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

平成　２９　年　　６　月　１４　日現在

機関番号：　１２４０１
研究種目：　挑戦的萌芽研究
研究期間：　2014～2016
課題番号：　２６５４０００２

研究課題名（和文）通信複雑性に対するブラインド量子計算による方法論の確立

研究課題名（英文）Communication Complexity based on Blind Quantum Computation

研究代表者
小柴　健史（KOSHIBA, Takeshi）

埼玉大学・理工学研究科・教授

研究者番号：６０４００８００

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：幾つかの計算問題について量子通信複雑度を議論するために，比較対象として（古典秘匿計算の一方式としての）準同型暗号によるプライバシー保護データ検索の効率的なプロトコルを提案し計算機実験を通して実効性を確かめた。また，量子ブラインド計算において参加者が不正を行ったときに，情報理論的安全性を確保しつつ，それを第三者が検証できる仕組みを導入することに成功した。

研究成果の概要（英文）：In order to discuss the quantum communication complexity of several problems, we propose efficient protocols for secure database search based on homomorphic encryption for comparison. In addition, we have computational experiments to verify the effectiveness of our proposals. We have a new result with respect to quantum blind computation. We devise an information-theoretic mechanism where a third-party can arbitrate between a client and a server if one party is cheating and incorporate the mechanism into quantum blind computation.

研究分野：　量子計算

キーワード：　暗号理論　量子計算　暗号プロトコル　準同型暗号

１．研究開始当初の背景

(1) 量子情報科学は，量子力学に基づいた計算・通信モデルを考えることにより，従来の情報科学の限界を超えた強力な情報処理を可能にする分野として注目され発展してきている。例えば，Bennett&BrassardによるBB84プロトコルは二者間通信における情報理論的に安全な鍵共有法を与えている。また，Broadbent, Fitzsimons & Kashefiは万能ブラインド量子計算(Proc. FOCS 2009, pp.517-526)と呼ばれる二者間プロトコルを構築している。これは，一方(Alice)のみが持つ入力情報に基づいた計算を他方(Bob)に実行させるが，BobはAliceの入力情報，さらには何を計算したのかさえ分からないという性質を持つ計算方式であり情報理論的な安全性が保証されている。一方で，古典計算においては情報理論的なブラインド計算を達成する方法は知られていない。

(2) また，分散環境下での計算(例えばAliceとBobが通信を介して計算)においては，計算時間や計算メモリ容量よりも通信量がボトルネックになることが多い。量子情報科学においても，Buhrman, Cleve & Wigderson (Proc. STOC 1998, pp.63-68)など量子通信・量子計算を援用することで通信複雑度が削減できるか検討されてきている。さらには，Jain, Radhakrishnan & Sen (J.ACM 56(6), 2009)などプライバシーを保護することを前提とする量子通信複雑度についても研究されている。

２．研究の目的

ブラインド量子計算はユーザとサーバ間のプロトコルでユーザの持つアルゴリズムやその入出力に関する情報をサーバに情報理論的な意味でも漏洩することなくサーバに代理計算させる技術である。ブラインド量子計算技術を利用して，ユーザのプライバシー保護を保証しつつ計算を遂行するのに必要な総通信量を議論することを可能にする新たな方法論を確立することを目的とする。また，この方法論の有効性を確認するために，秘匿情報検索などのユーザのプライバシーが重要と思われる具体的な問題群について通信複雑度を導出し，従来のアプローチからの導出方法と比較して優位となるような事例を見出すことを目指す。

３．研究の方法

(1) まず，研究対象を量子秘匿情報検索に限定し，その量子通信複雑度の究明に注力する。具体的には，既存の量子秘匿情報プロトコルの調査，量子通信複雑度下界研究の調査，プロトタイププロトコルの精査，ブラインド計算を用いた方法論の一般的性質の検討，を行う。

