「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.実施の概要

量子暗号を短距離応用だけでは無く、より広範な実用化を可能とする為、量子中継技術を初めとする量子情報処理通信技術の基盤技術、特に量子絡み合いを主とした光子状態制御技術を開発する。これまでに各グループから以下の様な成果が得られており、今後さらにこれらを発展させ、量子情報処理通信技術の総合的な底上げを実現する。

＜中村グループ＞

昨年までに量子状態の評価手法であるトモグラフィーを用いて、高い量子絡み合いの度合いを有する光子対源を開発すると共に、量子操作を評価するプロセストモグラフィーの手法を確立した。さらに今年度量子状態を高精度で推定する方法を開発した。又、量子状態制御デバイスとして候補となる量子ドットの評価を開始し、1μmより長波長領域で単一ドットからの発光を初めて観測に成功した。今後、新たな近接場顕微鏡等の評価方法により、制御デバイスへ向けた取組を進める。一方、理論では量子中継に必須となる量子絡み合いの回復についてその効率を決める指標、及び回復可能性を判断する尺度を求める事に成功した。

＜Wangグループ＞

フォトニック結晶ファイバーを量子絡み合い光源として用いる事により、相関光子対の生成に成功した。実用化へ向け、さらなる背景雑音の低減が課題となる。量子情報を担う単一光子の貯蔵を冷却原子トラップを利用した方法で実現しようとしており、冷却原子をトラップするシステムが完成しつつある。

＜小林グループ＞

昨年度までに連続光における振幅スクイーズド光の発生と制御に成功し、これをさらに発展させ、非局所性を有する光子対の発生を達成する。単一モードスクイーズド状態の2光子状態から多光子干渉実験へと進め、非局所性を実験的に確認する。又、周波数領域において相関を持つ光子対の実験的検証、パルス光励起による光子数スクイーズド状態の発生、量子情報処理に関連する基礎的な実験状況に即した理論等を新たに展開する。

＜広田グループ＞

エンタングルメントを利用する量子暗号の多機能化を目指すため、当該グループが開

発してきた 非直交状態のエンタングルメント状態の理論をさらに発展させ、それらの生成法を解明した。
量子暗号プロトコルの最適化を目指す量子情報理論的諸問題において極めて有意義な成果を得た。
＜井筒グループ＞
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-空間モードのパルス位置変調符号を行うための符号回路を開発し、Ｈ１４年度は、この装置を用いて量子通信路符号化の原理実証を世界に先駆けて行った。また、光子数識別器の低雑音化に成功した。

2. 実施内容
チームの研究目標：
量子暗号のより広範な実用化の為、量子中継技術を初めとする量子情報処理通信技術の基盤技術を開発する。この基盤技術は量子情報処理通信システムの送信部（光源等）、通信路（中継等）、受信部（受信器等）にわたって幅広く開発されるべきもので、これらの基盤技術を統合する事で、より大きな市場に対応した量子暗号システムの実現が期待出来る。これらの技術は量子暗号だけでなく量子情報技術全般に大きな波及効果をもたらすものである。
以下、各グループでの研究目的と今年度の研究成果をまとめる。
＜中村グループ＞
研究目的：
量子中継等の量子情報処理通信技術では量子絡み合いの取り扱いが重要であり、特に光源部、通信路における中継部等での量子絡み合い制御技術を開発する。この為に、まず量子絡み合いに関する定量的評価技術を実験・理論の両面から確立する。さらに半導体量子ドットを用いて量子情報処理通信における制御用デバイスを開発し、量子情報処理通信システムの光源部、中継部への応用を図る。
研究結果：
(1) 量子中継（量子絡み合いの回復）効率の評価方法の理論的確立
量子中継の効率は量子絡み合いの回復効率によって決まり、その上限は量子絡み合いの一つの尺度である「相対エントロピー・エンタングルメント」で決定されるが、この量を計算する事は極めて難しく、中継効率評価の困難の原因となっていた。今回、最も重要な2量子ビットの場合におけるこの尺度を計算する為の解析式を導出し、中継効率を評価する方法を確立した。今回導出した解析式は、中継効率だけでなく種々の量子情報処理の効率を判断する評価手段となる。
又、上述の尺度とは別に、量子絡み合い状態を回復出来るかどうかの判定を行うのに適した新たな尺度を考案した。

