様式 C-7-2

自己評価報告書

平成２１年　４月２８日現在

研究種目：基盤研究(B)
研究期間：2006～2010
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・大学院理工学研究科・准教授
研究者番号：60400800

研究分野：総合領域
科研費の分科・細目：情報学・情報学基礎
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．研究計画の概要

当該研究は，(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，ことを目的とする．以下に具体的な計画概要を方向性毎に記載する．

(1)の方向性の研究として主に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いる．当該研究では，対話証明における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．

(2)の方向性の研究として主に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，当該研究では，量子情報理論的な性質を考慮することで従来結果を発展させて一般の量子一方向性関数の性質の解明を目指し，さらに量子情報理論的な性質も考慮することにより，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)の方向性としては主に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．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成功例が散見される．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・その手法の確立を目指す．

２．研究の進捗状況

(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導かれる．

３．現在までの達成度
②おおむね順調に進展している．
（理由）
量子対話証明の観点からの量子エンタングルメントの性質究明の研究は２年目，３年目とそれぞれコンスタントに研究成果を得ることができており順調に進展している．研究の遂行とともに，量子エンタングルメントは量子計算における根源に深く関与し，その理解が必須であると考え，当初３年目以降の予定であった量子通信路と量子対話証明との関係解明の研究は必要最小限に留まっている．量子暗号理論の研究においては，量子公開鍵暗号の安全性や量子ビットコミットメントの提案など，一定の研究成果を得ているが散発的ともいえる．量子アルゴリズムの研究においては，量子アルゴリズムを考察する上での基本的問題の量子状態識別問題について重要な研究成果を得ている．量子暗号理論・量子アルゴリズム研究の成果はやや散発的であるが，本課題の目的である融合技術の創出という観点からすると，大きな成果となっていると判断できる．

４．今後の研究の推進方策
三年間の研究を通して感じたことは，量子情報理論と量子計算量理論の融合のみならず，古典計算量理論に関する知見が大きく求められたことである．また，今後，研究成果を発散させないためにも融合技術の適用先をある程度限定する必要性があると思われる．このような観点からすると，古典暗号理論に関して支援して貰える研究分担者の参画が望ましいと判断し，前年度応募を利用して研究計画の発展的修正を行うことにした．次年度からは，上記修正点を考慮した後継課題（課題番号 21300002）として研究を遂行する．個々のトピックについて言及すると，量子対話証明の研究が量子暗号理論・量子アルゴリズムの研究と深く関連してこなかったことが問題点として挙げられる．複数証明者による量子対話証明の研究は，暗号理論において複数参加者でのセキュア計算と関連することが予想されるので，各トピックがより有機的に融合するように研究の方向性を調整しながら研究を推進する．

５．　代表的な研究成果
（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 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
② 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.
③ 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
④ 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, 採録決定済

〔学会発表〕（計１２件）

〔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