「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)基礎・環境研究所　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

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＞

誘導放出過程に基づく光子検出方法を開発し，コヒーレント状態の光子状態を精確に評価することが可能であることを実証した．昨年までに開発した量子操作を評価するプロセストモグラフィーの手法によって２量子ビットの量子状態フィルターの評価を行った．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では，励起子状態の蛍光ピークの測定により，偏光状態，１励起子，２励起子状態を評価した．一方、理論では量子絡み合い状態の一つである束縛エンタングルメント状態について新たな知見が得られた．

＜Wangグループ＞

フォトニック結晶ファイバーを利用した量子絡み合い光源をこれまでに構築し，相関光子対の生成に成功している。Ｈ１５年度は背景雑音の低減に成功し，光子対の生成効率を偶発的に計数される背景雑音の８倍にまで上昇させることができた．これは競合グループに比較して最高のシグナル強度である．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＞

光パラメトリック発振器を発振閾値以下で動作させ，量子相関光子対源としての動作を検証した．発振帯域が発振器によって制限されるため，マルチモードでの光子対の発生が可能であることが強度干渉実験によって確認された．

＜広田グループ＞

量子暗号の高速化を目指すため、当該グループが開発してきた コヒーレント状態による量子暗号の理論をさらに発展させ、それらの実現を解明した。また、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＞

Ｈ１４年度までに、単一光子の偏波-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、量子通信路符号化の原理実証に成功した。Ｈ１５年度は、この回路をさらに改良を施し、データ圧縮に関する量子情報源符号化の原理実証に世界に先駆けて成功した。これにより、量子情報通信に2つの柱となる基本概念の実験的検証が終了した。また、光子数識別器に関しては暗電流0.14カウント/秒という極めて低雑音の検出性能を達成した。但し、繰返し動作はまだ数Hzと極めて遅く今後、高速化にも取り組んでゆく。

2.研究実施内容

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。

研究成果：

（１）誘導放出過程を利用した初の光子検出方法の開発および実証

光子の吸収過程において，物質は光子を吸収した結果，励起状態に遷移する．通常の光子検出器では，光子吸収において励起された電子を電流として検出する．一方，誘導放出過程では，励起状態にある物質に共鳴した光子が入射することで，励起状態から基底状

態への遷移が生じ，このとき新たに光子が放出される．この誘導放出過程は吸収過程の逆過程であり，誘導放出過程を利用した光子検出も可能であることが提唱されていた．昨年度は，非線形結晶による誘導パラメトリック下方変換を用いて誘導放出過程を利用した光子検出の方法を開発した．この方法を用いてコヒーレント状態の強度相関検出を行うことで，誘導放出を利用した光子検出が可能であることを初めて実証した．この方法は，吸収過程による光子検出とは異なり真空状態のゼロ点振動に感度があるため，光子状態をより精確に評価することが可能である．

（２）量子中継に関連する２量子状態の理論的評価

量子状態のうち、エンタングルしているにもかかわらず、そのエンタングルメントを局所的な操作と古典的な通信だけでは取り出せない「束縛エンタングルメント状態」の存在が知られており、この状態は量子情報にとって有用ではないと思われていた。今回、これまで通常のエンタングルメント対だけでは不可能とされていたエンタングルメントの項数を増やす事が、この状態を一緒に用いる事で可能になる事を初めて明らかにした。これは、長らく予想されていたが未証明であった関係式の証明に成功したことにより達成された．

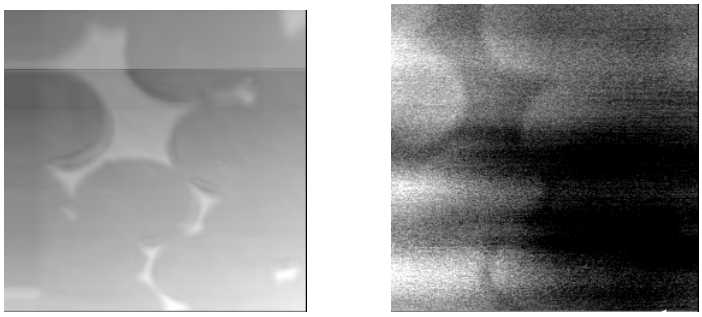
また，真空の電磁場揺らぎと相互作用している２つの連続変数量子状態からなる物理系において、相互作用に完全な相関がある場合、２つの量子状態全体としては、環境系(真空の電磁場揺らぎ)の効果を全く受けない（温度ゼロのとき）か、ほとんど受けない（有限温度のとき）状態が存在することを具体的に示した．この効果は、連続変数状態、特にコヒーレント状態を用いた量子計算機における量子メモリーへの応用が期待できる．

