「量子暗号の実用化を可能にする光子状態制御技術」

平成１２年１１月～平成１８年３月

研究代表者：中村　和夫
（物質･材料研究機構　若手国際研究拠点、副センター長）

１　研究実施の概要

【研究構想】

現行暗号技術が立脚する計算機の能力限界という不安定な基盤では無く、物理法則に絶対的安全性を保証された量子暗号技術が注目を集めている。この技術は量子情報技術の中でも最も実用化が近く、特に100km程度以内の短距離の応用においては、製品化も含め、実環境での試験も行われる様になってきている。しかしながら、この短距離応用から、さらに長距離化や単純な鍵配布以外の通信プロトコルなどの広範な実用化へと進める為には、送信部（光源）、通信路（量子中継）、受信部（光子検出器）の各部において、量子絡み合い(エンタングルメント)を用いた要素技術の開発による総合的な量子情報技術の底上げが不可避である。特に量子暗号の長距離化の為に、量子情報を中継して行く量子中継技術の開発は量子絡み合い光源から、量子情報伝達媒体の変換・検出技術、量子情報の保存、測定技術など、量子情報技術の広範囲に渡る多様な技術集積が必要であり、技術牽引のvehicleとなる為に、当プロジェクトを開始するに当たっての一つの重要なターゲットとして設定した。

【研究実施における目標】

この様な背景の元、総合技術である量子中継や暗号鍵配布以外の量子プロトコルなど、量子暗号のより広範な実用化を目的に、本チームでは今後の量子情報処理通信システムの重要な要素となる量子絡み合いに関わる以下の基礎基盤技術の高度化を進めていく事にした。

(1) 送信部での量子絡み合いの生成技術
(2) 通信路での量子状態の制御・変換技術
(3) 受信部での量子状態の検出技術

これらの成果をベースに短距離ではあるが、従来のシステムと比べ、高性能でより実用化に近いシステムが期待でき、また将来の量子中継を含むシステム展開への布石を打つ為、以下の項目を追加した。

(4) 量子暗号システムの実証実験

【研究実施の体制】

本チームにおける参加グループの構成は、研究を遂行して行く上で必要な技術を有するNEC筑波、マックスプランク（NECプリンストン）、東大、玉川大、情報通信研究機構（NICT）の５つのグループである。具体的には、NEC筑波で(1)～(4)、NECプリンストン（マックスプランク）で(1)、東大で(1)、(3)、(4)、玉川大で(2)、(4)、又、NICTで(2)、(3)の項目が実施された。量子情報技術の今後の展開に多様性があることを考慮し、候補となる技術が複数ある場合でも、一つに絞る事はせず、敢えて並行して開発する道を選択した。

【研究成果】

以下に本プロジェクトによって得られた主要な成果を示す。

(1) 送信部での量子絡み合いの生成技術

①量子状態トモグラフィーと呼ばれる量子絡み合い評価技術により、フェムト秒短パルス励起で高い量子絡み合いを有する光子対の生成技術を実現（NEC筑波）

②フォトニック結晶ファイバを用いた、低ノイズ、高効率の量子絡み合い光子対の生成を実現（マックスプランク（NECプリンストン））

③パラメトリック共振器を用いた多モード絡み合い光子対生成、多光子（３光子）の量子絡み合い状態を生成する光子源技術を実現（東大）

これらの光源はそれぞれトップレベルの性能を有している。用途により適した光源が使われていくことになると考えられる。また多光子の絡み合い技術は量子プロトコルなどへの応用も期待される。

(2) 通信路での量子状態の制御・変換技術

①量子状態を制御する量子操作の評価技術（量子プロセストモグラフィーと呼ばれる）により2ビット操作であるビームスプリッタで新たな知見を獲得（NEC筑波）

②量子インターフェースやゲート操作へ向けた単一量子ドットの分光研究と低温・強磁場環境での近接場顕微鏡の開発（NEC筑波）

③量子情報源符号化と量子通信路符号化の各々の技術でシャノン限界を超える世界初の実証実験に成功（NICT）

④量子絡み合いのコヒーレント状態への拡張と量子光通信の理論限界（玉川大）

⑤量子絡み合いの定量化と劣化の回復に関する理論的成果を獲得（有名な未解決問題の一つの解決を含む）（NEC筑波）

これらの技術はいずれも量子状態の制御・変換に関する重要な基盤技術となるもので、今後のこの分野の発展に大きなステップとなる。

(3) 受信部での量子状態の検出技術

①従来に比べて1桁以上、低ノイズ・高感度な光子検出器を開発（NEC筑波）

②従来の検出器が吸収過程を用いるのに対し、誘導放出過程を用いて真空に感度を有する新たな光子検出技術を実現（NEC筑波）

③量子暗号の安全性保証や光量子計算へ繋がる光子数識別器を開発（NICT）

④量子絡み合い状態の干渉や位相を観測する新たな検出技術を開発（東大）

１番目の検出器は次の実用化システムへも応用された。また２番目の検出器は真空に対して感度がある事から論理的に可逆な測定を実現できる可能性がある。一般に光子数識別器は量子絡み合い状態との組合せで、現在の技術でも光量子計算が可能になる事が明らかになっており、この意味で３番目の光子数識別器の今後の発展が期待さ

れる。

(4) 量子暗号システムの実証実験

①高性能単一光子検出器を用いた量子暗号システムで世界最長150km伝送を実現（NEC筑波）

②量子絡み合い光子対の片方の受信信号を伝令信号とした量子暗号システムを用いた実験に成功（東大）

③多値強度変調方式を用いたコヒーレント光通信による新量子暗号システムの開発に成功（玉川大）

１番目のシステムは単一光子を用いた量子暗号の実用化を大きく前進させると同時に、将来の量子中継を用いたシステム展開への布石ともなっている。２番目は伝令信号により、検出器のノイズを大きく減らす事ができるメリットがある。また３番目はコヒーレント光を用いた原理の異なる量子暗号であり、安全性の証明に関してはまだコンセンサスが得られていないが、用途によって従来の単一光子量子暗号との棲み分けも考えられる。

【成果の意義と今後の展望】

当チームの以上の結果は、ほとんどが世界トップレベルの成果であり、卓越した成果を挙げることができたと言える。(1)～(3)の基礎基盤技術だけでなく、(4)の量子暗号システムも含めて、量子情報技術の幅広い分野をカバーし、その技術レベルを本プロジェクトによる成果によって、大きく押し上げたということができる。これらは量子情報における大きなステップやマイルストーンとなるものであり、他への波及効果も期待される。

ここで得られた成果は世界トップレベルのものであるが、基礎基盤技術に関しては、さらなる改善や高度化が達成されることにより、量子中継などへの応用が実現していくことになる。一方、量子暗号システムに関しては、性能のさらなる改善、最適設計、安定性などの課題をクリアすることで実用化が進展していくことになる。

2　研究構想及び実施体制

(1) 研究構想

【基本構想】

省庁ホームページ改竄、ATM での情報漏洩等、現有セキュリティ技術の脆弱性が浮き彫りになる中、絶対的安全性を保証する量子暗号技術が注目を集めている。欧米や日本でも、既に量子暗号鍵配布の実証実験が行われ、又、一部、製品化も進められているが、短い専用線の限られた応用が中心である。この段階から一般の広いユーザへの実用化の為には、中継による伝送距離の向上や、ビットレートの増大、暗号鍵配布以外の秘匿通信プロトコルの実現など、現在の量子暗号の問題点を解決する必要がある。

この為には、量子絡み合い（エンタングルメント）とよばれる量子力学的相関を持つ光子対の利用が不可欠である。例えば量子暗号の伝送距離を延ばす為の量子中継では、この量子絡み合い光子対を用いる量子テレポーテーションと呼ばれる技術により、送信者の手元にある光子を、離れた距離において全く同一の光子として再生する事ができる。この技術をシリーズに繋げて行くことで、現状の量子暗号が有する距離の限界を大きく越える事が可能となる。この繋げる地点で量子中継器が必要になるが、これには量子絡み合い光子対を発生する光源技術、量子状態測定技術などが必須技術となる。さらに伝送路に損失がある場合には、量子情報伝達媒体である光子を別の媒体に変換するインターフェース技術、量子状態の保存技術などが加えて必要になる。従って、量子中継の実現には、これらの個々の要素・基盤技術の高度化が不可欠であると共に、これらは量子情報技術の全てに渡っている為、これらの基盤技術の高度化は量子情報技術全体のレベルをアップする事になる。

当プロジェクトを開始するに当たり、量子中継技術を一つの重要なターゲットとしたのは上述の理由からであり、これらの基盤技術の高度化により、暗号鍵配布以外の秘匿通信プロトコルなどの量子ネットワークを実現する事も可能となり、量子暗号技術の幅を大きく広げる事にも繋がる。

従って、本提案では量子絡み合い光子状態の生成と評価、及び制御を実現すると共に、量子暗号の高度化へ向けた量子中継や暗号鍵配布以外のプロトコルなどを支える要素となる量子情報基盤技術の開発を目的とした。又、同時に絡み合い光子状態に関する理論を進展させ、各技術開発における指導原理を得る事とした。

【研究開始時の目標・計画・実施体制】

上述の目的を実現する為、研究開始当初、欧米に対抗して本量子情報分野を推進する上で、NEC 筑波、NEC プリンストン（現マックスプランク）、東京大学を中心とするデバイス・システム技術と、玉川大学、情報通信研究機構（NICT；旧通信総合研究所）を中心とする理論との融合により力を結集し、量子暗号通信に関わる基盤技術を確立

する事を目指した。

具体的には、以下を目標・計画として各実施機関で設定した。

(a) 送信部での量子絡み合いの生成技術（NEC 筑波、NEC プリンストン、東大）

(i)量子絡み合いの評価手法を用いた高い絡み合いを有するパルス励起による光子対の生成。この手法を発展させた量子操作の評価（NEC 筑波）

(ii)フォトニック結晶ファイバを用いた高効率絡み合い光子対生成（NEC プリンストン）

(iii)パラメトリック共振器を用いた多モード絡み合い光子対生成、多体（３光子）量子絡み合い状態の生成（東大）

(b) 通信路での量子状態の制御・変換技術（NEC 筑波、プリンストン、玉川大、NICT）

(i)量子情報の制御ゲートを狙った単一量子ドット等の光学的基盤研究（NEC 筑波）

・光子から電子への量子インターフェースとなる単一量子ドットの分光研究

・量子ゲート操作へ向けた低温・強磁場環境で動作可能な近接場顕微鏡の開発

(ii) 量子情報の保存へ向けた原子のスピン状態の絡み合い（NEC プリンストン）

・光子の量子状態を原子のスピン状態に変換して保存・再生する技術の開発

(iii) 量子暗号通信のベースとなる量子通信路における量子符号化の実証（NICT）

・量子特有の効果を用いたシャノン限界を超える符号化の実証

(iv) 量子絡み合い状態に関する量子暗号理論の開発（玉川大学、NEC 筑波）

・量子絡み合いのコヒーレント状態への拡張と量子光通信の理論限界（玉川大学）

・量子絡み合いの定量化と劣化の回復に関する理論（NEC 筑波）

(c) 受信部での量子状態の検出技術（NEC 筑波、東大、NICT）

(i) 量子状態を認識する為の新たな光子検出技術の開発（NEC 筑波）

(ii)量子絡み合い状態の干渉や位相を観測する新たな検出技術の開発（東大）

(iii)量子暗号の安全性保証や光量子計算へ繋がる光子数識別器の開発（NICT）

本研究分野の性格から、上記の各項目は５年の研究目標としては非常に挑戦的であり、それぞれマイルストーンを設定し、実現性をチェックしながら研究遂行を行った。

【その後の新展開から生まれた目標、計画の変更・追加等】

上述の目標を遂行する中で、高性能の光子検出器の開発成功やコヒーレント状態の量子暗号への利用の展開などがあり、量子暗号の実用化促進、また将来の量子中継を含むシステム展開へ布石を打つ為、以下の量子暗号のシステム実証も新たに計画の中に組み入れる事とした。

(d) 量子暗号システムの実証実験（NEC 筑波、東大、玉川大学）

(i)高性能単一光子検出器を用いた量子暗号システム（NEC 筑波）

(ii)量子絡み合い光子対の片方の受信信号を伝令としたシステム（東大）

(iii)コヒーレント光通信による新量子暗号システム（玉川大）

また上述の研究項目(b)(ii)に関してはグループリーダのWang氏がNECプリンストンからマックスプランク（エアランゲン）へ移籍した事で、研究リソースを見直し、同時に他機関からの優れた報告が相次いだ事などから目標からは外し、マックスプランクとして(a)(ii)の量子絡み合い光子対光源の開発に全力を尽くす事とした。

研究実施の概要でも述べた様に、本研究分野の量子情報技術は中長期的な基礎・基盤技術であり、現時点では将来の展開を予想することは困難であることを考慮し、本研究チームでの目標・計画設定においては、候補となる技術が複数ある場合でも、一つに絞る事はせず、敢えて並行して開発する道を選択した。

最終年度の2005年7月1日に研究代表者である中村はNECから物質・材料研究機構へ移籍したが、引き続き研究代表者としてチーム全体を統括した。この移籍に伴い、NEC筑波のグループリーダは富田章久主任研究員に引き継ぎ、最終年度の研究を遂行した。

以上の研究目標の追加・変更などを含めてグループ毎に纏め直すと以下の様になる。

① 量子絡み合い状態の生成・評価・制御　(NEC筑波； 富田グループ)

　量子絡み合い状態にある光子対の発生技術、評価技術、これらを用いた制御技術、さらには基礎理論など、量子中継の最も基礎となる要素技術の高度化。さらには高性能光子検出器を用いた量子暗号システムの開発。

② 量子絡み合い光子対光源の研究開発　(マックスプランク； Wangグループ)

　フォトニック結晶ファイバを用いた高効率エンタングル光子対の生成。

③ 量子絡み合い光源と検出技術　(東大； 小林グループ)

　多体を含む量子絡み合い状態の生成と新たな検出技術、さらに量子絡み合いを用いた量子暗号システムの開発。

④ 光通信の極限の理論的探求とその理論の応用としての新量子暗号の開発

(玉川大； 広田グループ)

　コヒーレント状態を用いた量子絡み合い理論研究と新量子暗号システムの開発

⑤ 量子符号化技術と光子数検出技術の研究開発　(NICT; 佐々木グループ)

　シャノン限界を超える量子符号化の実証と光子数識別（検出）器の開発

本報告書では、上述の項目毎に研究成果等が記述される。これらは量子暗号を量子情報処理通信システムとして見た場合、送信部、通信路、受信部の各部分において必須となる下図の様な各要素技術が、各研究機関で分担・遂行され、これらの成果により、量子情報処理通信システム全体の技術的レベルアップが実現される。

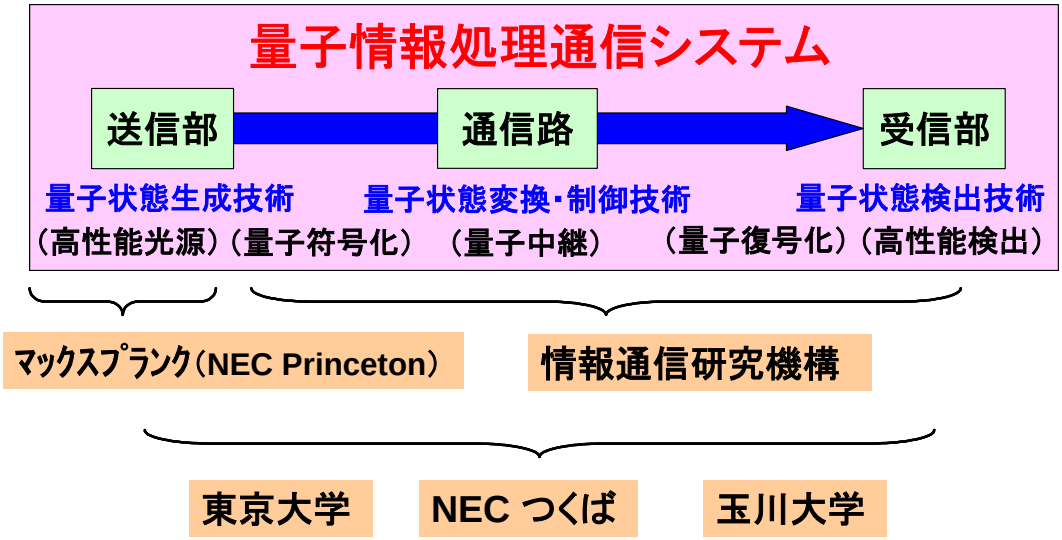
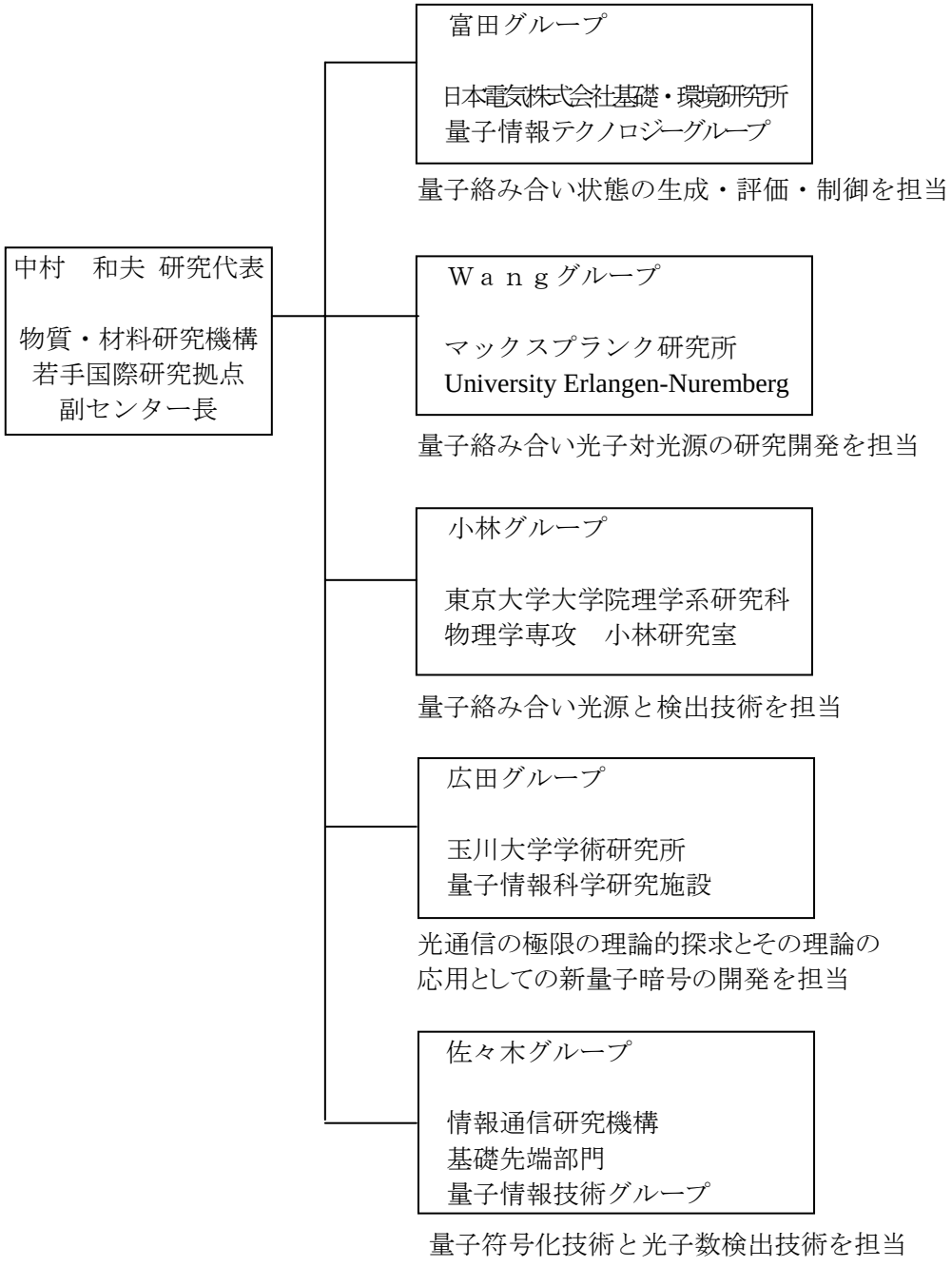


図1 量子情報処理通信システムの技術課題と本チームの研究体制

(2)実施体制

【研究実施の組織体制】



【各研究項目の概要と達成度】

① 量子絡み合い状態の生成・評価・制御　(NEC 筑波； 富田グループ)

量子絡み合い状態にある光子対の発生技術、評価技術、基礎理論について大きく進展し量子中継技術の最も基礎になる部分を確立した。量子中継デバイスについても、近接場光学顕微鏡による単一量子ドットの光学特性測定技術を開発した。また、

無中継量子暗号システムでも世界最長(150km)の伝送に成功し、実用化にも目途をつけるなど当初の目標を達成した。

② 量子絡み合い光子対光源の研究開発（マックスプランク； Wang グループ）

フォトニック結晶ファイバを用いて、低ノイズで最も高い photon flux を有する量子絡み合い光子対光源の開発に成功した。これは同種のフォトニック結晶ファイバを使った光源だけでなく、通常の非線形結晶のパラメトリック下方変換を使った光源（PPLN 型も含む）と比べても優れている。今後、量子絡み合い光子対光源として、注目を集めて行くものと期待され、設定された目標は達成された。

③ 量子絡み合い光源と検出技術（東大； 小林グループ）

縮退パラメトリック共振器を閾値以下で用いる事により、量子絡み合い状態にある光子対の生成、量子干渉の観測などに成功した。また多光子の絡み合い状態（W 状態が主）においても従来と比べて高効率な生成を実現した。また量子絡み合い光子対の片方を光子検出器により受信し、この信号を伝令とした量子暗号鍵配布システムを構築し、伝送距離と安全鍵生成率の向上が達成できる事を示した。

④ 光通信の極限の理論的探求とその理論の応用としての新量子暗号の開発
（玉川大； 広田グループ）

光通信の限界特性を理論的に解明した。またコヒーレント状態でも完全エンタングルメント状態が可能である、これを用いた量子テレポーテーション法、及びそのデコヒーレンス耐性などを明らかにした。また、米国で提案されたコヒーレント光を用いた新たな量子暗号法の提案に対して、強度変調方式を提案し、実証実験にも成功した。

⑤ 量子符号化技術と光子数検出技術の研究開発（NICT； 佐々木グループ）

現在の情報通信技術の根底をなすシャノン理論により符号化時の伝送容量限界が与えられているが、近年、この限界を量子力学の原理により超えられることが明らかにされてきた。本研究では量子情報源符号化と量子通信路符号化の本質的原理を抽出し、それを 2～3 の少数の量子ビットに適用する事で、シャノン限界を超える事を初めて実験的に実証した。また、量子情報通信の受信部で重要となる通信波長帯用の光子数識別（検出）器に関しても InGaAs PIN フォトダイオードを用いた積分型の検出器を開発し、数十個レベルのフォトン数の識別に成功している。低ノイズ性等の総合的な性能と汎用性という点から現在ベストな方式といえる。

3　研究成果

3．1　チーム全体の成果

研究概要・構想の章でも述べた様に、本チームは現在の量子暗号システムをより広範に実用化して行く上で、量子中継などの量子絡み合いを利用する技術が重要となる。これには前章の図に示した様に、量子暗号を量子情報通信システムとして見直した時、送信部における量子状態の生成技術、通信路における制御・変換技術、受信部における検出技術など各要素基盤技術の高度化が不可欠である。これにより、量子情報全体の技術のレベルアップも期待される。

本チームでは各要素基盤技術を各グループの保有するポテンシャルを使い、種々の手法で高度化を行った。また同時に、本プロジェクトの成果をベースに量子暗号システムの実証実験に関するテーマもその後の展開として追加した。いずれも詳細は3．2以降で報告される。

(1) 送信部での量子絡み合いの生成技術

①量子状態トモグラフィーによるフェムト秒短パルス励起で量子絡み合い光子対の高効率生成技術（従来のタイプII結晶より高効率)、②フォトニック結晶ファイバを用いた量子絡み合い光子対の生成技術（結晶を用いる方法よりも高photon flux)、さらに③3光子の量子絡み合いを生成する光子源技術の実現にも成功した。関連代表論文はそれぞれ、IF値2.9（引用件数11)、IF値1.7（引用10)、IF値2.9（引用3）である。いずれも最近の論文で、今後、引用数は増大すると期待される。

フォトニック結晶ファイバ光源は発生する絡み合い光子対の波長相互に違いが有り、片方を単一光子源とする量子暗号などに応用されて行くであろう。また、多光子絡み合い技術は前者の技術との組合せでさらなる高度化が可能であり、また種々の量子プロトコルへの応用も期待される。

(2) 通信路での量子状態の制御・変換技術

①量子状態を制御する量子操作（量子チャネル）の評価技術（2ビット操作のビームスプリッタで新たな知見)、②量子インターフェースやゲート操作へ向けた単一量子ドットの分光研究と低温・強磁場環境での近接場顕微鏡開発、③量子情報源符号化と量子通信路符号化技術（シャノン限界を超える世界初の実証実験）を実現しており、さらに④量子絡み合いのコヒーレント状態への拡張や量子絡み合いの定量化と劣化の回復に関する理論的成果(有名な未解決問題の一つの解決を含む)を得た。関連代表論文はそれぞれ、IF値7.2（引用件数0)、IF値3.1（引用未定)、IF値7.2（引用10)、IF値7.2（引用3）を有する。

