論 文 内 容 の 要 旨

博士論文題目

The Ability of Quantum Information Processing Under the Resource-restricted Circumstances

(資源を限定した状況下における量子計算の能力に関する研究)

氏　名　　Yumiko Murakami (村上　ユミコ)

(論文内容の要旨 1200字程度)

本論文は、量子情報処理分野のうち、特に計算資源が限定された状況下での量子計算に関する研究により得られた成果をまとめたものである。量子計算は、量子力学に基づく新しい計算パラダイムであり、従来の計算（古典計算と呼ばれる）に比べ潜在的に強力な情報処理が可能である。しかし現在の技術では理想的な量子計算機を構築することはできず、実際に実現される量子計算機にはその操作について様々な制約が課されることが予想される。よって、様々な制約状況下での計算能力を考える必要がある。本研究の主要な成果は以下の通りである。

第一に、メモリがスタックに限定された量子計算モデルである量子プッシュダウンオートマトンの認識能力について、従来の決定性プッシュダウンオートマトンとの比較を行っている。計算モデル理論においては、量子オートマトンと古典オートマトンの認識能力の関係は未解決の問題である。量子オートマトンの方が古典のものよりも能力的に劣っているとの否定的な結果がいくつか報告されており、量子計算の優位性は自明のものではないことがわかっている。オートマトンの能力を特徴付ける際には、認識できる言語のクラスの包含関係を示すことが一般的であるが、本論文では、言語ではなくプロミス付きの問題を考え、あるプロミス付き問題について、量子プッシュダウンオートマトンではエラーなしで解けるものの、古典の決定性プッシュダウンオートマトンでは解けないことを示している。なお、この問題を解く量子プッシュダウンオートマトンは、ドイチェ・ジョザのアルゴリズムをオートマトンに適切に適用することによって構成している。また、古典プッシュダウンオートマトンがその問

題を解けないことについては、一般化された Ogden の補題を修正したものを用いて証明を行っている。この結果は、量子プッシュダウンオートマトンが古典のものよりも強い能力を持っていることを示唆するものである。

第二に、量子状態を送信可能な量子直接秘密通信プロトコルを提案している。従来の量子直接秘密通信プロトコルは、量子エンタングルメントと呼ばれる状態維持の非常に難しい量子計算特有の資源を利用するものが多い。しかし提案手法は、この資源を一切使用せず、また、光子数分割攻撃と呼ばれるデバイスの精度の低さにつけこむ攻撃に対して耐性があるため、他の提案手法に比べ、現在の技術でも実装がしやすいと考えられる。提案手法は、古典情報に加えて量子情報を送信することができるため、安全性の評価として、量子情報に関する何らかの定量的な基準が必要になる。本論文では、量子状態の忠実度に基づく安全基準を提案し、提案手法がなりすまし攻撃に対してその安全基準を満たしていることを証明している。

氏　名	村上　ユミコ

（論文審査結果の要旨）（Ａ４　１枚　１、２００字程度）

量子計算は、ニュートン力学に基づく従来の計算原理（古典計算と呼ばれる）とは異なり、量子力学に基づいて動作するものである。そのため、従来の計算よりも強力な情報処理を実現することが期待されている。しかし、期待される能力を発揮する量子計算機を実現することは、現在の技術では非常に困難だと考えられており、より実現可能な範囲での量子計算の能力を研究することが重要であると言える。本論文は、量子計算資源の使用が制限された状況下における量子情報処理の能力に関する考察を行ったもので、得られた主要な成果は以下のとおりである。

【１】量子プッシュダウンオートマトンと古典プッシュダウンオートマトンの、エラーなし計算における能力比較。プッシュダウンオートマトンとは、スタックを持ったオートマトンであり、量子メモリのアクセスに制限を持った計算モデルに相当する。計算モデルによる比較において、量子オートマトンのほうが古典のものよりも能力が劣っているという否定的な結果もいくつか報告されており、資源が制限された状況下において量子計算の優位性は自明のものではない。オートマトンの能力を特徴付ける際には、認識できる言語のクラスの包含関係を示すことが一般的であるが、本論文では、言語ではなく、プロミス付きの問題を考え、ある種のプロミス付き問題について、量子プッシュダウンオートマトンではエラーなしで解けるものの、古典の決定性プッシュダウンオートマトンでは解けないことを示している。このことは量子プッシュダウンオートマトンが古典のものよりも強い能力を持っていることを示唆している。

【２】新しい量子直接秘匿通信プロトコルの提案とその安全性解析。量子直接秘匿通信は、暗号化鍵を無条件安全に共有する量子鍵配布プロトコルと異なり、秘密情報を直接やりとりすることを目指したものである。本論文では、既存の量子直接秘匿通信プロトコルとは異なり、現在の技術では制御困難な量子計算資源を一切用いずに、任意の量子情報を安全に共有することのできるプロトコルを提案した。提案プロトコルは光子数分割攻撃に対する耐性が高いため、実装上高精度のデバイスを必要としないことが特徴である。安全性の議論に関しては、提案プロトコルは古典状態だけでなく、量子状態を送信できるプロトコルであるため、従来は考慮されていなかった、「量子状態の送信に対する安全性の尺度」が必要となる。本論文では、量子状態を送信するプロトコルが満たすべき安全性尺度を、量子状態の忠実度の観点から定義し、提案手法がある種のなりすまし攻撃に対し耐性をもっていることを示した。

以上、本論文は学術上、実際上寄与するところが少なくない。よって、本論文は博士(工学)の学位論文として価値あるものと認める。