様式 C-19

科学研究費補助金研究成果報告書

平成２２年　４月　１日現在

研究種目：基盤研究(B)
研究期間：2006～2008
課題番号：18300002
研究課題名（和文）　量子情報理論と量子計算量理論の融合とその応用

研究課題名（英文）　Crossover between Quantum Information Theory and Quantum Computational Complexity Theory

研究代表者
小柴　健史（KOSHIBA TAKESHI）
埼玉大学・理工学研究科・准教授
研究者番号：60400800

研究成果の概要（和文）：量子情報処理を遂行できる実体の可能性・将来性について，対話型証明・暗号理論・アルゴリズム理論の観点から考察し，対話型証明においては量子エンタングルメントが有効であることを確認し，暗号理論においては非対話型のビット委託方式の提案を行い，アルゴリズム理論においては代表的な問題である隠れ部分群問題に対する量子アルゴリズムの限界を導出した．

研究成果の概要（英文）：We investigated the potential abilities of quantum information processing from the viewpoints of interactive proofs, theory of cryptography and algorithms. We showed that quantum entanglement is effective in multi-prover systems, proposed a non-interactive bit commitment scheme, and derived a limitation of quantum algorithms for the hidden subgroup problem.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2006 年度	4,300,000	1,290,000	5,590,000
2007 年度	3,700,000	1,110,000	4,810,000
2008 年度	3,500,000	1,050,000	4,550,000
年度			
年度			
総　計	11,500,000	3,450,000	14,950,000

研究分野：総合領域
科研費の分科・細目：情報学・情報基礎
キーワード：量子計算理論，量子情報理論，暗号理論，量子アルゴリズム

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より強力な情報処理を可能にする分野として，近年大いに注目されている．例えば，大きな合成数の素因数分解を効率よく行うことは従来の計算機上では不可能と予想されているが，Shorは量子計算機を用いれば効率のよい素因数分解アルゴリズムが存在することを示した．一方，BennettとBrassardによって最初に提案された量子鍵配送は，安全性に計算量的仮定を必要としない究極の暗号として現在世界の研究グループ間でその早期実現が競われている．ま

た，これらに続く大結果を求めて情報理論，計算機科学双方の分野で世界的に年々研究が盛んになっている．しかし一方で，その二つの分野の間には隔たりがあり，現在のところ，それぞれの分野が独自に発展を遂げている．

当該研究では，量子情報理論と量子計算機科学の双方の特長を融合した新たな技法・基礎理論を展開することにより，量子情報科学の分野全体の更なる発展に貢献することを目標とする．

その意義を具体的に述べる．量子情報理論の最大の成果の一つである量子鍵配送は二者間通信における究極の暗号基礎技術を与えるが，現代暗号の中心的成果である多者間の多様なプロトコルは鍵配送のみでは実現しない．しかも，多者間通信を想定した現代暗号の安全性の重要な根拠である素因数分解の困難性の仮定がShorの結果により崩れるため，量子計算機の存在下でも安全な暗号系の構築が最重要課題となる．さらに，例えばビットコミットメントやコイン投げなどの基本プロトコルにおいては，量子情報理論的な安全性は達成不可能であると証明されている．従って，量子計算量的な安全性の概念は不可欠で，計算量理論に基づき，かつ量子情報理論の特長を生かした量子暗号基礎理論が必須となる．このような問題意識は世界的にも広まり始めており，2006年にはPost-Quantum Cryptographyという国際会議が開催される．この流れにおいて，当該研究のテーマである量子情報理論と量子計算機科学，特に量子計算量理論との融合は，将来の暗号・通信技術の核となる要素技術や基礎理論の確立に重要な役割を果たすと考えられる．