（３）プロセストモグラフィーによる量子相関チャンネルの評価

量子中継に必要な量子ゲートデバイスの性能評価のためには，その特性や量子相関の生成能力を評価する方法が必要である．これまでに開発したプロセストモグラフィーの方法を発展させ，２量子ビットの量子デバイスの実験的評価を可能にする方法を開発した．本方法を用いた検証実験として，２量子ビットの量子状態フィルターであるビームスプリッタを評価し，光子が射影される状態が、従来から信じられている１重項状態ではなく、３重項状態であることを明らかにした。この誤解が生じた理由は、ビームスプリッタでの反射における偏光ヘリシティの反転を考慮に入れなかった為である。

（４）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ために，半導体単一量子ドットをデバイスの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．前年度までに、近赤外領域における顕微分光装置と微小な開口のある金属マスクを設けたInAs/GaAs量子ドットサンプルとを組み合わせ、単一量子ドット由来の蛍光ピークを観測した．今年度は，この蛍光ピークが励起子の波動関数に固有の偏光状態を示すことを確認し，１励起子状態および２励起子状態を示唆する蛍光ピークの弁別に成功した．これらは，量子ドットを利用して単一光子に対する操作を行う上で重要な情報である．



図：評価用試料のトポグラフィック像（左）と近接場像（右）．評価用試料ではガラス基板上の金属膜に多数の開口（直径５００ｎｍ）が設けてある．トポグラフィック像では金属膜のある部分の高さが高く（図中白色部分）なっており凹凸像として検出されている．これに対し近接場像では金属膜のない部分を透過する光を観測しており，トポグラフィック像に対して反転した像が得られている．また，観測された構造のもっとも微小な部分から近接場像の空間分解能が使用波長（６３２ｎｍ）の５分の１程度まで得られていることがわかる．

また，新たなデバイスを開発するためには，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．今年度は昨年度課題となっていた改造を施し，評価用の試料を用いて近接場像の測定に成功した（図）．さらに近接場光を集光する光学系について、新たな光学系を考案した．平成１６年度中にこの方式を用いて信号感度がより向上したシステムを構築し，磁場中，低温における測定を実現する予定である．

＜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ことで、単一光子検出器における雑音を減らすことができるため，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光波混合過程を利用して開発する．また，量子中継などで必要に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用いて実現する．

研究成果：

昨年度までにフォトニック結晶ファイバー中における４光波混合過程を利用して，ストークス光およびアンチストークス光を発生するのに成功した．さらに，これらのストークス・アンチストークス光に関して，単一光子レベルで同時計数を行い，相関光子対の発生を確認した．

今年度は発生したストークス・アンチストークス光の周波数選択を最適化するなどして，相関光子対の生成効率を向上させ，生成された相関光子対のノイズスペクトルを測定

することで，生成効率の定量的な評価を行った．図１に生成されたストークス・アンチストークス光それぞれに含まれるある周波数での雑音の和（■），および相関部分を差し引いた雑音（●）のポンプ光強度依存性を示す．相関部分を差し引いた信号では雑音が大幅に低減されていることがわかり，生成されたストークス・アンチストークス光の間に十分な相関が現れている．さらに，波数整合条件に対する生成された光子対の相関の依存性を図２に示す．波数整合が成立している条件では相関が最大値の６０％に達していることが観測され，発生された光子対の半数以上の光子が相関を有していることが示された．

