「電子・光子等の機能制御」
平成12年度採択研究代表者

中村　和夫

（日本電気株式会社基礎研究所　研究部長）

「量子暗号の実用化を可能にする光子状態制御技術」

１．研究実施の概要

Ａ研究所：

量子情報技術のキーである量子絡み合い（エンタングルメント）の実験及び理論的研究を行っている。量子トモグラフィーと呼ばれる断層写真と似た、量子絡み合いの定量評価手法を立ち上げ、その信頼性を実験的に検証した。又、本評価法により、フイルタリングで光子対の量子相関が回復することを見いだした。今後、本評価法を応用し、量子絡み合いの大きい光子対をより効率良く生成する光源の開発に取り組む。又、多光子の量子干渉実験にも取り組んでいく。

Ｂ研究所：

原子と光子との間のコヒーレンスを量子通信や量子計算へと応用する新たな方法を開発する。量子通信では、コヒーレンスとエンタングルメントの２つの側面がかかわりあっており、原子・光子アンサンブルの最も簡単なシステムを研究している。

Ｃ大学：

平成12年度は、１）量子テレポーテーションの理論的な解析、２）量子雑音を検出できる光検出器の製作、３）進行波型リングチタンサファイアレーザの特性評価を行った。平成13年度にはOPOを用いたスクイーズド光、EPRビームの発生を行う予定である。

Ｄ大学：

近年広田グループによって新たに見いだされた最大絡み合い状態である対称振幅エンタングルドコヒーレント状態を利用した量子暗号プロトコルを開発する。またこれまでに開発してきた量子情報理論に基づき量子暗号の安全性の本質を解明する。

Ｅ研究所：

光の量子状態に符号化された情報を最適に検出するための量子信号検出理論の構築と原理実証を進めている。H12年度は単一光子レベルの多値偏波変調信号に対して、古典的な信号検出限界を上回ることができる量子最適検出回路を開発し

て来た。現在、相互情報量と呼ばれる検出基準で世界トップクラスの検出性能を確認できた段階である。

２．研究実施内容

Ａ研究所：

単一の量子系における未知の量子状態を知ることは、量子クローニング定理により禁止されるが、同一の量子状態にある多数の量子系の測定から、その量子状態を再構成することは可能である。本研究では、そのような技術のうち最も簡便な、量子トモグラフィー手法により、パラメトリックダウンコンバージョン(PDC)過程により生成した偏光状態の相関した光子対の量子状態を測定し、その量子エンタングルメントを定量的に評価した。量子トモグラフィーにより得られた量子状態と独立に行った二光子偏光干渉実験の結果の間に良い一致が得られ、我々の実験装置および手法の信頼性が証明できた。また、我々の用いた超短パルスレーザ光により発生した光子対の量子エンタングルメントが、スペクトルフィルターにより回復することをみいだいした(図１および２)。これは新しいタイプの量子抹消実験として捉えることができる。

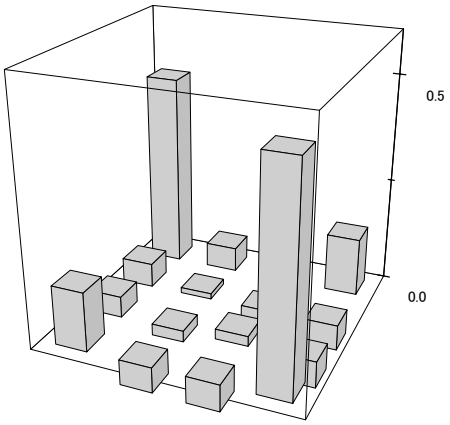

図１．バンド幅の広いフィルター(FWMH： ８ nm)を用いた時の密度行列の実部（虚部は無視できるほど小さい）

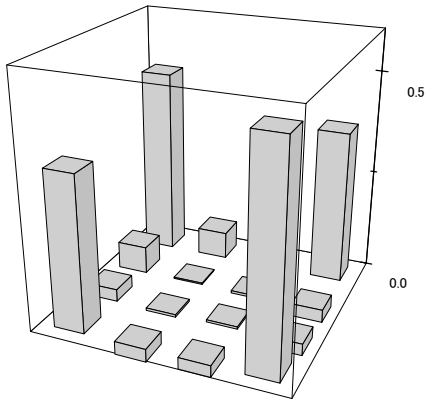

図２．バンド幅の狭いフィルター(FWMH： １ nm)を用いた時の密度行列の実部（虚部は無視できるほど小さい）

Ｂ研究所：

光ファイバーによる高出力単一光子源を実現する実験を始めた。通常のファイバー及び特注の「honeycomb」ファイバー(Corningより)の両方を試みており、予備実験の結果が得られた段階である。