これらの技術はいずれも量子状態の制御・変換に関する重要な基盤技術であり、今後のこの分野の発展に大きなステップとなる。これに伴ない引用件数も増大するものと考える。

(3) 受信部での量子状態の検出技術

①低ノイズ・高感度な光子検出器の開発（従来より１桁以上の高性能)、②真空に感度を有する新たな光子検出技術（従来の検出器が吸収過程を用いるのに対し、誘導放出過程を初めて用いる)、③量子暗号の安全性保証や光量子計算へ繋がる光子数識別器の開発（他と比べ総合性能と汎用性で優る)、④量子絡み合い状態の干渉や位相を観測する新たな検出技術の開発に成功した。関連代表論文はそれぞれ、IF 値 3.9（引用件数 17)、IF 値 7.2（引用 0)、IF 値 4.3（引用 2)、IF 値 2.9（引用 0）である。

これらの検出器は実用システムへ搭載したり、新たな量子情報研究用として用いられたりと各場面に応じて使い分けられて行くものである。今後、引用の少ない検出技術もその価値が認められて行くと期待され、また本プロジェクトで量子情報の広い範囲に渡る基盤技術が育成されたことが判る。

(4) 量子暗号システムの実証実験

その後の展開から加えられたテーマで、本研究での成果をベースに短距離ではあるが、従来のシステムと比べ、高性能でより実用化に近いシステムの実現を目指したものである。①高性能単一光子検出器を用いた量子暗号システム（世界最長 150km 伝送、実用フィールドでの２週間連続動作（16km))、②量子絡み合い光子対の片方の受信信号を伝令信号とした量子暗号システム、③コヒーレント光通信による新量子暗号システム（多値強度変調方式）の開発にそれぞれ成功した。関連代表論文はそれぞれ、IF 値 1.1（引用件数 4)、IF 値 2.9（引用 0)、IF 値 2.0（引用 2）である。

前者２つは光源が異なるが同じ単一光子による量子暗号である。特に１番目は単一光子を用いた量子暗号の実用性を大きく前進させるものとなっている。また３番目はコヒーレント光を用いた原理の異なる量子暗号であり、安全性の証明に関してはまだコンセンサスが得られていないが、用途によっては、従来の単一光子量子暗号と棲み分ける可能性も考えられる。

以上、示した様に、本プロジェクトでは量子情報の重要な要素となる基礎基盤技術の他、実用化に近いシステムまで含め、広範な量子情報技術をテーマにし、その全体の技術的レベルアップに大きく貢献した事を強調しておきたい。

３．２　量子絡み合い状態の生成・評価・制御（ＮＥＣつくば；富田グループ）

(1)研究成果の内容

量子絡み合い状態の生成・評価・制御

当グループでは単一光子を用いた量子暗号鍵配布を真に実用化するために必要なシステム技術の開発と更なる高度化のための要素技術の開発を行った。具体的には(ｉ)システムとして新たに開発した高感度光子受信器を用いて世界最長レベルの100km超の量子暗号伝送実験に成功し、また要素技術開発として(ⅱ)量子中継など将来の高度なシステムに不可欠な量子絡み合い(エンタングルメント)の生成と評価、(ⅲ)エンタングル光子対を利用した量子チャネルの評価、(ⅳ)これらの技術を応用した「論理的に可逆な」測定を狙った真空揺らぎに感度をもつ光子検出実験など量子情報光学の先端的な成果をあげた。(ｖ)また量子情報処理に必要な制御量子ゲートを目指した単一量子ドットの分光学研究も大きく進展した。特に低温で強磁場、さらに電界印加・電流検出が可能な近接場光学顕微鏡の開発は本プロジェクトの大きな成果であり今後の活用が期待できる。これらの量子情報技術の基盤となる(ⅵ)量子情報理論についても進展し、特に混合状態のエンタングルメントについて新たな知見を得た。以下各項目を具体的に述べる。

（ｉ） 量子暗号伝送実験

量子暗号鍵配布において最も重要なデバイスは光子検出器である。光子検出器は光子を確実に検出する(量子効率が高い）が、光子検出には一般に光通信用のアバランシェフォトダイオード（APD）を光子計数(ガイガー)モードで用いられる。ガイガーモードではAPDに印加する電圧をブレークダウン電圧より高くして大きな増倍率を得ている。光通信用APDは可視光用のAPDに比べダークカウント確率が高く、従来1ビットスロット当たりの量子効率が2-10%程度のときダークカウント確率は10^{-6}から10^{-3}程度であった。これに対して我々は２つのAPDの差動出力を用いることで光子検出の閾値を低減することができ、量子効率を犠牲にすることなくダークカウント確率を低減させることができた。量子効率10%においてダークカウント確率2×10^{-7}と従来のものより1桁以上性能を向上させることができた[1]。

性能が向上した光子検出器を用いることで量子暗号伝送の長距離化が期待できる。我々はまずプラグ＆プレイ方式を試み、100kmの伝送に成功した[2]。光は受信機から送信機に送られ、ファラディミラーで折り返されて再び受信機に戻る。光ファイバを伝送中に生じる偏光の乱れはファラディミラーで折り返すことにより自動的に補償され、システム全体の干渉性を安定に保つことが比較的容易である。伝送路として使用した光ファイバの伝送損失は約0.25dB/kmでこれは通常敷設されているものと同等である。ここでは送信機から受信機への復路の１パルス内の平均光子数が0.1となるよう受信機からの光量を光減衰器により調節している。また駆動パルスの繰り返し周波数は500kHzとした。100k

m伝送後の平均光子検出レートは6.9 counts/secで誤検出レート（約0.7 counts/sec）の10倍あり、誤り率は10%以下になることが期待される。実際得られた変調の明瞭度(あるいは干渉度)はAPD１、APD2でそれぞれ83%、80%であり、これに対応する誤り率はそれぞれ8%、10%が得られた。この際光源の狭帯域化によってレーザ光の自然放出光成分を低減し、同時に分散による光子パルス波形の劣化を抑えることが重要であった。誤検出は検出器のダークカウント（約

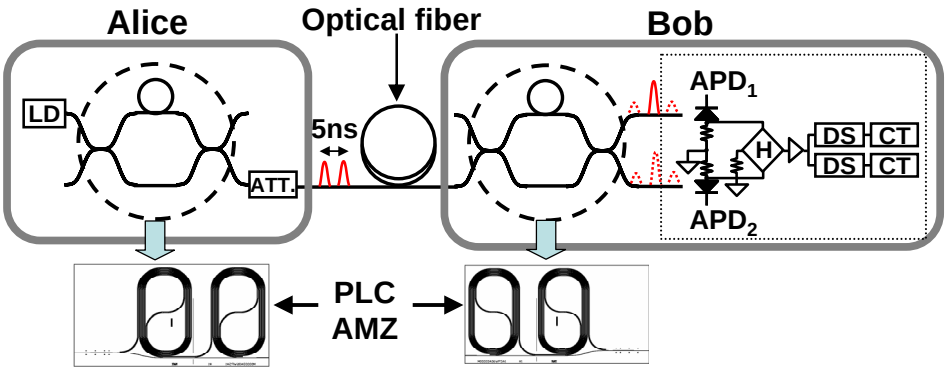


図1 平面光回路（PLC）を用いた量子暗号伝送系　レーザ光（LD）はPLCによる非対称Mach-Zehnder干渉計(AMZ)で2連パルスに変換される。ファイバ伝送後に再びAMZで合波されて干渉する。いずれかのアームに現れる光子を光子検出器（APD1,APD2）で検出する。

0.1 counts/sec）とファイバからの後方散乱光子数（約0.6counts/sec）からなる。検出器の高感度化により、従来伝送距離が光子検出器の雑音で制限されていたのに対し、光ファイバでの散乱で制限されるようになった。この散乱は伝送路と同じ長さのファイバを送信機内にバッファとして持ち、信号光と散乱光が同時に存在しないようにするバースト法により回避することが可能だが、その場合伝送レートはさらに1/3になる。検出器雑音のみを考慮した場合には140ｋｍまで伝送可能である。

しかし、プラグ＆プレイのような往復型のシステムは次の理由で長距離伝送には不向きである：①動作条件が装置間距離に依存、設置条件に応じた装置調整が必要　②通信路の接続ポイントからの光反射による動作不安定性　③インストール時のタイミング調節　④　トロイの木馬盗聴の可能性。

これに対して図1に示すような一方向型にはこのような問題がなく、長距離伝送に有望である。一方向型では送受信器におのおの非対称干渉計が必要でその光路差が等しくなければならない(往復型では1個の干渉計を往復で2回使うので光路差は自動的に一定に保たれる)。我々は（Planar Lightwave Circuit: PLC）技術を利用した単一方向型量子暗号システムの開発を行った。PLC技術を利用することにより干渉計を小型の基板上に構成できるため機械的に安定で温度制御も比較的小さなペルチェ素子で行うことができる。温度を±0.01℃

に安定化することにより送受信器間でアクティブな光路差制御を行わなくとも高い干渉の明瞭度が得られることを示した。シリカベースのPLCによる非対称Mach-Zehnder干渉計（AMZ）は片方のアームが5 ns分長くなっている。光学損失はカップラ部を除いて2 dB、偏光依存性は0.32 dBのものが得られている。カップラの一つは導波路損失を補償するため透過率が非対称に設計されている。量子暗号伝送系を実現するたには2個のAMZを光ファイバで結ぶ。

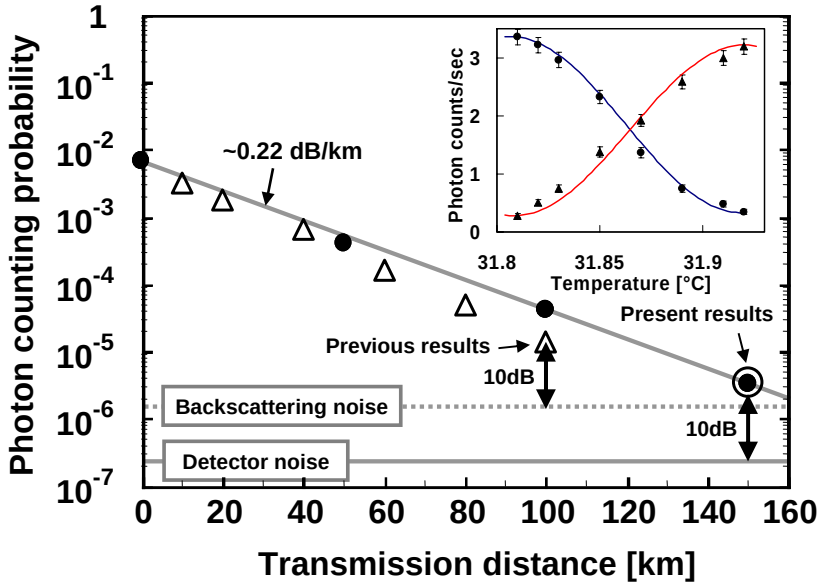


図2 単一光子伝送実験における光子検出率。　黒丸はPLCを用いた一方向伝送系での結果。三角は折り返し（プラグアンドプレイ）伝送系での結果。挿入図は送信側のPLC の温度を変えて2連パルス間の位相差を変化させたときの干渉フリンジ（150km伝送後）を示す。

一方向型の長距離伝送の可能性を実証するために光ファイバ長を150 kmとして伝送実験を行った[3]。Alice側のPLCには1550nmのDFBレーザ(パルス幅200ps)の出力を入力する。クロック周波数は1MHzとした。良好な干渉を得るためには２つのAMZの間の位相調節だけでなく、AMZの導波路の屈折率の偏光依存性を補償する必要がある。これらはBob側のAMZの温度を制御することで可能である。位相制御は２つのAMZの光路差の違いを$\Delta L=\lambda/n$（ただしシリカの屈折率$n\sim1.5$）以下にすればよい。ΔLは基板の熱膨張のためデバイスの温度に比例係数5μm/Kで線形に変化し、２つのアームの屈折率の偏光依存性は、偏光間の相対的な光路差を$L_B=\lambda/\Delta n$で定義されるビート長の整数倍にすることでバランスさせることができる。ただしΔnは偏光の固有モードに対する屈折率差である。$\Delta n\sim0.01$なので屈折率の偏光依存性の補償は位相制御よりも温度に鈍感である。このため両者を同時に満足させることができる。Alice側のAMZの光路差を変化させて光ファイバ伝送後の光子検出レートを測定し干渉パターンを得た。図2に示すように光子検出レートはファイバの損失から見積もった値とよく一致した。150km伝送後の干渉の明瞭度は挿入図に示すとおり82%ないし84%でこれは誤り

率9%と8%に相当し、安全な量子暗号鍵生成が可能な値である。量子暗号の伝送距離は世界的にも現在この150kmが最長である。

（ⅱ）エンタングルメントの生成と評価

混合状態も含んだ一般的なエンタングル状態をあらわすには4×4の密度行列を用いればよい。量子状態トモグラフィーで密度行列の16個の成分を実験から定めることができる。具体的には同じ状態にある多数の光子対に対して16種類の同時計測を行って結果を蓄積する。この同時計測は波長板と検光子の組み合わせで$\{|H\rangle, |V\rangle, |D\rangle, |L\rangle\}_1 \otimes \{|H\rangle, |V\rangle, |D\rangle, |L\rangle\}_2$の各々に射影測定することで得られる。ここで$|H\rangle$は水平偏光、$|V\rangle$は垂直偏光、$|D\rangle$は斜め45°直線偏光、$|L\rangle$は左回り円偏光の状態を表している。同時測定の結果から密度行列の成分を推定する。推定には例えば最尤推定を用いればよい。最適な推定法について

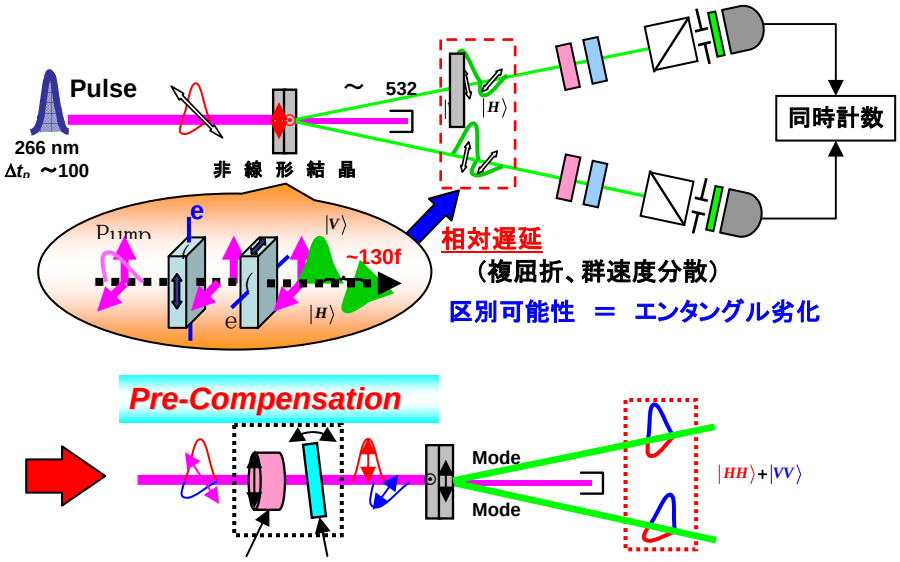


図3 パラメトリックダウンコンバージョンによるエンタングル光子対発生スキーム。非線形結晶の複屈折と群速度分散のため2つの結晶で発生する光子対に時間差が生まれ、エンタングルメントが低下する。そのため、時間差をあらかじめ補正する。

も理論的な検討を行った。密度行列がわかればそれからエンタングルメントの指標を計算することができる。実験では密度行列から直接計算できる量であるコンカレンスを求めている。

パルス光を用いると時間的な分離の可能性が生まれるため、エンタングルメントが失われやすくなる。注目しているのは光子の偏光であるが、結晶の分散や複屈折のために偏光についての情報と光の波数と周波数（または時間と空間的な位置）についての情報が絡み合うようになる。具体的には正常光と異常光の群速度が異なるためパルスの到達時刻により偏光の情報も得られてしまい、エンタングルメントが失われる。非線形光学結晶が長くなるとパルスの到達時刻の差も顕著になるためパルス光では薄い結晶を使う必要があり、エンタングルド光子対の生成効率が低く抑えられてしまう。以下では、このような区別の可能性を消すことによってフェムト秒ポンプしたにもかかわらず高いエンタ

ングルメントを実現した[4]。

実験は図3に示すように繰り返し周波数82MHzのモードロックTi:Sレーザの第3高調波(266nm)をポンプ光としている。ポンプ光のパルス幅は150fs程度、平均出力は約150mWである。2個の光子に独立な操作をすることが容易なノンコリニア配置での光子対発生を行った。非線形光学結晶にはタイプIの位相整合をするBBO結晶を用い、光学軸が直交した2枚の結晶を重ねてポンプ光を入射する。各々結晶から放出されるSPDC光(532nm)はポンプ光の偏光に直交した同じ方向に偏光する。ポンプ光の偏光を45°に傾けておくと第一の結晶はポンプ光の垂直偏光成分から水平に偏光した光子対を放出し、第二の結晶はポンプ光の水平偏光成分から垂直に偏光した光子対を放出する。結晶を薄く(0.13mm)することで空間的な重なりを大きくし、光子対がどちらの結晶から放出されたかを光の進行方向からは決められなくしている。SPDCが起きる確率は小さいため、両方の結晶から光子が放出される確率は無視できる。2個光子が観測されたときの光子の状態は$|H\rangle|H\rangle$と$|V\rangle|V\rangle$の重ね合わせ状態$r|H\rangle|H\rangle+\sqrt{1-r^2}\exp[i\phi]|V\rangle|V\rangle$になる。重ね合わせの振幅$r$と位相$\phi$はポンプ光の偏光状態で決まり、2つの偏光方向について効率が等しいとき、45°直線偏光のときは$r=2^{-1/2}$, $\phi=0$、135°直線偏光のときは$r=2^{-1/2}$, $\phi=\pi$となる。また、ポンプ光が垂直または水平偏光の場合には$r=0$または$r=1$となりエンタングルし

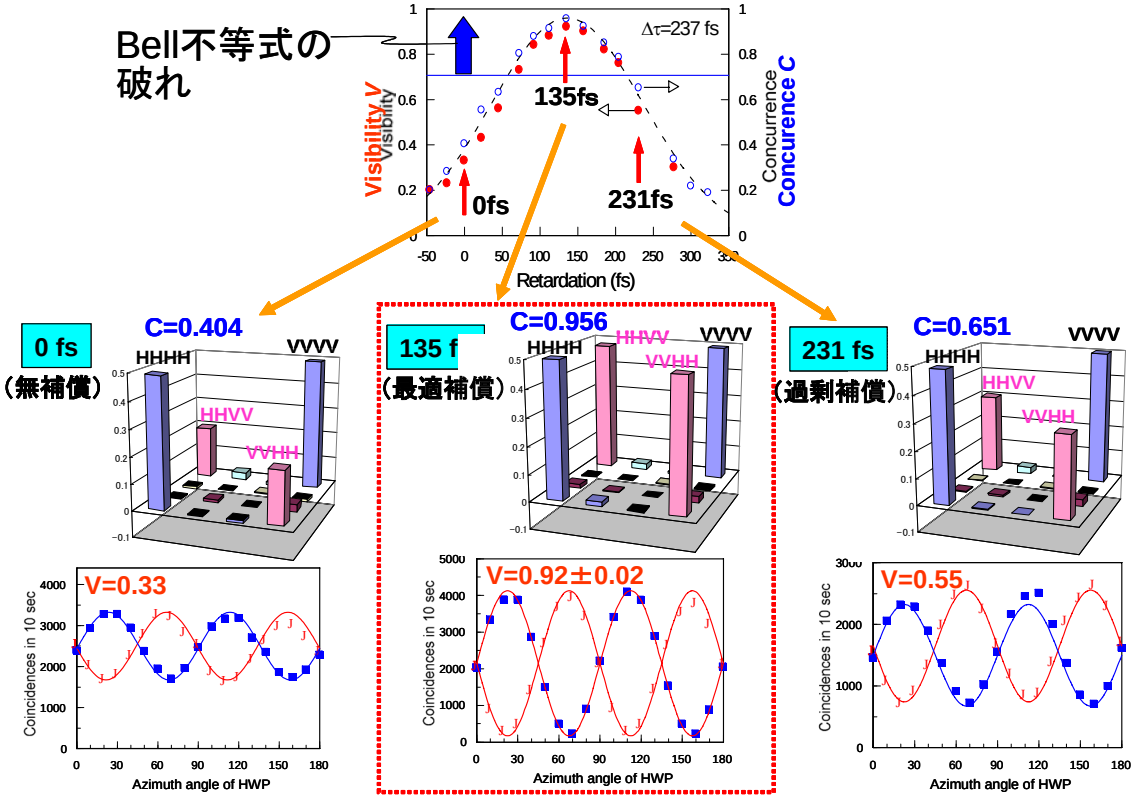


図4　pre-compensationによるエンタングルメントした光子対の発生。最適補償条件ではコンカレンスとして0.956を得た。

ていない光子対が得られる。最大にエンタングルした光子対を得るためにはポンプ光の偏光を正しく合わせることが必要になる。さらに高いエンタングルメントを得るためには前にも述べたように、2つの2光子放出過程を区別できないようにする必要がある。時間情報を消去するため、ポンプ光の水平偏光成分が垂直偏光成分よりも早く非線形光学結晶に到達するようにポンプ光を複屈折板（水晶板）とBereck型偏光補償器による可変波長板を通すことで補正を行う(pre-compensation)。水晶板の厚さを変えることで偏光成分同士の350fs程度以下の時間差を補正することができる。波長以下の小さな位相のずれは偏光補償器により調整した。

得られた光子対の状態を量子状態トモグラフィーによって解析する。16 通りの同時計測を行って密度行列を再構成した。完全にエンタングルメントが失われた状態では非対角成分が 0 になる。図４に示すように補正を行わない場合では *HHHH* 成分と *VVVV* 成分が大きく、非対角成分である *VVHH* 成分や *HHVV* 成分が小さい。コンカレンスを計算するとこの場合 0.404 となった。ポンプ光の垂直偏光成分を水平偏光成分に対してして遅らせていくとエンタングルメントが大きくなっていく。pre-compensation が 135fs のとき、コンカレンスは最大になり 0.956 が得られた。更に pre-compensation を大きくすると逆にエンタングルメントが低下する。

（ⅲ）量子チャネル評価

図5のように光子の偏光自由度を用いた１量子ビットの光学的量子チャネルの評価実験を行った。パラメトリックダウンコンバージョンにより発生する、水平（*H*）偏光した光子対の一方の光子を光子対発生のトリガとして、他方の光子を着目する１量子ビットのキャリアとして用いる。キャリアとなる光子は入力側の半波長板（HWP）および1/4波長板（QWP）により、評価に必要な４つの初期偏光状態 $\{|H\rangle,|V\rangle,|D\rangle,|L\rangle\}$ のひとつに準備される。量子チャネルを通過した光子偏光状態は、出力側のHWP、QWPおよび偏光ビームスプリッター（Pol）により観測基底状態 $\{|H\rangle,|V\rangle,|D\rangle,|L\rangle\}$ 成分に射影され、光子検出器およびカウンタにより計数され、１秒当たりの生起事象数（レート）R_H、R_V、R_D、R_Lが求められる。入力状態を順次変化させることにより、出力状態 $\mathsf{E}^A(|H\rangle\langle H|)$、$\mathsf{E}^A(|V\rangle\langle V|)$、$\mathsf{E}^A(|D\rangle\langle D|)$、$\mathsf{E}^A(|L\rangle\langle L|)$ を評価することができる。これより、実験結果から任意の入力状態に対する量子チャネルの出力状態を与える行列（χ–行列）を求めることができる。典型的な１量子ビットの量子チャンネルである、デコヒーレンスチャネルの評価実験を行った。不完全な通信チャネルを想定し、入力量子状態をできるだけ保存するようなデコヒーレンスチャネルを考えた。第一の例として、偏光空間上の１軸まわりのランダム回転のみを光子に与えるような量子チャネルを考える。このようなビットフリップチャネルは、光学軸方位４５°の偏光解消板により模擬することができる。光学軸が直交する２枚のくさび型水晶板により構成された偏光解消板は、その複屈折特性の空間的不均一性により、進相および遅相軸方向の光子偏光成分間に横方向（波数

ベクトルに垂直方向）空間自由度に依存した位相変調を与える。キャリア光子の横モードサイズが十分に大きく、観測に光子の横方向自由度に関する情報を利用しないとすれば、偏光解消板＋光子の横方向自由度は環境としての役割を果たし、環境による光子偏光状態の１軸まわりのランダム回転を模擬できる。偏光解消板は２枚の同一焦点距離のレンズ系の共焦点付近に配置し、偏光解消板とレンズ系の相対位置(z)の制御により偏光解消板上の光子の横モードサイズを可変できるようにした。これにより、光子の感じる複屈折特性の不均一性を可変し、実効的にデコヒーレンスの大きさを可変した。図5はビットフリップチャネルの理論と実験の結果を示し、良い一致が得られている。

我々はさらに線形光学素子と事後事象選択＝ポストセレクションに基づいた、確率的ではあるが決定論的な２量子ビット状態操作の評価を行った。SPDCにより生成した既知の偏光状態に準備された娘光子対を着目する２量子ビットのキャリアとし、娘光子対のアンサンブルに対し、偏光素子を用いて２つの娘光子に偏光変調を行い、各々４種の純粋状態$\{|H\rangle, |V\rangle, |D\rangle, |L\rangle\}$のいずれかの状態にある１６種類の初期偏光状態の光子のアンサンブルを順次準備した。準備されたアンサンブルに対して着目する２量子ビット状態操作を施し、その出力光子対アンサンブルの娘光子に対し各々４種の射影測定$\{|H\rangle, |V\rangle, |D\rangle, |L\rangle\}$を行うことによって、２量子ビットの量子状態トモグラフィーに基づく状態評価を行う。

