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　１３　日現在

機関番号：　１２４０１
研究種目：　基盤研究(A)（一般）
研究期間：　2012～2016
課題番号：　２４２４０００１

研究課題名（和文）量子プロトコル理論の深化

研究課題名（英文）Deepening Theory of Quantum Protocols

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）　　27,700,000円

研究成果の概要（和文）：量子対話型証明の一般化モデルを提案し完全問題の存在やBabaiの崩壊定理の量子版などの計算量的構造を明らかにした。半環上の行列積およびグラフ上の三角形発見問題に対して高速量子アルゴリズムを構築し解析方法を発展させ量子分散プロトコルを構築した。観測系と計算系が分離可能な補助キュービット駆動型モデルでも量子ブラインド計算が実現することを示した。計算量クラスBQPの古典計算量クラスAWPPに対し事後選択の概念を利用した量子計算量クラスによる特徴付けを与えた。AWPPがBQPの最良上界である自然な理由を与えAWPPの研究への量子計算量理論的アプローチの可能性を切り拓いた。

研究成果の概要（英文）：We propose a generalized model of quantum interactive proof systems and show the existence of complete problems and a quantum version of Babai's collapse theorem. We construct efficient quantum algorithms for matrix multiplication of semi-rings and for finding triangles in graphs and develop their analysis to obtain their quantum distribution protocols. In ancilla-driven model where computation systems and measurement systems are separable, we show that quantum blind computation is achievable. We characterize a classical computational complexity class AWPP, which corresponds to a quantum computational complexity class BQP, by using the notion of post-selection. We give a natural reason why AWPP is the tightest upper bound of BQP and develop a quantum complexity theoretic approach to the study of AWPP.

研究分野：　量子計算

キーワード：　量子プロトコル　暗号理論　量子アルゴリズム　ゲーム理論　量子計算量理論

１．研究開始当初の背景

量子情報科学は，量子力学の原理に基づいた計算・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無条件安全な鍵共有法となっている。また，2009年，Broadbent, Fitzsimons & Kashefi は万能ブラインド計算(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。ブラインド計算は，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 の持つ入力情報，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る。これらの方式は，従来の暗号技術では実現不可能であり，かつ，無条件安全性と呼ばれる高い安全性を達成している。特に，ブラインド計算は，「観測ベース量子計算」と呼ばれる新しい量子計算モデルを基盤として理論構築されており，量子計算と量子情報がうまく融合している好例である。

前身研究課題「量子情報理論と量子計算量理論の融合技術の展開」において，量子情報理論と量子計算量理論の融合技術について探究し，多くの量子プロトコルの設計に寄与した。計算量理論，量子暗号プロトコルに重要な基礎概念の量子対話型証明に関しては，並列実行時のプロトコル間の量子的相関の与える影響や，通信量に制限がある場合やゼロ知識性などにおいて未解明な部分が多い。特に多証明者の場合においては，証明者間にエンタングルメント共有を許した場合の正確な検証能力が未解明である他，エンタングルメント共有量の影響，必要証明者数など未解決な難問が多い。また，近年，エンタングルメントなどの相関を利用して誤り確率を低減する通信プロトコルの研究が進み，ゼロ誤り通信容量が増大する場合があることなどが示されている。これらは不完全情報ゲームにおける量子非局所性と密接に関連するため，多証明者量子対話型証明とも深く関係すると思われる。一方，効率的なエンタングルメント共有や量子情報転送を可能にする量子ネットワーク符号は，研究分担者らが世界に先駆けて提案したものであるが，その研究は未だ世界的に端緒についたばかりといえる。高効率な符号化による量子通信量の削減が今後の重要なテーマとなっていくと考えられ，どのようなリソース制約のもとで効率的な符号化プロトコルが可能であるか，解明すべき点が多く残されている。古典暗号理論において，情報理論的方法論と計算量理論的方法論が互いに補完しあう形で，暗号理論が形作られている。BB84 プロトコルによる鍵共有法は情報理論的方法論の一つに位置付けられ，量子暗号研究の潮流として情報理論的な範疇をどこまで拡大できるかということを目指して研究が進められている。量子計算量理論的な方法論も量子情報理論的な暗号技術を補完することが期待でき， 量子情報を扱う際に生じる諸問題を克服する形で量子版のビット委託・紛失通信・ゼロ知識対話型証明・セキュア計算などの暗号要素技術が整備されつつある。