(2) 次いで，ブラインド計算を用いた量子秘匿情報検索の研究を一般のプロトコルに対しても応用できるように一般化を目指した研究を行う。具体的には，Equality や Disjointness と呼ばれる基本的タスクの量子通信複雑度に関する既存研究の調査，Equality や Disjointness に対してブラインド計算にもとづくプロトコルの検討，非対称な設定での通信複雑度の既存研究の調査，ブラインド計算を用いた方法論へ適用可能なその他のプロトコルの模索，を行う。

(3) 通信複雑度の観点から量子プロトコルの効率性を検討するための比較として，対応する古典プロトコルについて研究を行う。とくに，準同型暗号を用いた方式について検討を行う。

(4) 副次的な研究として，量子ブラインド計算に関して拡張を行うことも想定する。

４．研究成果

(1) Broadbent,Fitzsimons,Kashefi(2009)によって提案された量子ブラインド計算はクライアントとサーバ間の代理計算プロトコルであり，クライアントの情報をサーバには一切漏らさない。量子通信複雑さを議論するための枠組みとして量子ブラインド計算を活用することを新たなアイデアとし，これを一般化した概念について，従来方式と同様に安全性(秘匿性)があることを確認した。Broadbentらのオリジナルのプロトコルはサーバがクライアントからの要求に答えるのみの設定なのに対して，安全性を損なわずにサーバにも入力を持たせるように拡張することで，一般の暗号プロトコルへ適用できるようにした。 また，この枠組みを応用することで，秘匿情報検索に応用した。具体的には，Groverアルゴリズムを構造的なデータベースに適用するというアルゴリズムを拡張量子ブラインド計算に適用するとことで，量子秘匿情報検索プロトコルを構築した。

(2) 量子ブラインド計算の通信効率との比較対象との観点から，代理計算を行わせる他の暗号技術である準同型暗号計算に着目し，格子問題に基づく準同型暗号のための効率的データ埋め込み手法の可能性を検討した。このデータ埋め込み手法をもとにして，データを秘匿したまま統計量(平均値や分散)を計算する効率的な手法を提案した。また，格子理論をもとにした暗号方式の鍵依存安全性を利用

した，暗号化データの所有権を移譲する効率的な手法を提案した。また，データのプライバシーを保護したままデータベース内の属性値が一致するデータを一括して抽出する手法，データを暗号化したままで複数の文字にマッチできるワイルドカードを利用したパターン照合する手法を考案した。これらの提案手法が現実的な意味で効率的に動作することを確認するために計算機実装を行い，既存の方式よりも効率的であることを確認した。
(3) 量子ブラインド計算において，参加者が不正を行ったときに不正検出はできるが，不正を指摘されたときにそれを否認されてしまうと正当化できないという問題がある。この問題に対応するための従来技術として，公開鍵暗号技術を利用して第三者に検証させる方法があったが，安全性(プライバシー)の根拠が計算量理論的なものに低下してしまう。これに対して，量子ブラインド計算の途中に第三者が仲介者としてプロトコルに関与する形の方式を提案し，安全性(プライバシー)が情報理論的であることを保証することに成功した。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計９件）


① Tushar Kanti Saha, Takeshi Koshiba, Private conjunctive query over encrypted data, Lecture Notes in Computer Science (AFRICACRYPT 2017), vol.10239, pp.149-164, 2017, 査読有
DOI: 10.1007/978-3-319-57339-7_9

② Masaya Yasuda, Kazuhiro Yokoyama, Takeshi Shimoyama, Jun Kogure, Takeshi Koshiba, Analysis of decreasing squared-sum of Gram -Schmidt lengths for short lattice vectors, Journal of Mathematical Cryptology, vol.11, pp.1-24, 2017, 査読有
DOI: 10.1515/jmc-2016-0008

③ Tushar Kanti Saha, Takeshi Koshiba, An Enhancement of Privacy-Preserving Wildcards Pattern Matching, Lecture Notes in Computer Science (FPS 2016), vol.10128, pp.145-160, 2017, 査読有
DOI: 10.1007/978-3-319-51966-1_10