冷却原子トラップを用いた実験は，当グループがマックスプランク研究所に移籍したため，実験系の立ち上げを現在行っている．

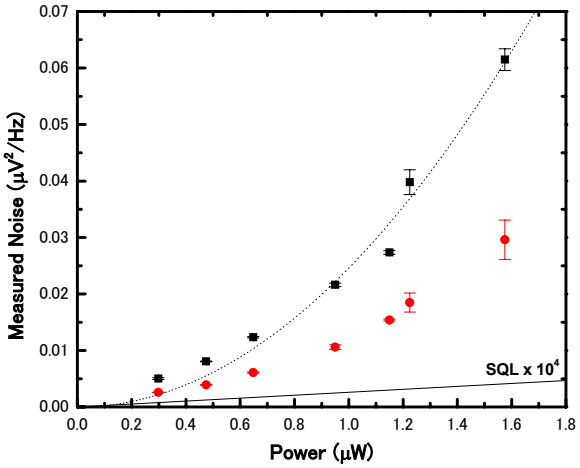


図１：雑音成分のポンプ光強度依存性

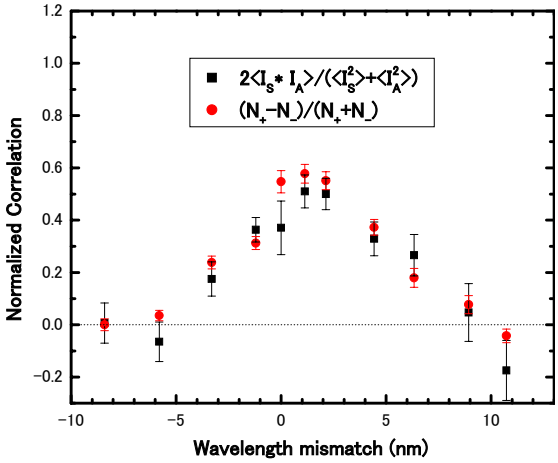


図２：相関関数の波数整合条件依存性

＜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：

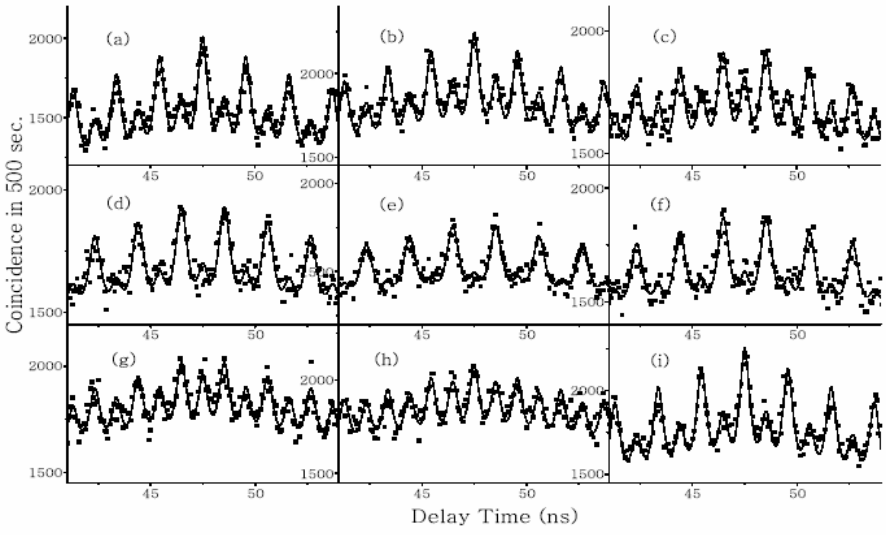
光パラメトリック発振器（OPO）を閾値より非常に小さいポンプ光で励起することによって、2光子対状態の供給源になることがOu等により示され、非古典的な光子統計の観測に応用された。共振器がないパラメトリック過程によって得られる2光子対と違い、OPOによってバンド幅が制限されるため狭バンド幅で相関時間が長い2光子対が得られる。発生する2光子対はそのバンド幅内に存在する多数の共振器モードのいずれかになるため、出力は多モードの光子対の重ね合せになる。その強度相関関数を計算すると櫛状のものとなる。この現象を観測するには光子のOPO周回時間が検出器の分解能よりも長くなければい

けないが、我々は物理的に長いOPOを用いて光子同時係数をとることで、強度相関関数を測定し理論と合致することを確認した。

またOPOから出力された2光子対を光路差のあるMach-Zehnder干渉計に入射させ、それによる2光子干渉を観測する実験を行った。この干渉計の光路差は、OPO共振器の周回時間の半分になっている。それにより干渉計の短いパスと長いパスを1光子ずつが通過した場合は識別可能性があるので干渉は生じない。しかし2光子が同じパスを通る場合はどちらのパスを通ったかという識別ができないので干渉を生じることになる。よって2光子の検出される時間差が干渉計の光路差分ずれるごとに、干渉するピークとしないピークが現れることが予想される。そのようにして得られた結果が図である。

図中の(a)-(i)はそれぞれπ/8ごとに干渉計の光路差をずらしたものに対応している。干渉はシグナルアイドラー光の波長に対してπの周期でおきると予想され(a)と(i)がほぼ同一であることから、その観測ができたとわかる。中央ピークから1つおきごとに干渉しており、位相が変わるごとにピークの高さも変わっている。干渉計の光路差に対応するピークは(a)-(i)までほぼ変化がなく、長短の光路差による識別可能性があるために干渉が起きないのが示されている。

このように光路長の長い共振器を用いることで、光路差の整数倍だけ時間的にずれたマルチモードの2光子対を得ることができ、それによって特殊な干渉効果を観測することに成功した。



図：OPO共振器から得られる光子対の強度干渉

＜広田グループ＞

研究方法：

伝送路の損失による通信距離の制限と暗号鍵生成速度の制限を克服するため、単一光

子系の改善方法と光通信による新量子暗号の性能を比較検討する。また認証への応用を目指したプロトコルや符号理論の開発を行う。

研究成果：

（１）単一光子量子暗号の高速化の研究

誤り率基準である１１％と２５％の意味を分析し、通信距離が長くなれば安全性の保証の意味が異なってくることを示した。２５％以内でも安全性を保証できないことに注意が必要である。また、実験系が安全な鍵配送の真の実現であるためには誤り率基準に適した量子誤り訂正符号が必要であり、それが未解決な段階で実験系の安全性を断定できないことを示した。したがって、誰もまだ安全な量子暗号を実験で示していないことになり、今後このグループが初の安全な量子暗号の実証をできる可能性がまだあることが解った。（広田）

（２）新量子暗号設計の計算に必要な信号誤り確率の解析法の開発.

従来、混合状態信号の誤り率最小検出過程を表す決定作用素に関する解析解は困難とされていたが、暗号に用いられる対称性のある混合状態に対して解析解の導出に成功した。これは光通信量子暗号において，盗聴者の能力を推定する際に有効な結果である．（加藤、広田）

（３）量子暗号のための符号化法の研究

本年度は特に光通信量子暗号の安全性向上のための研究を行っている．第一段階として新量子暗号への個別測定型の攻撃を無力化するような情報拡散化法を開発した．これを元に、ジョイント攻撃を無力化する方式の開発に向かっている。（加藤、広田）

（４）量子情報のセキュアな伝送について研究

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．平成15年度は，前年度までに提案していた，１量子ビット伝送のための(3,1)量子符号と２量子ビット伝送のための(6,2)量子符号の機能を一般化したm量子ビット伝送のための(3m,m)量子符号を提案した．また，この符号に対し，量子プロトコルに応用する際に本質的な，一部の量子ビットのみを用いた誤り訂正が可能であることを示した．（臼田）

（５）ユーエンとキム（YK）プロトコルの鍵生成速度の性能改善

YKプロトコルの実用化を促進する為、その鍵生成速度の性能改善法に関して詳細な検討をおおこなった。その結果、エネルギー減衰による鍵速度劣化特性が著しい改善されることを数値的に解明した。（山崎）

