審査の結果の要旨

論文提出者氏名　　松浦　孝弥

提出された学位論文は、光をはじめとする調和振動子と等価な量子系において、ホモダイン測定などの連続値を出力する測定を用いて情報処理を行う手法に関する理論的研究の成果についてまとめたものである。情報処理を行う現実的な装置はデジタル信号すなわち離散量しか扱えないため、上記のような連続変量系の量子力学的性質を利用した量子情報処理を実行するためには、離散量と連続量の間の橋渡しをする仕組みを工夫する必要がある。本論文は、量子情報の重要な応用である量子暗号通信と量子計算について、離散量と連続量をつなぐ理論的手法を新たに提案することにより、これまで懸案とされていた問題の解決や、量子情報処理のより効率的な実行方法の提案へとつなげている。

本論文では、第一に、量子暗号通信の代表である量子鍵配送（QKD）の新たな手法提案とそのセキュリティ証明を行っている。QKD 方式は、光子検出器を用いる離散量 QKD と、ホモダイン検出器を用いる連続量 QKD に大きく分類される。前者に比べて、後者は波長弁別性や既存技術との親和性などの応用上の利点が指摘されている反面、連続量をデジタル信号処理に落とし込む部分の理論構築が難しく、有限の時間であらゆる盗聴攻撃からの安全性を確保するという目標は、永らく未解決の問題として残されていた。本論文では、離散量 QKD において、正規の状態との忠実度を光子検出器により測定し、盗聴量の推定に用いている点に着目し、ホモダイン検出器を２台用いるヘテロダイン測定の測定結果から忠実度を推定する新たな手法を開発している。この手法に基づき、デジタル信号処理で実行可能な連続量 QKD プロトコルを提案し、有限の通信時間での完全なセキュリティ証明を与えている。

第二に、Gottesman-Kitaev-Preskill (GKP)符号を用いた量子計算の理論を拡充し、調和振動子系を用いた量子計算を従来よりも効率的に行う手法を提案している。GKP 符号は、調和振動子系に量子ビットの情報を符号化する手法として知られ、ゲート操作や誤り訂正操作をガウシアン操作のみで実行できることから、光などの調和振動子系を用いた量子計算の実装法として有力視されている。GKP 符号自体は非物理的な極限であるため、実際に生成できるのはその近似状態である。これまで、目的に応じて異なる複数の定義の近似状態が用いられてきたが、本研究ではそれらの関係性を明らかにし、近似状態の標準形を定義することで、既存の近似状態を統一的に扱える理論を構築している。さらに、GKP 符号化された量子ビットの状態の中で、標準基底の状態とは異なる特定の状態が万能量子計算のリソースとして高い能力を持つことを見出し、この一種類の GKP 状態とガウシアン操作だけで万能量子計算が実行できることを示している。この手法は、標準基底の GKP 状態を用いる類似の先行研究に比べて GKP 状態の必要数を大きく低減できる特長を持つ。

本論文は、全６章から構成される。以下に各章の内容を要約する。

第１章では、導入として本研究の背景について述べ、その上で本研究の概要を示し、さらに本

論文の構成について述べている。

第２章では，本論文で前提とされる、量子情報理論の基本的な枠組みについて説明している。量子系の状態準備、操作、測定の記法と、量子状態の識別可能性の指標である忠実度とトレース距離の諸性質について述べている。

第３章では、連続変量系特有の量子情報理論の前提知識についてまとめている。正準交換関係から出発し、特性関数、ウィグナー関数による状態表現と、ガウシアン操作の一般論について説明している。さらに、光系の量子的な取り扱いについて説明し、コヒーレント状態、スクイーズド状態の導入と、ホモダイン測定、ヘテロダイン測定の量子情報理論的な記述について述べている。

第４章では、ホモダイン測定とヘテロダイン測定を用いる QKD プロトコルの提案と、その安全性の証明について述べている。まず、この章で用いる記法と、数学および情報理論の前提知識について説明し、QKD プロトコルの安全性の証明で用いられる一般的な技法について説明している。次に、ヘテロダイン測定を用いて、コヒーレント状態との忠実度の厳密な下界を算出する推定手法を提案し、この手法を用いた QKD プロトコルを提案している。続いて、このプロトコルの厳密な安全性証明を与えている。さらに、誤り訂正の方向を逆方向としたプロトコルの解析を緻密に行い、鍵生成効率を改善する手法について述べている。

第５章では、GKP 符号を用いて調和振動子系で量子計算を実行する上で、有用な理論的技法の提案と、GKP 状態の必要数を低減する新たな手法の提案を行っている。章の前半では、GKP 近似状態として従来３種類の異なる状態が用いられてきた経緯を説明した上で、それらが簡単なガウシアン操作で関連付けられることを示し、統一的な取り扱いを可能にする GKP 近似状態の標準形を提案している。章の後半では、量子ビットの標準基底ではない特定の状態を符号化した GKP 状態を１種類だけ準備することで、ガウシアン操作のみで万能量子計算を実行する手法を提案し、これまでに知られた手法よりも GKP 状態の必要数を大きく低減できることを示している。

第６章では，以上の結果をもとに本研究の成果を整理し、今後の展望をまとめている。

以上のように、本論文で述べられている理論研究の成果は、連続量 QKD において懸案であったセキュリティの未解決問題を解決し、光系をはじめとする調和振動子系を用いた量子計算の効率化に貢献するなど、連続変量系を用いた量子情報処理手法を著しく発展させるものである。

よって本論文は博士（工学）の学位請求論文として合格と認められる。