(2) 量子状態（２光子の偏光状態）の高精度な推定法の開発

どの様な量子状態が得られているかを知る事は、光源開発や通信路での量子制御が適切かを判断する上で基本となる。今年度、量子状態を推定する標準的手法である量子状態トモグラフィーの推定精度の理論限界を明らかにすると共に、この理論限界に近い推定精度を実現できる推定法（推定すべき変数の数を実験データによって最適な数にする方法）を新しく開発する事ができた。

(3) 自己成長型InAs/GaAs量子ドットの単一ドット分光

量子暗号通信における情報キャリアとしての単一光子を変換制御する量子情報処理通信用デバイスを実現する為に、単一量子ドットを重要な候補として選び、これを単一光子と相互作用させようとしている。今年度は自己成長型InAs/GaAs量子ドットに直径0.5μm～1μmの微小な開口のある金属マスクを用いた顕微分光を行い、少数個の半導体量子ドットを発光スペクトル上で分解することに成功した。図１は多数個の量子ドットを観測した為、サイズのばらつきによる不均一幅により、ブロードな単一ピークが見られている。これに対し、図２では顕微鏡の視野に入る量子ドットの個数を実効的に少なくした為、少数個の量子ドットに由来する鋭い発光ピークが観測された。これは1μm以上の長波長領域での初めての結果であり、今後の通信波長帯への応用上重要な成果である。

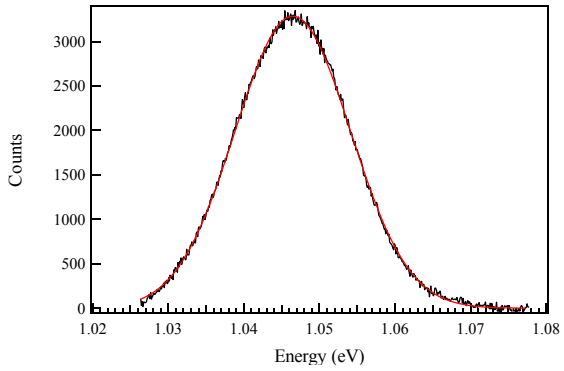

図１．多数個の量子ドットの発光スペクト

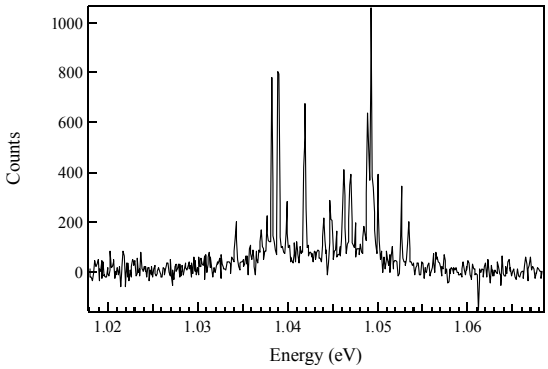

図２．少数個の量子ドットの発光スペクトル

又、新たなデバイスを開発する為には、新たな実験手段の開発が不可欠である。その目的で，本研究グループでは近接場効果を利用した極低温走査型プローブ顕微鏡の開発を進めている。今年度はこの装置の設置、トンネル顕微鏡・原子間力顕微鏡としての機能を確認した。しかし光学系の構築に伴い、装置に改造を施す必要がある事がわかり、この改造は平成１５年度中に完了させ，研究を遂行する予定である。

＜Wangグループ＞

研究目的：

量子暗号の光源に量子絡み合いの関係にある単一光子対を用いる事で単一光子検出器における雑音の影響を減らせる為、量子暗号システムの性能向上が可能となる。この量子相関光子対を高効率で発生する光源を、フォトニック結晶ファイバーにおける4波混合過程を利用して開発する。