量子状態フィルタであるHOM干渉系中のビームスプリッターの機能の評価を

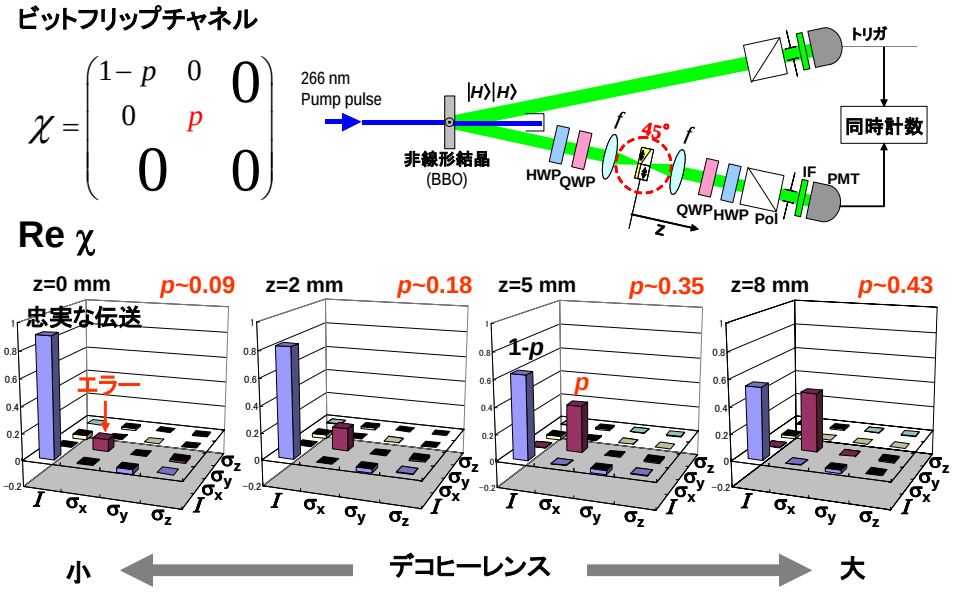


図5 ビットフリップチャネル評価実験の結果．左上は理論的χ–行列を、右上は実験系の配置を示している．下図は偏光解消板とレンズ系の相対位置（ｚ）を変えることによってデコヒーレンスの度合いを可変したときのχ–行列（実部のみ）の評価結果を示す．

行った。この評価から、この状態操作のクラウス演算子の特定、デコヒーレンスモデルの構築による分析や、その理想的機能に関する新知見など、多くの成果が得られた[5]。

（iv）真空揺らぎに感度を持つ光子検出

以上述べたパラメトリックダウンコンバージョン技術の応用として、我々は反正規順序による光子検出を初めて実現した[6],[7]。通常光子検出の過程は光子の生成消滅演算子が正規順序で並んだ過程（光子の吸収)表される。この場合、電磁場の真空揺らぎは測定結果には現れない。そのため、測定前の場の密度行列は測定後の密度行列と測定結果から再現することはできない。このような測定は論理的に不可逆な過程と呼ばれる。真空揺らぎは反正規順序による光子検出（量子カウンター）によって可能になる。我々は誘導パラメトリックダウンコンバージョンの出力のHanbury Brown-Twiss(HBT)型の 2 光子相関を測定した。HBT 型の強度相関には、光の生成消滅演算子の非可換性が顕在化するため、光の量子的な統計性を調べる上で強力な手段になるからである。通常の光子検出器での 2 光子の同時検出確率は、正規順序の物理量$\langle \hat{a}^+\hat{a}^+\hat{a}\hat{a}\rangle$に比例する。このとき、規格化した強度相関は、

$$g^{(2)} = \frac{\langle \hat{a}^+\hat{a}^+\hat{a}\hat{a}\rangle}{\langle \hat{a}^+\hat{a}\rangle\langle \hat{a}^+\hat{a}\rangle}$$

と定義される。一方、誘導放出を基にする量子カウンタでの 2 光子同時検出確率は、$\langle \hat{a}\hat{a}\hat{a}^+\hat{a}^+\rangle$という反正規順序の物理量に比例する。ここで、規格化した反正規順序での強度相関を、

$$g^{(2[A])} = \frac{\langle \hat{a}\hat{a}\hat{a}^+\hat{a}^+\rangle}{\langle \hat{a}\hat{a}^+\rangle\langle \hat{a}\hat{a}^+\rangle}$$

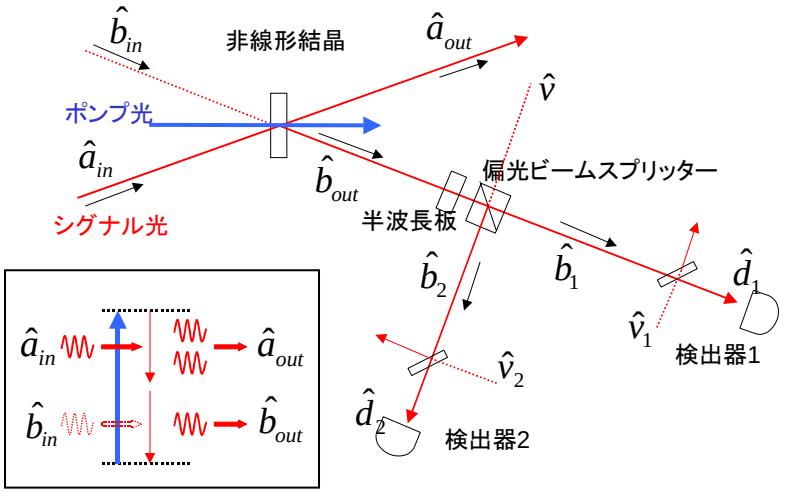


図6 誘導パラメトリック過程を利用して反正規順序強度相関を取るための実験の概念図。挿入図は、パラメトリック過程のエネルギーダイアグラム。

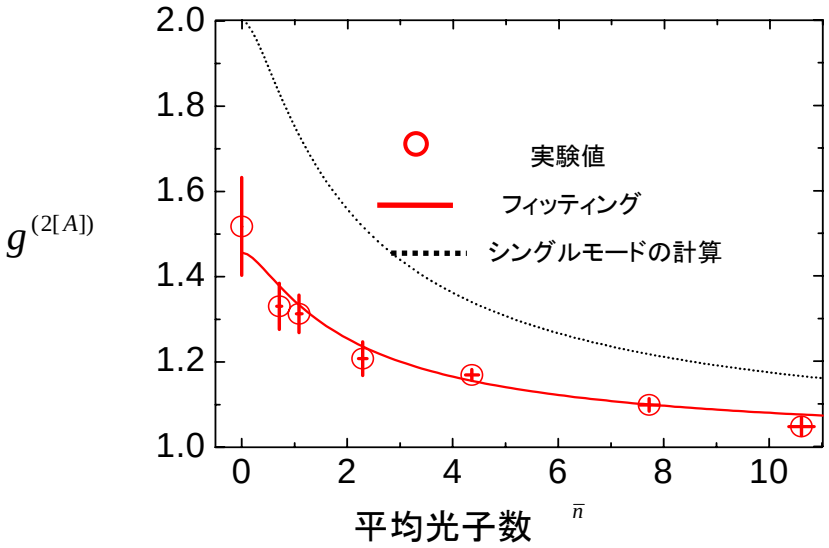


図7 反正規順序でのコヒーレント光の強度相関の測定結果。横軸は、平均光子数 $\bar{n} = \langle \hat{n} \rangle$。縦横のエラーバー（$3\sigma$）付きの丸は実験値で、点線は、図２(b)に示した理論値。実線は、時間的、空間的なモードミスマッチがあるとした計算から実験値にフィッティングした。

と定義する。通常の光子検出は真空揺らぎに感度がないため、式(6)の分母、分子ともに０となり、$g^{(2)}$ は $\bar{n} \to 0$ とした真空状態 $|0\rangle$ で定義できなくなる。ところが、反正規順序での強度相関 $g^{(2[A])}$ の場合、フォック(Fock)状態、コヒーレント状態、熱輻射状態、そして、真空スクィーズド状態など、どんな量子状態から外挿しても真空状態では２に収束する。これは量子カウンタが真空揺らぎを検出できることを反映している。

特に我々はコヒーレント状態の $g^{(2)}$ と $g^{(2[A])}$ の差に着目した。実験では、BBO 結晶をモードロックされたチタンサファイアレーザーの２倍波（波長:399nm）でポンプする。シグナルモード（$\hat{a}_{in}$）の光（波長 798nm）がパラメトリック過程で誘導放出される。このときアイドラーモード（$\hat{b}_{in}$）と結晶内でパラメトリックに結合する。結晶を出たアイドラー光を２つのモードに分割し、通常の光子検出器で検出する。検出器の量子効率などの実験上の不完全性は、補助的なモード $\hat{v}_1$、$\hat{v}_2$（真空）を導入することでモデル化できる。初期状態としては、シグナルモード $\hat{a}_{in}$ にのみ実励起した光子がいるので、検出器１と２での光子検出確率はそれぞれ、

$$\langle \hat{n}_{d1} \rangle \equiv \langle \hat{d}_1^+ \hat{d}_1 \rangle = \eta_1 |T|^2 \sinh^2(sL) \langle \hat{a}_{in} \hat{a}_{in}^+ \rangle$$
$$\langle \hat{n}_{d2} \rangle \equiv \langle \hat{d}_2^+ \hat{d}_2 \rangle = \eta_2 |R|^2 \sinh^2(sL) \langle \hat{a}_{in} \hat{a}_{in}^+ \rangle$$

のようになる。ここで、結晶の長さを L、２次の複素非線形感受率やポンプ光の強度等のパラメトリック相互作用にかかわるパラメーターは、絶対値部分を s、位相部分を ϑ とする。このようにして、シグナル光の反正規順序での光子検出、つまり量子カウンターが、誘導パラメトリック過程を利用することで実現できる。さらに、検出器１と２での光子の同時検出確率は、

$$\left\langle \hat{n}_{d1}\hat{n}_{d2}\right\rangle \equiv \left\langle \hat{d}_1^{+}\hat{d}_1\hat{d}_2^{+}\hat{d}_2\right\rangle = \eta_1\eta_2|T|^2|R|^2\sinh^4(sL)\left\langle \hat{a}_{in}\hat{a}_{in}\hat{a}_{in}^{+}\hat{a}_{in}^{+}\right\rangle$$

のように反正規順序の項のみが残る。したがって、$\left\langle \hat{n}_{d1}\hat{n}_{d2}\right\rangle / \left\langle \hat{n}_{d1}\right\rangle\left\langle \hat{n}_{d2}\right\rangle$を評価することで、反正規順序での強度相関測定を実現できる。強度相関の結果を図 7 に示す。平均光子数が 0 に近づくにつれて増大するが 2 には達していない。これはモード間に時間的、空間的なミスマッチがあったためだと考えられる。

（ｖ）単一量子ドットの分光学的研究

量子中継デバイスとして量子ゲート、量子インターフェースが考えられるが、これらのデバイスの基礎として、能動物質として有望な量子ドット励起子の分光学的研究を行った。原子に比べ量子ドットは励起子の振動子強度が大きい。また、固体であるため共振器の電場強度が最も高い場所に固定できるなどの利点がある。量子ドットの物性を明らかにして量子ゲート、量子インターフェースの設計に役立てるため特に波長 1 μm 以上における単一量子ドットの分光測定装置を開発した。共鳴波長が 1μm を超える InAs/GaAs 量子ドットは、その強い閉じ込め効果によって物理的にも興味深い性質が期待される。我々は 2 種類の装置を開発した。一つは共焦点顕微鏡を基本にした顕微分光装置で、もう一つは近接場光学顕微鏡である。

顕微分光装置の分解能は 4μm 程度で、これでは面密度約 50dots/μm^2 で分布している単一量子ドットを分解できない。そこで直径 500-1000nm の金属マスクを用いて視野を制限し、20 個程度の量子ドットスペクトルを得る。量子ドットサイズの不均一性のためそれぞれの遷移エネルギーがことなり、分光器を用いると単一量子ドットからの光を分解できる。量子ドットからの光は弱いため長時間積算が必要である。金属マスクの像を画像処理することで 顕微鏡の視野の動きを補正し長時間に渡って安定な測定ができる位置決め制御系を開発した。

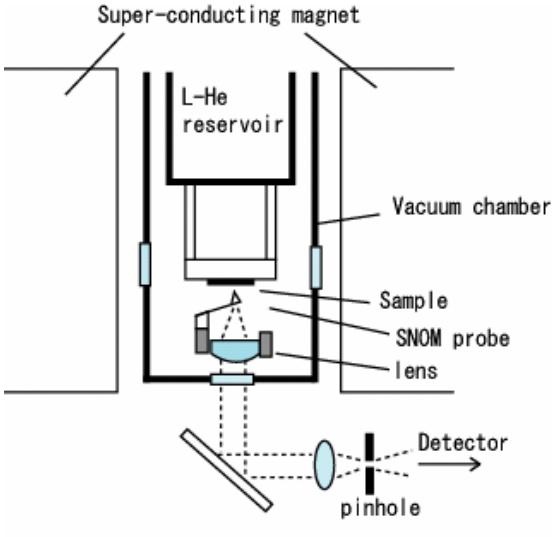


図8 低温・強磁場で動作する近接場光学顕微鏡の構成図

この装置を用いて 1.18 μm 付近に第 1 励起状態のある単一の量子ドットに由来する励起子・励起子分子の蛍光寿命を時間相関光子計数法によって測定した[8]。励

起子及び励起子分子の蛍光強度の時間依存性をレート方程式によって解析した。励起子分子を構成する２つの励起子が独立している場合、励起子(τ_X)と励起子分子(τ_B)の輻射寿命の比は$\tau_X/\tau_B=2$ であることが期待されるが、解析の結果、輻射寿命の比は２よりも小さくなり、InAs/GaAs 量子ドットにおける励起子分子は独立した２励起子と見做すことはできないことが示唆された。

近接場光学顕微鏡(SNOM)はプローブ先端の近接場が虚数の波数を持つため、空間分解能が光の波長に制限されないという特徴を持つ。例えば、半導体量子ドット一つ一つを光で励起し、発光を分離して捕らえることが可能となる。我々は、単なる高分解能顕微鏡ではなく、試料に対し局所的な外場制御を行う装置としてSNOMを位置づけている。このため、我々の装置は低温(10K)、強磁場(7T)環境下での試料の局所応答を観測できるように設計されている。装置は原子間力顕微鏡(AFM)を基本とし、金属コートして不透明にしたカンチレバーにあけた直径500-1000nmの穴から漏れ出す近接場を伝搬光に変換する。我々のシステムでは、近接場信号を自由空間中にコリメートされた平行光として取り出している。プローブとしてAFMカンチレバーを用いているので、SNOMとAFMの同時観測ができる[9]。

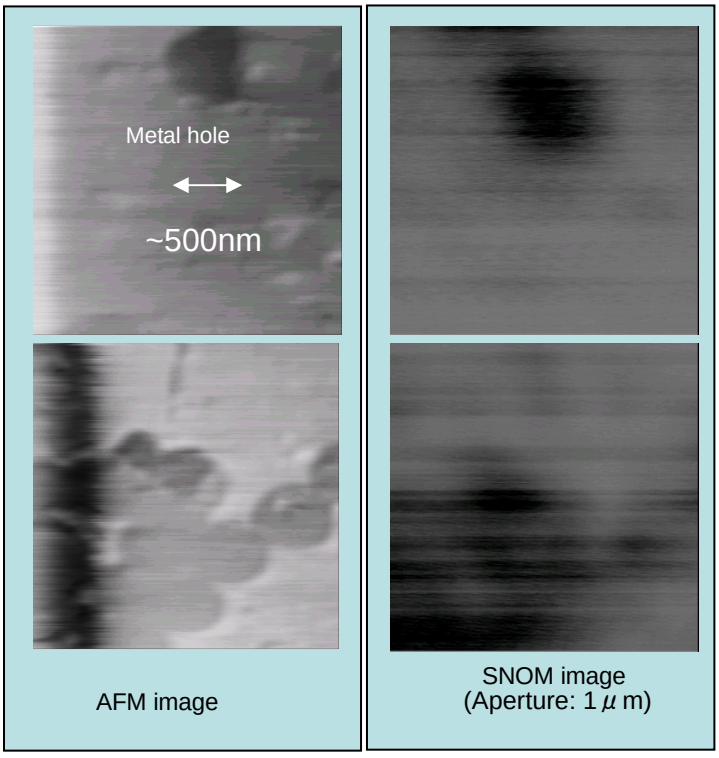


図9 近接場光学顕微鏡で得られた金属膜上の開口のAFM像とSNOM像。

我々のSNOMの概略図を図８に示す。サンプルとプローブは真空チャンバーの中に入れられている。我々のシステムではプローブを変えることでSTM測定も可

能になっているため、高真空中で電気的なトンネル測定も可能である。カンチレバーが金属コートされて導電性を持つため、局所的な電場印加や電流測定が可能である。サンプルに対して下側からプローブがアプローチすることで、近接場を測定している。近接場信号を集光するための対物レンズは、プローブと一体化されてチャンバーの中に入れられている。チャンバーの中にレンズを入れることで、プローブからの近接場信号を効率よく集光することができる。また、我々の走査システムでは、サンプルを効率よく冷却するために、プローブをスキャンしている。このとき、プローブとレンズが一体化されていれば、走査時にもプローブとレンズの相対位置がずれないので、確実な集光が可能になる。この最近接の対物レンズは、近接場信号がおおよそ平行光になる位置に固定されているが、低温中や磁場中などでは、位置ずれが生じ、近接場信号は収束光あるいは発散光となる。そのため、それを補正するためのフォーカシングユニットを別途チャンバーの外に用意しユニット内の凸レンズを動かすことにより、信号を確実に平行光にして自由空間に取り出す。集光した光を平行光にする無限共役方式を採用することで、超伝導マグネットの中心から、狭いボアを通して光学テーブルまで信号をロスなく長い距離運ぶことができる。また、途中にフィルタを挟んでも、アラインメントに影響がない。自由空間中に信号を取り出すシステムは伝送中偏光を安定に保持することができ、材料分散の影響がない。このため、偏光測定や短パルスの光源を利用した時間分解測定など、多様な測定が可能となる。

現在、低温・強磁場のそれぞれで図９に示すようにAFM像によく対応したSNOM像が得られている。サンプルは金属薄膜の微小開口を用いた。SNOM像はサンプルの裏側からレーザを入射して近接場を励起する、コレクションモードで得た。AFM像とSNOM像の位置のわずかなずれはプローブ開口の幾何学的な位置と、力を感じる位置の違いによるものである。

（vi）エンタングルメント理論

量子中継などのプロトコルではエンタングルメントの共有が必要だが、エンタングルメントは伝送中に劣化し、いくつかのエンタングル状態の混合となる。このような混合状態のエンタングルメントをどのように定量化するか、エンタングルメントを高める操作（蒸留）がどのような条件で可能になるかといった基本的な問題でさえ十分に解明されていなかった。我々はエンタングルメントに関する状態空間の幾何学を発展させ、エンタングルメントの指標として相対エントロピーを解析的に与えることに成功した[10],[11]。密度行列ρで表される状態の相対エントロピーは状態空間内でエンタングルしていない状態（$\sigma \in D$）からの最小距離を表すもので以下のように定義される。

$$E_R(\rho) = \min_{\sigma \in D} [Tr\rho \ln \rho - Tr\rho \ln \sigma]$$

相対エントロピーを求めるには最小距離となる点σが必要で我々はこれを解析的に求めることができた。また、この点を通る D の接平面を考えることによりエンタングルメントをしているかの判定をよりタイトにすることができる。従来エンタン

グルメントの判定にはベル不等式が用いられるが、エンタングルしているにもかかわらずベル不等式を満たす状態もありうる。相対エントロピーを用いる方法ではこのような状態でもエンタングルメントしていることが示される。

また、2 次元（量子ビット）空間の状態ではエンタングル状態は全て蒸留可能である。しかし、高次元空間の状態では蒸留不能なエンタングル状態（束縛エンタングル状態）が存在する。従来、エンタングルメントの判定条件(Majorization Criterion)と蒸留不能条件(Reduction Criterion)が知られていたがこれらの関係は未解決であった。我々は 2 体系においてエンタングル状態が蒸留可能であることを示した[12]。

⑵得られた研究成果の評価及び今後期待される効果

（ｉ） 量子暗号伝送実験

光ファイバを用いた長距離伝送実験ではジュネーブ大67km、三菱電機96km、東芝ケンブリッジ122kmなどが報告されている。ジュネーブ大と三菱はフィールドに敷設されたファイバを利用しているので正当な比較ではないが単一光子の伝送としては我々の150kmが最長である。さらにこの成果を利用して100kmを超えた量子暗号鍵配布実験、16.3kmの架空ファイバによる14日間連続の量子暗号鍵配布実験にも成功している。これらの成果により近距離(<100km)の量子暗号鍵配布システムの実用化に大きく近づいた。関連論文[1]は17件、[2]は11件、最も新しい[3]でも4件引用されている。

（ⅱ）エンタングルメントの生成と評価

フェムト秒パルスによるエンタングル光子対は量子中継の基本要素であるエンタングルメントスワッピングに必須であり、高いエンタングルメントが要求される。今回我々が開発した手法によりフェムト秒エンタングル光子対が従来のタイプII結晶を用いる方法よりも高い効率で得られるようになった。また、量子状態トモグラフィーによるエンタングル状態評価も我々の論文発表以来広く用いられるようになっている。関連論文[4]の引用は11件である。

（ⅲ） 量子チャネル評価

量子チャネルの評価は量子プロトコルの動作を評価するのに必要な技術である。我々の量子プロセストモグラフィーを用いた量子チャネル評価は世界的にも先駆的なものである。我々は評価ツールとしての量子プロセストモグラフィーが十分な実用性を持つことを示すと同時に、量子情報処理用デバイスやシステムにおける評価技術の重要性を示した。この研究の副産物としてビームスプリッターの2光子に対する作用が従来信じられていた１重項フィルタではなく３重項フィルタであることを明らかにした。関連論文[5]の引用件数は0だがこれは論文発行が2005年であるためだと思われる。

（ⅳ） 真空揺らぎに感度を持つ光子検出

このような研究はユニークであり、最初に発表された国際会議では高い評価を受け、この会議の論文撰集に掲載された。また、日本物理学会誌より依頼されて解説記事を執筆した。この研究は量子測定・量子揺らぎの本質に関わる問題であり今後

の発展が期待される。

（ｖ）単一量子ドットの分光学的研究

量子中継などを実現するためには光と相互作用する物質が不可欠である。単一量子ドットは有力な候補であるが、従来光通信波長での単一量子ドットの物性は十分に調べられていなかった。本プロジェクトにより光通信波長における量子デバイス研究への道が開かれたと考えている。多機能な量子デバイスの実現には、外場によって電子状態を局所的に制御する技術が重要となる。我々が開発した近接場顕微鏡を用いれば、磁場印加により、異なるスピン状態をゼーマン分裂させることができる。また、局所的プローブによる電子注入や電圧印加により局所的な荷電状態を作り、励起子エネルギー準位を動かしたりすることもできる。このような電子状態制御は、将来の量子情報処理技術に必要なものである。

（vi）エンタングルメント理論

本プロジェクトにより混合状態のエンタングルメントについての理解が深まった。これらの成果はエンタングルメントを用いたプロトコルの性能の上限を与えるもので将来エンタングルメント応用プロトコルの研究が進展するにつれ重要性が増すものと考える。また、論文[12]はこの分野での有名な未解決問題の一つを解いたもので専門家の間での評価は高い。関連論文の引用は[10]4件、[11]2件、[12]3件である。

[1] Tomita, A; Nakamura, K: “Balanced, gated-mode photon detector for quantum-bit discrimination at 1550 nm,”Optics Lett. **27**, pp. 1827-1829 (2002).

[2] Kosaka, H; Tomita, A; Nambu, Y; Kimura, T; Nakamura, K: “Single-photon interference experiment over 100km for quantum cryptography system using balanced gated-mode photon detector,”Electron. Lett. **39**, pp. 1199-1201 (2003).

[3] Kimura, T; Nambu, Y; Hatanaka, T; Tomita, A; Kosaka, H; Nakamura, K: “Single-photon interference over 150 km transmission using silica-based integrated-optic interferometers for quantum cryptography,”Jpn. J. Appl. Phys. **9A**, pp. L1217-1219 (2004).

[4] Nambu, Y; Usami, K; Tsuda, Y; Matsumoto, K; Nakamura, K: “Generation of polarization-entangled photon pairs in a cascade of two type-I crystals pumped by femtosecond pulses,”Phys. Rev. A **66**, 33816 (2002).

[5] Nambu, Y; Nakamura, K: “Experimental investigation of a nonideal two-qubit quantum-state filter by quantum process tomography,”Phys. Rev. Lett. **94**, 10404 (2005).

[6] Usami, K; Nambu, Y; Shi, BS; Tomita, A; Nakamura, K: “Observation of antinormally ordered Hanbury Brown-Twiss correlations,” Phys. Rev. Lett. **92,** 113601 (2004).

[7] Usami, K; Tomita, A; Nakamura, K: Int. J. Quantum Inform. **2** (2004) 101.

[8] Kono, S; Kirihara, A; Tomita, A; Nakamura, K; Fujikata, J; Ohashi, K; Saito, H; Nishi, K: “Excitonic molecule in a quantum dot: Photoluminescence lifetime of a single InAs/GaAs quantum dot,” Phys. Rev. B **72**, 155307 (2005).

[9] Kirihara, A; Kono, S; Tomita, A; Nakamura, K: “Development of scanning near-field optical microscope working under cryogenic temperature and strong magnetic field,” submitted to Optical Review.

[10] Ishizaka, S: “The reduction of the closest disentangled states,” J. Phys. A **35**, pp. 8075-8081 (2002).

[11] Ishizaka, S: “Analytical formula connecting entangled states and the closest disentangled state,” Phys. Rev. A **67**, 60301 (2003).

[12] Hiroshima, T: “Majorization criterion for distillability of a bipartite quantum state,” Phys. Rev. Lett. **91**, 57902 (2003).

