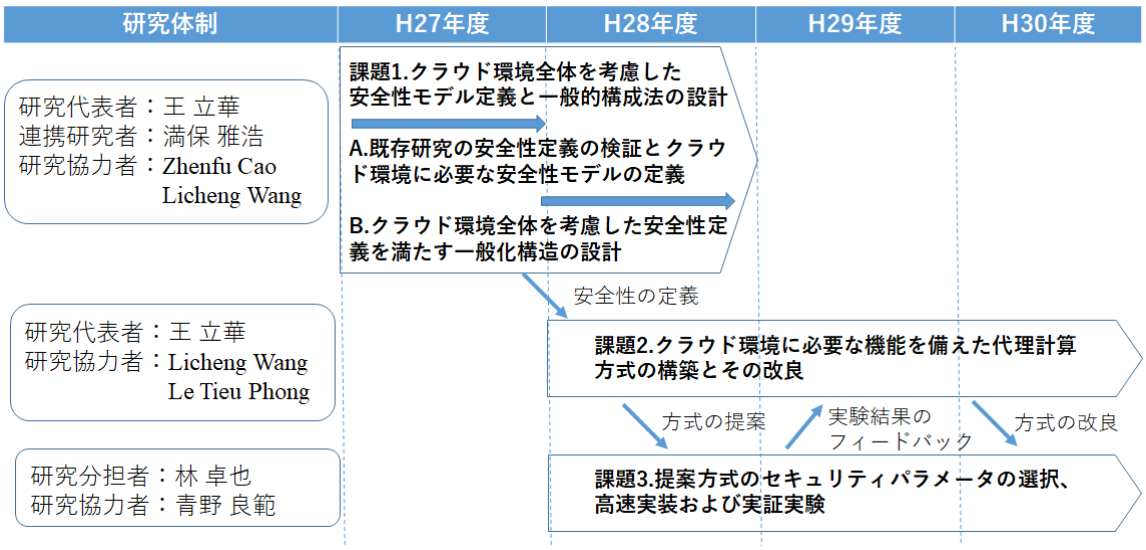

図１．研究体制とスケジュール

4. 研究成果

下記成果(1)〜(2)は課題1に関する成果、(1)、(3)と(4)は課題2、3に関する成果である。

(1) 準同型暗号を用いた秘密計算：量子計算機に対しても安全であると期待される格子暗号について、加法ならびにテンソル積について準同型性を満たすとき、既存研究よりも効率の良いセキュア内積、すなわち安全に計算委託が可能な内積計算の一般的構成法を提案した。提案手法は既存の LWE ベースや Ring-LWE ベース準同型暗号方式に適用できる。本成果は国際会議 NSS2017 で発表した。NSS2017 で発表した準同型内積計算の構築方法を応用し、効率的な秘匿行列乗算方式を提案した。提案方式の Packing 方法では、行列 A、B に対して、行列積 AB、BA を一回の乗算で計算できるという特徴がある。行列の次元が小さいときのテスト実装を行った成果を国際会議 CANS2017、国内学会 SCIS2018 で発表し、特許出願を行った。また、整数の値を秘匿したまま大小比較を行う方式を提案し、既存研究と比較して 2 倍以上高速であることを実証実験で確認した。さらに、暗号化データベースにおける検索結果に対して準同型暗号による計算を行う際に、検索結果以外の値が計算結果に含まれるかどうかを復号者が検知できる暗号方式を提案し、実装による速度評価を行った（国内学会 CSS2016、国際会議 ASIACCS 2017 で発表、CSS2016 最優秀論文賞受賞）。【5.雑誌論文④⑤⑥⑦、学会発表①③④⑤と特許①参照】

(2) 代理再暗号：クラウド環境におけるプロキシ再暗号化技術の安全性評価手法について、既存のプロキシ再暗号化方式(PRE: Proxy Re-Encryption)の安全性の強弱関係を整理し、結託攻撃に対する安全性要求との帰着関係について調査･研究を行った。PRE では依頼人 A は他のユーザ B への再暗号化鍵を代理人（プロキシ）に渡し、代理人はその鍵を使って A 宛の暗号化されたデータを復号することなく B 宛の暗号化データに変換できる。B は自分の秘密鍵を使って変換された暗号文を復号できる。PRE 技術を活用することで、ファイルを暗号化したまま指定した人と共有することが可能であり、セキュアで柔軟なファイル共有が実現できる。既存の PRE 方式では、再暗号化できる回数によって single-hop PRE と multi-hop PRE に分けられており、既存の multi-hop PRE では再暗号化回数をコントロールできないという問題点がある。本研究では、再暗号化回数が事前に定められた h-hop PRE 及び IND-CPA 安全性モデルを定義し、その IND-CPA 安全から Collusion-safe や Non-transitivity への帰着関係を明らかにした。【5.学会発表⑥⑦⑧⑨参照】