（この高効率光源には、位相整合条件を満足する為、ファイバー中で負の群速度分散が必要になるが、これをフォトニック結晶ファイバーの異常分散で実現する。）

又、量子中継等で必要となる量子情報を担う単一光子の貯蔵を冷却原子トラップにて実現する。

研究成果：

(1) フォトニック結晶ファイバーからの相関光子対の生成

図１に示した断面形状を有するフォトニック結晶ファイバーを用いて4波混合過程による相関光子対の研究を進めているが、今年度はフェムト秒レーザをピコ秒レーザに取り替える事により、背景雑音を大幅に低減する事に成功した。図２にレーザの強度を上げて行くに連れ、ストークス光とアンチストークス光が明瞭に観測される様子が示されている。又、単一光子レベルのストークス光とアンチストークス光の同時計測を行い、偶然に生じる同時計測の２倍以上のレートが得られ、相関単一光子対の発生が確認された。実用化へ向けては、さらにラマン散乱による背景雑音のさらなる低減が必要となる。

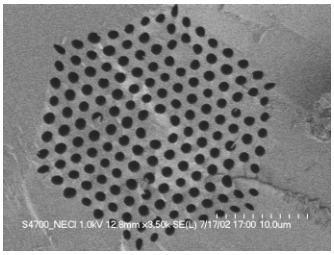

図1. ﾌｫﾄﾆｯｸ結晶ﾌｧｲﾊﾞｰの断面

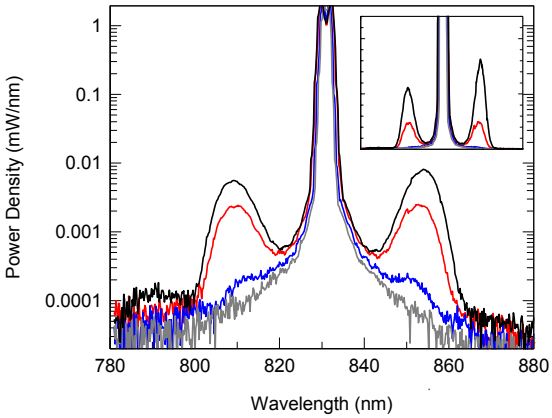

図2. 相関するｽﾄｰｸｽ、ｱﾝﾁｽﾄｰｸｽ光の発生
各線は4，5，7.5，8mWの励起強度に対応

(2) 単一光子の冷却原子トラップへの貯蔵

担当するポスドクの到着が米国の新たなVISA問題で遅れているが、冷却原子トラップシステムの構築が漸く完成しつつある。今後、このシステムを用いて単一光子の貯蔵へ挑戦する。

＜小林グループ＞

研究目的：

量子情報処理、特に他グループで開発される量子回路の検査に必要となる量子相関光源を非線型光学的手法により生成する。そのために、相関を持つ２～複数光子状態の発生とその物理的性質の解明を行う。さらに、現実的に問題となる損失、非理想的な検出器による量子信号への影響を理論的に解明する。

研究成果：

(1) 非局所性を持った光子対の発生とその観測

光パラメトリック発信器（OPO）をしきい値より非常に小さいポンプ光で励起すると、２光子状態を発生できることが知られている。本実験ではチタンサファイアレーザからのポンプ光（波長860nm）の二倍波により、共振器内に置かれたニオブ酸カリウム結晶（KNbO3）を励起した。この2光子対は共振器のバンド幅に制限され、大きなコヒーレンス長をもつという特徴がある。以下の3条件が満たされた場合、2光子状態の相関関数に周期的構造が観測できる。

1. 共振器のスペクトル幅が共振器の自由スペクトル間隔より大きい。
2. 自由スペクトル間隔の逆数（光子がOPO内を1周する時間）が光子計数器の分解時間より大きい。
3. 光子計数器の分解時間内の同時計数値は１より小さい

