「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㈱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

NEC 筑波研究所：

量子暗号の長距離化に不可欠となる量子中継技術の実現へ向け、そのキーとなる量子絡み合い（エンタングルメント）の実験及び理論的研究、さらに中継用デバイスの評価装置の立ち上げを行っている。量子トモグラフィー（量子絡み合いの定量評価手法）を用い、量子絡み合いの度合いが大きい光子対を効率良く生成する光源を開発する一方、量子チャネルのプロセストモグラフィー（量子操作の評価手法）に成功した。

NEC 北米研究所：

量子情報の潜在的な応用法をさらに探る為、種々のコヒーレントな量子現象の研究を進めている。主に量子暗号に用いる光ファイバを利用した量子絡み合い光源の開発、原子集団を利用した量子ビット保存の理論的可能性を研究している。

東京大学：

光の量子力学的性質を利用し、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。ボウタイ型リングレーザーを用いてスクイズ光の発生を行った。

玉川大学：

強い非古典的特性を持つ種々の量子状態を用いた量子暗号、量子テレポーテーションのプロトコルを開発する。特に本年度は本研究グループのオリジナルである対称振幅エンタングルドコヒーレント状態によるテレポーテーションスキームの構成法を解明する。また、量子暗号のシステム機能の最適化に関する設計理論を開発する。

通信総合研究所：

単一光子レベルの信号で伝送容量を確保するための技術、量子通信路符号化技術を研究している。単一光子の偏波変調信号に対する量子最適検出回路をH12年度で実現し、H13年度は、偏波自由度にさらに空間モード自由度を加えてパルス位置変調符号を行うための符号回路の開発を進めた。これは量子通信路符号化の原理実証を世界に先駆けて行うためのものであり、現在、予備実験において良好なデータを取得しつつある。

2. 研究実施内容

NEC 筑波研究所:

研究目的:

量子暗号の長距離化に必須となる量子中継技術の実現を目標に、その鍵となる量子絡み合い状態の制御・定量評価に関して研究を進めている。

(1) 量子トモグラフィーを用いた高い量子絡み合いを有する光源開発

研究方法:

張り合わせた2つの非線形結晶とパルス光源の組み合わせで構成した量子絡み合い光源に対して、さらに補償光学系(図1の Pre-Compensation)を付加し、前年度に立ち上げた量子絡み合いの定量評価法である量子トモグラフィーにより最適化を図る事で、高い量子絡み合いを有する光子対の光源を開発する。

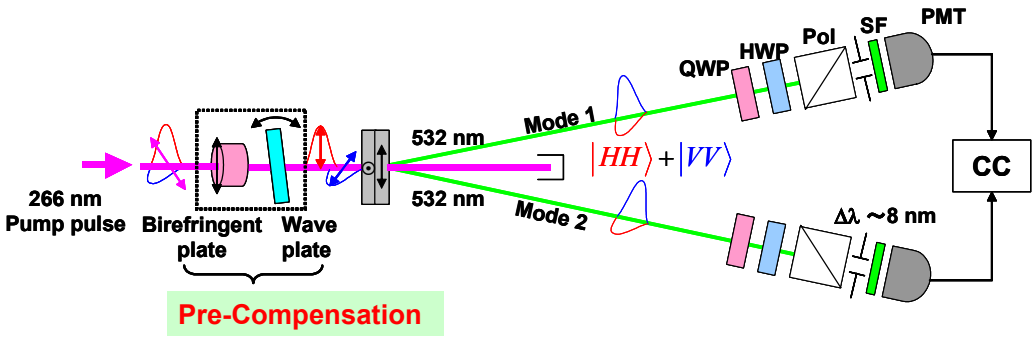

図1 量子絡み合い光源の模式図

成果:

図1に示す様に、意図的に水平成分と垂直成分に時間差を付ける事で、2つの非線形結晶から出てきた量子絡み合い状態を完全に重ね合わせる事ができ様になり、図2に示した様に、約 130fs の遅れを導入する事で、量子絡み合いの程度をほぼ完全な状態に近づける事ができた。