Ｃ大学：

光の量子力学的性質を利用し、量子テレポーテーション、デンスコーディング、

新たなスキームによる量子暗号などの理論的・実験的研究を行っている。キンブルらによる連続量量子テレポーテーションは古典的なレーザー光（コヒーレント状態）を転送したものであった。将来の通信を考えた場合、非古典的な光の状態である１光子状態を転送することが望まれる。平成12年度は、連続量量子テレポーテーションを光子数状態で記述するトランスファーオペレータの方法を１光子状態に適応し、その状態が受信側でどのような変化を受けるかを解析した。一方、実験においては、量子テレポーテーション実現に必要な以下の項目を行った。１）温度･機械的不安定性に起因する相対的位相関係の変動を相殺するため、FMサイドバンドロックという手法を実験した。２）高いスクイージングに現在最も有利と考えられているリング型光パラメトリック共振器の設計を行った。３）ホモダイン検出で量子雑音を捕らえる低雑音、高量子効率の高周波用光検出器を製作した。

D大学：

量子鍵配送プロトコルの開発に加えてもっと一般的な量子情報セキュリテイの可能性を解明するためには絡み合いとよばれる量子力学的相関を持った光子状態の利用が不可欠である事が、本研究代表者のグループを始め、海外での理論的研究により自明となっている。

絡み合い光子状態の生成・制御に関しては、光による量子ゲートの実現が理想的で、単一光子、連続変数量であるスクイーズド状態も大きなポテンシャルを有する技術であるが、最近玉川大グループでは対称振幅エンタングルドコヒーレント状態は非直交状態を基礎にするにも関わらず最大エンタングルメントを持つことを発見した。

$$\begin{cases} |\Psi_1\rangle = |\psi_1\rangle_A |\psi_2\rangle_B + |\psi_2\rangle_A |\psi_1\rangle_B \\ |\Psi_2\rangle = |\psi_1\rangle_A |\psi_2\rangle_B - |\psi_2\rangle_A |\psi_1\rangle_B \\ |\Psi_3\rangle = |\psi_1\rangle_A |\psi_1\rangle_B + |\psi_2\rangle_A |\psi_2\rangle_B \\ |\Psi_4\rangle = |\psi_1\rangle_A |\psi_1\rangle_B - |\psi_2\rangle_A |\psi_2\rangle_B \end{cases}$$

ここでKを任意定数として　$\langle\psi_1|\ \psi_2\rangle = \langle\psi_2|\ \psi_1\rangle = K$

本プロジェクト独自の量子暗号プロトコルの開発を目指すにあたり、まず我々独自のエンタングルド状態の応用とその生成理論を開発する。対称振幅エンタングルドコヒーレント状態の生成の第一段階はコヒーレント状態のシュレーデインガー猫状態の生成である。一般にそれらは共振器内での生成理論が主であったが、最終目的のためには共振器の外でそれらの性質を保存できることを保証せねばならない。したがって、今後、共振器の内外におけるシュレーデインガー猫状態の生成に関して実験可能な方法を開発する。第二の課題である量子暗号の安全

性の理論では最も高度な盗聴者はエンタングルメントを利用することが知られている。その結果、鍵配送は安全であるがビットコミットメントは完全な安全性を保証できないことが証明されている。しかしながらこのエンタングルメント攻撃も万能ではないことが指摘されており、その可能性は量子情報理論を駆使して解決され得ると考えられる。当該グループはエンタングルメント測度理論と量子情報理論の融合によってそれを試みる。