３．３　量子絡み合い光子対光源の研究開発
（マックスプランク研究所；Wangグループ）

1. Background and Summary

Quantum information science based on the quantum entanglement between multiple parties is fundamentally changing the way we view information and our physical world. Research in these areas has made rapid progress in recent years, although many daunting tasks remain. In particular, the practical success of many quantum communication and cryptography applications will require a robust source of correlated photon pairs.

The main process used in generating photon-pairs is parametric down-conversion in $\chi^{(2)}$ materials. It has been recently demonstrated that parametric amplification in fibers [1,2] using four-wave mixing (4WM) in $\chi^{(3)}$ materials can be a source of correlated photons. Here, as shown in Fig.1a, two pump photons are absorbed to generate a pair of Stokes and anti-Stokes photons. Such a process is also a parametric process and owning to energy conservation, the pair of photons in the Stokes and the anti-Stokes sidebands are correlated. Furthermore, it has been suggested that parametric generation [3] can lead to generation of entangled photons with a proper choice of an anomalous dispersive fiber. And we demonstrated this experimentally [4,5]

Microstructure fiber (MF), with its central silica core surrounded by patterned air holes, can have very small effective mode diameters (~ 1 to 2 μm) allowing for high field intensities and a wide range of wavelengths (400 nm to 1500 nm) that can propagate as a single spatial mode. These effects greatly increase optical nonlinearities in the fiber, and ease photon collection. Four-wave mixing (FWM) in MF is starting to be considered as a correlated photon source [5-8] alternative to the well-accepted method of parametric down conversion (PDC) [9-12].

Using parametric generation via 4WM, we efficiently generate correlated Stokes and Anti-Stokes photons by tuning the laser wavelength slightly above the zero-dispersion point in order to compensate for the self-phase modulation. The negative group dispersion in the near infrared is provided by the use of a micro-structured fiber (see Fig.1b) with a micron-sized core and with the zero-GVD point just below 830 nm. The small core allows us to achieve high irradiances at low input power, for high efficiency generation of correlated sidebands.

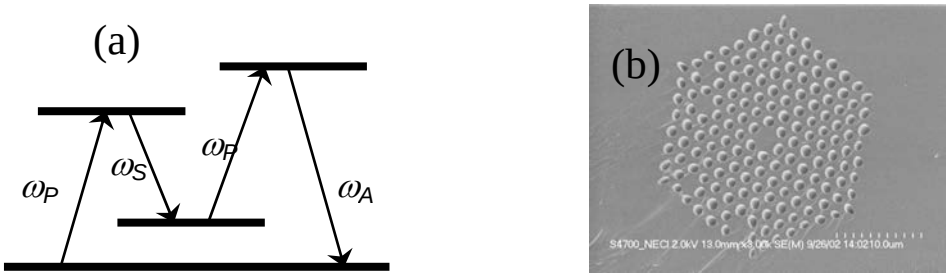


Fig. 1. (a) Schematic Energy diagram of the four-wave-mixing process used in the generation of correlated photons (b) SEM image of the cross-section of the "photonic crystal fiber" used in the experiments.

There are two key parameters in measuring the performance of a single photon source. These are the Coincidence-to-accidental ratio, i.e., the C/A contrast, and the photon generation rate (photon flux). Comparing to other previous experiments, we have achieved in this project a record in the photon flux, at a relatively high C/A contrast.

For per mW pump power and per nm collection spectral bandwidth, the present result (53.7 kHz/mW/nm) also exceeds coincidence rates by a PDC in bulk crystals (0.2 kHz/mW/nm) [13], and it is comparable to the rates by PDC in poled crystal waveguide sources (~ 50 kHz/mW/nm) [14-16]. In the opposite regime, where we maximize contrast at the expense of count rate, we achieved a contrast of 300:1 at 50 μW with a coincidence rate of 45 Hz.

2. Annual Progress and Technical Development

There are a few stages during the course of the project. During the first half, we concentrated on demonstration of the effect, and on solving all related technical issues. After the mid-term review, we concentrated on developing a high-performance, robust, all-fiber source, and the study of other novel effects, such as the fiber optical parametric amplifier (F-OPA), and the reverse four-wave-mixing process. During the first stage, one key technical problem was the high Raman scattering noise level. In order to solve this problem, we have made a large number of attempts, including cooling the fiber to liquid Nitrogen temperature, etc. We eventually solved the problem by carefully tuning the four-wave-mixing phase-matching, and go beyond the Raman scattering window. In addition, we improved the single photon collection efficiency using a double reflection grating spectrometer setup which we developed. These technical developments were unique in our group and enabled us to achieve results better than all competitors.

3. Research Achievements and Comparison with Competing Groups

We have performed and published four experimental works. These are (1) the observation of correlated photon generation, both in bright beam regime and at the single photon level, (2) the observation of optical parametric amplification in a micro-structured fiber, (3) the observation of the

reversed four-wave-mixing process and correlated photon generation with this method, and (4), the highly efficient generation of correlated single photon pairs.

All four results compare favorably in terms of time of publication and quality of results, with those achieved by a competing group funded by DARPA. In the following, we describe some of the results more in detail.

3.1 Observation of correlated photon pair generation

Fig. 2 shows the experimental setup. The generation of correlated beam via 4WM takes place in the 1-meter long micro-structured fiber where we send 3ps pulses from a Ti-Sapphire oscillator. A grating is used to separate the Stokes and Anti-Stokes beams. The beams are collimated, frequency filtered using adjustable slits, and finally reflected back to the grating, but vertically shifted in order to permit the separation of the beams. They are then combined with another pump beam and focused into a second microstructured fiber, which provides the parametric amplification. The new Stokes and Anti-Stokes beams are again separated using a grating.

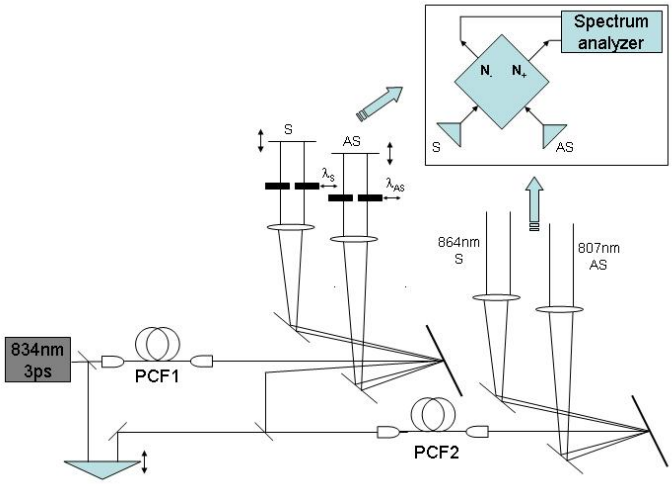


Fig. 2. Experimental setup for 4WM and parametric amplification in microstructured fibers.

We reported single photon correlation measurements,[4,5] where we achieved significant quantum correlation and generation of photon pairs. Here we achieved similar correlation measured classically, by monitoring the noise fluctuations of the beams. The noise spectra and their fluctuations are measured by mixing the signals from two amplified low-noise detectors into a phase-shifting mixer, which provides the following signals $N_{\pm}$:

$$N_{\pm} = < I_S^2 > + < I_A^2 > \pm 2 < I_S \cdot I_A >, \quad (1)$$

where I_S and I_A represent the Stokes and Anti-Stokes detector signals, respectively.

When we detect the beams generated via 4WM in the first fiber by monitoring the noise fluctuations on the left side of Fig. 2, we observe strong classical correlation between the two beams. Fig. 3a shows the quadratic dependence of the noise in the two beams with the optical input power in each detector.

Because of the strong correlation between the beams, the circles showing N_- given by Eq. (1) indicate a much reduced signal.

In Fig. 3b we show the measured noise as function the wavelength mismatch between the beams. The perfect matching situation is when the wavelengths of the detected beams conserve momentum in the 4WM mixing process when the pump photons have 834 nm. The maximum correlation is 60%, which means more than half of the photons in the beams are correlated.

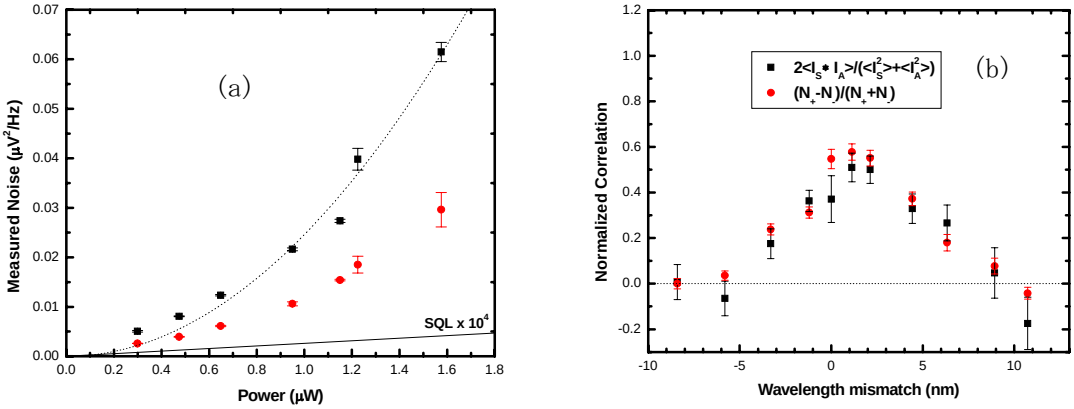


Fig.3 a: Measured noise $<I_S^2>+<I_A^2>$ (squares) and N_- (circles) at 20 MHz show quadratic behavior as functions of the optical power in the balanced Stokes and anti-Stokes detectors. The solid line shows the measured standard quantum limit (SQL), for reference. b: Normalized correlation of the noise of I_A and I_S as function of the mismatch between the probed beams. The squares are calculated using Eq. (1) with the measured I_A ,I_S, and N_-, while the circles show direct measurement of N_+ and N_-.

3.2 Observation of parametric amplification in a micro-structured fiber

We selected a narrow spectral portion of one of the beams generated via 4WM in the first fiber, and used it as a seed for the parametric amplification process in the second fiber. In Fig. 4a we show the spectra of the Stokes beam being amplified up to 40 dB in a 2 m micro-structured fiber by increasing the 834 nm optical pumping. The inset in Fig. 4a shows the spectrum of the amplified Stokes beam at 864 nm.

The measured gain for the parametric amplification increases monotonically with peak pump power, as shown in Fig. 4(b). The nonlinear coefficient γ and the group velocity dispersion parameter D used in the least-square fitting procedure are γ=71/W/km and D=2.2ps/nm/km, respectively. It is noticed from the fitting that there exists a critical peak pump power P_{cr}, only above which parametric amplification starts. For this specific 1.7m long microstructure fiber used in our experiment, P_{cr} is approximately 15W. It is expected that the critical peak pump power drops when increasing the length of the fiber, because the gain depends on the product of PL.

The relative noise correlation is determined by $\Gamma = \frac{< I_+^2 > - < I_-^2 >}{< I_+^2 > + < I_-^2 >} = \frac{< 2 I_I I_S >}{< I_I^2 > + < I_S^2 >}$. For equal detection efficiency, if the detected signal and idler pulses are fully correlated, Γ approaches unity. Without seeding of the signal pulse, the correlation between the signal and idler pulses is shown in Fig. 5(a), with a maximum correlation at about 80% at relatively low power. This is consistent with the earlier photon counting measurements [4,5]. With seeding of the signal pulse present, we measure a higher correlation between the amplified signal and idler pulses, with Γ approaches unity as shown in Fig. 5(b).

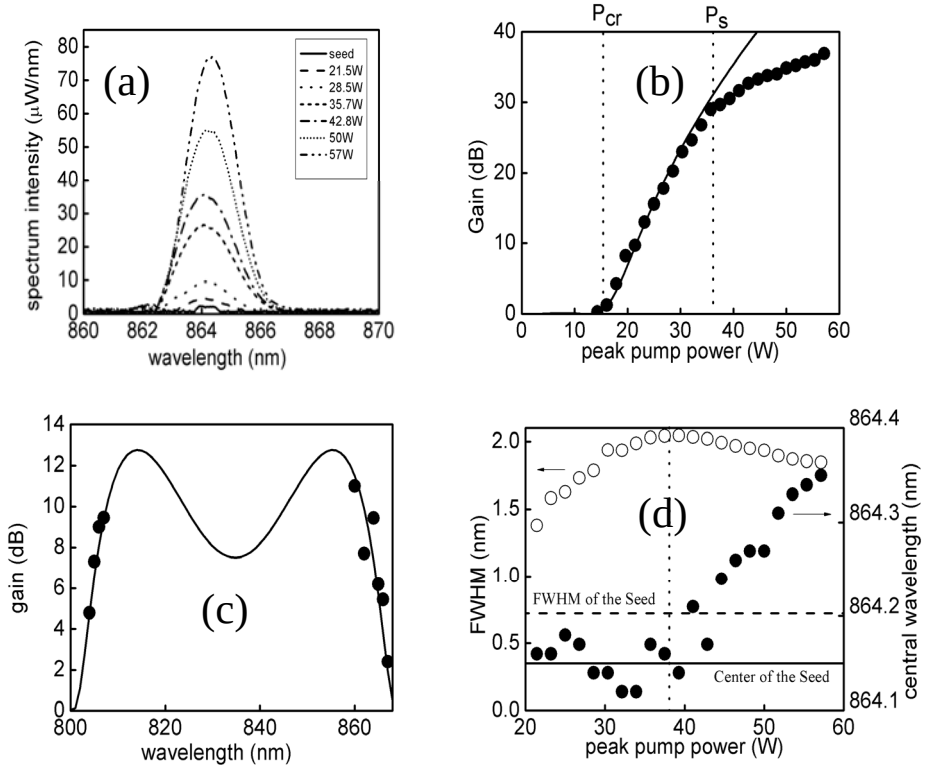


Fig. 4. (a) Measured spectral of the amplified signal pulse at different peak pump power. Incident signal pulse: central wavelength 864.16nm, average power 0.75μW, FWHM bandwidth 0.7nm. Incident pump laser pulse: central wavelength 834.7nm, FWHM bandwidth 0.3nm. (b) Measured gain of the amplified signal pulse versus peak pump power, filled dots: experimental data; smooth line: fitting results with Eq.(1). Conditions are the same as in (a). (c) Measured parametric gain spectrum. The filled dots are the experimental measurements. The smooth line is calculated using Eq.(1) and the fitting parameters in Fig. 2(b). (d) Measurement of spectral shift and broadening as functions of the peak pump power. The filled dots and open dots are the central wavelengths and the FWHM bandwidths of the amplified signal pulses, respectively, obtained by fitting the measured spectra with Gaussian functions.

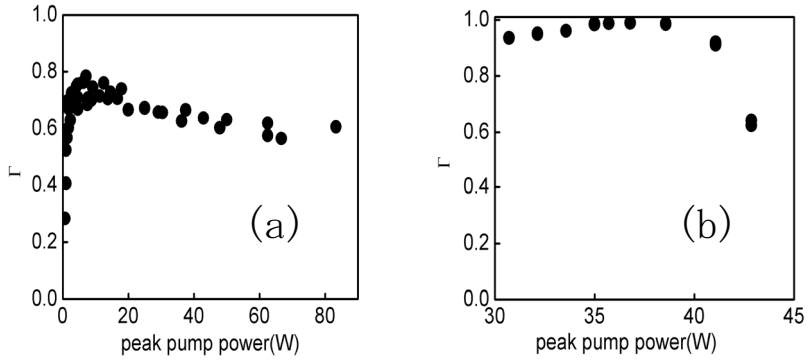


Fig. 5. Intensity cross correlation measurement, (a) without the seeding of the signal pulse; (b) with the seeding of the signal pulse, the seeding pulse is the same as used in Fig. 2(b).

In conclusion, we have built a fiber-based near-IR photon-pair source based on four-wave mixing in a micro-structured fiber. We have significantly improved the correlation between the Stokes and Anti-Stokes beams by using parametric amplification in a second fiber, using as seeds the beams generated in the first fiber. This system proves to be a very efficient fiber-based optical parametric amplifier pumped by a Ti:Sapphire oscillator. The signal and idler beams are strongly correlated, and spectrally narrow. The conversion efficiency is on the order a few percent, allowing the generation of several mW of average power; while the noise measurements indicate that the correlated photons exceed by 2 orders of magnitude the uncorrelated ones, with a big C/A contrast.

3.3 Observation of the reversed four-wave-mixing process and correlated photon generation

As we have shown, the spontaneous four-wave-mixing process is sufficient to generate correlated Stokes and anti-Stokes photons[6]. In these cases, two photons from the pump field (ω) are simultaneously absorbed in a nonlinear $\chi^{(3)}$ medium to create a pair of signal (ω_s) and idler (ω_I) photons at different wavelengths, under the condition $\omega_s + \omega_I = 2\omega$. Of course, another possibility exists. Here, a pair of signal and idler photons can be annihilated to create two “pump” photons of the same color, $2\omega = \omega_s + \omega_I$. This is the reversed process of the degenerate FWM process. These two new photons are necessarily generated simultaneously and hence are correlated, owing to energy conservation. The experimental setup is schematically shown in Fig. 6.

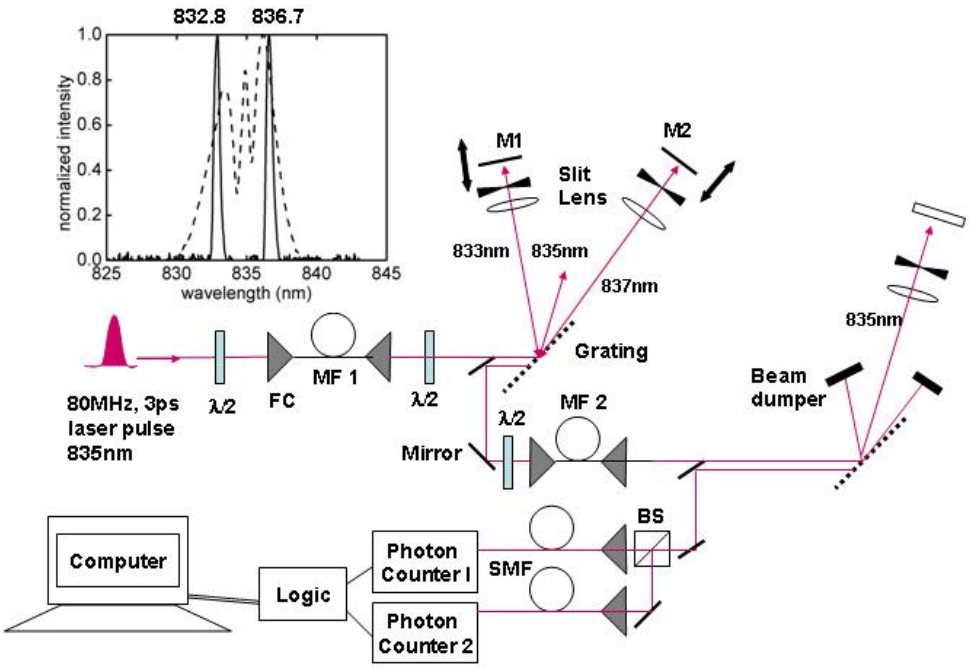


Fig.6. Schematic experimental setup. FC: fiber coupler, BS: beam splitter, SMF: single mode fiber, λ/2: half wave plate. M1 and M2 are mirrors. The inset shows the normalized spectra. The dashed line is for the pulse exiting from MF1. The solid line is for the selected signal (836.7nm) and idler (832.8nm) pulses.

A linearly polarized laser pulse of 3ps at 835nm drives the FWM process in a first 1m long microstructure fiber MF1. The output of MF1 is collimated onto a high power diffraction grating (2,200 lines/mm). Using two narrow slits, a pair of parallel polarized pulses at conjugate frequencies (λ_{signal}=837nm and λ_{idler}=833nm) are selected and they are overlapped in the second 1.5m long fiber MF2. MF1 and MF2 have zero dispersion wavelengths at 835nm. The spectra of the FWM output from MF1 and the selected conjugate pulses are respectively normalized and plotted in the inset of Fig. 6.

Photons at the middle frequency (λ=834.8nm) in the output light pulse from MF2 are selected and directed to a 50/50 non-polarizing beam splitter, with an overall collection efficiency of approximately β=0.7. The output photons from the beam splitter are coupled into two single mode fibers and they are detected by photon counters with overall efficiencies of η_1=0.06 and η_2=0.09, respectively. Photoelectric pulses from the two photon counters are analyzed by gated logic units for coincidence measurements. In the experiment, the photon counting rate at each photon counter is kept at such a level that, on average, less than 0.05 photon per pulse is emitted at the wavelength of 834.8nm from the nonlinear optical process in MF2.

The experimentally measured coincidence counting rate (the filled dots) as a function of peak pump power P is plot in Fig. 7(a). The theoretical values (the solid line) contain both that calculated using a simple theory and the calculated accidental coincidence counting rate. As can be seen in Fig. 7(a), the experimental data qualitatively agree with the theoretical calculations, but are generally smaller.

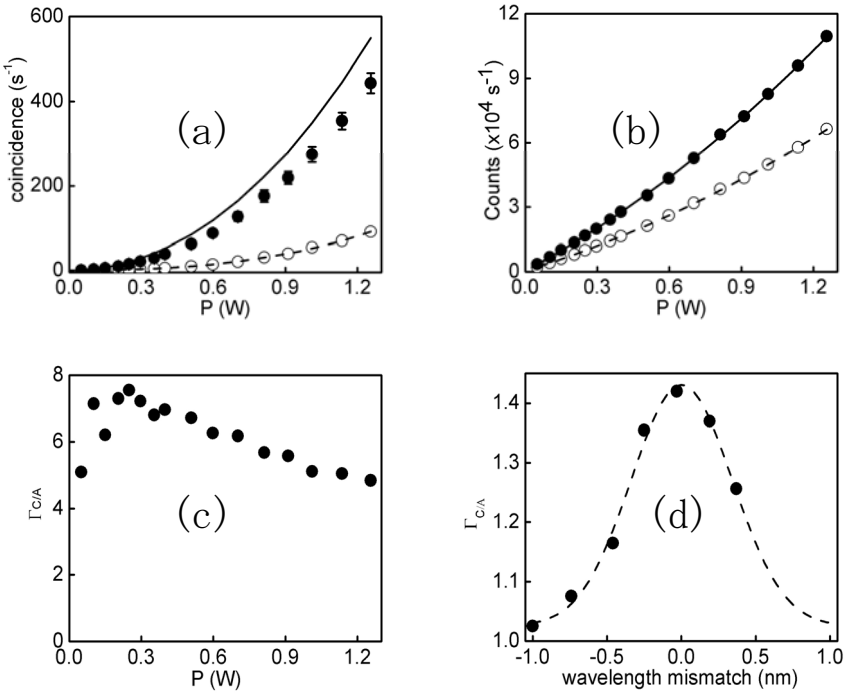


Fig. 7. (a) Coincidence rates versus peak pump power (P). The filled and open dots are experimentally measured coincidence and accidental rates, respectively. The solid and dashed lines are calculated coincidence and accidental rates, respectively. (b) Measured photon counting rates (filled and dots) versus peak pump power (P) at two photon counters, fitted with a parabolic function $N=N_d+a_1P+a_2P^2$ (solid and dashed lines), respectively. (c) Measured $\Gamma_{C/A}$ versus peak pump power (P). (d) Measured $\Gamma_{C/A}$ versus wavelength mismatch. The signal pulse is fixed at the wavelength of 836.7nm with P_1=0.5W; the idler pulse is tuned at around the wavelength 832.8nm (corresponding to 0 in wavelength mismatch). P_2 is kept at 0.06W. Filled dots: experimental data, dashed line: Gaussian fitting. Each experimental point in (a)-(d) is taken as a 10-minute average.

3.4 Highly efficient generation of correlated single photon pairs

For high-speed and high-fidelity quantum communication and cryptography applications, two basic conditions are required for the correlated photon source - a high coincidence rate and a high C/A contrast. Here, we report significant advances in each of these parameters using a fiber-based correlated photon source and a degenerate FWM scheme. With signal and idler photons separated in wavelength by 100 nm, we achieve a coincidence rate of 37.6 kHz with a C/A contrast of 10:1 with a collection bandwidth $\Delta\lambda =$ 0.7 nm in free space operation. This is the highest measured rate per bandwidth in a fiber-based photon source to date.

As shown in Fig. 8, we couple linearly polarized laser pulses from a Ti:Sapphire oscillator into a 1.8 m MF, with polarization along one of the principal axes of the MF. The laser wavelength is 735.7 nm (with $\Delta\lambda =$ 0.1 nm), which is the zero dispersion wavelength of the MF. The broadband output from the MF is directed to a high efficiency grating (1,800 lines/mm). A two-pass grating geometry is used to spectrally spread, select, and then re-image the beam to achieve efficient single mode collection. The selected signal and idler wavelengths are λ_s = 688.5 nm and λ_i = 789.8 nm, each with

$\Delta\lambda =$ 0.7 nm set by an adjustable slit. Interference filters ($\Delta\lambda =$ 10 nm) at the collection lenses suppress scattered pump and stray light. The signal and idler photons are coupled into single mode fibers and detected by photon counters and a coincidence circuit, with overall detection efficiencies experimentally determined to be $\eta_s = 0.097$ for signal photons and $\eta_i = 0.076$ for idler photons. In the experiment, photon generation rates in the signal and the idler bandwidths are kept below 0.1 photons per pulse.