２．研究の目的

量子情報科学の根幹を成す量子情報理論と量子計算量理論は，量子通信・量子アルゴリズムの進展に貢献してきたが，とりわけ量子通信と量子アルゴリズムの双方の要素を持つ量子プロトコルの進展は，量子情報理論・量子計算量理論それぞれにおける技術のみならずそれらが有機的に融合した技術の創出に拠るところが大きい。本研究課題では，量子プロトコルの可能性を追及し，量子プロトコルの限界を究明することを目的とし，そのためにも量子プロトコルの性能解析に必要な量子情報理論的・量子計算量理論的な（融合）技法を発展させ，さらには量子プロトコルの理論として昇華させることを目指す。量子プロトコルは量子情報理論・量子計算量理論に根差しているため，一般の計算機科学の諸問題の解決につながる視点や技法も合わせて追求する。

３．研究の方法

研究体制として，暗号的要素が少ない量子プロトコル班（A班），量子暗号プロトコル班（B班)，量子攻撃安全暗号プロトコル班（C班）を導入する。量子暗号プロトコルは一般の量子プロトコルと比較して満たすべき条件が厳しい。A班において，量子プロトコルを構成する上で必要な量子情報理論と量子計算量理論の融合技術の展開と理論整備を行うことを想定している。C班では量子計算を遂行する敵対者に対して安全な（古典）暗号プロトコルの可能性について検討する。また，古典暗号の新しいパラダイムとしてゲーム理論に基づいた暗号理論が構築されつつあり，量子の設定におけるゲーム理論的暗号理論の可能性について模索することも行う。B班ではA班やC班で得られた知見を生か

し，さらに厳しい条件を満たすべく付加的な技術や必要な理論構築を行う。また，B班で得られる知見に関して，A班やC班にフィードバックを行う。

４．研究成果

(1) 量子対話証明に関して，証明者と検証者の間に事前に定数個のEPR対の共有を許せば健全性が定数誤りのプロトコルでQMAの片側誤り化が可能であることを示した。QMAに限らず一般に任意の量子対話型証明に対してメッセージ数を1回増やすのみで片側誤り化するプロトコルを構築し従来の結果を改良強化した。長年の未解決問題である１ラウンド量子対話型証明の能力の究明に向けて，量子計算量クラスにおいて困難である局所ハミルトニアンの冗長性問題について検討し当該問題が多項式階層第2レベルの量子版に属さないと思われる証拠を与えるとともに適切な形に問題を再定義することで完全性を証明した。Mariott-WatrousのArthur-Merlin型量子対話型証明を一般化したモデルと計算量クラスを提案し，完全問題の存在やBabaiの崩壊定理の量子版などの計算量的構造を明らかにした。QMAの検証者の計算能力をクリフォード回路に制限してもQMAは不変であることを証明した。

(2) 量子アルゴリズムに関する研究に関して，行列積を求める量子アルゴリズムに関する先行研究は基本的に質問計算量の枠組みでこの問題を扱っていたのに対して，時間計算量の枠組みでも従来のアルゴリズムより高速な量子アルゴリズムを構築した。プロトコルの構築や解析に必要不可欠な行列積に着目し，その問題の複雑さを究明するための新しい代数的手法を開発し，従来の方法より高速に半環上の行列の積を計算する量子アルゴリズムの構築に成功した。理論計算機科学の基本的な問題である部分グラフ発見問題に着目し，量子ウォークに基づく既存の技法を発展させて，グラフ上の3クリーク及びハイパーグラフ上の4クリークに対して従来の方法より高速な量子アルゴリズムを構築した。開発した量子アリゴリズムの設計解析方法を発展させ疎グラフ上の三角形発見問題に対する量子アルゴリズム及び量子分散プロトコルの構築に成功した。その量子計算の解析手法に触発され，行列積アルゴリズムの計算量を解析する手法を開発し現在の行列積アルゴリズムの限界を明らかにした。

(3) 計算量理論的アプローチとして，Gowersテストと呼ばれる標数3以上の多項式に対する性質検査の解析を行い低次多項式関数に対する困難性増幅手法を与えた。暗号理論についてほぼk-独立な置換族の鍵長下界を考察することで頑強性を持つ対称鍵暗号を設計しその情報理論的安全性を証明した。素体上多項式の低次性判定に必要な質問計算量の上界と困難性増幅への応用，耐量子計算暗号にも応用されるランダム線形符号の復号のための質問計算量解析のフーリエ解析的なアプローチを与えた。また耐量子性を持つ頑健な共通鍵暗号の鍵長の限界について既存方式が最適であることの証明も与えた。直積定理と呼ばれる暗号理論や計算量理論の基礎となる平均時計算困難性を増幅させる技法の限界について証明手法である帰着を用いた場合どの程度の最悪時計算困難性を損耗するかを評価した。符号理論の重要な問題であるランダム線形符号に対するリスト復号問題の質問計算量の上界の新たなフーリエ解析的手法を得た。