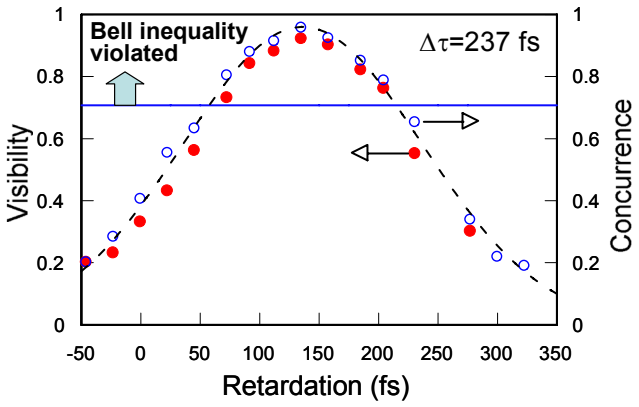

図2 補償光学系での時間差と量子絡み合いの度合い

(2) 量子操作の評価

研究方法:

量子トモグラフィー法を発展させ、量子操作を評価する為の量子プロセストモグラフィー法を確立し、実証を行う。

成果:

図3に示した様な構成により入力と出力の相関を取る事で、量子状態への操作(量子チャネル)を評価する方法(プロセストモグラフィー)へと量子トモグラフィーを発展させた。具体的に図4に示

した様に、偏光状態を全ての軸でランダム化するチャネルの例を取り上げ、実際に予測されるチャネルの機能を実証した。

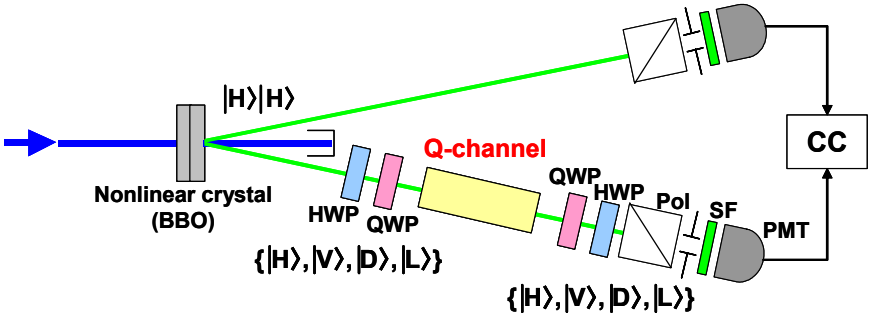

図3　プロセストモグラフィーの構成図

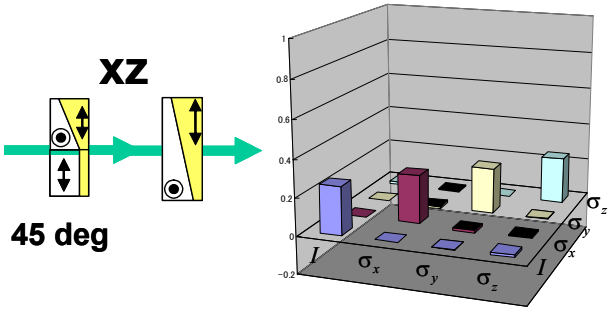

図4　偏光ランダム化チャネルとその評価結果

NEC 北米研究所:

研究目的:

簡易で高効率な量子絡み合い光子対生成光源を実現する。

研究方法:

フォトニック結晶ファイバにおける非線形性(4 波混合、図5)を用いて、量子絡み合い光子対(ストークス光:ω_S、アンチストークス光:ω_A)を生成しようとしている。位相整合条件を取る為に群速度分散を負にする必要があり、図6に示したハニカム構造のフォトニック結晶ファイバを用いた。用いたファイバの長さは 2m で、この 4 波混合特性を調べた。

成果:

図7には入力パワーに依存したファイバからの出力光の強度を示しており、入力パワーの増大に伴い、予想される通り、サイドバンドの分離が大きくなっている事が判る。このサイドバンドは相関を持っている事を確かめている。