④ Masaya Yasuda, Takeshi Shimoyama, Narishige Abe, Shigefumi Yamada, Takashi Shinzaki, Takeshi Koshiba, Privacy-preserving fuzzy commitment for biometrics via layered error-correcting codes, Lecture Notes in Computer Science (FPS 2015), vol.9482, pp.117-133, 2016, 査読有
DOI: 10.1007/978-3-319-30303-1_8

⑤ Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama, Takeshi Koshiba, New packing method in somewhat homomorphic encryption and its applications, Security and Communication Networks, vol.8, pp.2194-2213, 2015, 査読有
DOI: 10.1002/sec.1164

⑥ Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama, Takeshi Koshiba, Secure statistical analysis using RLWE-based homomorphic encryption, Lecture Notes in Computer Science (ACISP 2015), vol.9144, pp.471-487, 2015, 査読有
DOI: 10.1007/978-3-319-19962-7_27

⑦ Masaya Yasuda, Takeshi Koshiba, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama, Secure data devolution: Practical re-encryption with auxiliary data in LWE-based somewhat homomorphic encryption, Proceedings of the 3rd International Workshop on Security in Cloud Computing (SCC@ASIACCS 2015), pp.53-61, 2015, 査読有
DOI: 10.1145/2732516.2732521

⑧ Masaya Yasuda, Kazuhiro Yokoyama, Takeshi Shimoyama, Jun Kogure, Takeshi Koshiba, On the exact decryption range for Gentry-Halevi's Implementation of Fully Homomorphic Encryption, Journal of Mathematical Cryptology, vol.8, pp.305-329, 2014, 査読有
DOI: 10.1515/jmc-2013-0024

⑨ Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama, Takeshi Koshiba, Privacy-preserving wildcards pattern matching using symmetric somewhat homomorphic encryption, Lecture Notes in Computer Science (ACISP 2014), vol.8544, pp.338-353, 2014, 査読有
DOI: 10.1007/978-3-319-08344-5_22

〔学会発表〕(計 20 件)

① Ei Mon Cho, Takeshi Koshiba, Secure SMS transmission based on verifiable hash convergent group signcryption, The 18th IEEE International Conference on Mobile Data Management (MDM 2017), 2017年5月29日～6月1日, Daejeon (South Korea)

② Ei Mon Cho, Takeshi Koshiba, Big data cloud deduplication based on verifiable hash convergent group signcryption, IEEE International Workshop on Big Data Security and Services, 2017年4月6日～9日, San Francisco (USA)

③ Ei Mon Cho, Takeshi Koshiba, Secure Deduplication in a Multiple Group Signature Setting, The 31st IEEE International Conference on Advanced Information Networking and Applications (AINA 2017), 2017年3月27日～29日, Taipei (Taiwan)

④ 大澤卓矢, 黒河徳大, 小柴健史, フーリエ基底を用いた関数秘密分散, 2017年暗号と情報セキュリティシンポジウム (SCIS 2017), 2017年1月24日～27日, ロワジールホテル那覇 (沖縄県那覇市)

⑤ 井上義治, 小柴健史, Bloom Filterによる和・共通集合濃度の多者間秘匿計算プロトコル, 2017 年暗号と情報セキュリティシンポジウム (SCIS 2017), 2017 年 1 月 24 日～27 日, ロワジールホテル那覇 (沖縄県那覇市)

⑥ 切上太希, 小柴健史, Zig-zag 積を利用したグラフ拡張における Almost-everywhere agreement, 2017 年暗号と情報セキュリティシンポジウム (SCIS 2017), 2017 年 1 月 24 日～27 日, ロワジールホテル那覇 (沖縄県那覇市)

⑦ 岩元遼太, 小柴健史, アファイン誤りに対する頑健符号, 2017 年暗号と情報セキュリティシンポジウム (SCIS 2017), 2017年1月24日～27日, ロワジールホテル那覇 (沖縄県那覇市)

⑧ 飯島京嗣, 小柴健史, Proof-of-Stake に基づく電子投票プロトコル, 2017 年暗号と情報セキュリティシンポジウム (SCIS 2017), 2017 年 1 月 24 日～27 日, ロワジールホテル那覇 (沖縄県那覇市)