本研究では比較的大きいOPO（周回時間　～2ns）と高性能光子計数器（分解時間　～0.3ns）を用いてこの条件を達成し、周期的構造の測定に初めて成功した。この実験結果は、図１に示すように、理論計算と極めて良い一致を示した。我々の開発したOPOを使って得られた2光子対は、これまで報告されたものと異なる特徴をもつ。この特徴を生かして以後の研究を推進していく予定である。

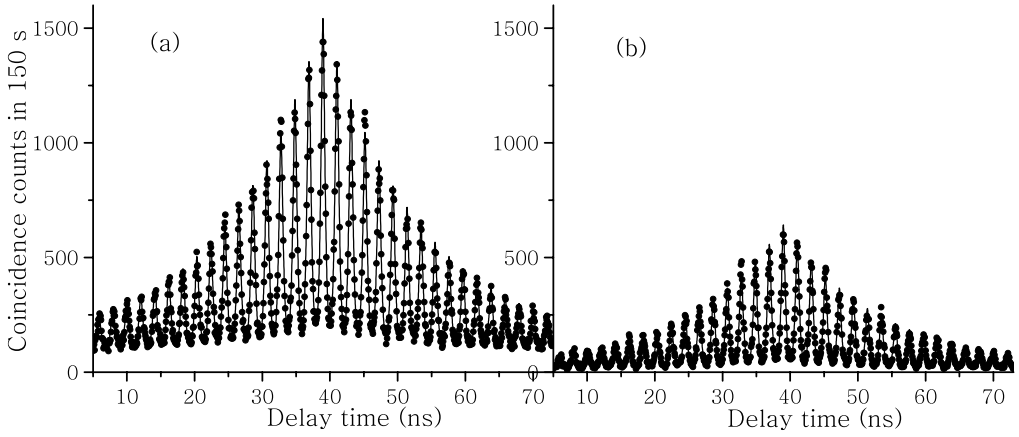

図１：多モード二光子相関計測の結果。左図は右図の約二倍のポンプ高強度で得られた結果。点が実験結果、曲線が理論で得られた結果。

(2) 周波数領域において相関を持つ光子対の実験的検証

SPDC (Self Parametric Down Conversion)では通常、偏光や波数ベクトルの絡み合いを用いることが多いが、ここでは周波数の相関に着目し、その応用を検討する。タイプⅡのBBO結晶をチタンサファイアレーザの二倍波でポンプすることにより、860nm近傍の波長を持った光子対を発生させた。この光子対は周波数が非縮退で発生するが、光子対を構成する光子同士の周波数の和は常にポンプ光の周波数に等しく、その点で互いに周波数相関を持っている。さらにこの光子対を偏光ビームスプリッタで分けることにより非局所性を

持たせている。現在、光子対が持つ周波数の相関について、基礎的な測定に成功したが、今後、現在の実験系を改良し、明確な周波数相関を得ることを予定している。

(3)超高感度分光検出器の開発

量子情報処理のために、単一量子ドットや結合ドットの非線型光学測定が必要になる。これに対応出来るように、単一量子井戸を非線型光学測定出来る分光計の開発をしている。

(4)非古典的な光を用いた量子情報処理における現実的な問題点の理論的取り扱い

量子情報コヒーレント基底を用いて、テレポーテーションの場合の理想的でない検出器、絡み合った光子対を発生する非線型結晶の影響および実際に得られる信頼度に関するフィデリテイーなどを計算し、方式の実現性を理論的に明らかにした。

＜広田グループ＞

研究目的：

エンタングルメントを利用する量子暗号の多機能化と最適化を目指すための量子情報理論を開発する。

(1) 擬ベル状態（非直交状態のエンタングルメント状態）による量子ゲート

研究方法：

Knillらによって提案された単一光子、線形光学による量子ゲートは現実性が無いとして、Ralphらはcoherent状態によるゲートを提案している。しかしそれもまた、擬直交性を必要とするため高輝度光が必要となる。玉川大学ーベル研によって開発された擬ベル状態理論に基づき、その生成法と量子ゲート理論を開発する。