また，(量子ではない)従来の情報理論と計算機科学の融合による成功事例に，例えば確率的検査可能証明や統計的ゼロ知識証明の研究がある．特に前者は計算量クラスNPの新たな特徴付けを与え，近似不可能性という新たな理論体系の開拓や，符号理論に対する新展開など，計算機科学と情報理論双方の進展に大きく寄与した．一方，擬似乱数生成や計算量的エントロピーなど，情報理論的概念に計算量理論的概念を導入することにより新たな研究分野を創成した事例もある．従って，量子の場合においても，量子情報理論と量子計算機科学，特に量子計算量理論の融合は，量子暗号に限らず，量子情報科学分野全体に貢献することができると期待される．

２．研究の目的

当該研究の目的は以下に大別される．

(1) 量子情報理論的概念を計算量理論的立場から解析し，量子情報理論への新展開を与える．

(2) 量子情報理論と量子計算量理論の双方の特長を生かした量子暗号の要素技術を確立する．

(3) 量子計算機科学，特に量子計算量理論に量子情報理論的手法を応用し，個々の計算機科学的問題の解決につながる新しい統一的な視点や技法を追求する．

量子情報理論と量子計算機科学，特に量子計算量理論との双方向での融合を通して，量子暗号を始めとして，量子計算，量子通信など，量子情報科学の分野全体の進展に貢献できる基礎理論の構築を目標とする．

３．研究の方法

目的(1)は情報理論的側面が強い研究で，主に小林と松本が担当する．目的(3)は計算量理論的側面が強い研究で，主に河内が担当する．目的(2)は中間的な研究で主に研究代表者の小柴が担当する．特に(2)は中間的技術が暗号への応用へつながるという点のみならず中間的な存在であるために(1)と(3)との間のパイプ役あるいは統括的な役割も兼ねる．なお，サブテーマは独立ではなく相互に連携しているため横断的な研究が存在する．つまり，(1)にもアルゴリズム的な要素が要求される一方で，(3)でも情報理論的な要素が要求され，相互に連携を図りつつ研究を遂行する．以下，目的ごとの方法について述べる．

(1)「エンタングルメントや量子通信路の計算機科学的性質の解析」に焦点を当てる．エンタングルメントは量子情報科学の根底をなす最重要概念の一つであるが，その性質は未解明の部分が非常に多い．従来のこの方面の研究の殆どは情報理論の立場からなされており，計算機科学の立場からはAaronson (STOC 2004, pp.118-127)によるエンタングルメント分類へ向けた問題提起など数えるほどしかない．これに対し当該研究では，NPの量子版であるQMAにおける証拠間のエンタングルメントの有無と検証能力の関係などを通じて，エンタングルメントを従来とは異なる視点から計算

機科学的に解析する．また，証明者間のエンタングルメントの多証明者量子対話型証明に与える影響に関する基本結果や量子対話型証明と量子通信路判別問題の関連付けなどを糸口に，量子対話型証明の諸性質を解明することにより，エンタングルメントや量子通信路の計算機科学的解析につなげる．

(2)「量子一方向性関数の性質解明と量子暗号への応用」に焦点を当てる．一方向性関数は現代暗号における最重要概念の一つであり，計算量理論に基づいた量子暗号系においても，量子一方向性関数の概念は不可欠と考えられるが，その性質は殆ど未解明である．現状では，量子一方向置換という特殊ケースに関する特徴付けや，Dumais, Mayers, Salvail (EUROCRYPT 2000, pp.300-315)によるビットコミットメントへの応用が知られているのみで，一般の量子一方向性関数に関する結果は殆どない．また，量子計算においては素因数分解などの困難性の仮定が崩れるため，既知の量子一方向性関数の候補も少なく，量子一方向性置換に関しては一つも候補が知られていない状況である．そこで，量子情報理論的な性質を考慮することで，量子一方向性関数の候補の発見や量子暗号プロトコルへの応用へ役立てる．

(3)「量子情報理論における測定理論の量子アルゴリズムへの応用」に焦点を当てる．量子計算が対象にしている問題は多くの場合，本質的には与えられた量子状態が何であるかを同定する問題に帰着される．例えば，ある種の群に対する隠れ部分群問題に対して，Bacon, Childs, van Dam (FOCS2005)は問題に隠れている群構造に対応する量子状態を生成・同定することに帰着し，量子情報理論における最適測定を利用することで効率の良い量子アルゴリズムの設計に成功している．一方でこの結果のように量子アルゴリズムの設計における量子情報理論的応用は他には殆ど知られていない．そこで当該研究では最適測定設計の理論を機軸とした新しい量子アルゴリズムの設計手法の確立を目指す．