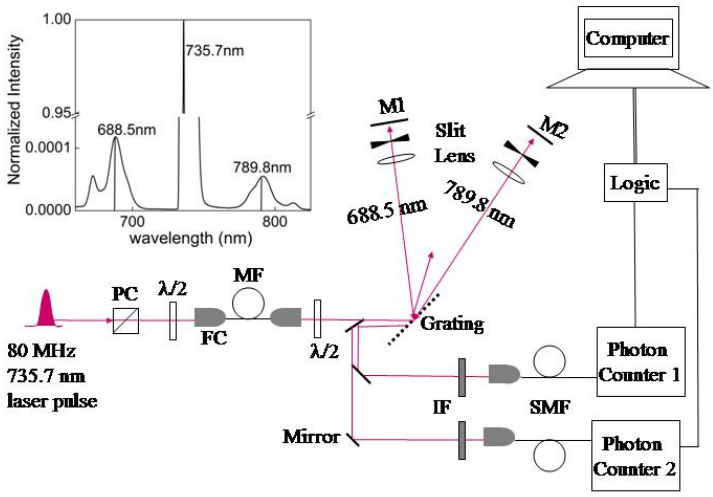


Fig.8. Schematic experimental setup. PC: polarizer, FC: fiber coupler, BS: beam splitter, SMF: single mode fiber, λ/2: half wave plate, IF: interference filters. M1 and M2 are mirrors. MF: microstructure fiber. The inset is a normalized spectrum of the output from the MF at an average pump power of 12 mW.

Fig. 9(b) shows the signal and idler count rates as a function of *P*, both exhibiting strong quadratic dependence with pump power. Because Raman scattering is the main noise source competing with the two-photon process in fiber,[17] and it is biased toward longer wavelengths,[16] the idler rate exceeds the signal rate even though $\eta_s > \eta_i$. A maximum coincidence rate of 37.6 kHz with a C/A contrast of 10:1 with $\Delta\lambda$ =0.7 nm at P =1 mW is shown in Fig. 9(c). This exceeds the recent record rate of 6.8 kHz with $\Delta\lambda$ =5 nm to 10 nm at P= 100 mW. This is the highest coincidence rate demonstrated to date with a fiber-based correlated photon source.

We attribute this high coincidence and high contrast to several advantages of our scheme. First, it is known that the gains of FWM and spontaneous Raman scattering are not uniform with wavelength, so it is possible to optimize the FWM relative to the Raman signals. In our experiment, this corresponds to placing the signal and idler wavelengths in the first-order FWM gain spectral regions shown in the inset of Fig.8. This wavelength arrangement enables us to achieve a high photon pair production rate with a relatively low noise level in the MF. This optimization method relies on the spectral selectivity of the phase-matching feature of FWM, the Raman gain profile, and dispersion property of the silica fiber. So, we expect to achieve a similar advantage in any silica-based high

nonlinearity MF with similar Raman response and dispersion property. A second advantage comes from higher nonlinearity due to both a higher nonlinear

coefficient (γ = 110/km/W) and a higher intensity resulting from the small effective mode diameter (1.2 μm) of the MF used in the experiment. Lastly, we retain single-mode collection with the two-pass grating arrangement, which could be replaced by an all-fiber wavelength demultiplexer for high efficiency and multichannel operation. These three advantages together make possible our MF-based photon source's high correlated pair detection rate and high C/A contrast relative to other previous experiments.

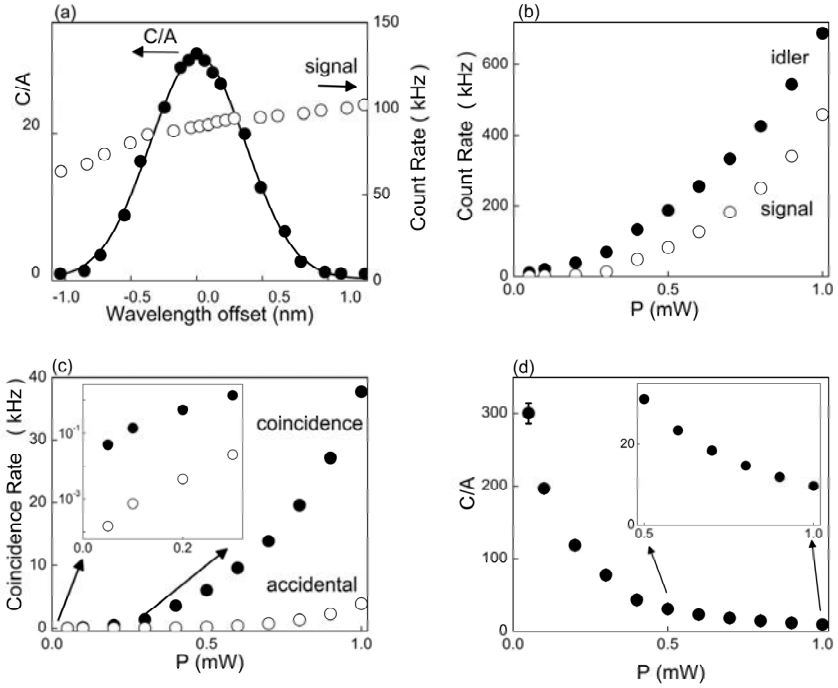


Fig. 9(a) Spectral scan of C/A (filled dots) and signal photon count rate (open dots) as the signal channel is tuned around the central phase-matching wavelength λ_s= 688.5 nm (corresponding to zero wavelength offset) with λ_{pump} = 735.7 nm and λ_i = 789.8 nm, with P = 0.5 mW. C/A is fitted to a Gaussian function (line). (b) Signal (opened dots) and idler photon count rates (filled dots). (c) Detected coincident rate (filled dots) and accidental coincidence rate (open dots). (d) Contrast between the measured coincidence and accidentals. For (a) to (d), each data point is averaged over 30 s for $P \geq 0.4$ mW and 600 s for $P < 0.4$ mW.

For per mW pump power and per nm collection spectral bandwidth, the present result (53.7 kHz/mW/nm) also exceeds coincidence rates by a PDC in bulk crystals (0.2 kHz/mW/nm) [13]. and it is comparable to the rates by PDC in poled crystal waveguide sources (~ 50 kHz/mW/nm) [14-16]. In the opposite regime, where we maximize contrast at the expense of count rate, we achieved a contrast of 300:1 at 50 μW with a coincidence rate of 45 Hz.

We have further examined the photon generation process. For a classical source, there is a Zou-Wang-Mandel inequality $V \leq 0$. V is a Cauchy-Schwarz type quantity [17]. We showed that the fiber photon source is highly nonclassical such that the above inequality is violated by the ratio of

V/σ ranging from 360 σ to 1100 σ.

4. Self-evaluation of the Results and Future Development

In conclusion, we have experimentally demonstrated the efficient generation of correlated photons in a micro-structured fiber. In a simple system, we have obtained a high twin photon coincidence rate of 53.7 kHz/mW/nm with a contrast of 10:1. This is the highest detection rate of correlated photon pairs in a single mode fiber-based photon source scheme. The classical limit is violated by up to 1100 σ. We also show that a coincidence/accidental contrast, as high as, 300:1 can be achieved, albeit at lower count rates. These high contrasts may be particularly useful in some fundamental tests of quantum mechanics. Our experiment suggests a practical polarization-entangled correlated photon source can be made with MF and that is being pursued.

Of the most relevant publications, there are the following few which I base the self-evaluations on. Paper-1 received 10 citations in a 1.746 journal. Paper-2 received 1 citation in a 1.5 journal. Paper 5 received 5 citations in a 0.164 journal. And papers 7 and 9 were published in an IF 3.9 journal very recently (June and December, 2005) and have received only 1 citation. Paper-8 was published in November, 2005 in a 2.2 journal.

In general, the citations are relatively low. However, there are three main reasons. One, the field is relatively new and there are rather few groups working in this. Second, our results are published rather late, such as papers 7-9. Citations will grow in time. As an example, paper-5 received 5 citations, and this is way ahead of the average citation number of papers published in that journal (IF~0.16).

Our study showed that the approach of generating correlated single photon-pairs in a single mode optical fiber is a very promising approach. The results of the research represent the development of a new tool in experimental quantum optics, as well as a new approach to quantum cryptography. Often, providing a new research tool can bring major changes to the field. Much of today's quantum information research is based on "parametric down-conversion." The original technical paper of 1969 by Burnham and Weinberg [9] is of very high importance for the development of the field. Of course, it will take some time for the method to mature and become widely accepted. Judging from the present status of the method, since our initial theoretical work [3] published in 2001, it has rapidly developed into a promising new field in quantum optical sciences.

List of Publications:

1. L. J. Wang, C. K. Hong, and S. R. Friberg,"Generation of Correlated Photons via Four-Wave-Mixing in Anomalously Dispersive Optical Fibers," *J. Opt. B* **3**, 246 (2001).
2. L. J. Wang, "Causal Filters and Kramers-Kronig Relations," *Opt. Commun.* **213**, 27 (2002).
3. 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*, **20,** 560 (2003).
4. J. Fan, A. Dogariu, and L. J. Wang,"Amplified Total Internal Reflection," *Optics Express*, **11,** 299 (2003).
5. A. Dogariu, J. Fan, and L. J. Wang "Correlated Photon Generation for Quantum Cryptography," *NEC R&D Journal* **44**, 983 (2003).
6. A. Dogariu, M. Hsu, and L. J. Wang,"Reducing Far-Field Diffraction by Structured Apertures," *Opt. Commun.* **220**, 223 (2003).
7. J. Fan, A. Dogariu, and L. J. Wang, "Generation of Correlated Photon Pairs in a Micro-structured Fiber," *Opt. Lett.* **30,** 1530 (2005).
8. J. Fan, A. Dogariu, and L. J. Wang,"Parametric Amplification in a Microstructure Fiber," *Appl. Phys. B, Lasers and Optics*, **81,** 801(2005).
9. J. Fan, A. Migdall, and L. J. Wang,"Efficient Generation of Correlated Photon Pairs in a Microstructure Fiber," *Opt. Lett.* **30,** 3368(2005).

Conference Publications:

1. J. Fan, A. Migdall, and L. J. Wang, 2005 CLEO/IQEC, Conference on Lasers & Electro-Optics Postdeadline Papers “Efficient generation of correlated photon pairs in a microstructure fiber”
2. J. Fan, A. Migdall, and L. J. Wang, 2005 CLEO/IQEC, Conference on Lasers & Electro-Optics Technical Digest “Generation of Correlated Photons with Conjugate Pumps in a Microstructure Fiber”
3. J. Fan, A. Migdall, and L. J. Wang, 2005 Proceedings of SPIE: Quantum Communications and Quantum Imaging III “A microstructure fiber two photon source with conjugate laser pumps”
4. A. Dogariu, J. Fan, L.J. Wang, G. Leuchs,2004 CLEO/IQEC, Conference on Lasers & Electro-Optics Technical Digest, “Classical and Quantum Correlation of Four-wave Mixing in Micro-Structured Fiber.”
5. A. Dogariu, J. Fan, L.J. Wang, J.A. West, 2003 CLEO/IQEC, Conference on Lasers & Electro-Optics Technical Digest, “Photon-pairs Generation in Micro-structured Fiber.”

３．４　量子絡み合い光源と検出技術（東大；小林グループ）

(1)研究成果の内容

(i) モードロック2光子状態の生成

光パラメトリック共振器によって生成された多モード2光子対は、櫛状の強度相関関数を示す。我々のグループは初めてその構造を観測した。

(i-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光子状態を発生させられることが知られている。本実験では波長 860nm チタンサファイアレーザーの二倍波で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。以下の条件 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より小さいの 3 つが満たされた場合、2 光子状態の相関関数に周期的構造が観測できる。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。(図 1)　この実験結果は、理論計算と極めて良い一致を示した。我々の開発した OPO を使って初めて得られた 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。

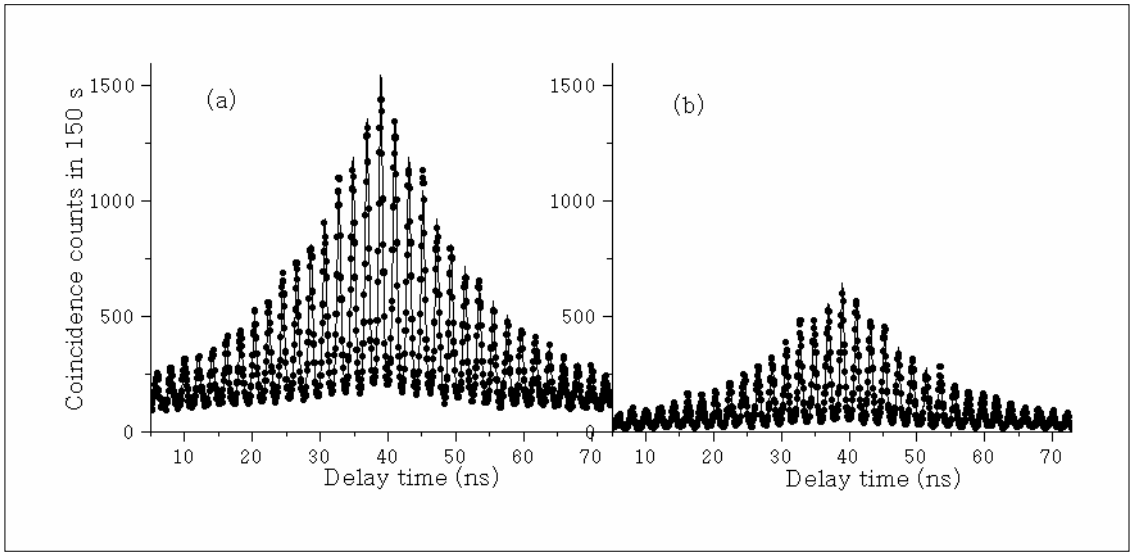


図 1

(i-2) 非古典的干渉の観測

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下の図 2 である。

(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れが観測できたとわかる。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。

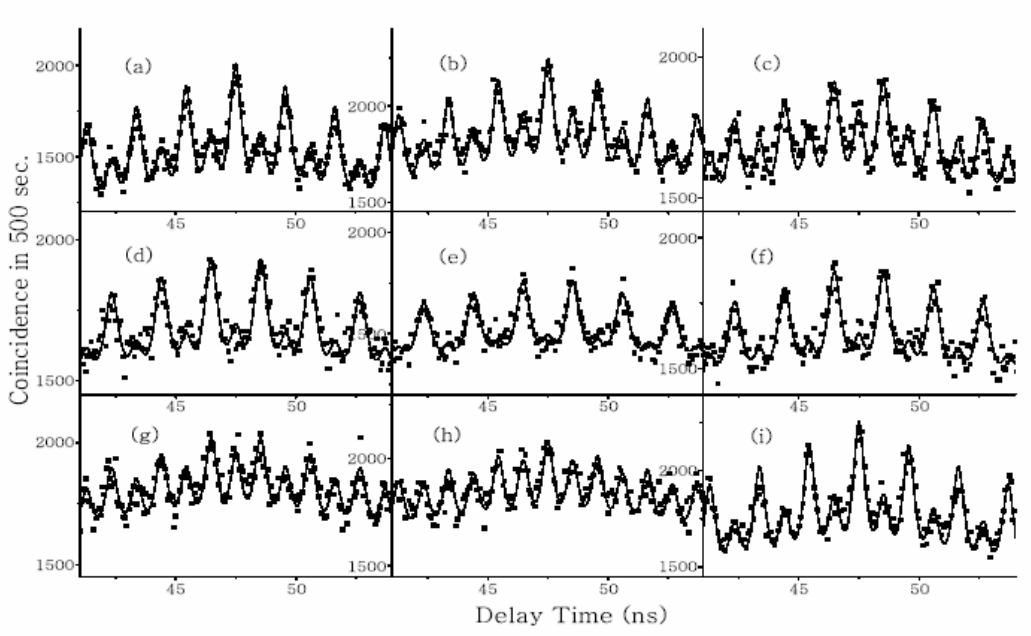


図2

(ii) 量子光学における線型光学素子ネットワークの応用

(ii-1) 3光子を用いたハイゼンベルグ限界での位相測定

位相測定は精密測定において基本的な役割を果たしており、基礎研究ならびに実用的な側面においても広く行われている。我々は 3 光子ハイゼンベルグ限界での精密位相測定の新しい方法を提案した。提案した方法は、光路長に差のあるマッハツェンダー干渉計(MZI)のみで構成されるため、実験的な実現が容易である。

図3に図示された精密位相測定の概念図を考える。2個のビームスプリッタ（BS,反射率2/3）が不可欠な構成要素である。入力状態$|\Psi_a\rangle=|2\rangle_a$は，BS1- 2/3の入力ポート$a$ から入射し、1光子状態 $|\Psi_b\rangle=|1\rangle_b$はもう一つのポート$b$ から入射する。

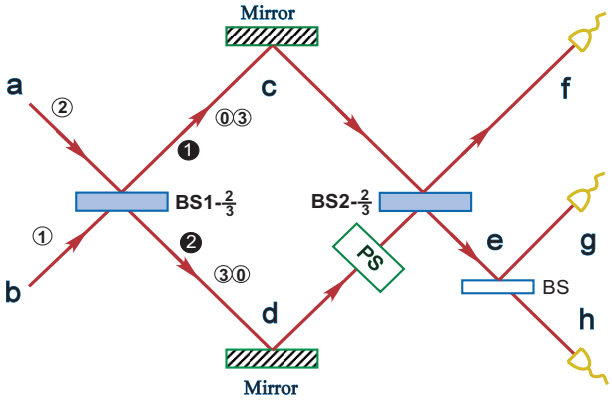


図3 3光子ハイゼンベルグ限界精密位相測定の実験概念図

モードｅの２光子とモードｆの１光子との相関関数は次のように計算できる。

$$\Gamma_3 = \langle\psi_a,\psi_b|\hat{f}^{+}\hat{e}^{+}\hat{e}^{+}\hat{e}\,\hat{e}\,\hat{f}|\psi_a,\psi_b\rangle$$
$$= C(1-cos3\phi)$$

C は検出効率とモードeの2光子確率およびモードfの1光子確率に比例する定数である。このMZIにおける量子干渉の振動周期は古典の場合よりも3倍短く明瞭度は100%である。よってこの方法における精密位相測定はN=3のハイゼンベルグ限界に達している。

(ii-2) 量子ハイ- ローパスフィルターによるサブポアソン状態の生成

現在に至るまで全てのスクイーズド状態実現方法は非線型物理過程に基づいてきた。我々は線型光学素子からなる量子ハイパスフィルター（HPF）とローパスフィルター(LPF)を導入した。これらを用いてスクイーズド状態を発生させられる事を示した。

図 4 は量子フィルターの光学系を示している。類似の系は光子数状態の量子非破壊測定を行う系で用いられている。任意の入力状態に関して系の解析を行いどのように量子フィルターとして作用するか示した。図４のビームスプリッタ A, B, C は位相非対称であると仮定する。 鎖線側での反射は符号を変化させる。ビームスプリッタ C は非線型π位相シフトを行う重要な部分を構成する。

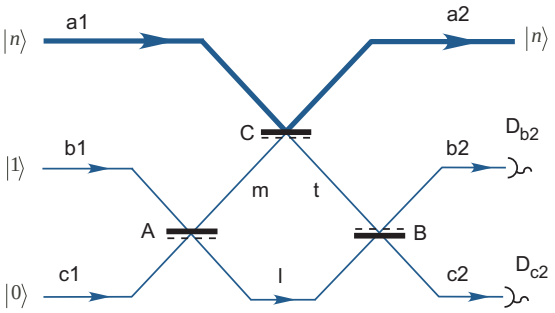


図4 量子フィルター概念図。ビームスプリッタA,B,Cは位相非対称。鎖線側での反射は符号反転をもたらす。

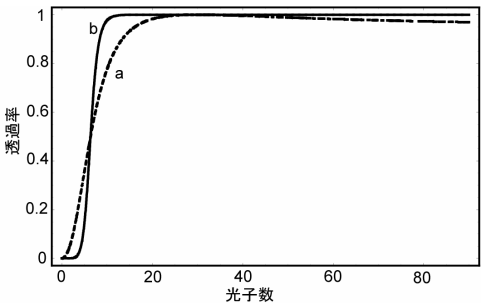


図5 量子HPFの応答

ここで検出器D_{b2}、D_{c2}がそれぞれ1光子を検出し他の検出器は光子を検出しない場合を考える。ポートa_1の入力状態は光子数状態を用いて展開すると$|\psi\rangle=\sum_{n=0}^{\infty}C_n|n\rangle$となる。

トリガー信号によって状態を取り出す条件つき状態生成を用いる。我々の場合ではトリガー信号は検出器D_{b2}、D_{c2}のどちらかが1光子を検出しもう片方は光子を検出しないという状況に対応する。トリガー信号によって、量子フィルターがHPFとして働くかLPFとなるかが決定される。例えば検出器D_{c2}が1光子を検出しD_{b2}が検出しなかった場合、図5のaがフィルターの規格化された出力確率の光子数依存性を示す。このaは古典的HPFの典型的な応答を表しているのがわかる。このようにして量子HPFが量子領域で実現できる。量子フィルターの出力特性は2次、3次の量子フィルターによって改善できる。2次のフィルターを作る最も単純な方法は、2つフィルターをつなげる事である。図5のbは3次の量子HPFの応答を示した物である。bの傾きは1次HPFよりも急であることがわかる。このようにしてサブポアソン状態が量子LPF, HPFからなるバンドパスフィルターによって、コヒーレント状態から生成される事がわかる。

(iii) マイケルソン干渉計を用いた2光子量子干渉実験

フォトンを用いた量子干渉実験は、ノンコリニアーなフォトンペアに対して行うものが大半である。フォトンペアの同種粒子性によって、空間的に分離させるのに扱いにくいことが1つの理由として挙げられる。本研究では互いに平行な偏光、もしくは互いに直交した偏光のコリニアーフォトンペアに対してマイケルソン干渉計を用いて量子干渉させ、干渉計の光路差ゼロ付近からフォトンの可干渉距離以上のところまでに対して、量子干渉の振る舞いを初めて観測し理論的に説明した。任意の偏光コリニアーフォトンペアを用いても両者の振る舞いは全く同じであることが確認された。

この実験結果によって特に干渉計の光路差が波長四分の一の整数倍に保たれて

いるとき、ＨＢＳの２つの入力ポートにそれぞれ入射する状態のみを排他的に選択することが可能であることが示された。すなわち状態ベクトルを干渉計のアームの違いによるモードで分けたとき、$|1,1\rangle$の状態に対してポストセレクションできることが示される。また、初めて互いに直交した偏光のコリニアーフォトンペアに対してもHong-Ou-Mandel干渉（ＨＯＭ干渉）に似た現象が現れることを示した。

光路差のバランスされたマイケルソン干渉計に入力するフォトンペアを、水平偏光のフォトンペア、水平と垂直偏光のフォトンペアの２通りに対して実験を行った。それぞれType-I、Type-II位相整合させた非線型結晶を用いる。図6、図7はそれぞれType-I、Type-II用いたときの実験系の概念図である。

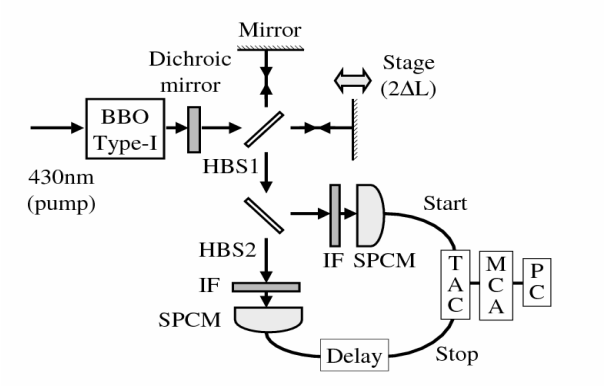


図6 Type-Iのとき

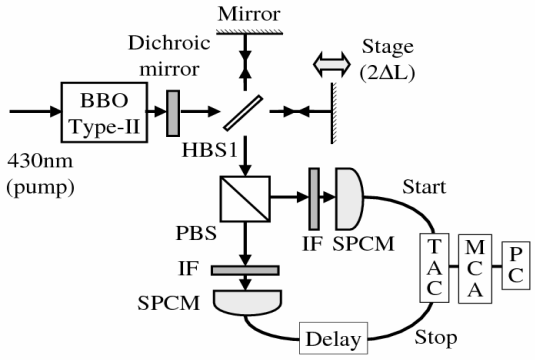


図7 Type-IIのとき

パラメトリック下方変換によるフォトンペアの生成効率は、結晶の有効非線型整数の違いから、Type-Iに比べてType-IIは一桁低い。検出効率を上げるため、Type-IIからのフォトンペアをシングルフォトンカウンティングモジュール（ＳＰＣＭ）に入射するとき、マルチモードファイバ（ＭＭＦ）を用いてカップリングさせた。Type-Iからのフォトンペアをカップリングするときは、シングルモードファイバを用いた。ＭＭＦを用いたことによる偶発手的なカウント数を減らすため、偏光ビームスプリッタ（ＰＢＳ）から出力されたフォトンペアを同時計数測定する。

図8、図9はそれぞれ、Type-I、Type-IIからのフォトンペアをマイケルソン干渉計に入射し、干渉計の出力ポートで同時計数カウントを測定したものである。横軸は、干渉計の光路差・L、縦軸は同時計数カウントである。Type-Iの場合、光路差・L=0～40・m付近は振動周期約860nm可視度約98±1%、光路差・L=100～140・m付近は振動周期約430nm可視度約46±3%であった。Type-IIの場合、光路差・L=0～30・m付近は可視度約97±1%、光路差・L=120～140・m付近は可視度約41±4%であった。ここで、フォトンの中心波長は約860nmである。

