

氏名(本籍)	おおくぼ ゆう た (茨城県)		
学位の種類	博士(理学)		
学位記番号	博甲第5276号		
学位授与年月日	平成22年3月25日		
学位授与の要件	学位規則第4条第1項該当		
審査研究科	数理物質科学研究科		
学位論文題目	On the implementation of quantum information processing with linear optics (線形光学による量子情報処理技術の実装について)		
主査	筑波大学教授	博士(工学)	富田章久
副査	筑波大学教授	理学博士	舛本泰章
副査	筑波大学准教授	博士(理学)	池沢道男
副査	筑波大学教授	理学博士	有光敏彦
副査	筑波大学講師	博士(理学)	水落憲和

論文の内容の要旨

本論文は、線形光学素子を用いて分散型量子情報処理を実現するための光量子回路に関する研究を述べたものである。

第1部では、第1章の序論で量子情報処理について簡単に述べた後、第2章で量子情報処理に必要な演算と線形光学素子による実現法を概説している。第2部と第3部は本論文の核心となるものである。第2部では、第3章で分散型情報処理アルゴリズムの典型的な問題である匿名リーダー選挙を実現する量子プロトコルを実現する方法を提案し、実際に正しく動作することを実験で確かめている。また、平均的な通信量の比較から量子アルゴリズムの優位性を示している。第3部は量子暗号鍵配付の安全性について検討している。第4章で量子暗号鍵配付を概説した後、第5章で安全性を実験的に検証するための一手段として量子クローナーによる盗聴を取り上げ、線形光学素子を用いた実現法を提案した。さらに、第6章で1:2クローナーと1:3クローナーにおいて盗聴によって得られる情報量と受信者に渡す状態への擾乱との関係を求め、量子クローニングによる盗聴に対して安全な鍵配付ができる誤り率を求めた。特に1:3クローナーでは盗聴者の量子状態測定の最適化を行っている。最後に第4部で本論文の内容をまとめ、その意義を述べた後、今後進むべき研究の方針を論じている。

審査の結果の要旨

量子情報処理は、従来のスキームでは実現できない情報処理を可能にするものとして近年関心が高まっている。量子情報処理で実現されるものとして、素因数分解や離散対数問題に代表される超並列演算による計算の高速化や、無条件安全な鍵の共有を可能にする量子暗号鍵配付などがあげられている。ところが、量子情報処理の理論的研究の進展に比べて実験的な検証は十分に進んでいるとはいえない。これは量子情報の基本単位である量子ビットを物理的に実現することが難しいからに他ならない。

このような状況の下で、著者は光子による量子ビットに着目して量子情報処理の実現に向けた検討を行った。光子は他との相互作用が小さいため、量子状態が良く保存されるが、反面2量子ビットの演算が難しいという欠点がある。これを解決するために線形光学素子による確率的量子演算（量子ゲート）が提案されている。著者は、これまでの大半の研究が量子ゲートの実現に留まっているのに対し、量子回路システムの構築によって情報処理機能を実現することを目指した。このようなデバイスからシステムへの質的転換は、量子情報処理技術の今後の発展に寄与するものと思われる。

また、著者は光子が情報の伝送媒体として優れた特質を持つことを利用して、離れた場所にいるパーティーが情報処理にかかわる分散型量子情報処理を取り上げた。分散型量子情報処理はネットワークにおいて必須であるにもかかわらず、これまで量子暗号鍵配付を除いて検討がなされていなかった。分散型量子情報処理に着眼したことも本論文の優れた点であると考えられる。

本論文では、分散処理における基本問題のひとつである匿名リーダー選挙問題を取り上げている。ロバストでフレキシブルなコンピュータネットワークには必要な課題であるが、古典的には有限時間で確定的に解くアルゴリズムは存在しないことが知られている。一方、2004年に発見された量子的なアルゴリズムを用いると有限時間で確実にリーダーを決めることができる。このアルゴリズムの実装の検討を行った結果、2者間の場合には比較的単純な量子回路を用いて1回の演算でリーダーが決まることを見出した。線形光学素子による量子ゲートは確率的に動作するため、これを用いた量子情報システムは一般には常に失敗する確率がある。しかし、匿名リーダー選挙問題ではリーダーとなる状態の定義を適切に選ぶことにより確定的な動作が可能であることを示した。線形光学素子で確定的に動作する量子アルゴリズム実装の発見は本研究が初めてである。

さらに著者は、リーダー選挙問題を解く量子回路を線形光学素子によって実際に構成し、装置の不完全性に起因するエラーを除いて正しく動作することを確認している。量子回路を現実の素子を用いて構成するためには、量子ビットとして適切な物理的な状態を選択し、さらに動作の安定性を考慮する必要がある。実験系のデザインにセンスが問われるところだが、真空と1光子状態を量子ビットとすることで必要な光子数を削減し、結果として信号対雑音比の良好な実験を行っている。さらに、装置が不完全な場合でもリーダー選出に必要な通信量の平均値を比較することで量子アルゴリズムが古典に対して優位にあることを示した。このような解析は著者が実験だけでなく、量子情報理論についても十分な知識を持っていることを示している。

著者は線形光学素子の次の応用として、量子クローナーによる量子暗号鍵配付の安全性の実験的検証を選んでいる。量子暗号鍵配付の安全性は理論的に証明されているが、実験的に盗聴情報量と状態に与える擾乱の関係を示して安全性を検証した例はほとんどない。量子暗号鍵配付装置が実用化に近づいている中で盗聴器による安全性の実験的検証は意味のあることだと考える。量子クローナーは量子暗号鍵配付に対する個別盗聴法として最適であることが知られている。なお、線形光学素子で構成したクローナーによる盗聴は、量子ゲートの確率的動作による失敗があるが、その場合光子を送らなければ伝送路における光子の損失と区別がつかないため、確率的な動作であっても意味のある例となっている。

本論文では量子クローナーとして、1:2クローナーと1:3クローナーについて具体的な構成を与えている。1:2クローナーが最適であるが、実装には時間的に分岐比を可変できるビームスプリッターが必要になる。これは 2×2 変調器で実現可能ではあるが、1:3クローナーであれば分岐比固定のビームスプリッターだけで構成が可能になる。本論文では、1:3クローナーによる盗聴を最適化するため相互情報量が最適になるように状態の測定法を決めた。その結果、現在の技術でも実現可能な測定が最適になることを見出し、この場合はクローナーとして最適な1:2クローナーで得られる相互情報量と大きな差がないことを示した。この例においても著者による巧妙な実験系の構成と量子情報理論の知識で裏付けられた解析が行われている。

第4部において著者は線形光学素子による量子情報システムを大規模化するためには、システムを構成す

る干渉計の安定化と量子メモリの実現が課題であるとしている。過度に楽観的な記述に陥ることなく今後の課題を分析している。

以上のような本論文の記述から、著者の研究は、線形光学素子で構成した量子情報システムで量子情報処理機能を実現するという明確な指針に基づいて進められたことが見て取れる。著者が自立した研究者として十分な能力を有していることが結論付けられる。

よって、著者は博士（理学）の学位を受けるに十分な資格を有するものと認める。