４．研究成果

(1) 量子対話証明の観点からエンタングルメントの諸性質について解明することに成功している．具体的には，量子対話証明の観点から共有エンタングルメントによる不正攻撃の導出に成功し，量子対話証明において複数証明者モデルが単一証明者モデルよりも能力が高いことを証明した．また，証明者を１名追加することで 100%の完全性を保ちつつ１ラウンドに並列化できることを示した．更に，証明者は古典のままで検証者のみ量子操作ができる複数証明者量子対話証明モデル(MIP*)において計算量クラス PSPACE や NEXP に対するプロトコルの構成を与え，証明者間の共有エンタングルメントを用いた不正攻撃の強い限界を与えた．証明者の事前エンタングルメントの有効活用性も示すことに初めて成功し，検証者も量子である複数証明者量子対話証明のモデル(QMIP)の重要な諸性質を導いた．

(2) 計算量理論の観点からの量子暗号プロトコルの諸性質の導出に成功している．具体的には，量子公開鍵暗号の安全性概念として，識別不可能性と量子情報強秘匿性の等価性を証明し，研究代表者らが提案した量子公開鍵暗号がより高い安全性を有することを示した．また，古典では構成不可能な非対話型の統計的秘匿量子ビットコミットメント方式を量子一方向性関数のサブクラスを用いて構成できることを証明した．

(3) 隠れ部分群問題と呼ばれる量子アルゴリズムの能力および限界を量子情報理論的な観点から導くことに成功した．具体的には，有限群の広いクラスにおいて隠れ部分群問題を解くための量子状態のサンプル数の情報理論的に緊密な上下界を与えることができた．この性質により，上述の量子公開鍵暗号の性能評価として利用でき，発行する公開鍵の数が少ないときは，量子公開鍵暗号が量子情報理論的な安全性保証が系として導かれた．

量子対話証明とエンタングルメントの諸性質の解明については，大きく理解が進んだものと考えられる．これらの研究成果は，計算量理論の国際会議では権威のある IEEE Conference on Computational Complexity で発表されており対外的な評価も高いと判断できる．また，チューリング賞受賞者でもある Yao を初めとして，国際的に著名な研究者らと共同研究を遂行できている点も特筆

すべきことと考えている．また，計算量理論的な暗号理論研究と測定理論に基づいた量子アルゴリズムの限界の研究に関しては，「融合」という考え方が機能して達成された結果であり，当該研究の方向性の正しさを実証することができた．国際会議等で招待講演を行うなど，研究成果について対外的な評価もあるものと考えられる．

これらの研究成果は融合技術の初期的な段階の成果であり，更なる研究を重ねて融合技術を展開を行うことが重要である．今後は応用的な視点も考慮しつつ発展させることが重要で，基盤研究(B)「量子情報理論と量子計算量理論の融合技術の展開」（課題番号：21300002，研究代表者：小柴健史，2009年度～2012年度)において継続研究を行う．