研究成果：

マイクロ共振器内での原子とレーザ光の共鳴ー反共鳴現象を応用して進行波型擬ベル状態を 生成することが可能であることを解明した。これらを量子ゲートとして活用するための局所的操作の方法を検討し、量子光通信の分野で発明されたKennedy型信号識別方式が有用であることを 示した。（広田）

(2) 量子暗号の安全性強化と多機能化

研究方法：

伝送路の損失による通信距離の制限を克服するため、様々な多光子系の状態を用いた量子暗号の性能を比較検討する。また認証などを可能にするためのプロトコルや符号理論の開発を行う。

研究成果：

・量子情報のセキュアな伝送について研究を進め、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，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検討した．昨年度提案した，１量子ビット伝送のための(3,1)量子符号を，２量子ビット伝送に適用できないか，考察した結果，エンタングルした２量子ビットに対しては，適用不可能であることを明らかにした．このため，任意の２量子ビット伝送に適用可能な(6,2)量子符号を新たに提案し，所望の機能が得られることを示した．（臼田）

・量子一括復号機構を有する量子通信システムに古典符号理論で開発された符号を適用し

た場合の誤り率特性を調査した．その結果，(7, 4)，(17, 7)，(15, 5)，(31, 6)の各ＢＣＨ符号，および(4, 3)，(8, 4)，(16, 5)の各リードマラー符号のいずれもが符号長を固定した場合に量子信頼性関数で予測される誤り率を下回るという意味で「良い符号」であることが明らかになった．（加藤）

・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，伝送路にエネルギー損失が存在し，盗聴者が検出・再送型盗聴において曖昧さの無い検出と誤り率最適検出を用いた場合の安全性を検証した．その結果，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，ある程度のエネルギー損失が有っても安全であることが確認できた．（大崎）

・対話型秘密鍵系列の一致法の通信回数を削減することを目標に，連接符号を用いたプロトコルを提案し，その特性を調べた．その結果，プロトコルを一往復の通信で完了させるためには，秘密鍵系列の一致のもう一つの重要な評価基準である公 開ビット数が非常に多くなることが明らかになった．ユーエンとキムが提案したYKプロトコルの実用化を目指すため、その鍵速度の性能改善法を提案した。（山崎）

＜井筒グループ＞

量子状態を使って情報を符号化し、量子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。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：

量子パターンマッチングに関する前年度までの理論的成果を実用に向けて具体化するために、学習マシーンの回路構成を調べ、２クラス判定の具体的回路を導出した。

(2) 量子通信路符号化の原理実証

研究方法：

前年度までに開発した多段干渉回路を用いて、超加法的量子符号化利得と呼ばれる新しい量子効果の実証に成功した。具体的には、光子の空間帯域を２倍に増やしたときに２倍以上の情報が伝送されることを実証した。図２に実験結果を示す。