＜井筒グループ＞

研究目的：

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。

研究成果：

（１）量子信号検出理論の構築とその応用

混合状態まで含む一般的な量子状態信号の集合の中から特定の一つの信号を確実に取り出すための量子測定法（量子状態フィルタリング）について明らかにし、離散及び連続スペクトルを持つ量子チャンネルの推定法への応用を明らかにした。これはまた量子暗号における信号検出にも有効と期待される。

（２）量子情報源符号化の原理実証

これまでに開発してきた単一光子の多段偏波干渉回路を用いて、量子情報のデータ圧縮に関する量子情報源符号化の原理実証に世界に先駆けて成功した。図に実験結果を示す。量子状態間の非直交性という量子力学的効果を適切に処理すること(図中P1, P2)で、従来の圧縮方式(図中P3)では到達できなかった復元精度が達成された。

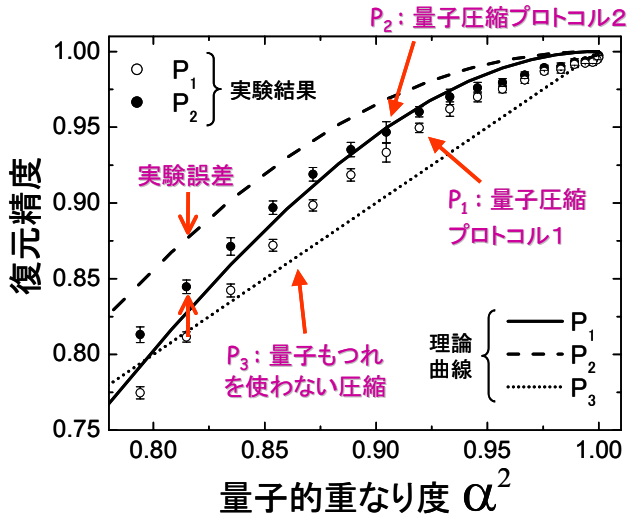


図　3ビット量子信号圧縮における復元精度測定の実験結果

3. 研究実施体制

＜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・環境研究所、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（Max Plank Research Institute、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（情報通信研究機構基礎先端部門、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) 論文発表

＜中村グループ＞

○ T. Hiroshima, ″Majorization Criterion for Distillability of a Bipartite Quantum State″, Phys. Rev. Lett. Vol. 91, 057 902 (2003)

○ S. Ishizaka, “Analytical formula connecting entangled states and the closest disentangled state”, Phys. Rev. A 67, 060301(R) (2003)

○ 宇佐見 康二、南部 芳弘、津田 美幸、松本 啓史、中村 和夫、”Accuracy of quantum-state estimation utilizing Akaike’s information criterion”, Physical Review A 68, 022314 (2003)

○ 宇佐見 康二、南部 芳弘、史 安森、富田 章久、中村 和夫、”Observation of Antinormally Ordered Hanbury Brown and Twiss-type Correlation”, Physical Review Lett. Vol.92, No.11, 113601 (2004)

＜Wangグループ＞

○ A. Dogariu, J. Fan, L. J. Wang, and J. West, “Photon-pairs generation in micro-structured fiber,” in Quantum Electronics and Laser Science Conference QELS 2003, Baltimore, MD (2003).

○ A. Dogariu, J. Fan, and L. J. Wang, “Correlated Photon Generation for Quantum Cryptography,” NEC R &D Journal Vol.44 No.3 (2003)

＜小林グループ＞

○ H. Goto, Y. Yanagihara, H. Wang, T. Horikiri, and T. Kobayashi, “Observation of an oscillatory correlation function of multimode two-photon pairs,” Phys. Rev. A 68, 015803 2003

○ A. Yabushita, and T. Kobayashi, “Spectroscopy by frequency-entangled photon pairs,” Phys. Rev. A 69, 013806, 2004
○ Y. Li, and T. Kobayashi, “Four-photon entanglement from two-crystal geometry,” Phys. Rev. A 69, 020302, 2004
○ H. Goto, H. Wang, T. Horikiri, Y. Yanagihara, and T. Kobayashi, “Two-photon interference of multimode two-photon pairs with an unbalanced interferometer,” Phys. Rev. A 69, 035801, 2004