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 13 件）

① T. Koshiba, T. Odaira, Statistically hiding quantum bit commitment from approximable preimage size quantum one-way function, Lecture Notes in Computer Science, 査読有, Vol.5906, 2009, pp.33-46
② M. Hayashi, A. Kawachi, H. Kobayashi, Quantum measurements for hidden subgroup problems with optimal sample complexity, Quantum Information and Computation, 査読有, Vol.8, 2008, pp.345-358
③ T. Ito, H. Kobayashi, D. Preda, X. Sun, A. C. -C. Yao, Generalized Tsirelson inequalities, commuting-operator provers, and multi-prover interactive proof systems, Proc. 23rd Annual IEEE Conference on Computational Complexity, 査読有, 2008, pp.187-198
④ J. Kempe, H. Kobayashi, K. Matsumoto, T. Vidick, Using entanglement in quantum multi-prover interacitve proofs, Proc. 23rd Annual IEEE Conference on Computational Complexity, 査読有, 2008, pp.211-222
⑤ K. Kurosawa, W. Kishimoto, T. Koshiba, A combinatorial approach to deriving lower bounds for perfectly secure oblivious transfer reductions, IEEE Transactions on Information Theory, 査読有, Vol.54, 2008, pp.2566-2571
⑥ A. Kawachi, K. Tanaka, K. Xagawa, Concurrently secure identification schemes based on the worst-case hardness of lattice problems, Lecture Notes in Computer Science, 査読有, Vol.5350, 2008, pp.372-389
⑦ A. Kawachi, C. Portmann: On the power of quantum encryption keys, Lecture Notes in Computer Science, 査読有, Vol.5299, 2008, pp.165-180
⑧ K. Kurosawa, T. Koshiba, Simple direct reduction of string (1,2)-OT to Rabin's OT without privacy amplification, Lecture Notes in Computer Science, 査読有, Vol.5155, 2008, pp.199-209
⑨ K. –Y. Cheong, T. Koshiba, More on security of public-key cryptography based on Chebyshev polynomials, IEEE Transactions on Circuits and Systems II, 査読有, Vol.54, 2007, pp.795-799
⑩ T. Izu, J. Kogure, T. Koshiba, T. Shimoyama, Low-density attack revisited, Desings, Codes and Cryptography, 査読有, Vol.43, 2007, pp.47-59
⑪ A. Kawachi, K. Tanaka, K. Xagawa, Multi-bit cryptosystems based on lattice problems, Lecture Notes in Computer Science, 査読有, Vol.4450, 2007, pp.315-329
⑫ A. Kawachi, T. Koshiba, Progress in quantum computational cryptography（招待論文）, Journal of Universal Computer Science, 査読無, Vol.12, 2006, pp.691-709

〔学会発表〕（計 12 件）

① T. Ito, H. Kobayashi, K. Matsumoto, Oracularization and two-prover one-round interactive proofs against nonlocal strategies, The 12th Workshop on Quantum Information Processing, 2009 年 1 月 14 日, Santa Fe, USA
② T. Koshiba, On quantum oblivious

transfer (招待講演), JST-CNRS Joint Workshop on Quantum Computer: Theory and Feasibility, 2008 年 9 月 25 日, Paris, France

③ M. Hagiwara and A. Kawachi, Relations between orthogonality and linear independence (招待講演), JST-CNRS Joint Workshop on Quantum Computer: Theory and Feasibility, 2008 年 9 月 25 日, Paris, France

④ T. Ito, H. Kobayashi, D. Preda, X. Sun, A. C. -C. Yao, Generalized Tsirelson inequalities, commuting-operator provers, and multi-prover interactiveproof systems, The 11th Workshop on Quantum Information Processing, 2007年12月17日, New Delhi, India

⑤ J. Kempe, H. Kobayashi, K. Matsumoto, T. Vidick, Using entanglement in quantum multi-prover interactive proofs, The 11th Workshop on Quantum Information Processing, 2007 年 12 月 17 日, New Delhi, India

〔図書〕(計 1 件)

① 小芦雅斗, 小柴健史, サイエンス社, 量子暗号理論の展開(臨時別冊・数理科学 SGC ライブラリ 67), 2008, pp. 79-129

６．研究組織

(1)研究代表者

小柴　健史 (KOSHIBA　TAKESHI)

埼玉大学・大学院理工学研究科・准教授

研究者番号：60400800

(2)研究分担者

松本　啓史 (MATSUMOTO　KEIJI)

国立情報学研究所・准教授

研究者番号：60272390

小林　弘忠 (KOBAYASHI　HIROTADA)

国立情報学研究所・プロジェクト研究員

研究者番号：60413936

河内　亮周 (KAWACHI　AKINORI)

東京工業大学・大学院情報理工学研究科・助教

研究者番号：00397035