E研究所：

研究目的：

物の識別は、あらゆる情報処理の根幹である。特に量子状態の識別に関する問題は「量子情報」という概念の理解と深く関わっており、また量子情報通信を現実にして行く上でまず明らかにして行くべき重要課題の一つである。本研究の目的は、量子状態を使って情報を符号化し、量子暗号システムのような量子限界にさらされた通信路で最適な情報伝送を行うための基礎技術を開発することにある。研究内容は理論と実験に分けられる。

⑴　量子信号検出理論の構築

研究方法：

これまで限られた例でしか明らかにされていない量子信号検出器の数理的構造を汎用的な量子状態信号の場合に対しても導出できる様、理論の構築を進める。特に、量子状態によりブロック符号化された「量子符号語」に対する最適復号回路の構成理論を重点的に研究する。

成果：

ある種の対称性をもつ量子符号語に対して、最適復号回路を系統的に構成するアルゴリズムを開発した。

⑵　量子最適検出回路の開発

研究方法：

単一光子による多値偏波変調信号は、量子信号検出理論の原理実証を行う上でもっとも簡単な信号系である。一方、信号の識別に必ず有限の誤りを伴い、それゆえに、これを逆に利用して量子暗号のプロトコルを構成することができる。このような信号系を用いてこれまで存在が予言されているにも関わらず、まだ実験的に実証されていなかった一群の量子最適検出戦略の実証を行った。

成果：

図３は５値偏波変調信号（点線）とそれに対する最適測定器の数理的解である。最適測定器は３値の出力を出し、長さの異なる３つのベクトル(実線）で表現される。

この最適測定器は図４のような単純な単一光子干渉系で実現することができ、予言されている量子最適検出限界の約96%まで迫る検出性能を実証した。

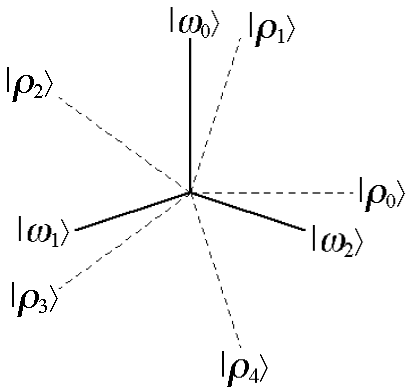

図３．５値偏波変調信号(点線)と最適測定器の解(３値、実線)

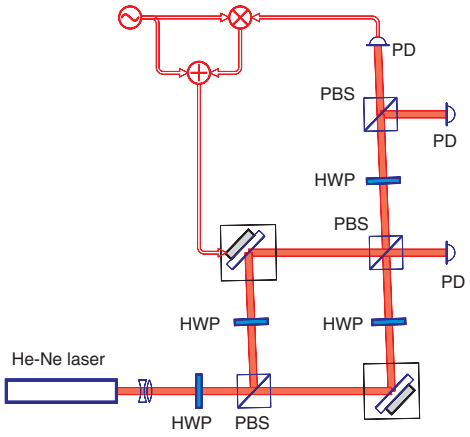

図４．最適測定器の単一光子干渉系による実証実験系

３．主な研究成果の発表（論文発表）

○A. S. Holevo, M. Sohma, and O. Hirota, "Error exponents for quantum channels with constrained inputs," Report on Mathematical Physics vol.46, no. 3, pp. 343-358, 2000

○M. Sohma and O. Hirota, "Binary discretization for quantum continuous channels," Physical Review A. vol. 62, no. 5, pp. 052312-1-4, 2000

○A. S. Holevo, and O. Hirota, "Quantum Gaussian Channel," IEEE Proc. ISIT 2000, 2000.

○O. Hirota, "A foundation of quantum channels with super additiveness for Shannon information", Applicable Algebra in Eng. Communication and Computing, vol-10, no. 4 /5, pp. 401-423, 2000.

○S. M. Barnett, C. R. Gilson and M. Sasaki,
"Fidelity and the communication of quantum information",
Journal of Physics A : special issue in QUANTUM INFORMATION AND COMPUTATION (ed. by Richard Jozsa, Noah Linden and Sandu Popescu), (2001).