様式３

論　文　内　容　の　要　旨

氏　　名　（　　生田　拓也　　）	
論文題名	量子もつれを用いた高次元量子鍵配送のためのスケーラブルなタイムビン量子状態制御

論文内容の要旨

本論文は、量子もつれを用いた高次元量子鍵配送のためのスケーラブルなタイムビン量子状態制御に関する研究をまとめたものであり、以下の6章で構成されている。

第1章は序論であり、本研究の背景として、量子コンピュータ技術の発展などに伴う現代暗号通信の抱えるリスクと、その対策のひとつである量子鍵配送(QKD)およびそれと量子もつれ状態との関係について概観した。さらに、近年盛んに研究されている、高次元量子状態(多値の物理量を取る量子状態)を用いることにより鍵ビット生成効率を高める高次元QKD、中でもタイムビン量子状態を用いる方式の優位性およびこれまでの関連研究の課題について述べた。そして、通信の基本三要素である信号の生成/伝送/測定の観点から高次元タイムビン量子もつれ状態について検討する、という本研究の目的・位置づけを明確化した。

第2章では、タイムビン量子状態や量子もつれ状態の定義、後の章の基盤となる状態密度演算子や測定演算子及び量子もつれ状態が持つ特異な相関特性など、量子情報理論の基礎的事項について述べた。また、2次元量子もつれQKDの代表的なプロトコルであるBBM92及びその安全性証明の概略を紹介し、高次元量子もつれQKDおよびその安全性を議論するための基礎とした。

第3章では、高次元量子もつれ状態の実験的検証に用いられるCGLMP不等式について議論した。まず、2次元量子もつれ状態について、古典的相関を前提とする隠れた変数理論から導かれるベル不等式を紹介した。この不等式が成り立たなければ(破れれば)、量子的相関が観測されたと言える。さらに、この不等式の高次元量子もつれ状態への拡張版であるCGLMP不等式について議論し、高次元量子もつれ状態の確率振幅を変調する状態最適化により、量子通信で広く用いられる最大量子もつれ状態よりも大きな不等式の破れが得られることを述べた。そして、タイムビン量子状態について、このような高次元量子もつれ状態を簡便かつ安定に生成/測定する手法について述べたのち、上記状態最適化によるCGLMP不等式の破れの増大を実験的に検証した。これにより、高次元タイムビン量子もつれ状態が量子相関特性を備えていることのみならず、状態最適化により最大量子もつれ状態との差が明確に確認できるほどに、安定した状態制御が可能であることを実証した。

第4章では、量子状態トモグラフィー(QST)と呼ばれる、高次元タイムビン量子状態を表す状態密度演算子の推定法を提案し、この手法により高次元タイムビン量子もつれ状態の100km伝送後の特性を評価した。量子もつれ状態を通信に応用するには、光ファイバーを介した量子状態の長距離伝送が不可欠であるが、ファイバーでの伝搬損失により光子が失われるため、伝搬後の量子状態測定には長時間を要するという課題がある。提案手法により少ない装置数及び設定パラメータ数で測定が可能となることを示したのち、提案手法を実装し、その有効性を実験的に示した。また、伝送後の量子状態に対するQST実験を行い、得られた状態密度演算子から様々な物理量/情報量を見積もり、高次元タイムビン量子もつれ状態の2次元量子もつれ状態に対する優位性を示した。

第5章では、高次元量子状態を用いたQKDプロトコルの一つである、$(d+1)$測定基底QKDプロトコルとその実装法について議論した。d次元QKDは、現在の主流である2次元QKDプロトコルより高い秘密鍵生成率を得ることが出来る。一方、同じ次元数dにおいても、$(d+1)$種類の測定系を用いることで、2つの測定系しか用いないQKDプロトコルよりも誤り耐性を向上させ、さらに高い秘密鍵生成率を達成することが出来るが、その安全性証明はこれまで次元数dが素数の場合に限られていた。そこでまず、有限体を利用した一般化Weyl演算子、一般化ベル基底及び対応する測定基底である相互不偏基底(MUB)を用いることで、素数の累乗次元まで安全性証明を拡張した。また、この証明に利用されるMUBを、高次元タイムビン量子状態に対して効率的に実装する手法を提案した。さらに、提案手法を4次元タイムビン量子状態の場合に実装し、$(d+1)$測定基底QKDプロトコルに適用可能な低いシンボルエラーレートが得られることを実験的に示した。

第6章では、本研究で得られた上記結果を総括し、本論文の結論を述べた。

様式 7

論文審査の結果の要旨及び担当者

氏　名	（ 生田　拓也 ）	
	（職）	氏　名
論文審査担当者	主 査　教授　井上　恭	
	副 査　教授　丸田　章博	
	副 査　教授　滝根　哲哉	
	副 査　教授　三瓶　政一	
	副 査　教授　宮地　充子	
	副 査　教授　鷲尾　隆	
	副 査　教授　駒谷　和範	
	副 査　准教授　五十嵐　浩司	

論文審査の結果の要旨

情報化社会の進展に伴い、暗号通信技術の重要性が増している。現在の暗号システムは解読に要する計算量の膨大さを安全性の根拠としているが、これに対し、量子力学に基づき、原理的に安全な暗号通信を実現する量子暗号の研究が進められている。これは、ワンタイムパッド暗号のための秘密鍵を離れた２者に供給する技術であり、量子鍵配送（Quantum Key Distribution: QKD）と呼ばれている。これまでに様々なQKDプロトコルが研究・開発されているが、その中に、量子もつれ状態と呼ばれる特異な相関特性を有する光子ペアを用いる方式がある。この方式は、QKDシステムの長距離化が可能、安全性証明との親和性が高い、といった特徴を有する。本論文は、量子もつれ状態を用いるQKDに関するものである。特に、高次元量子もつれ状態を用いるQKDを研究対象としている。

QKDでは、２つの状態をとり得る量子状態（二次元量子状態）を用いて秘密鍵情報を伝送するのが定番であるが、より多くの状態をとり得る量子状態（高次元量子状態）を用いる方式も研究されている。高次元化することにより、ひとつの量子状態の伝送情報量が増え、秘密鍵生成効率の向上につながる。そこでこれまで、QKDへの適用を意識した高次元量子もつれ状態の研究がいくつか報告されている。しかしながら、これまでの報告例では、高次元化するために装置構成が複雑化し、QKDのシステム実装に適した形態ではなかった。また、その安全性証明は特定のシステム条件に限定されていた。そこで本論文では、高次元量子もつれQKDシステム実装に向けた要素技術を提案・実証している。特に、ファイバ伝送に適した量子状態である、タイムビン（時間位置）高次元量子状態を検討対象とし、その生成/伝送/測定に関する研究を行っている。具体的な内容は以下の通りである。

(1) 生成された高次元状態が真にもつれ状態であるか否かは、CGLMP不等式により検証される。被測定状態についての様々な条件下での測定結果が、CGLMP不等式を満たしていなければ（破っていれば）量子もつれ状態と判定され、この破れが大きいほど良質な量子もつれ状態と言える。本論文では、自発的パラメトリックダウンコンバージョンと呼ばれる光非線形現象を利用する高次元タイムビン量子もつれ状態生成法の動作条件を適切に制御することにより、量子もつれ状態最適化による破れの増加を観測している。これにより、この生成法により高品質な高次元タイムビン量子もつれ状態が制御性良く生成できることを実証している。

(2) QKDシステムへの応用には、生成された量子状態が長距離ファイバ伝送されることが望まれるが、これまで高次元量子もつれ状態を長距離伝送した報告例はない。そこで本論文では、上記手法により生成した高次元タイムビン量子もつれ状態を100kmファイバ伝送し、伝送後でも高い品質が保たれることを実証している。そこでは、品質評価に量子状態トモグラフィー（QST）と呼ばれる測定法を用いている。これは量子状態に関する全ての情報を取得する測定法であるが、そのためには様々なパラメータを測定する必要がある。高次元になるほど測定すべきパラメータ数は増大し、測定が長時間化する。特に長距離ファイバ伝送後では、伝送損失のため多くの量子状態が消失し、現実時間内での測定が困難となる。そこで本論文では、多段接続された遅延干渉計を用いて効率的にQST測定する手法を提案し、それを用い

て、現実時間内での状態測定を可能とした。その結果、生成した高次元タイムビン量子状態が、高品質のまま長距離ファイバ伝送されることを実証している。

(3) QKD では、伝送された量子状態に対して相互不偏基底(MUB)と呼ばれる非直交な状態測定をし、その結果に基づいて秘密鍵を生成するが、用いる MUB の種類が多いと鍵生成率が高くなることが知られている。一般に高次元化すると、そのような測定系は装置構成が複雑化して実装が難しくなる。そこで本論文では、1 台の位相変調器と多段の遅延干渉計の従属接続という簡便な構成による多種の MUB 測定系を提案し、秘密鍵生成に十分な性能を備えていることを実証している。また、高次元 MUB 測定系の構築にあたり、従来は安全性が証明されている次元数が限定的であったところを、より広い範囲の次元数まで安全性証明を拡張している。

以上のように、本論文は、QKD システムの長距離化並びに秘密鍵生成の高効率化を可能とする高次元量子もつれ QKD のための要素技術（具体的には生成/伝送/測定）に関して、実装に適した構成・手法を提案・実証している。長距離・高効率な QKD システム構築へのひとつの方向性を示すものであり工学的意義があるとともに、量子もつれ状態に関する理解を深めており学問的にも意義深い。

よって本論文は博士論文として価値あるものと認める。