この実験では量子リミットにまだ入っていないが、2002 年度の成果として量子性の確認を行う。

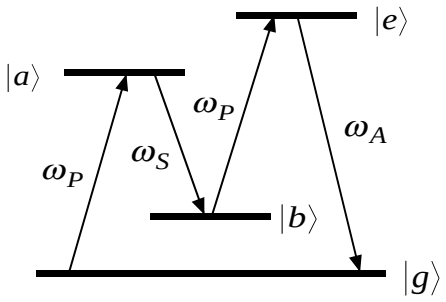

図5　4波混合の概念図

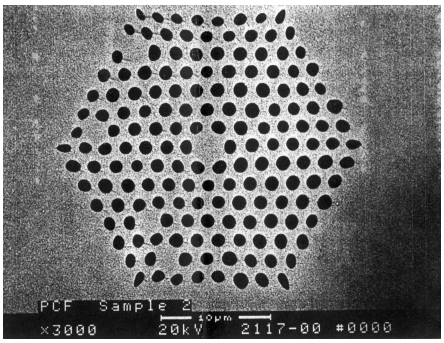

図6　ハニカム構造フォトニック結晶ファイバ

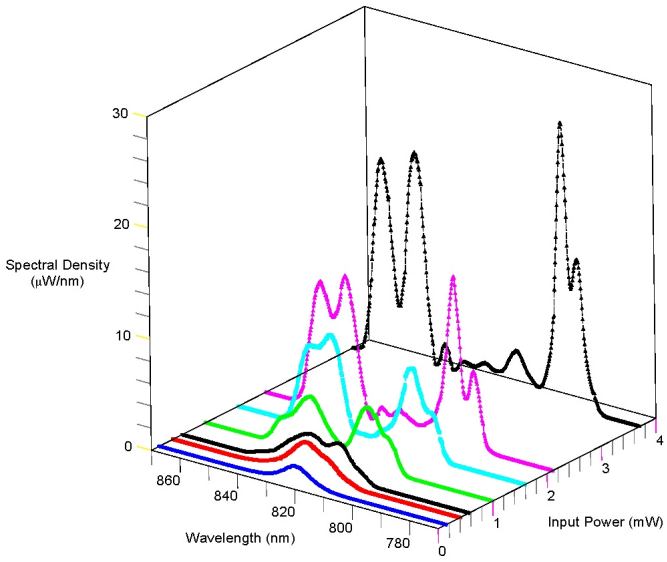

図7　出力光強度の入力パワー依存性

東京大学:

研究目的:

光の量子力学的性質を利用し、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を理論的、実験的に構築する。

研究方法:

実験に用いた要素技術

1) 光パラメトリック発振器(OPO)

構造はボウタイ型のリング共振器であり、結晶はニオブ酸カリウム(KNbO3)を採用した。波長 430nm の励起光を入射し、波長 860nm の光へパラメトリック下方変換を行い、結晶は温度制御により Type I の非臨界位相整合を行った。

2) 光ヘテロダイン検波

上述の OPO に発振閾値以下の強度の励起光を入射し、発生した光を検出した。

成果:

約 2dB の直交位相振幅成分のスクイージングが観測された。さらに今後の EPR 対発生のため観測系に対するスクイーズ方向の位相の制御を行った。真空スクイーズド光を発生させるために OPO に波長 860nm の微弱な種光(seed 光)を入射させ、平均光子数が1よりも大きくならない程度にする。そして OPO からの出射光の揺らぎが最小になるように OPO に入射する励起光と種光の相対位相を制御した。これにより数分間スクイーズされた状態が維持された。

玉川大学:

対称振幅エンタングルドコヒーレント状態によるテレポーテーションスキームを明らかにし、その性能を解析した。また、量子暗号への応用の際に重要になる、対称振幅エンタングルドコヒーレント状態の局所的デコヒーレンス特性を解明した。(広田)

2モードスクィズド状態を用いた暗号鍵配送システムにおいて、盗聴者がホモダイン検出と誤り率最適検出を用いて検出・再送型盗聴を行った場合とホモダイン検出を用いて傍受型盗聴を行った場合について正規の受信者の誤り率の変化を明らかにした。その結果、伝送路でのエネルギー損失を無視しうる状況下において2モードスクィズド状態を用いた暗号鍵配送システムは安全であることを確認した。(大崎)

実際の量子暗号鍵配送で避けるとことのできない量子通信路で発生するビット誤りの訂正処理速度の改善を試みた。対話型の誤り訂正法において従来使われている二分探索法の代わりにブロック符号を適用した。まず、検査ビットのみ送る手法に対し送受信者が交換する情報量が最少となる完全符号の構成法を示した。つぎに、既存の誤り制御符号を効果的に適用する手法を提案した。これらの手法により、処理速度で問題となる通信回数を従来方式に比べ 1/4 から 1/3 に削減した。(山崎)

量子情報のセキュアな伝送について検討した。量子情報セキュリティの各種機能のためには、痕跡を残さず盗聴等の操作ができないことが、重要な要素となっているが、このことは、量子情報を伝送する際、盗聴者等の悪意ある第三者により、容易にデータが破壊されることを意味している。しかし、量子非複製定理により、前もって量子情報のバックアップをとることは不可能であるため、データが破壊された場合に対処可能な、量子誤り訂正符号を1量子ビット伝送に対し検討した。(臼田)