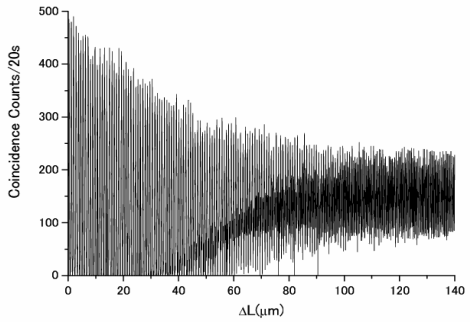


図8 Type-Iのとき

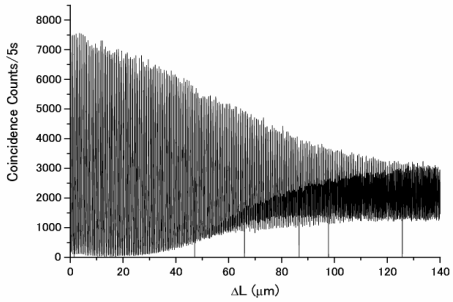


図9 Type-IIのとき

フォトンペアは干渉計に用いたＨＢＳ１において共に反射、共に透過、それぞれ透過と反射の３つの組み合わせがある。光路差がフォトンの可干渉距離以内であるとき、これら３つの寄与が働き、同時計数の確率振幅は$\left|1+2e^{i\theta}+e^{2i\theta}\right|^2$に比例する。ここで、θは干渉計の光路差による相対位相である。本研究で用いたフォトンペアの可干渉距離は、約74mμである。しかし、干渉計の光路差がフォトンの可干渉距離を越えると干渉に寄与する項が異なる。ＨＢＳ１において、それぞれ透過と反射したフォトンペアは、干渉計の各アームを通り、再度ＨＢＳ１に入射される。すなわちこのフォトンペアは、光路差が可干渉距離以内であるときＨＯＭの干渉を起こす。逆に言えば、光路差が可干渉距離を越えるとこれらのフォトンペアは、ＨＢＳ１でＨＯＭ干渉が崩壊しランダムに反射もしくは透過してくることになる。すなわち、$\left|1+e^{2i\theta}\right|^2$の干渉効果と、ある一定の同時カウントが測定されることとなる。よって、可視度50%でフォトンの半波長の振動周期が観測されることとなる。

ここで、干渉計の光路差が波長四分の一の整数倍を取るときの同時計数カウントを考えるとType-I、Type-II共にフォトンがそれぞれのアームを通った状態のみをセレクトしていることが分かる。このようにして、コリニアーなフォトンペアに対して干渉計のＨＢＳ１で$|1,1\rangle$の状態を選択することが可能となる。

（iv）多体エンタングルメントの効率的な生成方法の実現

量子情報技術において、エンタングルメントは不可欠な要素である。従来は2つの粒子の間のエンタングルメントが主な研究対象であり、基礎的な性質はほとんど明らかになったと言える。例として代表的なのはEkertプロトコルであり、絶対的安全性を持つ量子暗号技術の典型的な例である。実験的にも二粒子のエンタングルメントを高効率で生成する研究が盛んに行われており、特に光子によるエンタングルメントの生成は目覚しい進展を遂げている。

近年は、三粒子以上のエンタングルメントが注目されている。二粒子に比べて非常に複雑な構造をもっているために、基本的な性質に関しても未解決な問題が多く残されている。多者間で通信を行うようなより洗練された量子暗号技

術や、大規模な量子コンピュータの開発のためには多体エンタングルメントが不可欠であり、応用の観点からも非常に重要である。しかし、実験において多粒子エンタングルメントを生成することは容易ではなく、これまでは非常に低い効率でしか生成することができなかった。

我々はこのような背景のもとで、多体エンタングルメントの典型的な状態のひとつである三体 W 状態 $|W_3\rangle = 1/\sqrt{3}\left(|001\rangle + |010\rangle + |100\rangle\right)$ を効率的に生成する方法を提案、実現した。従来、光の多体エンタングルメントの生成方法はパラメトリック下方変換と呼ばれる非線型光学過程をもちいたものがほとんどであったが、今回世界で初めてパラメトリック増幅と呼ばれる非線型光学過程を採用した。生成効率は1秒間におよそ 1.45 個であり、これは過去に別のグループにより行われた三光子 W 状態を生成する実験に比べて 40 倍以上であり、また生成に要するレーザー光の強度は 10 分の 1 程度で済んだ。我々は生成した状態に対して量子状態のトモグラフィを適用することにより密度行列を再構成し、得られた状態を完全に特定することに成功した。得られた状態の理想的な三光子 W 状態に対する忠実度は $\langle W|\rho_{\exp}|W\rangle = 0.80 \pm 0.04$ であった。また、密度行列から witness operator の期待値を計算することにより、得られた状態が真の三体エンタングルメントであることを確認した。更に部分系に Peres-Horodecki の判定法を適用することにより、部分系もエンタングルしているという W状態の特徴的な性質を確認した。

このように効率的に多体エンタングルメントを生成することは、応用の観点から重要な意義を持つ。特にリソースが光であることから、量子秘密共有などの洗練された量子暗号プロトコルへの応用が期待される。さらに今回のスキームは、量子最適クローニング等のそれと類似性があることから、これらの過程と多体エンタングルメントとのかかわりを調べる手がかりになることが期待され、基礎研究にも一石を投じた成果と言える。また、今回の提案は一般の n 光子 W状態を生成する方法へと発展させることができ、拡張性も優れている。

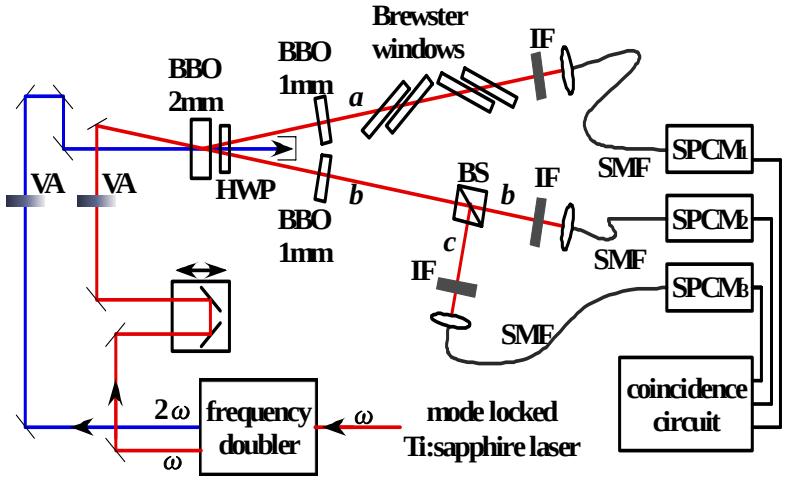


図10 三体W状態を生成する実験装置

（様々な種類の多体エンタングルメントの生成方法の提案）

多体エンタングルメントは実に多様な種類があるため、実験的に生成するにあたってはある一つの状態に特化された実験装置を用いるのが一般的である。特に理論的にも全く性質の異なる二つの状態を同一の実験装置で実現するような提案はなかった。更に生成方法に関する一般的な指針がないため、実現可能な生成方法が明らかになっていない状態も多く存在する。四体 W 状態 $|W_4\rangle = 1/2\left(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle\right)$ はその例である。我々は、この四体 W 状態を含む、様々な種類の多体エンタングルメントを同一の実験装置で生成する方法を理論的に提案し、実現可能性についての詳細な解析を行った。

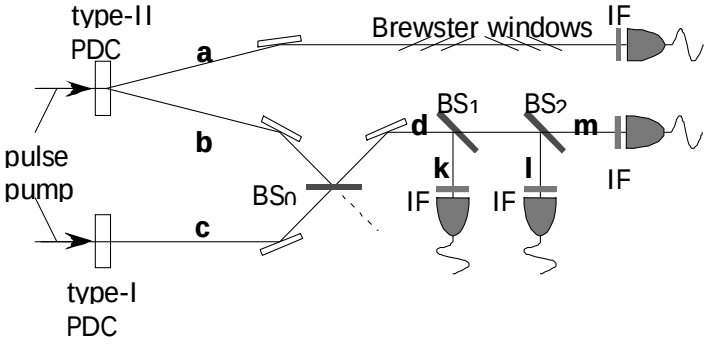
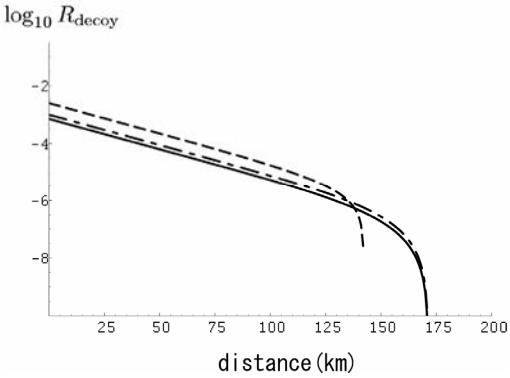


図11 提案した実験系

（v）自然放出パラメトリック下方変換光を用いた量子鍵配布

量子力学の原理により、盗聴不可能な情報伝送方法：量子鍵配布（量子暗号）の研究が多くの物理学者、情報学者等の下で進められている。しかし現実環境下での、不完全な信号源、雑音等による影響で実際には安全性が必ずしも保証されない事が実用化への妨げになっている状況である。安全性を保証するには信頼性の高い 1 光子源を用いる必要があるが、実用レベルには未だ至っていない。そこで現在多くのグループで行われているレーザー光を用いた量子鍵配布に対してより高い安全性とビットレートを実現できる系の提案を行い、かつ実験的に実現する事を目的として研究を行った。

本研究ではパラメトリック下方変換（SPDC）光子対の片方をトリガー信号とする 1 光子源（同時発生する 2 光子を利用）を用いた。ここでは同時発生した 2 光子を空間的に分離し片方を検出器で捉えた場合、もう片方の存在がわかるという性質を利用する。すでにいくつかのグループが実験的に生成しているが、この手法で生成される光はその光子数分布（ポアソン分布）において他の 1 光子源（サブポアソン）と比較した場合複数光子確率が増加してしまうと考えられるが、トリガー側で光子数識別を行うことができれば複数光子の場合には鍵として採用せずにすみ、より長距離での安全性を確保できかつレーザー光を用いた場合に比べ高いビットレートを得られることを計算により示した。（図 12）



$\log_{10} R_{\mathrm{decoy}}$：鍵生成率(∝ビットレート)

実線：効率=0.6

一点鎖線：効率=0.6の光子数識別器

鎖線：レーザー光の場合

図12

横軸は光ファイバー中の伝送距離であり、ここでは通信波長帯（1550nm）のファイバー減衰率(0.25dB/km)を用いた。縦軸は送信者から発信されるパルス当たりの鍵生成率である。

鎖線は従来のようにレーザー光を光源として用いた場合の鍵生成率曲線である。明らかにわかる通りトリガー検出器が不完全な効率であっても、より長距離での鍵配布が可能である。またトリガー検出器が光子数識別能力を備えた物であるなら、実線（識別能力がない）と一点鎖線（識別能力がある）の比較して、より高い鍵生成率を得られる事がわかる。

ここで計算に用いた光子数識別器は、我々が保有している光子検出器と光ファイバーを用いて構成できる。SPDC 光を用いる利点として同時計数を取ることによるノイズ軽減効果がある。このノイズ軽減によって、レーザー光より長距離での鍵生成が可能になる。同時計数を測定することによるこれらの利点により、単一光子源としての相対的な信頼性の低さをカバーして安全性の高い量子鍵配布システムを構築することができる事を示した。

(実験) より長距離での安全な秘密共有鍵生成を達成するために、SPDC を用いた量子鍵配布実験を行った。まず送信者側では SPDC 光の片側（シグナル）に電気光学変調器を用いて偏光変調を加え安全な鍵生成に必要な 4 つの偏光状態をランダムに付加した。ランダムな電圧は、PC 内でプログラムによって生成され、DA 変換ボードから出力した。その電圧は増幅器によって電気光学変調器の半波長電圧(300V)オーダーにまで増幅され、電気光学変調器に入力した。偏光情報（ビット情報）を付加されたシグナルは空気中を伝播し、受信者側へと送られた。光路中には可変減衰器が挿入され、0～50km までの光ファイバー中の伝送をシミュレートした。

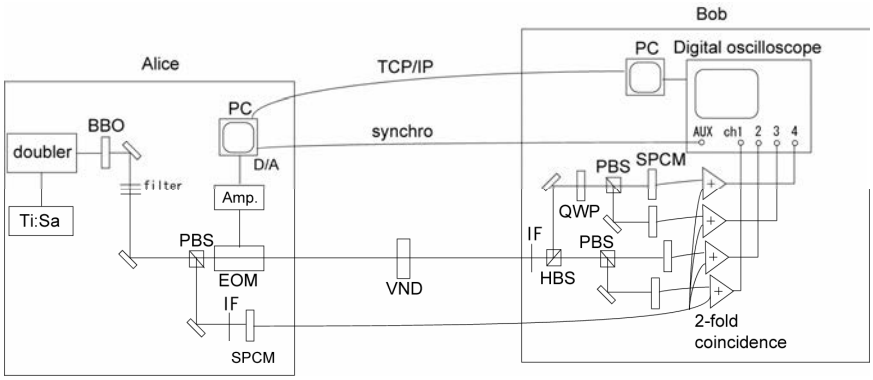


図13 実験系

受信者側では、送られた光を検出する受信者側光検出器ユニットが設置されており、そのユニットを構成する検出器の出力電気信号の記録を行った。このユニットは、無偏光ビームスプリッターと偏光ビームスプリッター及び 4 つの光子検出器で構成されており、検出した検出器番号を用いて受信者と送信者は鍵生成を行うためにその記録を保存する必要がある。その後に古典通信（LAN）を通じて受信者送信者各々が用いた基底照合を行う事で最終的な鍵生成を行った。受信者側の時間および受信ビットの基底記録はデジタルオシロスコープで行い、各々の測定時間は 4ms とした。1 度測定が終わるごとにそのデータを受信者側 PC に送り送信者側 PC との通信を行った。この測定を繰り返すことで長い鍵が得られた。本実験では 20 回の繰り返しを行い（80ms）、表 1 にあるとおり測定結果として、13kbits/s のビットレートが得られた。またより小さな光透過率での実験もおこない、透過率 10%の場合(10dB:光ファイバー通信波長帯 1550nm において 50km に相当)1kbits/s のビットレートが得られた。この値は電気信号の変調高速化及び、ポンプレーザーの出力増加により改善する事ができる。

表1 鍵生成実験結果

attenuation(dB)	sifted key (kbits/s)	error rate
0	13	0.031
1.5	4.7	0.053
10	1.0	0.073

(2)得られた研究成果の評価及び今後期待される効果

1. Observation of an oscillatory correlation function of multimode two-photon pairs
2. Two-photon interference of multimode two-photon pairs with an unbalanced interferometer
3. Polarization-entangled mode-locked photons from cavity-enhanced spontaneous parametric down-conversion
4. Quantum interference of a mode-locked two-photon state

上記論分は全て Physical Review A 誌に掲載されており、インパクトファクターは

2.902 である。また引用件数は、ごく最近印刷されたものであるために、多くはなく計 5 件であるが、これから多数引用されると期待される。以下の点に本研究の独創性がある。縮退パラメトリック共振器を閾値下で用いる事により、多モード 2 光子対の同時計数測定から振動する相関関数を初めて観測した。従来の強度相関関数の観測では検出器の時間分解能の制限により、振動を観測する事は不可能であった。しかし我々は共振器長を大きく取る事で、振動を時間分解できるように設計し初めて観測に成功した。またその共振器を用いて、マッハツェンダー干渉計による量子干渉の観測及び偏光絡み合い状態にある光子対の生成に成功した。
量子情報技術においては、様々な非古典的な性質を持った光源が必要とされており、本研究において開発した光源もまた将来的に大きく活躍する可能性がある。

5. Four-photon entanglement from two-crystal geometry
6. Four-photon W state using two-crystal geometry parametric down-conversion
7. Generation of the four-photon W state and other multiphoton entangled states using parametric down-conversion
8. Multi-photon entangled states from two-crystal geometry parametric down-conversion and their application in quantum teleportation

5-7 は Physical Review A 誌に掲載されており、インパクトファクターは 2.902 である. また 8 は Optics Communications に掲載されインパクトファクターは 1.581 である。引用件数は計 5 件である。本研究では多光子の絡み合い状態の生成手法の提案を行った。絡み合い状態は量子情報技術において不可欠なリソースであるが、これまで 2 光子の絡み合い状態生成実験は数多く行われており、生成効率も格段に進歩してきている。しかしながら 3 光子以上の絡み合い状態に関しては実験の数自体が未だすくなく、生成効率に関しては非常に小さいため現状では量子情報処理の過程において用いる事は困難である。そこで我々はW状態を主として、3 光子以上の絡み合い状態の高効率生成手法を研究し、幾つかの方法を提案した。依然として十分な生成効率ではないが、今後の絡み合い状態生成研究への参考となるであろうと考えられる。

9. Spectroscopy by frequency-entangled photon pairs

掲載誌：Physical Review A,インパクトファクター2.902 である。本研究においては、従来狭帯域で生成されていた周波数絡み合い状態を広帯域に広げ、その絡み合い光源を用いて分光を行った初めての論文である。

10.Generation of a sub-Poissonian state with quantum high- and low-pass filters

掲載誌:Physical Review A, インパクトファクター2.902. サブポアソン光は量子情報技術で重要な非古典光であり、従来では発生に非線型過程を必要としていたが本研究では線型光学素子を用いて生成できることを示した。量子コンピュータを線型光学素子で構築できる事が示されたように、線型光学素子を用いる事は弱い非線型性しか用

いる事のできない現在では代替手段として非常に有望である。

11. Security and gain improvement of a practical quantum key distribution using a gated single-photon source and probabilistic photon-number resolution
掲載誌：Physical Review A. インパクトファクター2. 902. 量子鍵配布において、単一光子源は安全鍵生成率と伝送距離の向上の為に不可欠な要素である。しかし現時点で応用に用いる事のできる単一光子源はまだ存在しない。そこで我々はパラメトリック下方変換光と簡便に作成できる光子数識別器を用いて、伝送距離と安全鍵生成率の向上が達成できる事を示した。量子鍵配布は実用化に最も近い量子情報科学の1分野だが、現在まで数多く作成されたシステムでは安全性の保証ができない。我々の手法は実用化が容易であり、量子鍵配布が社会に普及する場合利用に値すると考える。

３．５　光通信の極限の理論的探求とその理論の応用としての新量子暗号の開発　（玉川大；広田グループ）

(1)研究成果の内容

現代の主要暗号は安全性の根拠を計算量に置き、数理的研究としてすばらしい発展を遂げている。計算量的安全性は将来解読される危険性を排除できないため、無限の能力を持つコンピュータでも解読できない“*情報理論的安全*”あるいは“*解読処理不可能安全*”な暗号の開発も一方で重要である。その目的のため、通信過程において、その信号系の物理現象を安全性の保証に使う物理暗号があり、量子暗号はこれに属している。具体的技術としての最初の量子暗号は1984年のC.H.BennettとG.Brassardによる暗号用の鍵の配送プロトコル(BB-84)である。量子暗号の開発においてはBB-84のような鍵配送のみではなく、従来の暗号のように直接暗号通信する共通鍵暗号も考察の対象となり得る。しかし、単一光子や２次元量子ビットによる量子情報技術では現実社会とのインターフェースとコストに重大な問題があるため、従来の光通信で実現可能な準巨視的な無限次元量子ビット（コヒーレント状態）による暗号や量子情報技術の開発が期待される。玉川大学グループは２０年間にわたり、その可能性の追求のための物理から情報理論にわたる広範囲な課題について長期的研究を実施してきた。その主な研究課題は以下のようにまとめることができる。

（i）　光通信の限界特性の解明

現在の光通信は無限次元の量子状態を用いる通信系であり、その通信の理論限界を明らかにし、これによって次世代光通信の技術的可能性を検証すると共に、工学として意味のある研究が進むべき方向を提示する。

（ii）コヒーレント状態による量子情報処理の基礎理論

量子情報の要である非局所性理論をコヒーレント状態に拡張し、その結果をコヒーレント状態によって量子計算、通信、暗号を実施する方法論と具体的技術の開発に応用する。

（iii）光通信（コヒーレント状態）による新量子暗号の開発

課題１と２の成果に基づいて、これまでと全く異なる工業的に実用性のある新量子暗号を開発する。

ＣＲＥＳＴ研究プロジェクトの間に上記課題について研究した結果、以下のような成果を得たのでここで解説する。

（i）光通信の極限通信路容量に関する基本定理

光通信の究極的な通信路容量に関する研究は１９６０年代にGabor、高橋秀俊、Gordonによって考察され、Gaborと高橋秀俊は光子数による通信、Gordonはレーザ光による通信が究極的であると推論した。それ以来、多くの研究が行われたが厳密な証明は最近まで解明されなかった。しかし、その間、Glauberのコヒーレント状態理論からYuenのスクイズド状態理論が開発され、さらにHolevoの一般ガウス状態理論が確立された。

これらの基礎理論を用いて光通信の真の通信路容量とそれを達成する光通信方式の探求がロシア科学アカデミー、MIT、玉川大学グループで実施され、以下のような成果が得られた。

①損失も雑音もないときのみ、光子数光通信とレーザ光通信は同じ通信路容量となり、かつそれが最大値となる。

②エネルギー損失や背景光雑音が存在する通信路では、光子数通信はほとんど情報伝送の利点がない。これに反して、レーザ光通信は理想通信からの劣化が少ない。

③ エネルギー損失や背景光雑音が存在する通信路の光通信の通信路容量の公式が我々によって１９９９年に導出されHolevo・相馬・広田の定理と呼ばれている[1]。

[1] A.S. Holevo, M. Sohma, and O. Hirota. “Capacity of quantum gaussian channels”, Physical Review A vol. 59, no.3, pp.1820-1828, 1999.

④このような理論が“現実の光通信に対して新しい技術を提供するか”という疑問に対しては、現状の光通信が定量的にはすでに極限に近い性能を達成しており、残念ながら対費用効果の意味では量子情報理論の結果は現実的には有効ではないという結論がロシア科学アカデミー、MIT、玉川大学グループによって示唆された[2]。さらに有限次元の量子ビットによる量子情報理論の成果は、有限次元の量子ビットによる通信は古典の光通信よりも性能が悪いため、通信工学としては歓迎できるものではないことが明らかになった[2]。

[2]広田、量子情報科学の基礎、森北出版, ２００３.

⑤以上の知見を基礎に、本プロジェクトで無限次元系の量子情報理論の成果であるHolevo・相馬・広田の定理が光通信にもたらす工学的な新しい可能性とは何かを探索した結果、技術論として定量的に意味があるのは、超微弱光を受信しなければならない超長距離通信のみであり、そのとき、レーザ光の２値符号と量子最適受信の組み合わせで(Binary discretization)、従来のシャノン通信路容量の数百倍の情報伝送が可能であることを証明した[3]。また、超微弱光領域では超加法性があり、佐々木と臼田によって詳細が解明されている。したがって、NiCT が目指す超微弱光に対する量子最適受信機の実験的開発研究は深宇宙通信を含む光通信の極限技術として極めて有意義であることを担保した。

[3] M. Sohma and O. Hirota, “Binary discretization for quantum continuous channels”, Physical Review A. vol.62, no.5,.052312, 2000

[4] M.Sohma and O.Hirota, “Information capacity formula of quantum optical channels”, Recent research development in Optics I (2001), Research Signpost, Trivandrum, India

[5] A.S. Holevo, M. Sohma, and O. Hirota. “Error exponents for quantum channels with constrained input”, Report on Mathematical Physics vol. 46, no.3, pp.343-358, 2000

（ii）コヒーレント状態のエンタングルメント理論

非直交状態のエンタングルメントの代表的な理論は２モード･スクイズド状態に関するものである。これは連続量の物理量に対してモード間にエンタングルメントが発生する現象である。これに対して、有限次元及び無限次元の離散系集合の非直交状態にエンタングルメント現象があるとすれば、どのような特性を持つかは全く不明であった。さらに、非直交状態は完全エンタングルメントを持つことができないと信じられてきた。そのような、状況にあって、我々は無限次元の離散系コヒーレント状態が完全エンタングルメントを持ちえることを発見した[6]。

[6] O. Hirota, and M. Sasaki: “Entangled state based on non-orthogonal state,” Proc. of Quantum Communication, Computing, and Measurement 3 pp359-366, (Kluwer academic/Plenum publishers, New York 2001).

コヒーレント状態のエンタングルメントが完全性を持つことを量子情報処理理論に応用することが可能である。その応用例としてコヒーレント状態のエンタングルメント状態を用いた量子テレポーテーション法を開発し、それらがデコヒーレンスに対してどのような耐性があるかを解明した[7, 8]。

[7] S. J van Enk and O.Hirota, “Entangled coherent state: teleportation and decoherence”, Physical Review A, vol.64, no-2, 022313 (2001).
[8] S.J.van Enk and O.Hirota, “Entangled states of light and their robustness against photon absorption” Physical Review A, vol--71, 062322, 2005

マイクロ共振器理論の応用として進行波型のコヒーレント状態のエンタングルメント状態の生成法を発見した。 また、NEC の廣嶋と共同でマイクロ共振器内でのコヒーレント状態のデコヒーレンス・フリー特性を発見した[9]。

[9] T.Hiroshima, and O.Hirota, “Continuous variable noise free states in correlated quantum noisy channels,” Proc. of QCM&C, ed by S. M. Barnett, E. Andersson, J. Jeffers, P. Ohberg, and O. Hirota (Eds.), American Institute of Physics, New York, (2004).

（iii）従来の光通信による新量子暗号の開発

上に述べた基礎理論の成果をもとに光通信による新量子暗号の開発に成功したのでその成果に関する詳細を以下に示す。

概要：

現在、実際に稼働している光通信用デバイスは古典的な動作に見えるが、その全ての物理過程では量子力学的な現象が関与している。光信号を光ダイオードで受信したとき発生する光電ショット雑音は量子力学の射影公理の現実的な実証であり、その量子現象を暗号に応用しようというアイデアが光通信量子暗号である。最初の光通信量子暗号は鍵配送プロトコル（B-92）の変形版としての Yuen-Kim による鍵配送プロトコルであり、その原理実験は NEC と玉川大学によって実施された。この方法は単一光子量子暗号よりは遙かに高速（数 M bps）であり、実現技術も容易である。

[10] A.Tomita and O. Hirota: “Security of classical noise-based cryptography”, J. Opt. B, vol.2, no.6, 705-710 (2000)

一方、３年間の潜伏を経て２０００年に解読不可能かつ超高速な共通鍵量子暗号を光通信のみで実現する Yuen プロトコル（Y-00）が公表され、鍵配送と One time pad 法を用いなくても十分安全な暗号が可能となった。短い共通鍵による暗号でありながら、ある運用上の範囲では無限の能力のコンピュータでも解読できないプロトコルの開発は暗号学において夢であったが､Y-00 はその夢への第一ステップとして期待されている。このように通常の光通信による超安全性を有する暗号技術全般を光通信量子暗号と呼び、我々が目指す最も重要な課題である。特に、その Y-00 は以下のような原理で構成される。

量子通信の研究の萌芽期において現代量子情報理論の基礎定理群が発見されたが､その中で Helstrom・Holevo・Yuen・Hirota よって確立された非直交状態識別限界定理は今日の量子情報処理技術の未来を描くための指導的役割を果たしている。この定理は情報を伝送する信号の識別に量子力学の原理による制限があり､その限界は既存の装置を超えたところに存在することを示す。その限界は絶対に超えることのできない壁であり、かつ明確に計算することが可能である。これまではその量子限界を達成する量子光通信の実現法が主目的であったが､この定理を応用して以下のような暗号構成原理が提唱された。

（優位性の確立原理）：鍵を知る者と知らない者の量子最適測定の性能差によって優位性の確立が設定されれば､情報理論的安全な暗号が構成可能であり、その優位性を破ることは量子力学の法則を破ることに等しい。

上記の原理にしたがって現実の光通信による量子暗号の実施法が２００２～２００３年に Northwestern 大学と玉川大学によって提案された。前者は光多値位相変調方式、後者は光多値強度変調方式と呼ばれ、それぞれ用途によって優劣がある。Northwestern 大学では国防総省の DARPA プロジェクトとしてすでに当該方式による 650 Mbps, 200 Km のフィールドテストに成功している。玉川大学グループでは２００３年、日立ハイブリッドネットワークの協力の下､強度変調方式の 5 Mbps, 数 Km の原理実験、２００５年、松下電器の協力の下、実働可能な強度変調方式の１Gbps, 20 Km の試験装置の開発に世界で初めて成功した。

[11] O.Hirota, K.Kato, M.Sohma, T.Usuda, and K.Harasawa, “Quantum stream cipher based on optical communications, “ Proc. on Quantum Commun. and quantum Imaging, SPIE, vol-5551, 2004.
[12] O.Hirota, M.Sohma, M.Fuse, and K.Kato, “Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme.” Physical Review A, vol -72, 022335, 2005

Y-00 の暗号通信のしくみと実証実験成果：

光アクセス系等への早期適用・実用化を狙い、光強度変調方式に基づく Y-00 プロトコルの研究開発を行った。光強度変調方式は、低コストな光デバイスを利用できる経済性に加えて、充分な長距離伝送性能を有し、実用的な高セキュリティ・高速通信装置を

実現することが可能である。図 1 に、Y-00 プロトコルによる暗号通信装置の構成を示す。光送信器（Alice と呼ぶ）では、入力された 2 値データに所定のランダム符号 E を掛け合わせ、さらに鍵情報 Ki に基づき発生させた多値ランニング鍵 R と加算することによって、擬似的な多値信号 S を生成する。これにより、データ基底を、レベル a1 と b1、a2 と b2、a3 と b3・・・で構成される各レベル対にランダムにマッピングする。この多値信号 S を、光強度変調信号に変換し、光ファイバ伝送路へ送出する。光受信器(Bob と呼ぶ）は、光強度変調信号を自乗検波して多値信号 S を再生する。さらに、Alice と共有した多値ランニング鍵 R を閾値として信号 S を識別した後、ランダム符号 E を掛け合わせて 2 値データを復元する。一方、盗聴者光受信器（Eve と呼ぶ）は、高性能な光検出器を備え、かつ理想的な盗聴条件として光送信器から送出される全光電力を受信できるものとする。例えば図 1 では、Eve は、光ファイバ増幅器（EDFA）と pin フォトダイオードで構成され、Alice に直結された状態を想定している。但し、Eve は鍵情報 Ki または多値ランニング鍵 R を共有しないため、R を基準とした 2 値識別でなく、多値識別を行わざるを得ない。ここで、予め多値数を充分大きく設定し、多値信号の信号点間距離（例えば、|a1-a2|）を、当該光強度が有する量子ゆらぎの大きさ相当に抑圧することによって、多値識別時の誤りを大きくできる。これにより、Eve による暗号文の取得を著しく制限し、解読行為を不可能とする。

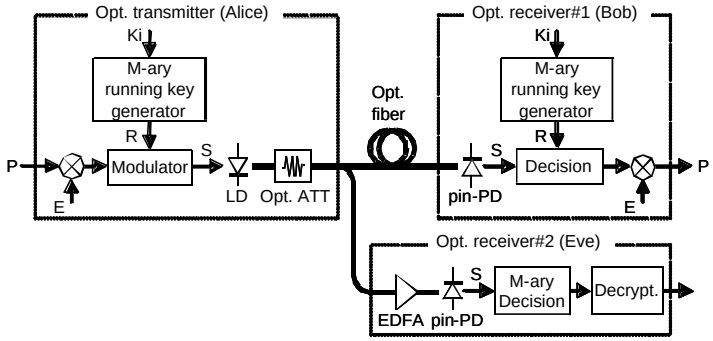


図1 Y-00プロトコルによる光強度変調型暗号通信装置

松下電器の協力を得て、光強度変調方式に基づく Y-00 プロトコルの有効性を検証するため、高速光伝送装置の開発を行い、その伝送特性評価を行った。光送信器（Alice）には、直接変調用光源として 1.55um 帯 DFB レーザを使用し、平均バイアス電流：15.8mA を注入して平均光強度：+5dBm の光信号を発生後、-12.3dBm まで減衰した。データレートを 1.0625Gbps とし、多値信号 S の多値数を 100ー200 値以上に設定して DFB レーザに入力した。光送信器から送出される光変調信号の最大／最小光強度は、それぞれ-9.8dBm、-18.5dBm である。なお、直接変調時の波形歪を抑圧するため、多値信号に対する最適帯域等化とバイアス電流の最適制御を行っている。光受信器（Bob）は、光ファイバ伝送後の光強度変調信号（平均受光電力：-16.3dBm、1.7×10^{5}photon/bit）を検波して、多値信号 S を再生後識別する。

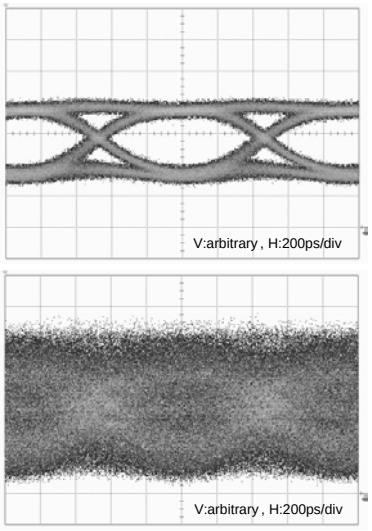


図2 受信光信号波形（上：Bob、下：Eve）

図 2 に、Bob および Eve の各受信信号波形（アイパターン）を示す。本条件において Eve が観測する量子ゆらぎ量は、受信多値信号の信号点間距離（5×10^3photon）を充分上回る。このため、Bob の受信信号波形は明確なアイ開口を有し、2 値識別が容易であるのに対して、Eve のアイはほぼ完全に閉塞し、多値識別も極めて困難であることが分かる。以上の実験結果から、Y-00 プロトコルは、100 値以上の超多値信号を光強度変調する構成により、1Gbps の高速信号を最大 24km 伝送した場合でも、高い安全性を保持できることが分かる。なお、図３に、開発した高速光伝送装置の外観を示す。

図3 松下電器による 1 Gbps　Y-00量子暗号通信装置・外観

(2)得られた研究成果の評価及び今後期待される効果

（i）光通信の限界特性の解明

ロシア科学アカデミー、MIT、および当該プロジェクトの玉川大学グループの研究により、究極の通信は現在の光通信に用いられている通常のレーザ光による通信方式であることが証明され、現代通信技術における量子情報理論が果たすべき役割が何であるか

が明確にされた。その結果、今後の量子情報の研究は無限次元の離散系（デジタル）量子状態による情報技術の開発が基本となり、そのための基礎理論としての量子通信理論が重要になる。結果的には、現在、国内外で多くの量子情報理論の研究が実施されているが、ほとんどが単一光子を含む有限次元量子ビットに関するものであり、通信技術には全く貢献できないことが明らかとなった。各国のプロジェクトとして多くの研究資金が基礎研究としての量子情報に投入されているが、緊急にその方向を修正すべきであることが明確である。

その根拠として、２００５年度のコヒーレント状態発見へのノーベル物理学賞に加えて、最近、プリンストン大学と MIT は通常のレーザ光（コヒーレント状態）による量子暗号への応用を視野に、Holevo・相馬・広田の定理を光マルチプルアクセス通信へ拡張するとことに成功した（文献１３）。この成果は我々の新量子暗号のための基礎理論の構築を見据えた量子情報科学の今後の方向性を示唆する上で極めて重要である。

[13] B.J.Yen, and J.H.Shapiro, Multiple access bosonic communications, Physical Review A, 72, 062312, 2005.（Holevo・相馬・広田の定理はプロジェクト前のため、自己調査：引用回数８, IF=2.9）

さらに、MIT の RLE では光宇宙通信から量子暗号を含めた未来通信として“従来の光通信の極限技術”を追求している。このような世界の動向を見れば、理論的に通信の性能が全くない単一光子系の量子情報通信研究は工業的将来性がないことは明白であり、これまでの玉川大学グループの主張と成果が世界の流れをコヒーレント状態による究極的な光通信、量子暗号、量子情報処理へ向けさせる鍵を握っていると言える。
短期間に世界の動向を一変させるまでの研究成果をあげたことは我々にとっても幸福である。特に、以下の成果は、これから数年の間に米国・ロシアの通信科学者にさらなる研究課題を提供し、量子通信理論の体系化において大きな足跡となると確信する。

[14] A.S. Holevo, M. Sohma, and O. Hirota. “Error exponents for quantum channels with constrained input”, Report on Mathematical Physics vol. 46, no.3, pp.343-358, 2000（CREST 引用回数調査結果：**１**）

[15] M. Sohma and O. Hirota, “Binary discretization for quantum continuous channels”, Physical Review A. vol.62, no.5, pp.052312-1-4, 2000（CREST 引用回数調査結果：0, IF=2.9）

[16] M.Sohma and O.Hirota, “Information capacity formula of quantum optical channels”, Recent research development in Optics I (2001), Research Signpost, Trivandrum, India（引用文献調査対象外）

[17] A.S. Holevo and O. Hirota, “Quantum Gaussian Channel”, IEEE, Proc. International. Symp. on Inform. Theory,,2000. （引用文献調査対象外）

[18] O. Hirota, “A foundation of quantum channels with super addictiveness for Shannon information”, Applicable Algebra in Eng. Communication and Computing, vol.-10, no.4/5, pp.401-423, 2000. （引用文献調査対象外）

（ii）コヒーレント状態による量子情報処理の基礎理論

現代光通信の基礎である無限次元の離散系コヒーレント状態を用いた情報通信技術の開発に不可欠なエンタングルメント特性を研究し、それらは予想に反して完全エンタ

ングルメントを持ちえることを発見した。この事実はこの分野において衝撃的であったと確信する。

[19] O. Hirota, and M. Sasaki: “Entangled state based on non-orthogonal state,” Proc. of Quantum Communication, Computing, and Measurement 3 pp359-366, (Kluwer /Plenum publishers, New York 2001).

（引用文献調査対象外）

事実、その応用例としてコヒーレント状態のエンタングルメント状態を用いた量子テレポーテーション法を開発し、それらがデコヒーレンスに対してどのような耐性があるかを解明した論文は量子コンピュータ構成原理に応用可能であることがベルギー、英国、オーストラリアのグループらによって発見され、極めて短期間のうちに我々の論文は当該分野のキー論文になっている（引用回数は世界トップ１％以内に入ったことが我々に通知されている）。

[20] S. J van Enk and O.Hirota, “Entangled coherent state: teleportation and decoherence”, Physical Review A, vol.-64, no-2, 022313 (2001). （CREST 引用回数調査結果：６３, IF=2.9）

[21] S.J.van Enk and O.Hirota, “Entangled states of light and their robustness against photon absorption” Physical Review A, vol-71, 062322, 2005 （CREST 引用回数調査結果：１, IF=2.9）

以上の理由により、上記論文は今後、量子情報科学の最も基本的な発見の一つとして歴史的な評価を受けると確信する。

（iii）光通信（コヒーレント状態）による新量子暗号の開発

単一光子量子暗号は物理学の基礎研究として重要な研究課題であることを認識した上で、課題（i）と（ii）の成果に基づいて、我々が最も重要と考えている量子情報科学から派生した工業的な実用性を備えた技術がここで開発した新量子暗号である。この暗号は従来の光通信で超高速・解読不可能を実現できるという画期的なものである。プロトコル自身は Yuen によって発明されたものであり、我々は Y-00 と命名した。一見、古典的に見える Y-00 プロトコルは、先の課題で解明されたレーザ光（コヒーレント状態）の量子通信理論が巧に応用されている。Yuen のアイデアを実現する技術として彼の同僚である Kumar は位相変調方式を提案し２００２年に世界初の光通信量子暗号を実現した。我々は２００３年に光強度変調方式を提案し原理実験に成功、さらに２００５年に実用に近いプロトタイプを実現した。

[22] O.Hirota, K.Kato, M.Sohma, T.Usuda, and K.Harasawa, “Quantum stream cipher based on optical communications, “ Proc. on Quantum Commun. and quantum Imaging, SPIE, vol-5551, 2004. （引用文献調査対象外）

[23] O.Hirota, M.Sohma, M.Fuse, and K.Kato, “Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme.” Physical Review A, vol -72, 022335, 2005 （CREST 引用回数調査結果：０, IF=2.9）

上記の新量子暗号はこれまでと全く異なる暗号であり、現時点では誤解も多く、今後、啓蒙活動が必要である。

本格的な実用化研究を始めるために、国内企業との共同研究が必要であるが、その前に、実用機を設計するための設計理論を確立する必要がある。幸いにも、課題（i）で

開発した理論と以下の論文で、実験系において安全性を担保するための変調・復調技術を設計することが可能であることが解った。

[24] K Kato and O Hirota, "Square root measurement for quantum symmetric mixed state signals," IEEE Transactions on Information Theory, vol.49, no.12, pp.3312-33137, 2003. （CREST 引用回数調査結果： 2, IF=2.0）

以上より、我々の全ての研究は一見広範に見えるが、一つの明確な目標（実用化）を目指していることが解る。すなわち、事業化できなければ、全ては無であるとの信念に基づいている。

高速光通信システムの現状と Y-00 への期待

インターネットの急速な普及と動画像を中心とする大容量データ伝送への要望が高まりアクセス網でも光ファイバー通信を適用したブロードバンド加入者が急増してきている。アクセス網のデータ伝送は、ここ数年で飛躍的に大容量化が進み、B-PON で 100Mb/s、GE-PON、G-PON で約 1.25～2.5Gb/s の伝送速度を提供する必要がある。これらインフラの普及に伴い、IT 産業は活発に展開され、Web サイトを利用した通信販売や金融機関の電子決算等、重要な個人情報やデータが頻繁に流れ出している。

一方、これら個人や企業の情報漏洩や流出に対する危険性が積極的に議論され、機密保持への意識向上が図られだした。企業等では既に情報を厳しく管理されだし、情報漏洩に対する安全性の向上対策が積極的に施されだしでいる。これらの対策は ID を管理することや、数学的な処理で計算を複雑化し暗号化を施したものが主流であるが、最近の端末レベルでは、データ管理に指紋や静脈認証を利用した物理的な安全性向上対策も利用されだしている。しかし、これらのデータを伝送する上で必要なネットワークを構成する線路自体は盗聴等の攻撃に対して無防備であり、物理的なセキュリティー保護は施されていない。光ファイバーは電線に比べると信号線上に電磁界が生じないため情報の自然漏洩は殆ど無いが意図的に伝送データを盗聴することは不可能ではない。特に加入者や端末に近いアクセス網のでは、情報の構成がシンプルであり盗聴さえできてしまえば情報の解読は可能である。

このようなデータ伝送に対して高度な安全性を確保するためには、通信ネットワーク上でも物理的に解読不可能な暗号化を実現する必要がある。しかし、このような物理的な安全を確保できる暗号方式を積極的に導入するには、コストを大幅に低減できること、既設のネットワーク環境を利用または応用できること、小型化が可能であること等の条件を満足させることが必須である。

玉川大学を中心とし研究・開発が進められている光多値強度変調方式を応用した光通信量子暗号 Y-00 は、現在の光通信で主流である光強度変調方式を積極的に利用することにより、現在使用されている光伝送システムとの親和性が高く、既存の光デバイス（LD や PD）や光ファイバ等の部品が適用でき、更に標準化されているデータ伝送での通信プロトコルを崩すことなく利用することができるため早期実用化に大きな期待がもてる。

一方、都市型の通信ネットワークやバックボーン通信での光伝送は、10Gb/s 以上の高速伝送、光ファイバーアンプを利用した長距離伝送や、更に大容量の光 WDM 伝送が主流である。これらの光通信システムで使用する暗号方式は、光波長の安定化や高速データ伝送への適応が必須となる。前述のように光強度変調を基本とし、安全性を保ちつつ光の強度を確保できる Y-00 は、従来の光通信・伝送技術を応用したシステム開発が可能であり、外部変調方式や波長制御技術への適応性も高いため、高速・大容量の光 WDM 伝送への早期適用が期待できる。

また近年研究開発が進められている光スイッチを利用した光交換システムが実用化でき、全光ネットワークが実現できれば、ルーティングやスイッチングを含めた全てのネットワークシステム上で安全性を確保するこが可能となる。これは将来の光通信ネットワーク開発へのロードマップに導入できる可能性も高く、適応範囲の幅が更に拡大できるため Y-00 実用化および将来性への期待も高まる。

新量子暗号は既存の光通信系に量子ゆらぎ拡散用の変調装置を実装するだけで実現でき、かつ最適設計時には量子ゆらぎに守られた情報理論的安全なストリーム暗号として動作するため、実現技術の開発は従来の量子暗号に比べて比較にならないほど容易である。さらに光増幅中継を用いて暗号通信速度：数 Gbps で、かつ 1000 Km まで通信可能なため、東京―札幌、東京―福岡を結ぶ全国規模の電子政府用暗号として十分機能する。また、小型軽量化が可能なため、民生用暗号装置としてのビジネスも期待できる。今後、国内企業と協力しながらビジネス化を目指す。

３．６　量子符号化技術と光子数検出技術の研究開発
（ＮＩＣＴ；佐々木グループ）

(1)研究成果の内容

量子通信と従来の通信を分ける決定的な違いは信号を運ぶ量子状態ρ_0、ρ_1の非可換性$\rho_0\rho_1 \neq \rho_1\rho_0$である。この性質は、高密度変調やエネルギー減衰によって信号間距離が狭まり、不確定性原理による位相・振幅の揺らぎ幅が信号間距離と同程度になった場合に顕在化する。このような非可換な量子状態のセットは、i)完全な識別が原理的に不可能、ii) 自由に複製を作ることができない、という２つの重要な性質を示す。i)は通信における伝送容量に最終的な物理限界を課し、ii)は量子暗号の基本原理となっている。我々のグループでは、このような非可換な量子状態を使う通信において、どのような符号化を行えばよいか、という問題に取り組んできた。

通信を成り立たせるためには、データの圧縮と伸長に関する情報源符号化と誤り訂正に関する通信路符号化という2つの符号化が必要になる。それぞれに量子特有の効果があって、それをうまく引き出すことで、従来のシャノン限界を超えることができる。我々はこの2つの符号化の原理実証を世界に先駆けて実証した。

量子情報源符号化

情報源符号化ではメッセージに含まれる冗長性を取り除いて圧縮を行う。従来方式での冗長性とは、アルファベットの出現確率の偏りである。つまり、頻繁に現れる文字ほど、短い０，１の系列で表現してやれば、効率よくメッセージを表現できる。逆に、文字の出現確率が等しい情報源は、圧縮が不可能である。一方、非可換な量子状態からなる情報源には、量子状態の重なりという古典的対応を持たない冗長性がでてくる。これをうまい量子操作で取り除くことで、出現頻度が等しい場合でも、さらなる圧縮が可能になり、量子メモリのサイズを節約できる。

一般に、情報の圧縮効率と復元精度は、扱うデータのサイズが大きいほど高いが、現在はまだ少数の量子ビットしか扱えない。その場合、一定の圧縮率のもとで如何に高い復元精度を実現できるかが問題となる。我々の実験では、量子もつれを適切に制御する事で、従来の圧縮方式では不可能な高い復元精度が達成されていることを示した。

我々の実証実験では、3ビットの信号を2ビットの信号に圧縮し、再び3ビットの信号へ復元するモデルを使う。量子的重なりを有する3ビット信号は、図1(b)のように単一光子を半波長板と偏光ビームスプリッタを介して4本の光路へ導波し、偏光と光路の自由度からなる8次元空間上で用意する。半波長板の角度を変えれば、信号の量子的重なりを調整できる。図1で左側の緑の点線上に量子的重なりを持つ3ビット信号が用意される。2ビット信号への圧縮は、4

本の光路のうち2本の光路を2つの半波長板と1個の偏光ビームスプリッタを介して交差させた後、2本の光路のみを残すことで実現する（図1(a)）。3ビット信号への復元は、圧縮に使った回路とほぼ鏡像対称の回路によって行われ、図1で右側の緑の点線上に3ビット信号が復元される。これより右側の回路は、復元された信号の状態が圧縮前の状態にどれだけ近いかという復元精度を測定するための回路である。

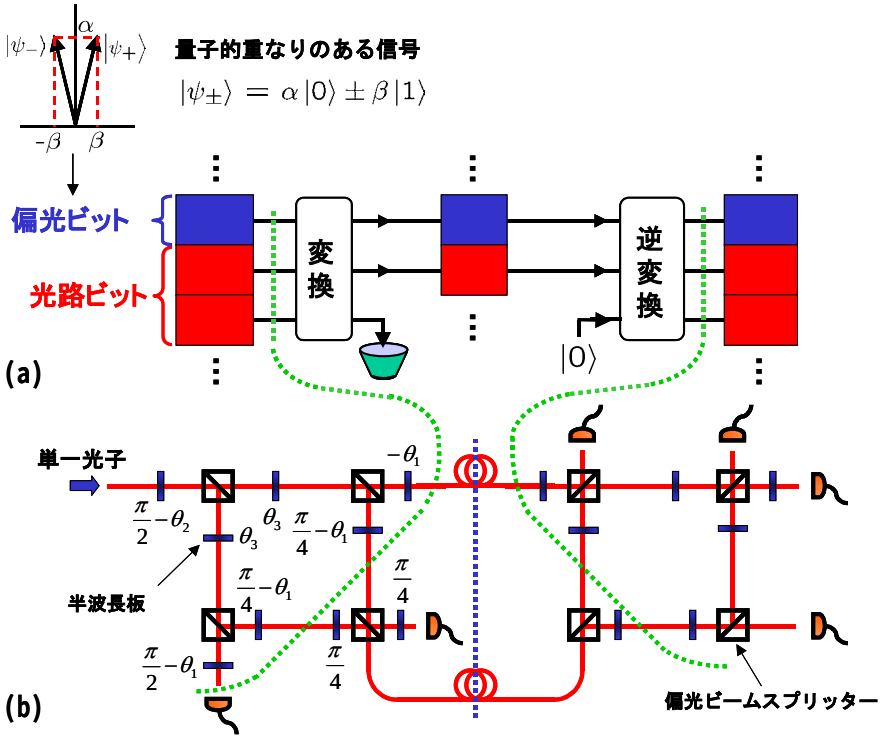


図1　(a)3ビット量子信号圧縮・復元の概念図。
(b)単一光子信号の圧縮・復元精度テスト実験回路。

一方、量子もつれを使わない従来の圧縮は、3ビットの信号に何も手を加えずに、ただ1ビットを捨てるという操作に対応する（図2）。図3は量子的重なりの度合いを変えた場合の、圧縮・復元精度（つまり、圧縮前の入力状態と復元された状態間の重なり）の測定結果である。復元過程では、単純に圧縮の逆変換を行う方法（プロトコル1）と、圧縮過程の結果に依存して逆変換の過程で光子を新たに加える方法（プロトコル2）の2種類の実験を行った。いずれの方法においても、理論的に予想される限界の95%程度まで迫る精度での実験に成功した。特に、信号の量子的重なりの度合いが大きな場合に、量子もつれを適切に制御する圧縮操作の方が、量子もつれを使わない圧縮操作よりも高い復元精度が達成されていることがわかる。このように量子的冗長性を有する信号に対して、その圧縮性を実験的に実証した。

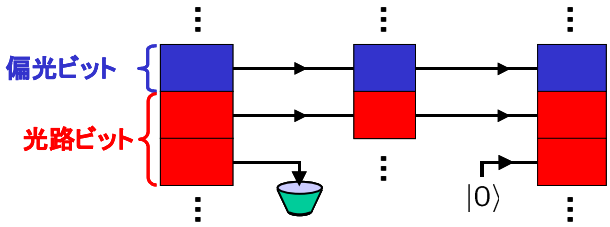


図2 量子もつれを使わない圧縮・復元操作(trivial compression)

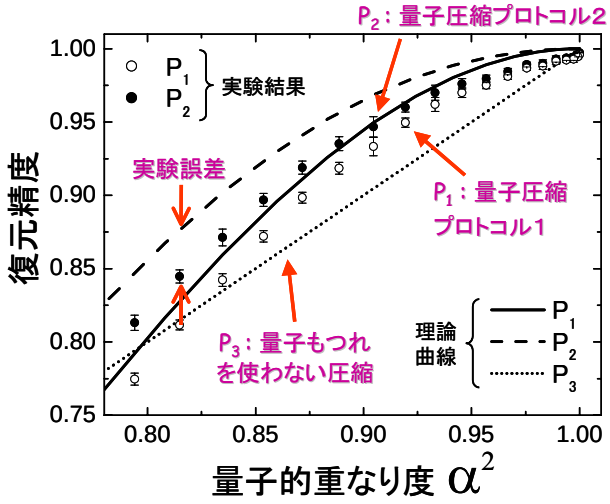


図3 3ビット量子信号圧縮における復元精度測定の実験結果

掲載誌：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. 91, 217902 (2003).

