審査の結果の要旨

氏名 長谷川 淳

本論文は「Theory and Experiment of the first decoy state quantum key distribution guaranteeing quantitative security in the real-world settings」と題し，6 章と付録からなる．量子計算・量子情報は新しい計算・情報処理のあり方として盛んに研究されているが，その中でも実用化に最も近いと考えられているのが量子情報通信を用いた暗号技術である．量子情報技術を用いて暗号鍵を通信すると，鍵が盗聴されたときには量子状態に変化が生じるため，その変化を調べることにより，どれだけの情報量が盗み見られたかを推定することが可能となる．盗聴されたことが分かれば鍵は安全でないとして捨てて，安全性が十分だと確認された鍵だけを暗号に用いることで，確実に安全な暗号が実現できる．これは現代暗号が「現実的な計算量で解けるアルゴリズムが知られていない問題」という計算量的な安全性に基づいていること，また，量子計算が実現すればこれらの問題が高速に解け，現代暗号が危険にさらされてしまうという状況とは根本的に異なっている．

量子通信を用いた暗号鍵配送の原理は，すでに実験的にも実証されたとされていた．しかし従来研究で前提としていた Gottesman, Lo, Luetkenhaus, Preskill (GLLP) による漸近解析は，有限長の符号では厳密には成立しない．すなわち，従来の実験での「実証」は，安全性の確認という最も根本的なところで不完全であった．

これに対し本研究では，有限長符号に対する安全性の理論を構築することにより，厳密な意味での安全性を確立した．実際にはこの方向性の最初の仕事は林らにより行われたが，実際のシステムでは通信中に信号に乗るノイズや測定装置における測定ばらつきによっても量子状態の変化が生じるため，「盗聴情報量」は多く見積もられてしまい，やや荒っぽい近似を行った林らの理論では鍵の安全性を確認することができなかった．これに対し本研究では林らの理論の精度を高めることにより，実際に安全性を保証された鍵を生成することに，世界で始めて成功した．また，この理論を実験と数値計算により分析し，この理論に基づく量子鍵配送の特性を分析した．

第 1 章「Introduction」では，問題の背景と本研究の学術的貢献がまとめられている．

第 2 章「Preliminaries」では，量子計算・量子通信の基礎や符号理論をはじめとする従来知見がまとめられている．量子鍵配送については，単一光子を用いた BB84 と呼ばれる手法とその問題点，そして BB84 の問題点を解決するデコイ状態法について説明されている．本研究はこのデコイ状態法の安全性を確立するものである．

第 3 章「New eavesdropper's information formula for QKD protocol with a finite code length incorporating statistical fluctuations」では，本研究の核となる理論を展開してい

る．まず林らによる先行研究が紹介され，その評価に基づいた実験では「安全性が保証された鍵」が得られなかったことが報告されている．そして林らの理論を精緻化した理論を展開している．

第 4 章「First experimental results of QKD protocol guaranteeing quantitative security incorporating statistical fluctuations」では，第 3 章で構築された理論に基づき，実験により「安全性が保証された鍵」を得ることに成功したことが報告されている．とりわけ，実際の実験環境におけるさまざまな条件 --- 機械に実装された機能上の制約，測定などによるばらつきの大きさ --- を考慮した，プロトコルの最適化が詳述されている．最適化されたプロトコルを用いることにより，20 km の光ファイバを経由して，最大で約 200 bps の速度で鍵を配送することができた．

第 5 章「Numerical analysis of proposed eavesdropper's information formula」では，現実の実験装置の制約を離れて，提案した安全性理論に基づく量子鍵配送プロトコルの性質を，数値実験により議論している．まず，配送距離が鍵の生成速度に与える影響を評価し，従来理論である GLLP と比較している．また，配送距離ごとに最適な光子強度やそれらの選択確率を分析している．さらに，盗聴されたビット数の推定値に相当する安全性パラメタを変化させ，十分な長さの符号化を用いれば，極めて高い安全性を要求しても鍵の生成速度に大きな影響を与えないことを示した．

第 6 章「Concluding remarks」では，研究成果をまとめ，今後の展望について述べている．

なお，「Detailed formulation of our proposed eavesdropper's information with a finite code length incorporating finite statistics」と題する付録において，本研究で提案する理論の証明が記述されている．

以上をまとめると，本論文では，安全性を保証した量子鍵配送を世界ではじめて可能とした理論を展開し，実験の報告とともに将来への展望を明らかにしたもので，量子情報通信の実現への大きな一歩となる成果を明らかにしており，情報理工学の進展に対して大きな貢献をしたといえる．

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる．