氏名	河内亮周（かわち あきのり）
学位(専攻分野)	博士（情報学）
学位記番号	情博第132号
学位授与の日付	平成16年9月24日
学位授与の要件	学位規則第4条第1項該当
研究科・専攻	情報学研究科通信情報システム専攻
学位論文題目	Studies on Quantum Query Complexity and Quantum Computational Cryptography （量子質問計算量および計算量的量子暗号に関する研究）
論文調査委員	（主査）教授 岩間一雄　教授 福嶋雅夫　教授 北野正雄

論文内容の要旨

本論文では，量子計算に対する数理的計算モデルに関して，理論計算機科学の立場から量子質問計算量および計算量的量子暗号の研究がなされている。具体的には，オラクル同定問題に対する量子アルゴリズム，量子サンプリングによるビンとボールのゲーム，3関数クロー探索問題に対する量子アルゴリズム，量子一方向性置換の万能検査に関する結果が与えられている。

第1章，第2章では研究の背景及び結果の概要，および量子計算の基本的概念が述べられている。量子計算研究の現状を踏まえ，量子質問計算量，計算量的量子暗号の重要性が指摘され，その研究の意義について議論されている。さらにそれぞれの章で示される結果の重要な点が直観的に分かりやすくまとめられている。また第3章以降の結果を知るために必要な知識についても簡潔に述べられている。

第3章ではオラクル同定問題についての議論を行っている。オラクル同定問題は非常に一般化された問題であり，グローバー探索等従来議論されてきた様々な問題がこの問題の特殊な場合となっている。本章ではこの問題に関して極めて巧みな量子アルゴリズムを示すことにより，オラクル同定問題の質問計算量の上界を与え，それにほぼ一致するような質問計算量の下界も証明している。

第4章では質問計算量が低い場合においての量子計算と古典計算の能力差について，ビンとボールのゲームを題材として量子計算と古典計算の差を議論している。ビンとボールのゲームに量子サンプリングを適用した場合にはランダムサンプリングの場合と比較してビンの最大高さが二次関数的に下がるという証明がされており，また連続モデルにおけるビンとボールのゲームに量子サンプリングを適用した場合の解析も行っている。

第5章では三関数に対する量子クロー探索アルゴリズムについて述べている。これまで二関数に対する効率の良い量子クロー探索アルゴリズムおよびその三関数への拡張が知られていたが，本章では最初の二関数についてのクローの数が少ない場合に，より低い質問計算量で三関数のクローを発見できる量子アルゴリズムを与え，その質問計算量の評価を行っている。

第6章では量子一方向性置換の万能検査についての結果を与えている。強力な計算能力を持つ量子計算機による盗聴に対しても安全性を保証できるような暗号系の構築のために量子一方向性置換を発見することは重要な課題である。本章では，その存在性の手がかりとして重要な未解決問題であった存在性の必要十分条件を完成させ，それを元にした量子一方向性置換の万能検査が示されている。

最後に第7章では，以上の結果をまとめ，さらに今後の方針が与えられている。

論文審査の結果の要旨

量子計算の能力の解析は古典計算の場合とは大きく異なる手法を要求され，そのための独特な手法が研究されてきた。本論文においても量子質問計算量のための新たなアルゴリズムの設計・解析手法を導入し，その結果として得られた知見は量

子計算の能力の本質を見極めるための良い指針を与えている。また量子計算における暗号系の設計は実用的にも重要な問題であり，その基礎に関する研究が注目されている。その研究の中で計算量的暗号の基礎は今後の暗号研究に大きな影響を及ぼす。これらの観点から，本論文の結果について特筆すべき点は以下の通りである。

1．オラクル同定問題という非常に一般的な問題を導入することにより，現在までに研究されてきた数多くの問題を包含する統一的な視点を与え，その質問計算量のほぼ一致する上下界を与えている。量子アルゴリズムの設計という観点からも斬新である。

2．量子サンプリングでのビンとボールのゲームについて解析することにより質問計算量が低い場合での古典計算と量子計算の能力差を考えるという新しいアイデアを示している。

3．三関数のクロー探索問題に対して，中間的な解，即ち最初の二つの関数に対するクローが少ない場合に従来知られていたものよりも質問計算量の少ない量子アルゴリズムを示している。

4．未解決問題として知られていた量子一方向性置換の存在性の必要十分条件を完成させ，その帰結から量子一方向性置換の万能検査を与えている。

論文の前半で議論されている量子質問計算量は現在の量子計算研究の中心的分野の一つであり，数多くの研究者により精力的に研究が行われている。それらの研究の中で例えばオラクル同定問題に関する結果は量子質問計算量にまつわる既存の問題への包括的な考察を与えており，それらの問題の本質の理解を助けている。また論文の後半で議論されている計算量的量子暗号についても近年その重要性から研究が盛んに行われている。特に本研究で議論されている量子一方向性置換はその構築に非常に有用であるため活発な研究がなされてきたが，その存在は従来知られていなかった。本研究により完成した必要十分条件は量子一方向性置換の存在性証明に向けて重要な進展をもたらすものと考えられる。

以上，本研究は量子計算に関するアルゴリズムの設計と解析，および計算量的暗号系の基礎に関して学術上意義深い結果を導いている。よって，本論文は博士（情報学）の学位論文として価値あるものと認める。

また，平成16年８月12日に施した論文内容とそれに関連した試問の結果合格と認めた。