審査の結果の要旨

論文提出者氏名　　川上　駿

光の量子力学的な性質を利用すると、物理法則によってセキュリティを担保しながら秘匿通信を行うことができる。その骨子となる手法は量子鍵配送と呼ばれ、微弱光による量子通信と公開通信を組み合わせることにより、送信者と受信者のみがその内容を知るランダムなビット列、すなわち秘密鍵を生成する。所定の長さの秘密鍵があれば、公開通信だけを用いて同じ長さまでの任意の秘匿通信が可能である。送信者と受信者が用いる装置が理想的な場合、すなわち、光の自由度の中から量子ビット（２準位系）を特定して操作、測定を行える場合には、そのセキュリティの理解はかなり進んでいる。一方、現実的な実装を想定する場合、送受信者が実際に用いるレーザー光源や光子検出器の不完全性、その不完全性の具体的な較正方法、通信時間が有限であることから生じる統計揺らぎの影響（有限長効果）などを考慮した上でのセキュリティ証明や、より効率的な量子鍵配送手法（プロトコル）の探索が重要である。本研究では、未解決のプロトコルについて新たにセキュリティ証明を与え、現実的な装置を用いる量子鍵配送手法の効率の向上をもたらすとともに、このプロトコルを含む多くのプロトコルに適用可能な、有限長効果の解析手法を構築した。

前者で着目したプロトコルは、ＤＱＰＳ（４値差動位相シフト）量子鍵配送プロトコルと呼ばれ、レーザー光源を用いて効率的な量子鍵配送を行うことを目的として過去に提案されたものであるが、そのセキュリティ証明は未解決であった。既存の提案では、符号化に用いるコヒーレントなパルス数（ブロック長）は無限であったが、ブロック長を２に制限すると、位相変調のＢＢ８４プロトコルに一致するため、ＤＱＰＳプロトコルは位相変調ＢＢ８４プロトコルの拡張と見なすことができ、また、ほぼ同様の装置で実装できる。セキュリティを証明する上で障害となるのは、盗聴の難易を定める物理量（隣接パルスの総光子数）が、符号化に用いる物理量（ブロック内の隣接パルス間の位相差）と非可換であるため、従来のＢＢ８４プロトコルの証明で用いられる盗聴の難易を示すラベルが定義できない点である。本研究では、送信者側に仮想的な量子ビットを導入し、事後にこのラベルを定義することでこの問題を回避し、セキュリティを証明した。また、位相変調のＢＢ８４プロトコルに比べて、効率が 8/3 倍に改善することを示した。

有限長効果は、量子鍵配送における盗聴の大きさの推定が、信号に生じた擾乱の大きさの推定を介して行われ、後者の推定には無作為抽出による測定結果の照合が用いられることから生じるものである。従来の理論では、抽出数を固定した単純無作為抽出が用いられ、その結果として超幾何分布を中心とした解析となっていた。本研究では、ＢＢ８４プロトコルのように基底選択を伴うプロトコルにおける抽出法が、ベルヌーイ抽出によってより自然に記述できることに着目し、二項分布を中心とした新たな解析手法を構築した。とく

に、レーザー光源を用いる場合には、単純無作為検出を用いる場合に比べて推定が大幅に簡略化され、取り出せる鍵の長さも大きくなることを示した。また、この解析手法をＤＱＰＳプロトコルに適用し、位相変調のＢＢ８４プロトコルに対する優位性が、有限長効果を考慮した場合であってもそのまま維持されることを数値的に示した。

本論文は 7 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，本論文で用いる量子情報理論の基礎的な定理、定義の導入と、量子鍵配送の概略的な説明を与えている。

第 3 章では，量子鍵配送の代表的な手法であるＢＢ８４プロトコルのセキュリティ証明について、相補性を用いた証明法を例として、理想的な装置を用いた場合の証明を具体的に記述している。

第 4 章では，レーザー光源を用いる量子鍵配送の問題点とその解決法について概観するとともに、ＢＢ８４プロトコルの場合に、送出光子数に応じて盗聴の難易をラベル付けする従来の証明手法を再整理して記述している。

第 5 章では，ブロック長の概念を導入したＤＱＰＳプロトコルのセキュリティ証明を与えている。証明した鍵長公式をもとに、鍵長の通信距離依存性をブロック長ごとに計算し、位相変調のＢＢ８４プロトコルに比べて、効率が 8/3 倍に改善することを示している。また、光源の光子数分布を実験的に較正する手法を与えている。

第 6 章では，ベルヌーイ抽出を用いた有限長効果の解析手法を提案している。レーザー光源を用いる場合に、従来の解析手法による結果と比較し、その優位性を主張している。ＤＱＰＳプロトコルに提案手法を適用し、前章で導いたＢＢ８４プロトコルに対する優位性が、有限長効果のもとでも保たれることを確認している。

第 7 章では、以上の結果をもとに本研究の主張を整理し、今後の課題と展望をまとめる。

以上のように、本研究では、特定の量子鍵配送プロトコルに着目して、そのセキュリティを初めて証明し、現実的な装置を用いた際の効率を向上させるとともに、そのプロトコルの有限長効果の解析にあたっては、より広範囲に適用できる解析手法を新たに構築することで解決している。前者の証明では、これまで広く用いられてきた盗聴の難易によるラベル付けの技法の適用範囲を拡大するものである。後者の解析手法は、従来の手法を大幅に簡略化するもので、とかく複雑になりがちな有限長解析の研究の進展を加速する効果も期待できる。このように、本研究の成果は、個別の事例における効率の向上を達成したことだけにとどまらず、今後の研究分野の進展にも資するところが大きいと判断できる。

よって、本論文は博士（工学）の学位論文として合格と認める。