＜広田グループ＞

○ Kentaro Kato and Osamu Hirota, ″Square root measurement for quantum symmetric mixed state signals,″ IEEE Transactions on Information Theory, vol.49, no.12, pp.3312-33137, 2003.
○ Osamu Hirota, Kentaro Kato, Masaki Sohma, and Tsuyoshi S. Usuda, ″Quantum key distribution with unconditinal security for all optical fiber net work,″ Proceedings of SPIE,Quantum Communications and Quantum Imaging, R.E.Meyers et al., Eds., vol. #5161, 2003.
○ Y. Fujihara, T. S. Usuda, I. Takumi, and M. Hata, “Relation between optimum quantum detection operators for pure and mixed-state signals,” Electronics and Communications in Japan (Part III: Fundamental Electronic Science), vol.86 (10), pp.8-18, John Wiley & Sons, (2003.10)

＜井筒グループ＞

○ J.A.Vaccaro, Y. Mitsumori, S.M.Barnett, E.Andersson, A.Hasegawa, M. Takeoka, and M.Sasaki: “Quantum data compression” Lecture Notes In Computer Science, vol.2827 98—107(2003).
○ A. Carlini and M. Sasaki: ″Geometrical conditions for completely positive trace-preserving maps and their application to a quantum repeater and a state-dependent quantum cloning machine″ Phys. Rev., **A68**(4) 042327/1--10(2003)
○ Y. Mitsumori, J. Vaccaro, S. M. Barnett, E. Andersson, A. Hasegawa, M. Takeoka, and M. Sasaki: ″Experimental Demonstration of Quantum Source Coding″ Phys. Rev. Lett., vol.**91**(21) 217902-1--217902-4(2003).
○ C.A. Fuchs, and M. Sasaki: ″Squeezing quantum information through a classical channel: measuring the ″Quantumness″ of a set of quantum states″ Quantum Information and Computation, Vol.**3**(5) 377--404(2003).
○ M. Takeoka and M. Ban, M. Sasaki: ″Unambiguous quantum-state filtering″ Phys. Rev., A**68**(1) 012307/1--7(2003).

○ M. Takeoka and M. Ban, M. Sasaki: ″Practical scheme for the optimal measurement in quantum interferometric devices″ Phys. Lett., A, vol.313(1-2) 16--20 (2003).

○ M. Akiba, and M. Fujiwara: ″Ultra low-noise near-infrared detection system with a Si p-i-n photodiode″ Optic. Lett., vol.28(12) 1010--1012(2003).

○ M. Sasaki, M. Fujiwara, M. Takeoka, and J. Mizuno: ″Quantum decoder for single photon communication″, Quantum Communication, Measurement and Computing, pp.185--188, ed. J.H. Shapiro and O. Hirota, (Rinton Press, New Jersey, 2003)

○ C.A. Fuchs, and M. Sasaki: ″The quantumness of a set of quantum states″, Quantum Communication, Measurement and Computing, pp.475--480, ed. J.H. Shapiro and O. Hirota, (Rinton Press, New Jersey, 2003)

○ M. Sasaki, and A. Carlini: ″Quantum learning and universal quantum matching″, Quantum Communication, Measurement and Computing, pp.315--318, ed. J.H. Shapiro and O. Hirota, (Rinton Press, New Jersey, 2003)

○ M. Takeoka and M. Sasaki: ″Two-frequency-mode entanglement generation inside an optical pulse by a nonlinear fiber and spectral pulse shaping″, Quantum Communication, Measurement and Computing, pp.103--106, ed. J.H. Shapiro and O. Hirota, (Rinton Press, New Jersey, 2003)

○ 佐々木 雅英: ″量子限界における符号化技術″ 数理科学, 11月号, NO.485, 23--29 (2003)

○ 佐々木 雅英: “量子情報通信” ITUジャーナル, Vol.34(1)(Jan. 2004)

(2) 特許出願

H15年度特許出願件数：0件 (CREST研究期間累積件数：0件)

日本版バイドール適用により、H16年度から出願予定。