(3) クラウド/フォグコンピューティング：広州大学と北京郵電大学と共同研究を行い、クラウド/フォグコンピューティングのシナリオのもとでクライアント側の計算コストを削減するための暗号化処理をクラウドサーバへ安全に委託計算が可能でかつ量子コンピュータに対して安全な Chebyshev 多項式ベースの CCA 安全な Chaotic 暗号を提案した。この成果は論文誌 Concurrency and Computation：Practice and Experience に採録された。また、北京郵電大学など日中仏連携で共同研究を行い、アクセス制御ができる属性ベース暗号に基づいた代理再暗号化や同値チェック機能付きの暗号など暗号プリミティブを次世代インターネットアーキテクチャ Named Data Network へ組み込むことで、Securing Named Data Networking を提案した。この成果は論文誌 IEEE Communications Magazine に掲載済み。【5.雑誌論文①②参照】

⑷ プライバシー保護データマイニング：完全準同型暗号を用いたNaive Bayes分類器の効率的な秘匿学習方式を提案し、完全準同型暗号ライブラリHElibを用いた実証実験を行った。また、三層ニューラルネットワークにおいて、Somewhat 準同型暗号を用いた効率的な秘匿推論処理を提案した。速度評価では、十分に実用的な計算時間で動作することを示した。また、精度評価では、準同型暗号の制約から活性化関数として二次関数を用いたことによる精度の低下は見られたが、実用的な高い精度で分類ができることを確認した。【5.雑誌論文③と学会発表②⑥参照】

＜引用文献＞

[1] S. Kamara, et al.: Outsourcing Multi-party Computation. IACR ePrint Archive, 2011-272.
[2] A. López-Alt et al.: On-the-fly Multiparty Computation on the Cloud via Multikey Fully Homomorphic Encryption. STOC2012: pp.1229-1233.
[3] P. Ananth, et al.: Achieving Privacy in Verifiable Computation with Multiple Servers – Without FHE and without Pre-processing. PKC 2014: pp.149-166.
[4] G. Hanaoka, et al.: Generic Construction of Chosen Ciphertext Secure Proxy Re-Encryption. CT-RSA 2012: pp.349-364.
[5] R. Hayashi, et al.: Unforgeability of Re-Encryption Keys against Collusion Attack in Proxy Re-Encryption. IWSEC 2011: pp.210-229.
[6] L. Wang, L. Wang, M. Mambo and E. Okamoto, “Identity-Based Proxy Cryptosystems with Revocability and Hierarchical Confidentialities”, IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E95-A, No. 1, 2012: pp.70-88.
[7] L. Wang, L. Wang, M. Mambo and E. Okamoto, “New Identity-Based Proxy Re-Encryption Schemes to Prevent Collusion Attacks”, Pairing 2010, Lecture Notes in Computer Science, Vol.6487, 2010: pp. 327–346.
[8] B. Libert, D. Vergnaud: Tracing Malicious Proxies in Proxy Re-encryption. Pairing 2008: pp.332-353.
[9] Y. Aono, X. Boyen, L.T. Phong and L. Wang, “Key-Private Proxy Re-encryption under LWE”, INDOCRYPT 2013, Lecture Notes in Computer Science, Vol.8250, 2013: pp.1-18.

5. 主な発表論文等

〔雑誌論文〕（計7件）

① Licheng Wang, Zonghua Zhang, Mianxiong Dong, Lihua Wang, Zhenfu Cao, Yixian Yang: Securing Named Data Networking: Attribute-Based Encryption and Beyond. IEEE Communications Magazine 56(11): 76-81 (2018)
② Jing Li, Licheng Wang, Lihua Wang, Zhengan Huang, Jin Li: Verifiable Chebyshev Maps-Based Encryption Schemes with Outsourcing Computations in the Cloud/Fog Scenarios. J. Concurrency and Computation: Practice and Experience (Accepted: 23 March 2018) (https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.4523)
③ Sangwook Kim, Masahiro Omori, Takuya Hayashi, Toshiaki Omori, Lihua Wang, Seiichi Ozawa: Privacy-Preserving Naive Bayes Classification Using Fully Homomorphic Encryption. ICONIP (4) 2018: 349-358
④ Lihua Wang, Yoshinori Aono, Le Trieu Phong: A New Secure Matrix Multiplication from Ring-LWE. CANS 2017: 93-111
⑤ Lihua Wang, Takuya Hayashi, Yoshinori Aono, Le Trieu Phong: A Generic yet Efficient Method for Secure Inner Product. NSS 2017: 217-232
⑥ Yoshinori Aono, Takuya Hayashi, Le Trieu Phong, Lihua Wang: Efficient Key-Rotatable and Security-Updatable Homomorphic Encryption. SCC@AsiaCCS 2017: 35-42
⑦ Keita Emura, Takuya Hayashi, Noboru Kunihiro, Jun Sakuma: Mis-operation Resistant Searchable Homomorphic Encryption. AsiaCCS 2017: 215-229

〔学会発表〕（計9件）

① Lihua Wang、Takuya Hayashi、Tushar Kanti Saha、Yoshinori Aono、Takeshi Koshiba、Shiho Moriai: An Efficiently Secure Comparison Scheme Using Homomorphic Encryption. 2019年暗号と情報セキュリティシンポジウム（SCIS2019）2A1-2, Jan. 2019.
② 手塚 雄大, 王 立華, 林 卓也, Kim Sangwook, 為井 智也, 大森 敏明, 小澤 誠一: 三層ニューラルネットワークにおける Ring-LWE ベース準同型暗号を用いた効率的なプライバシー保護推論処理. 日本人工知能全国大会 JSAI2019（採録済み、6月発表予定）
③ 王 立華, プラディプ クマル ミシュラ, 青野 良範, レ チュウ フォン, 安田 雅哉: Ring-LWE を用いたセキュアな行列乗算のためのパッキング方法. 2018年暗号と情報セキュリティシンポジウ

ム（SCIS2018）3C1-1, Jan. 2018.
④ 林 卓也, 青野 良範, レ チュウ フォン, 王 立華: 効率的な準同型内積演算の一般的構成. SCIS2017, Jan. 2017.
⑤ 江村 恵太, 林 卓也, 國廣 昇, 佐久間 淳:まぜるな危険準同型暗号. コンピュータセキュリティシンポジウム 2016 (CSS2016),1C3-2, Oct. 2016.
⑥ Lihua Wang: New Reflection on Delegatable Computation for a Secure Cloud Storage and Data Mining with Privacy-Protection. A3 Foresight Program: Annual Workshop in Korea, July 2016.【基調講演】
⑦ Lihua Wang: New Reflection on Classification & Security Reduction of Proxy Re-Encryption Applied to Cloud Environments. A3 Foresight Program: Annual Workshop in Okinawa, February 2016.
⑧ Lihua Wang, Licheng Wang, and Masahiro Mambo: A Study on the Security Evaluation Methods of Proxy Re-Encryption Applied to Cloud Environments. SCIS2016, Jan. 2016.
⑨ 王 立華: クラウド環境における暗号化状態での「情報共有」と「代理計算」に関する研究. MeltUp フォーラムパネリスト「クラウド環境における暗号化状態処理を廻って」, June 2015.【依頼講演】

〔産業財産権〕
○出願状況（計 1 件）

① 名称：暗号化システム
発明者：王 立華, 青野 良範,レ チュウ フォン
権利者：情報通信研究機構
種類：発明
番号：特願 2017-228792
出願年：2017 年
国内外の別：日本

〔その他〕
ホームページ等
https://dblp.uni-trier.de/pers/hd/w/Wang_0001:Lihua
https://www.nict.go.jp/security/index.html

6．研究組織

(1)研究分担者
研究分担者氏名：林 卓也
ローマ字氏名：HAYASHI, Takuya
所属研究機関名：独立行政法人 情報通信研究機構
部局名：ネットワークセキュリティ研究所・セキュリティ基盤研究室
職名：研究員 (2018 年 3 月末現在)
研究者番号（8 桁）：70739995

(2)研究協力者
研究協力者氏名：満保 雅浩
ローマ字氏名：MAMBO, Masahiro

研究協力者氏名：Licheng Wang
ローマ字氏名：WANG, Licheng

研究協力者氏名：青野良範
ローマ字氏名：AONO, Yoshinori

研究協力者氏名：Le Trieu Phong
ローマ字氏名：LE, Trieu Phong