量子暗号用の符号の開発を目指し研究を行っている。平成13年度は符号の理論性能評価に関する研究を行った。現在までのところ、古典－量子通信路に対しての信頼性関数の理論を応用することにより、一括復号を行う場合の、有限符号長の符号の理論性能を予測でき、具体的な符号の性能評価を行えるようになった(QIT5, SITA2001 にて発表)。平成14度の課題は、そのように予測される性能を達成するような、古典－量子通信路用の符号を開発することである。(加藤)

通信総合研究所:

研究目的:

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。これは、最小の通

信資源を使って如何に効率よく情報伝送を行うか、という究極的な通信に向けた基礎研究であり、理論と実験の両面から研究を進めている。

(1)　量子信号検出理論の構築とその応用

研究方法:

量子力学が許す究極的な信号検出過程は、確率作用素測度という数学概念によって表現される。これを具体的・実用的信号系に適用し、実際の物理的対応に訴える最適検出法を明らかにしてゆく。最終的目標は、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と量子パターマッチング等の新しい信号処理への応用である。

成果:

量子信号検出理論の応用として、量子パターマッチングという問題を定式化し、従来のアルゴリズムより優れたパターンマッチング法が存在することを明らかにした。

(2)　量子通信路符号化回路の開発

研究方法:

H12年度に開発した単一光子偏波変調信号に対する量子最適検出回路をさらに多段化し、空間モード自由度まで加えてパルス位置変調符号を行うための符号回路の開発を進めた。

成果:

システム全体は図8に示した様に、2段のマッハ・ツェンダー干渉系に帰着する。この回路を安定にロックし単一光子レベルで所望の復号性能を発揮させるための技術を開発した。現在、量子通信路符号化利得の最終データが得られつつある。

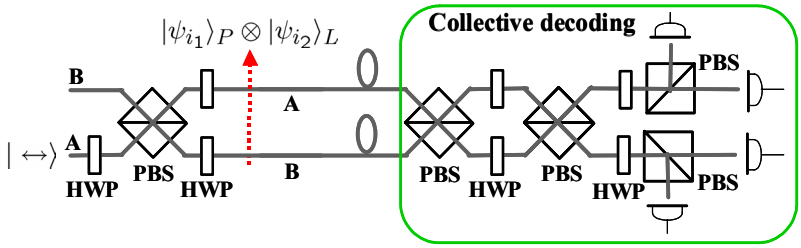

図8　量子最適検出回路のブロック図

3. 研究実施体制

NEC 筑波研究所グループ:

①　研究分担グループ長名:中村　和夫(日本電気(株)基礎研究所　研究部長)

②　研究項目:絡み合い制御素子開発

NEC 北米研究所グループ:

①　研究分担グループ長名:L.J. Wang(日本電気(株)北米研究所　Research Scientist)

②　研究項目:絡み合い光源開発等

東京大学グループ:

① 研究分担グループ長名:小林　孝嘉(東京大学大学院理学系研究科　教授)

② 研究項目:スクイーズド状態の絡み合い制御技術

玉川大学グループ:

① 研究分担グループ長名:広田　修(玉川大学学術研究所　教授)

② 研究項目:量子暗号安全性理論

通信総合研究所:

① 研究分担グループ長名:井筒　雅之(通信総合研究所基礎先端部門　上席研究員)

② 研究項目:量子通信符号化・復号化技術

4. 研究成果の発表

(1) 論文発表

NEC 筑波研究所:

○ Y. Nambu, K. Usami, Y. Tsuda, K. Matsumoto, K. Nakamura, "Generation of Polarization-entangled Photon Pairs in a Cascade of Two Type-I Crystals Pumped by Femtosecond Pulses", submitted to Phys. Rev. A

○ S. Ishizaka, "The reduction of the closest disentangled state", submitted to J. Phys. A Math. Gen.

○ T. Hiroshima, "Optimal dense coding with mixed state entanglement" J. Phys. A: Mathematical & General (Special Issue: Quantum Information and Computation, edited by R. Jozsa, N. Linden, and S. Popescu), Vol. 34, 6907 (2001).

○ K. Hirose, S.S. Li and N.S. Wingreen, "Mechanisms for Extra Conductance Plateaus in Quantum Wires" Physical Review B, vol.63, 033315 (2001).

○ K. Hirose, F. Zhou and N.S. Wingreen, "Density-Functional Theory of Spin-Polarized Disordered Quantum Dots" Physical Review B, vol.63, 075301 (2001).