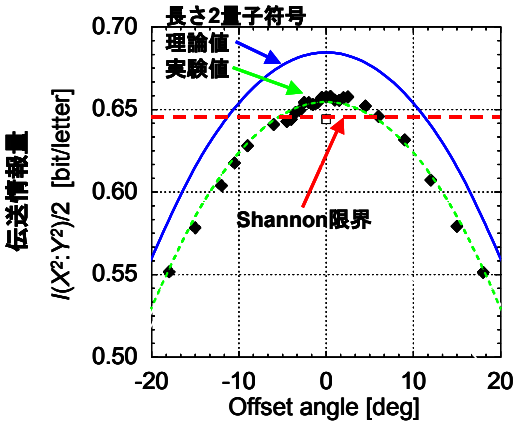

図2　自由度あたりの伝送情報量（縦軸）。横軸は信号状態ベクトルと測定状態ベクトルの相対角。

3.実施体制

＜中村グループ＞

① 研究分担グループ長：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と量子中継システム

＜Wangグループ＞

① 研究分担グループ長：L. J. Wang（NECラボラトリーズアメリカ、Research Scientist）

② 研究項目：絡み合い光源開発等

＜小林グループ＞

① 研究分担グループ長：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

＜広田グループ＞

① 究分担グループ長：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

＜井筒グループ＞

① 究分担グループ長：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：量子通信路符号化技術

4.主な研究成果の発表（論文発表および特許出願）

(1) 論文（原著論文）発表

＜中村グループ＞

○ A. Tomita and K. Nakamura:
"Balanced, gated-mode photon detector for qubit discrimination at 1550 nm," Optics Letters **27** (2002) pp. 1827-1829.

○ 南部芳弘、
「量子チャネルの評価技術」
応用物理72, 2003年2月号

○ 南部芳弘、宇佐見康二、津田美幸、松本啓史、中村和夫、
"Generation of Polarization-entangled Photon Pairs in a Cascade of Two Type-I Crystals Pumped by Femtosecond Pulses"
Physical Review A 66 (2002)

○ S. Ishizaka,
"The reduction of the closest disentangled states",
J. Phys. A: Math. Gen., Vol. 35, No. 38, pp. 8075-8081 (2002).

○ S. Ishizaka
"Analytical formula connecting entangled states and the closest disentangled state",Phys. Rev. A, Vol. 67, No. 5 (2003).

○ K. Hirose, Y. Meir, and N.S. Wingreen:
"Local Moment Formation in Quantum Point Contacts"
Phys.Rev.Lett., 90, 026804 (2003).
○ T. Hiroshima,
"An entanglement measure based on the capacity of dense coding",
Physics Letters A 301 (2002) 263-268.
＜Wangグループ＞
○ A. Dogariu, L. J. Wang, and J. A. West,
"Correlated photon generation in anomalous group dispersive fibre,"
Annual Meeting of the Optical Society of America, Orlando, FL, (2002).
○ A. Dogariu, J. Fan, and L. J. Wang,
"Correlated photon generation for quantum cryptography,"
NEC R&D Journal (in press).
○ L. J. Wang,
"Causal 'all-pass' filters and Kramers-Kronig relations",
Opt. Commun. **213**, 27 (2002).
○ H. Cao, W. S. Warren, A. Dogariu, and L. J. Wang,
"Reduction of optical intensity noise by means of two-photon absorption,"
J. Opt. Soc. Am. B, Vol. **20**, No. 3, 560 (2003).
○ J. Fan, A. Dogariu, and L. J. Wang,
"Amplified total internal refraction,"
Optics Express, Vol. **11**, No. 4, 299 (2003)
○ A. Dogariu, M. Hsu, and L. J. Wang,
"Reducing Far-field Diffraction by Structured Apertures,"
Opt. Commun., in press, (2003).
＜小林グループ＞
○ T.Ide, H.F.Hofmann, T. Kobayashi, and A. Furusawa,
"Continuous-variable teleportation of single photon states,"
Phys. Rev. A, 65,012313,2002
○ T. Ide, H. F. Hofmann, A. Furusawa, and T. Kobayashi,
"Gain tuning and fidelity in continuous-variable quantum teleportation,"
Phys. Rev. A, 65, 062303, 2002
○ A. Vukics, J. Janszky, and T. Kobayashi,
"Nonideal teleportation in coherent state basis,"
Phys. Rev. A, 66, 023809, 2002
○ H. Goto, H. Wang, and T. Kobayashi,
"Multimode squeezed state produced by an optial parametric oscillator,"

Phys. Rev. A, submitted.

○ J. Janszky, J. Asboth, A. Gabris, A. Vukics, M. Koniorczyk, and T. Kobayashi, “Two-mode Schroedinger cats, entanglement and teleportation,” Fortschr. Phys. 51, 2-3, 156-170, 2003

○ A. Vukics,J. Janszky, and T. Kobayashi, “Infinitesimal representation and a generalization of the quantum-scissors device,” Phys. Rev. A, accepted.