⑨ 佐藤豪, 森前智行, 小柴健史, Hayashi-Morimae ブラインド量子計算に対する第三者検証可能性, 2017 年暗号と情報セキュリティシンポジウム (SCIS 2017), 2017 年 1 月 24 日～27 日, ロワジールホテル那覇 (沖縄県那覇市)

⑩ 藤田舞騎, 小柴 健史, 複数の合理的な敵に対する安全なメッセージ伝達方式, 2017 年暗号と情報セキュリティシンポジウム (SCIS 2017), 2017 年 1 月 24 日～27 日, ロワジールホテル那覇 (沖縄県那覇市)

⑪ Lwin San, Ei Mon Cho, Takeshi Koshiba, Non-Transferable Proxy Re-Encryption for Group Membership/Non-Membership, 2017 年暗号と情報セキュリティシンポジウム (SCIS 2017), 2017 年 1 月 24 日～27 日, ロワジールホテル那覇 (沖縄県那覇市)

⑫ Tushar Kanti Saha, Takeshi Koshiba, Private Equality Test using Ring-LWE Somewhat Homomorphic Encryption, The 3rd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE 2016), 2016年12月4日～6日, Denarau Island (Fiji)

⑬ Maiki Fujita, Takeshi Koshiba, Perfectly Secure Message Transmission Scheme against Rational Adversaries, The 19th Japan-Korea Joint Workshop on Algorithms and Computation (WAAC 2016), 2016年8月30日～31日, Hakodate Citizen Hall (北海道函館市)

⑭ 黒河徳大, 小柴健史, 鍵サイズ長の単一値を持つGateによるGarbled化方式, 2016年暗号と情報セキュリティシンポジウム (SCIS 2016), 2016年1月21日, ANAクラウンプラザホテル熊本ニュースカイ (熊本県熊本市)

⑮ 藤田舞騎, 小柴健史, 合理的な敵に対する安全なメッセージ伝達方式, 2016年暗号と情報セキュリティシンポジウム (SCIS 2016), 2016年1月21日, ANAクラウンプラザホテル熊本ニュースカイ(熊本県熊本市)

⑯ Ei Mon Cho, Takeshi Koshiba, Secure Deduplication for Multiple Group Setting, 2016年暗号と情報セキュリティシンポジウム (SCIS 2016), 2016年1月22日, ANAクラウンプラザホテル熊本ニュースカイ (熊本県熊本市)

⑰ Takeshi Koshiba, Quantum Bloom Filter, Workshop on Secure Quantum Computing

(招待講演), 2015年03月19日, Tokyo Univ. (東京都文京区)

⑱ Amit Raj Baral, Takeshi Koshiba, Data Management over Garbled Bloom Filter for Private Set Intersection, 13th International Conference on Computer Applications (ICCA 2015), 2015年2月5日, Yangon (Myanmar)

⑲ Amit Raj Baral, Takeshi Koshiba, Harumichi Nishimura, Private Information Retrieval via Blind Quantum Computation, Australia-Japan Workshop on Multi-User Quantum Networks (招待講演), 2014年10月22日, Sydney (Australia)

⑳ Takeshi Koshiba, On the power of the Tri-Sum-And function, Collective Dynamics in Information Systems 2014 , 2014年10月10日, Beijing (China)

〔図書〕(計 2 件)

① 小柴健史,藤井啓祐,森前智行, コロナ社, 観測に基づく量子計算, 2017 年, 196（1-18,132-133,159,185-186）ページ

② 小柴健史, 岩波出版, 乱数生成と計算量理論, 2014年, 176ページ

## ６．研究組織

(1)研究代表者

小柴　健史（KOSHIBA, Takeshi）
埼玉大学・理工学研究科・教授
研究者番号：60400800

(2)連携研究者

西村　治道（NISHIMURA, Harumichi）
名古屋大学・情報科学研究科・准教授
研究者番号：70433323