○ K. Hirose and N.S. Wingreen, "Temperature Dependence Suppression of Conductance in Quantum Wires" Physical Review B, vol.64, 073305 (2001).

NEC 北米研究所:

○ L. J. Wang, C.K. Hong, and S.R. Friberg, "Generation of correlated photons via four-wave mixing in optical fibers", J. Opt. B: Quantum Semiclass Opt. 3, (2001) 346-352.

東京大学:

○ H. F. Hofmann, T. Kobayashi, and A. Furusawa, "Information losses in continuous variable quantum teleportation", Phys. Rev. A64, 040301 (2001).

玉川大学:

○ M.Sohma and O.Hirota, "Information capacity formula of quantum optical channels", Recent research development in Optics I (2001), Research Signpost, Trivandrum, India

○ S. van Enk and O.Hirota, “Entangled coherent state: teleportation and decoherence”, Physical Review A, vol.64, no-2, 022313 (2001).

○ K.Kurokawa and O.Hirota, “Properties of quantum reliability function and its applications toseveral quantum signals”, Electronics and communications in Japan, Part 3, vol.84, no.9, pp.31-41 (2001).

○ O. Hirota, M. Osaki, and M. Sasaki, “Entangled state based on nonorthogonal state,” Quantum Communication, Computing, and Measurement 3 pp359-366, ed. P. Tombesi and O. Hirota (Kluwer academic/Plenum publishers, New York 2001).

通信総合研究所:

○ R. B. M. Clarke, V. M. Kendon, A. Chefles, S. M. Barnett, E. Riis, and M. Sasaki, “Experimental realization of optimal detection strategies for overcomplete states,” Phys. Rev. A64, 012303-1~13 (2001).

○ S. M. Barnett, R. B. M. Clarke, V. M. Kendon, E. Riis, A. Chefles, and M. Sasaki, “Experimental quantum state discrimination,” *Quantum Communication, Computing, and Measurement 3,* pp59-67, ed. P. Tombesi and O. Hirota (Kluwer academic/Plenum publishers, New York 2001).

○ J. Mizuno, M. Fujiwara, M. Akiba, T. Kawanishi, S. M. Barnett, and M. Sasaki, “Optimum detection for extracting maximum information from symmetric qubit sets,” Phys. Rev. A65(1), 012315-1 -- 012315-10 (2002).

○ M. Takeoka, D. Fujishima, and F. Kannari, “Optimization of ultrashort-pulse squeezing by spectral filtering with the Fourier pulse-shaping technique”, Opt. Lett. 26(20) 1592-1594 (2001).

○ M. Takeoka, M. Ban, and M. Sasaki, “Quantum channel of continuous variable teleportation and nonclassicality of quantum states”, J. Opt. B; Quantum Semiclass. Opt, 4, 114-122 (2002).

○ M. Fujiwara, M. Sasaki, and M. Akiba, “Reduction method for low frequency noise of GaAs JFET at a cryogenic temperature,” Appl. Phys. Lett. Vol. 80(11) March (2002).

○ H. Tobioka, Y. Mitsumori, F. Minami, and A. Hasegawa, “Time-resolved three-pulse photon echoes in GaSe,” J. Lumin Vol.94－95,p601－604 (2002).

○ R. Kawahara, Y. Mitsumori, T. Kuroda, and F. Minami, “Ultrafast phase distortion of the transmitted pulse in GaAs quantum wells,” J. Lumin. Vol. 94－95, pp 645－648 (2002).

○ Y. Mitsumori and F. Minami, “Transient coherent emission from anisotropic semiconductors studied with phase-locked pulse pairs,” J. Lumin. Vol. 94－95, pp663－666 (2002).

○ M. Sasaki, A. Carlini, and R. Jozsa “Quantum template matching,” Phys. Rev. A64, 022317-1~11 (2001).

○ M. Sasaki, A. Carlini, and A. Chefles “Optimal phase estimation and square root

measurement," J. Phys. Math. Gen. 34, 7017-7027 (2001).

○ S. M. Barnett, C. R. Gilson, and M. Sasaki, "Fidelity and the communication of quantum information," J. Phys. Math. Gen. 34, 6755-6766 (2001).

○ M. Sasaki and A. Carlini, "Quantum state recognition," *Quantum Communication, Computing, and Measurement 3* pp31-34, ed. P. Tombesi and O. Hirota (Kluwer academic/Plenum publishers, New York 2001).

(2) 特許出願

なし