(4) プロトコル理論に対する新たな試みとしてゲーム理論的な枠組みを考察した。暗号プロトコルである紛失通信やコミットメントに対し，既存の安全性と等価であるようなゲーム理論的な安全性を与えた。既存の暗号理論的な安全性では正当性や秘匿性，束縛性などを個別に定義していたのに対し，複数の性質を１つのゲームで特徴付け複数の性質間のトレードオフを考慮するようなプレイヤーに対する安全性を捉えることを可能にした。代表的なプロトコルであるコミットメントに対しゲーム理論的な枠組みによる安全性の定義を与え，既存の暗号理論的な安全性と等価であることを示し，安全性における利得関数を既存研究と比べもっとも一般的な形で与えることに成功した。また，検証者が証明者に報酬を支払う仕組みをもつ合理的対話証明において，既存プロトコルでは悪意のある検証者が報酬を意図的に下げることができることを指摘し，それを防ぐための合理的対話証明の安全性定義を与え，それを満たすプロトコルを提案した。報酬を利用した対話証明プロトコルにおいて，証明者だけでなく検証者も合理的に振る舞う場合の委託計算可能な対話証明プロトコルを構築した。

(5) 量子暗号プロトコルに関しては，量子ブラインド計算と呼ばれるプロトコルが観測ベース量子計算モデルのもとで与えられているが，観測系と計算系が分けられていて観測は観測系だけで行うという補助キュービット駆動型に制限しても量子ブラインド計算が実現することを示した。また，サーバは量子状態を作成送信するだけでクライアントが観測を

行うタイプの量子ブラインド計算は，任意プロトコル中で用いても安全性を保つことができるという性質を有することを示した。
(6) 限られた量子資源での量子プロトコルの性質解明に向け，純粋状態に初期化された量子ビットが少ないモデルに焦点を当て，その計算成功確率が初期化を繰返すことなく増幅可能であることを初めて示した。この技法は極めて強力な性質を持ち，対数個のみの純粋状態を用いる成功確率が非常に小さい片側誤りアルゴリズムが与えられれば純粋状態を僅かに2量子ビットのみ用いる片側誤りアルゴリズムで成功確率が指数的に1に近いもの変換する。古典の計算量クラスを量子的に再検討するため，ポストセレクションを持つ量子計算のサブクラスを考え，そのサブクラスが最悪時一方向性置換を特徴付ける計算量クラスを含むことを明らかにした。その後，多項式時間量子計算に対応する計算量クラスBQPの古典計算量クラスAWPPに対しポストセレクションの概念を利用した量子計算量クラスによる特徴付けを与えた。AWPPがBQPの最良上界である自然な理由を与えAWPPの研究への量子計算量理論的アプローチの可能性を切り拓いた。

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 20 件）

① T. Morimae, H. Nishimura, Quantum interpretations of AWPP and APP, Quantum Information and Computation, vol.16, pp.498-514, 2016, 査読有
URL:http://www.rintonpress.com/xxqic16/qic-16-56/0498-0514.pdf

② I. Kerenidis, M. Lauriere, F. Le Gall, M. Rennela, Information cost of quantum communication protocols, Quantum Information and Computation, vol.16, pp.181-196, 2016, 査読有
URL:http://www.rintonpress.com/xxqic16/qic-16-34/0181-0196.pdf

③ F. Le Gall, H. Nishimura, S. Tani, Quantum algorithms for finding constant-sized sub-hypergraphs, Theoretical Computer Science, vol.609, pp.569-582, 2016, 査読有
DOI: 10.1016/j.tcs.2015.10.006

④ F. Le Gall, S. Nakajima, Quantum Algorithm for Triangle Finding in Sparse Graphs, Lecture Notes in Computer Science (ISAAC 2015), vol.9472, pp.590-600, 2015, 査読有
DOI: 10.1007/978-3-662-48971-0_50

⑤ M. Yasuda, T. Shimoyama, J. Kogure, K. Yokoyama, T. 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 H. Kobayashi, F. Le Gall, H. Nishimura, Stronger methods of making quantum interactive proofs perfectly complete, SIAM Journal on Computing, vol.44, pp.243-289, 2015, 査読有
DOI: 10.1137/140971944