○ H. Goto, Y. Yanagihara, H. Wang, T. Horikiri, and T. Kobayashi, “Observation of an oscillatory correlation function of multimode two-photon pair,” Phys. Rev. A, submitted.

○ H. Goto, H. Wang, and T. Kobayashi, “Multimode squeezed state produced by an optical parametric oscillator,” Phys. Rev. A, submitted.

＜広田グループ＞

○ M.Sohma and O.Hirota, “Squeezing is good at low information rate,” Physical Review A, vol.65, no-2, 022319 , 2002.

○ T. S. Usuda, S. Usami, I. Takumi, and M. Hata, “Superadditivity in capacity of quantum channel for q-ary linearly dependent real symmetric-state signals,” Physics Letters A, vol.A305, pp.125-134, (2002.11).

＜井筒グループ＞

○ Mikio Fujiwara, Masahiro Takeoka, Jun Mizuno and Masahide Sasaki: ″Exceeding classical capacity limit in quantum optical channel″ Phys. Rev. Lett., vol 90, No.16, 167906/1--4(2003).

○ Masahiro Takeoka, Masahide Sasaki, and Masashi Ban: ″Continuous Variable Teleportation as a Quantum Channel″ Optics and Spectroscopy, Vol.94, No.5, 734 -- 742(2003)

○ A. Chefles and M. Sasaki: ″Retrodiction of generalized measurement outcomes″, Phys. Rev. A67(3), 032112/1--12 (2003),

○ Masahiro Takeoka, Masahide Sasaki, and Masashi Ban: ″Continuous variable teleportation as a quantum channel″, Optics and Spectroscopy, 94 (5), 735--743 (2003).

○ Daisuke Fujishima, Fumihiko Kannari, Masahiro Takeoka, and Masahide Sasaki: ″Generation of entanglement between frequency bands via a nonlinear fiber

propagation and a spectral pulse shaping″,
Opt. Lett., 28 (4), 275--277 (2003).

○ A. Hasegawa and Y. Mitsumori:
″Ultrafast electron control of optical device″,
J. Commun. Res. Lab. vol. 49 (1), 97--103 (2002).

○ M. Takeoka, M. Ban, and M. Sasaki:
″Continuous variable teleportation of non-classical states in noisy environment″,
J. Commun. Res. Lab. vol. 49 (1), 119--127 (2002).

○ M. Sasaki, J. Mizuno, and M. Fujiwara:
″Quantum detection circuit for quantum channel coding″,
J. Commun. Res. Lab. vol. 49 (1), 105--118 (2002).

○ M. Ban, M. Sasaki, and M. Takeoka:
″Continuous variable teleportation as a generalized thermalizing quantum channel″,
J. Phys. A: Math. Gen. 35(28), L401--L405 (2002).

○ M. Sasaki, M. Ban, and S. M. Barnett,
″Optimal parameter estimation of a depolarizing channel,″
Phys. Rev. A66 022308-1--022308-8 (2002).

○ M. Sasaki and A. Carlini,
″Quantum learning and universal quantum matching machine″
Phys. Rev. A66 022303-1--022303-10 (2002).

○ 佐々木雅英、武岡正裕：
″量子通信路符号化″,
応用物理学、Vol. 72, NO. 2, 169--175 (2003).

○ 佐々木雅英、番雅司：
″量子情報理論 -量子効果を使う新しい情報操作とその限界を明らかにする理論-″,
物理学会誌、Vol. 57, NO. 1, 9--21 (2002).

○ 武岡 正裕, 藤島 大輔, 神成 文彦:
″非線形ファイバを用いた超短光パルススクイージング″,
レーザー研究 30(8), 443--449 (2002).

○ 佐々木雅英：
″量子力学が開く究極の情報通信技術″
光技術コンタクト、Vol. 40, NO. 10(通巻467) 58--62 (2002).

(2) 特許出願

H14年度特許出願件数：0件（研究期間累積件数：0件）