⑦ H. Kobayashi, F. Le Gall, H. Nishimura, Generalized Quantum Arthur-Merlin Games, Leibniz International Proceedings in Informatics (Conference on Computational Complexity 2015), vol.33, pp.488-511, 2015, 査読有
DOI: 10.4230/LIPIcs.CCC.2015.488

⑧ T. Morimae, M. Hayashi, H. Nishimura, K. Fujii, Quantum Merlin-Arthur with Clifford Arthur, Quantum Information and Computation, vol.15, pp.1420-1430, 2015, 査読有
URL:http://www.rintonpress.com/xxqic15/qic-15-1516/1420-1430.pdf

⑨ Akinori Kawachi, Benjamin Rossman, Osamu Watanabe, The query complexity of witness finding, Lecture Notes in Computer Science (CSR 2014), vol.8476, pp.218-231, 2014, 査読有
DOI: 10.1007/978-3-319-06686-8_17

⑩ M. Yasuda, K. Yokoyama, T. Shimoyama, J. Kogure, T. 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

⑪ A. Bogdanov, A. Kawachi, H. Tanaka, On Hard Functions for Low-Degree Polynomials over Prime Fields, ACM Transactions on Computing Theory, vol.5, pp.5:1-5:15, 2013, 査読有
DOI: 10.1145/2493246.2493248

⑫ T. Sueki, T. Koshiba, T. Morimae, Ancilla-Driven Universal Blind Quantum Computation, Physical Review A, vol.87, pp.60301(R)-1-5, 2013, 査読有
DOI: 10.1103/PhysRevA.87.060301

⑬ Francois Le Gall, Yuichi Yoshida, Property Testing for Cyclic Groups and Beyond, Journal of Combinatorial Optimization, vol.26(4), pp.636-654, 2013, 査読有

DOI: 10.1007/s10878-011-9445-8

⑭ F. Le Gall, Quantum Weakly Non-deterministic communication complexity, Theoretical Computer Science, vol.486, pp.43-49, 2013, 査読有
DOI: 10.1016/j.tcs.2012.12.015

⑮ Haruna Higo, Keisuke Tanaka, Kenji Yasunaga, Game-theoretic security for bit commitment, Lecture Notes in Computer Science (IWSEC 2013), vol.8231, pp.303-318, 2013, 査読有
DOI: 10.1007/978-3-642-41383-4_20

⑯ F. Le Gall, Quantum Private Information Retrieval with sublinear Communication Complexity, Theory of Computing, vol.8, pp.369-374, 2012, 査読有
DOI: 10.4086/toc.2012.v008a016

⑰ F. Le Gall, S. Nakagawa, H. Nishimura, On QMA Protocols with Two Short Quantum Proofs, Quantum Information and Computation, vol.12, pp.589-600, 2012, 査読有
URL:http://www.rintonpress.com/xxqic12/qic-12-78/0589-0600.pdf

⑱ S. P. Jordan, H. Kobayashi, D. Nagaj, H. Nishimura, Achieving perfect completeness in classical-witness quantum Merlin -Arthur proof systems, Quantum Information and Computation, vol.12, pp.461-471, 2012, 査読有
URL:http://www.rintonpress.com/xxqic12/qic-12-56/0461-0471.pdf

⑲ F. Le Gall, A Time-Efficient Output-Sensitive Quantum Algorithm for Boolean Matrix Multiplication, Lecture Notes in Computer Science (ISAAC2012), vol.7676, pp.639-648, 2012, 査読有
DOI: 10.1007/978-3-642-35261-4_66

⑳ H. Higo, K. Tanaka, A. Yamada, K. Yasunaga, A game-theoretic perspective on oblivious transfer, Lecture Notes in Computer Science (ACISP2012), vol.7372, pp.29-42, 2012, 査読有
DOI: 10.1007/978-3-642-31448-3_3

〔学会発表〕(計 20 件)

① H. Nishimura, Power of quantum computation with few clean qubits, Workshop around BQP (招待講演), 2015年12月08日, Center for ELC (東京都港区)

② Keiji Matsumoto, On maximization of measured f-divergence between a given pair of quantum states, Nagoya Winter Workshop 2015: Reality and Measurement in Algebraic Quantum Theory (招待講演), 2015年3月9日～13日, 名古屋大学 (愛知県名古屋市)

③ Harumichi Nishimura, Quantum network coding and the current status of its studies, International Symposium on Information Theory and Its Applications (ISITA2014) (招待講演), 2014年10月27日～29日, Melbourne (Australia)

④ Harumichi Nishimura, Generalized quantum Arthur-Merlin games, Australia-Japan Workshop on Multi-user Quantum Network (招待講演), 2014年10月22日～24日, Sydney (Australia)

⑤ Francois Le Gall, Improved quantum algorithm for triangle finding via combinatorial arguments, 55th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2014), 2014年10月20日, Philadelphia (USA)

⑥ Keiji Matsumoto, When one input is always better than the other?, New Horizons in Statistical Decision Theory (招待講演), 2014年9月7日～13日, Oberwolfach (Germany)

⑦ Harumichi Nishimura, Generalized quantum Arthur-Merlin games, ELC Workshop on Quantum Complexity Theory (招待講演), 2014年08月18日, 東京大学 (東京都文京区)

⑧ Kenji Yasunaga, Correction of samplable additive errors, 2014 IEEE International Symposium on Information Theory (ISIT 2014), 2014年07月01日, Honolulu (USA)

⑨ Harumichi Nishimura, Quantum Merlin and Quantum Arthur, 5th Nagoya Winter Workshop on Quantum Information, Measurement, and Foundations (招待講演), 2014年03月07日, 名古屋大学 (愛知県名古屋市)

⑩ Keiji Matsumoto, When is an input stat always better than the others? Universally optimal input states for statistical inference of quantum channels, 5th Nagoya Winter Workshop

on Quantum Information, Measurement, and Foundations (招待講演), 2014年03月06日, 名古屋大学 (愛知県名古屋市)

⑪ Tomoyuki Morimae, Takeshi Koshiba, Composable security of measuring -Alice blind quantum computation, 7th International Conference on Information Theoretic Security (ICITS 2013), 2013年11月29日, Singapore (Singapore)

⑫ T. Koshiba, Composable Security of Blind Computation, Quantum Science Symposium Asia 2013 (QSS-ASIA 2013) (招待講演), 2013年11月26日, 東京大学 (東京都文京区)

⑬ Francois Le Gall, Quantum algorithms for matrix multiplication, 13th Asian Quantum Information Science Conference (AQIS 2013) (招待講演), 2013年8月26日, Chennai (India)

⑭ Keiji Matsumoto, Universally optimal input states for channel estimation/query complexity problems, Intensive Month on Operator Algebra and Quantum Information (招待講演), 2013年07月09日, Madrid (Spain)

⑮ Francois Le Gall, Quantum Complexity of Matrix Multiplication, Satellite Workshop of ICALP 2013 on Quantum and Classical Complexity (招待講演), 2013年7月7日, Riga (Latvia)

⑯ Harumichi Nishimura, Quantum network coding - How can network coding be applied to quantum information?, 2013 IEEE International Symposium on Network Coding (NetCod2013) (招待講演), 2013年06月09日, Calgary (Canada)

⑰ S. P. Jordan, H. Kobayashi, F. Le Gall, D. Nagaj, H. Nishimura, Towards Perfect Completeness in QMA, The 16th Workshop on Quantum Information Processing (QIP 2013), 2013年1月22日, Beijing (China)

⑱ Hirotada Kobayashi, Francois Le Gall, and Harumichi Nishimura, Stronger methods of making quantum interactive proofs perfectly complete, 2013 ACM Conference on Innovations in Theoretical Computer Science (ITCS 2013), 2013年01月11日, Berkeley (USA)

⑲ F. Le Gall, Faster Algorithms for Rectangular Matrix Multiplication, The 53rd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2012), 2012年10月23日, New Brunswick (USA)

⑳ Takahiro Sueki, Takeshi Koshiba, Tomoyuki Morimae, Ancilla-Driven Blind Quantum Computation, The 2nd Conference on Quantum Cryptography (QCRYPT 2012), 2012年09月11日, Singapore (Singapore)

〔図書〕(計１件)

① 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)研究分担者

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

ルガル　フランソワ(LE GALL, Francois)
東京大学・情報理工学系研究科・特任准教授
研究者番号：50584299

田中　圭介 (TANAKA, Keisuke)
東京工業大学・情報理工学研究科・准教授
研究者番号：20334518

河内　亮周 (KAWACHI, Akinori)
徳島大学・ソシオテクノサイエンス研究部・講師
研究者番号：00397035

安永　憲司 (YASUNAGA, Kenji)
金沢大学・電子情報学系・助教
研究者番号：50510004

松本　啓史 (MATSUMOTO, Keiji)
国立情報学研究所・情報学プリンシプル系・准教授
研究者番号：60272390

小林　弘忠 (KOBAYASHI, Hirotada)
国立情報学研究所・情報学プリンシプル系・特任研究員
研究者番号：60413936