量子通信路符号化

通信路符号化とは、雑音に対抗するためにあえて冗長なビットを付加して誤り訂正を行う符号化で、通信路容量を直接決める重要な符号化である。ここでの問題は、信号の曖昧さの要因が、通信路の雑音ではなく、信号自身に内在する量子状態の非可換性である場合の通信路符号化である。

その鍵は測定過程にある。つまり、受信した信号の状態に、まず適切な量子計算の処理を施してから測定を行うことによって「超加法的量子符号化利得」という従来にはない効果が生み出される。これは、通信資源をn倍に増やした際に、送れるトータルな情報量がn倍以上に増えるという効果である。これに対して、従来の通信理論では、最大でn倍までは増えるが、決してn倍以上に増

えることはない。この場合には、全て古典計算で信号処理を行っている。図４にn=2の場合の概念図を示す。

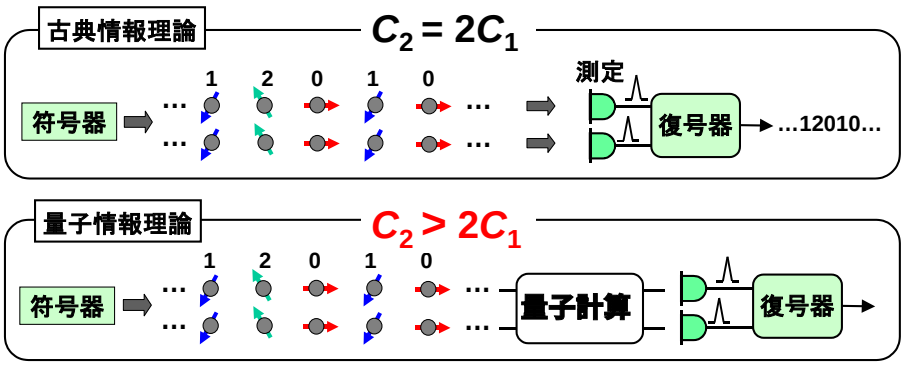


図4 ２個の光子からなる長さn=2の場合の古典情報理論に基づく復号方式と量子情報理論に基づく復号方式の比較。

この超加法的量子符号化利得を実証するため、我々は０，１，２の3値信号を図５に示すように互いに120度離れた単一光子の偏光面の量子状態$|\psi_0\rangle$, $|\psi_1\rangle$, $|\psi_2\rangle$で表すモデルを用いた。もし、３値の偏光状態が多くの光子からなっていれば、完全な識別が可能で、１つの偏光信号あたり$\log_2 3$ (=1.585)ビットの情報量を運ぶことができるが、単一光子の３元対称信号は、量子的重なりのため完全な識別は原理的に不可能であり、送れる情報量は１つの信号あたり最大でも0.645ビットに制限されてしまう。

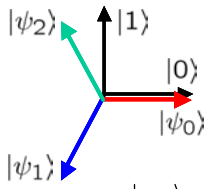


図5 単一光子の３元対称偏光信号$|\psi_0\rangle$, $|\psi_1\rangle$, $|\psi_2\rangle$。$|0\rangle$と $|1\rangle$は、**それぞれ水平及び垂直偏光の状態。**

次に３値信号０，１，２を１個の光子ではなくそれぞれ$|\psi_0\rangle\otimes|\psi_0\rangle$, $|\psi_1\rangle\otimes|\psi_1\rangle$, $|\psi_2\rangle\otimes|\psi_2\rangle$という２個の光子に載せて運ぶ場合を考える。１つの偏光光子対当り伝送される情報量の最大値をC_2と書くと、従来の古典情報理論では$C_2 = 2C_1$であり、伝送情報量は最大でも2倍までしか増えない。一方、量子計算を用いた復号を行うと$C_2 > 2C_1$、つまり伝送情報量を2倍以上に増やすことが可能である。これは量子干渉によって古典情報理論の確率法則を超えた復号操作が可能になるためである。

その実現には、2つの光子間で量子計算ができなければならないが、現在の技術ではまだ困難である。そこで、我々は光子数を倍に増やす代わりに、光子

の空間自由度（光路数）を倍に増やすことを考えた。そうすると必要な符号化・復号化回路は比較的簡単な光学素子で構成できる。実際には、図６に示すような偏光干渉系と光子検出器から構成される。

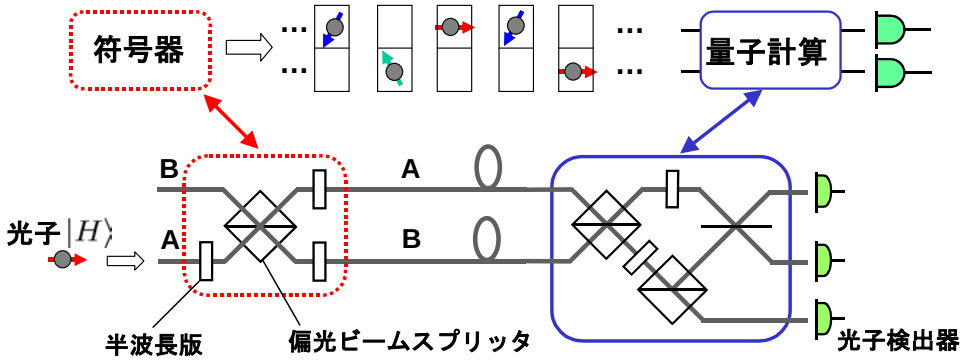


図6 偏光-パルス位置変調符号に対する符号化・復号化回路の概念図。

このような回路へ光子を一個一個導いて符号化・復号化の操作を行い、3つの光子検出器のどれに光子が出たかで0，1，2のどれだったかを判定する。0，1，2のそれぞれについて平均10万回以上、符号化・復号化操作を実行しその統計データから伝送情報量を評価する。図７に、最終的な実験データを示す。

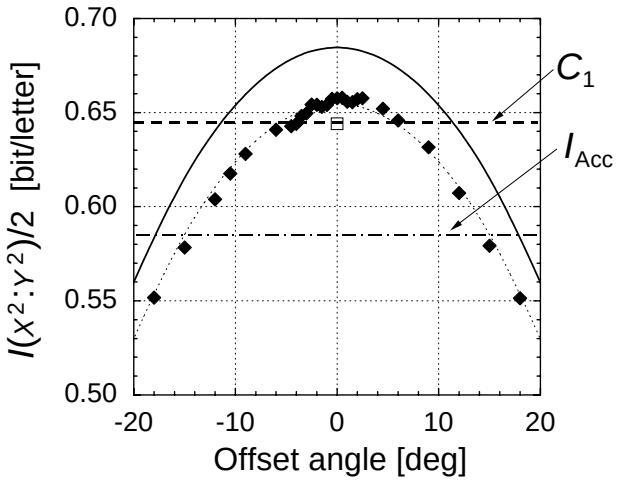


図7 実験データ。縦軸：光子の各自由度あたり伝送された情報量。横軸：offset angle（信号ベクトルと測定ベクトルの相対角）。

縦軸が$C_2/2$を表し、横軸のoffset angleとは、信号ベクトルと測定ベクトルの相対角に対応する復号回路のパラメータを表している。水平の破線が従来の限界C_1の理論値で、黒の角印が実験データを表す。水平の破線の上に飛び出た部分が$C_2/2 > C_1$という超加法的量子符号化利得の実験的証拠になる。$2C_1 = 1.2908$ビットを超えて$C_2 = 1.312 \pm 0.005$ビットの情報が復号されたこと

が示されている。実線が理論値で実験値との差は、光学素子や回路の調整限界からくる不完全さのためである。このように、不確定性原理が支配する通信路では、量子計算を適切に用いた復号を行うことで、通信帯域の増加とともに取り出せる情報量を超加法的に増やせることが実証された。

掲載誌：M. Fujiwara, M. Takeoka, J. Mizuno and M. Sasaki:"Exceeding classical capacity limit in quantum optical channel," Phys. Rev. Lett. 90, 167906 (2003).

光子数識別器

今後は上記の量子通信の2つの基本原理を実用的なコヒーレント信号に適用するための研究に移行してゆくことになる。そのためには、まず高い感度を持つ光子数識別器が必要である。これさえ手に入れば、実は、ガウス型操作と呼ばれる現在の技術と、電気的なフィードバック制御と組み合わせることで、任意の光相互作用（光の量子計算）を原理的に実現できることが、最近の理論研究でわかってきた。しかし、光子数識別技術はまだ世界的にも満足の行くレベルにはなく、現在でも挑戦的課題である。プロジェクトの後半では、光子数識別器の開発を重点的に進めてきた。

我々の方式は、電荷蓄積型の読出し回路を使うもので、Charge Integration Photon Detectorの頭文字をとってCIPDと呼んでいる。図８に示すように、最初の受光部では、通常の雪崩増幅に代わって線形増幅による低雑音の光電変換を行う。出てきた光電子は、低雑音の積分型読出回路で電圧信号のステップへ変換し、このステップの飛びから光子数を読み出すという方式である。

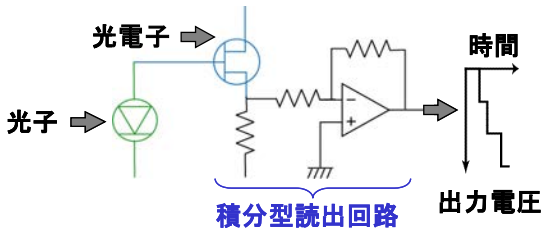


図8 電荷蓄積型光子数識別器（CIPD）

通信波長帯用の受光部にはInGaAsのp-i-nフォトダイオード（京セミ社製）を４Kまで冷却して使う。量子効率は80%強である。初段のアンプには、低雑音のGaAs JFET（ソニー社製）を使う。図９に装置の概観と検出器の心臓部を示す。検出器は液体ヘリウムのクライオスタットに収められ、信号は黄色のシングルモードファイバで受光部に導波される。

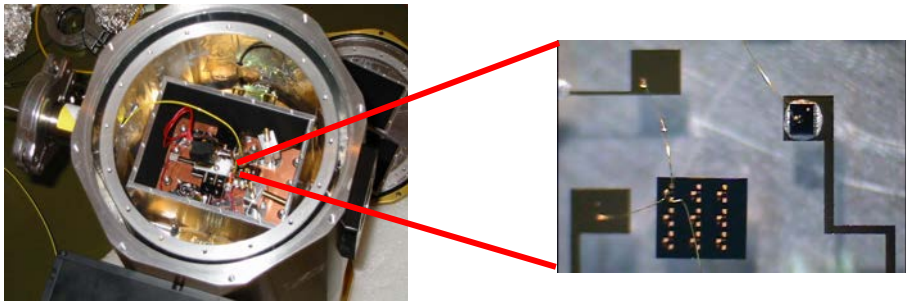


図9 装置の概観と検出器の心臓部

図 10 は、出力電圧の生波形から読み取った積分値の時間変化を示したもので、このステップの飛びから光子数を読み取る。雑音電圧の揺らぎは電子数換算で 1 電子より小さくなっており、光子数識別できる領域に入って来た。ダークカウントは 0.14 個/秒まで下げることに成功した。

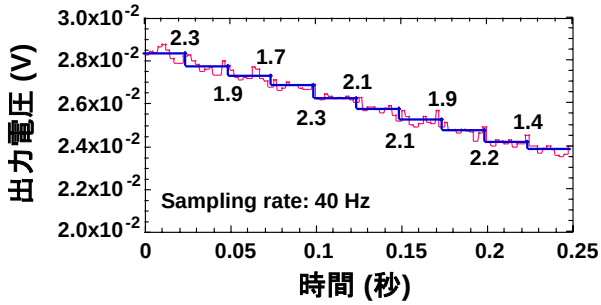


図10 出力電圧とその積分値の時間変化

図 11 に波長 1.53um の半導体レーザーを減衰させた信号のポアッソン統計をいくつかの光強度に対して示している。2 光子～22 光子程度まで、ポアッソン分布の系統的な変化を再現できている。広いダイナミックレンジで、線形性を保った光電変換ができていることを示している。今後は、現在の感度と分解能を保ったまま高速化するのが課題である。図 11 のデータは 40Hz のサンプリングレートに対応するが、最終的な繰返しレートは初段アンプの GaAs JFET の雑音特性で決まり、10ｋHz 付近までは上げられると期待される。ある程度高速化ができた段階で、今度は、スクィーズド光のような、偶数個しか光子が含まれないような状態の非古典的な光子数統計を直接観測するのが目標となる。その先に、光の万能量子ゲートの実現が待っている。

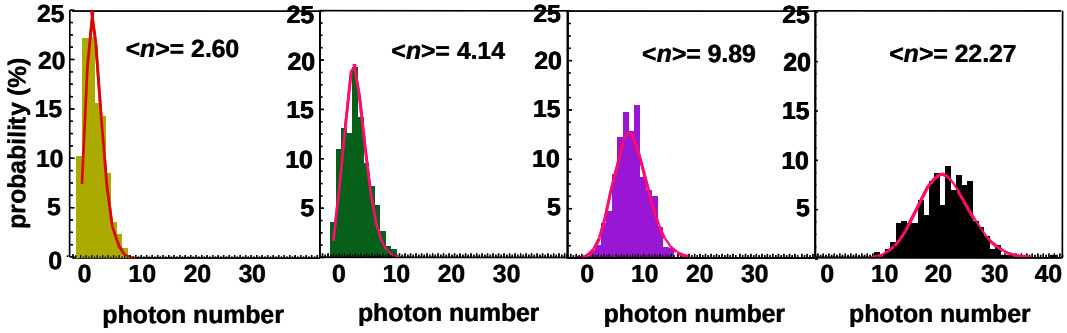


図11 波長1.53umの半導体レーザーの減衰信号に対するポアッソン統計の変化

掲載誌：M. Fujiwara, and M. Sasaki: “Multiphoton discrimination at telecom wavelength with charge integration photon detector,”Appl. Phys. Lett. 86(11), 111119/1--3 (2005).

(2)得られた研究成果の評価及び今後期待される効果

量子情報源符号化、量子通信路符号化

現在の情報通信技術の根底をなす理論は、シャノンが1948年に発表した情報源符号化と通信路符号化に関する基本定理である。この理論は、確率事象に伴う曖昧さとして情報量を定義することによって、雑音のもとでの最適な情報伝送と信号処理を設計する強力な手段を与えてきた。そこで示されたデータ圧縮や通信路容量の性能限界に迫る符号化技術が可能になってきたのは、発表から半世紀近くたったやっと最近のことである。

現在、急速に発展する量子情報技術の源流のひとつは、この2つの基本定理を量子限界へ拡張しようとする理論研究に遡る。1950年代からすでに始まっていたその研究が、量子情報源符号化定理と量子通信路符号化定理として完成したのは1990年代後半のことである。その究極の性能限界を実現するための研究開発はやっと緒についたばかりであり、シャノン限界への挑戦が辿った道程と同様、長い年月を要するだろう。実際、データ圧縮や通信路容量の限界は十分長い符号長で最適な符号化を行った漸近的極限で達成される。片や量子符号化に必要な量子ゲートはまだ実用レベルには程遠く、そのスケーラブルな集積化にはまだ目処すら立っていない。そのような現状にあって我々の第一の成果は、量子情報源符号化と量子通信路符号化の本質的原理を抽出し、それを2～3の少数の量子ビットに対して初めて実験的に実証した点である。

すでに前節で述べたように、量子情報源符号化の原理とは量子状態の重なりという量子的な冗長性を取り除く操作であり、量子通信路符号化の原理とは量子状態の重なりに起因する不可避なエラーがあるとき量子計算を用いた復号を行うことで符号長の増加とともに伝送情報量が超加法的に増えるという効果である。これらの原理を単一光子を複数の空間経路へ導波することで偏光量

子ビットと光路量子ビットを形成し、偏光素子と単一光子検出器を用いて実験的に実証した。そこで示された符号化の量子利得はまだわずかなものであるが、従来のシャノン限界を超える通信の世界があることを初めて実験的に実証したもので、これはまた量子情報理論に実験的基礎を与えたものでもある。実証理論の着想から5年を要した研究であった。その間、最終目標に至るマイルストーンとして偏光量子ビットを用いた量子最適測定に関する成果を

- R. B. M. Clarke, et al. Phys. Rev. A 64, 012303 (2001)
  [IF=2.902, 引用回数24]
- J. Mizuno, et al. Phys. Rev. A 65, 012315 (2001)
  [IF=2.902, 引用回数10]

で発表した。そして、最終的な成果は

- M. Fujiwara, et al. "Exceeding classical capacity limit in quantum optical channel," Phys. Rev. Lett. 90, 167906 (2003).
  [IF=7.218, 引用回数10]
- Y. Mitsumori, et al. "Experimental Demonstration of Quantum Source Coding," Phys. Rev. Lett. 91, 217902 (2003).
  [IF=7.218, 引用回数4]

という物理学分野で権威のある雑誌に掲載され、日経新聞、日経産業新聞、日経BP誌等による成果報道も行った。

このシャノン限界を超える実証実験は歴史上、いつの日か誰かが必ずなすべき課題であったが、このCRESTプロジェクトの一環のひとつとして我々が成し得た事を評価したい。ただ、その後のこの成果に対する反応は、まだ少数の専門家の関心を引き付けているのみである。その理由のひとつは、量子情報源符号化や量子通信路符号化の理解には情報理論の素養が必要であり理論的ハードルが高く、この分野の実験的研究を牽引している量子光学出身の多くの実験家が関心の対象とするには、まだ理論と実験の交流に時間を要するからである。もうひとつの理由は、基本原理は何とか実証できたものの光通信の実用的信号であるコヒーレント信号に適用するためには、コヒーレント信号に対する量子ゲートの実現という格段に高い技術的ブレイクスルーが必要とされ、すぐに実用化への道筋が付かないためである。我々の成果以降、量子符号化利得の実証実験としては、

- G. J. Pryde et al., "Demonstrating Superior Discrimination of Locally Prepared States Using Nonlocal Measurements," Phys. Rev. Lett. 94, 220406 (2005).
- N. K. Langford et al., "Measuring Entangled Qutrits and Their Use for Quantum B it Commitment," Phys. Rev. Lett. 93, 053601 (2004).
- J. Ball, A. Dragan, and K. Banaszek, "Exploiting entanglement in communication channels with correlated noise," Phys. Rev. A 69, 042324 (2004).
- K. Banaszek et al., "Experimental Demonstration of Entanglement-Enhanced Classical Communication over a Quantum Channel with Correlated Noise," Phys. Rev. Lett. 92, 257901 (2004).

などが挙げられるがまだ実験的成果は数少ない。

現状はコヒーレント信号に対する量子ゲートの実現に必要な基礎技術の開

発を地道に進めるしかない。我々は長期的なロードマップにしたがって一歩一歩研究開発を進めてゆくつもりである。特に、まず取り組むべき課題は測定誘起型非線形効果に基づく量子ゲート実現に欠かせない光子数識別器の開発であり、それに対する意義と自己評価について次に述べる。

光子数識別器

光パルスに含まれる光子数を正確に計測する技術は、光を使ったあらゆる量子情報技術の要となる。特に、補助的に用意した量子もつれ状態と光子数測定を組み合わせることで、光の量子ゲートを実現できることが明らかになってきた。また、光子レベルの高精度光計測は量子情報技術に止まらず、あらゆる計測分野に大きな波及効果をもたらす事は論を待たない。したがって、広い波長帯域において、光子数識別技術を確立することが急務である。しかし実際には、量子情報技術の中で最も困難で開発の遅れている課題である。21世紀前半の最重要技術課題のひとつと言っても過言ではない。

これまでに可視波長でStanford大の山本らが、ボーイング社が遠赤外帯用に開発した電子増倍に基づくshallow band Siフォトダイオードを使って高い量子効率(95%)の光子数識別器を試作し、非古典的な光子統計の測定に成功している。ただし、汎用化を目指した展開はその後報告されていない。通信波長帯では、市販品のInGaAs-APDが単一光子検出器として用いられているが光子数の識別は不可能である。通信波長帯で最も高性能のものは、NISTで開発されている超伝導エッジセンサーを使うもので、ほとんど暗計数がないのが特徴である。最近では、量子効率も共振器構造によって80%まで上げられることが報告されている。動作速度は現在400Hz程度である。この素子は基本的にはボロメータであるため広い波長感度を有するが、一方で背景光の影響を受けやすく遮光の特殊なパッケージ技術を必要とする。さらに100 mKまでの極低温の冷却が必要であり、読出回路についてもSQUIDを利用した高い技術を必要とする。これらは普及の大きな足枷となる。

これに対して我々の方式は、低雑音の積分型読出回路に基づく天文観測衛星搭載用の遠赤外検出技術を発展させたもので、通信波長帯用途にはInGaAs PINフォトダイオードを用いる。この検出器はほぼ民生用品だけで構築可能であり特殊な加工技術を必要としない。動作温度も液体ヘリウムで容易に冷却可能な範囲で、遮光も4.2 Kの熱輻射シールドで充分である。現在の性能としては、暗計数0.14 個/秒は半導体を用いた方式では最も低いものの、量子効率80%、光子数分解能S/N～3、繰返しレート40Hzは量子情報への応用ではいまだに十分なものとは言えない。しかし、世界的に見てこれを凌駕する検出器もすぐには見当たらないのが実情である。実際、上述の２つの方式に比べると汎用性と総

合的な性能という点から、今ある技術の組合わせでできるベストな方式と言うことができる。

これまでの成果は、

- M. Fujiwara, and M. Sasaki,"Multiphoton discrimination at telecom wavelength with charge integration photon detector,”Appl. Phys. Lett. 86(11), 111119 (2005).
[IF=4.308, 引用回数0]
- M. Fujiwara, et al., "Reduction method for low-frequency noise of GaAs junction field-effect transistor at a cryogenic temperature," Appl. Phys. Lett. 80(10), 1844 (2002).
[IF=4.308, 引用回数2]
- M. Akiba, et al., "Ultrahigh-sensitivity high-linearity photodetection system using a low-gain avalanche photodiode with an ultralow-noise readout circuit”Opt. Lett. 30(2), 123 (2005).
[IF=3.882, 引用回数1]

という応用物理、光技術で権威のある学術誌に掲載された。国際会議における発表に対しても反響は大きく、光子数識別技術への要求と期待の高さを示すものであった。量子情報技術への本格的な適用には、高速化や高量子効率化など多くの課題を残すが、この研究開発の延長線上にある光子レベルの高感度計測は、あらゆる計測技術分野に大きな波及効果をもたらすことから、今後さらに国家戦略的に研究開発を推進する必要がある。

4　研究参加者

研究代表者：中村　和夫

氏　名	所　属	役　職	研究項目	参加時期
中村　和夫	物質・材料研究機構　若手国際研究拠点	副センター長	研究統括	平成 17 年 7 月～ 平成 18 年 3 月

①中村/富田グループ（絡み合い制御素子開発と量子中継システムの研究）

氏　名	所　属	役　職	研究項目	参加時期
中村　和夫	NEC 基礎・環境研究所	研究部長	研究統括	平成 12 年 11 月～ 平成 17 年 6 月
富田　章久	NEC 基礎・環境研究所	主管研究員	素子開発実験	平成 12 年 11 月～ 平成 18 年 3 月
南部　芳弘	NEC 基礎・環境研究所	主任研究員	素子開発実験	平成 12 年 11 月～ 平成 18 年 3 月
河野　俊介	NEC 基礎・環境研究所	主任	素子開発実験	平成 13 年 5 月～ 平成 18 年 3 月
桐原　明宏	NEC 基礎・環境研究所	担当	素子開発実験	平成 16 年 4 月～ 平成 18 年 3 月
平山由希子	NEC 基礎・環境研究所	チーム事務員		平成 12 年 12 月～ 平成 18 年 3 月
廣嶋　透也	NEC 基礎・環境研究所	主任研究員	素子開発実験	平成 12 年 11 月～ 平成 16 年 3 月
石坂　智	NEC 基礎・環境研究所	主任研究員	素子開発実験	平成 12 年 11 月～ 平成 15 年 9 月
広瀬　賢二	NEC 基礎・環境研究所	主任研究員	素子開発実験	平成 13 年 6 月～ 平成 15 年 4 月
K. Kyhm	NEC 基礎・環境研究所	CREST 研究員	素子開発実験	平成 14 年 2 月～ 平成 15 年 10 月
宇佐見康二	NEC 基礎・環境研究所	研究補助員	素子開発実験	平成 12 年 11 月～ 平成 16 年 3 月
木村　直正	NEC 基礎・環境研究所	研究補助員	素子開発実験	平成 14 年 6 月～ 平成 16 年 3 月
中島とも子	NEC 基礎・環境研究所	研究補助員	素子開発実験	平成 14 年 6 月～ 平成 16 年 3 月
G. Guo	NEC 基礎・環境研究所	研究補助員	素子開発実験	平成 16 年 4 月～ 平成 16 年 4 月

②Wang グループ（絡み合い光源開発等の研究）

氏　名	所　属	役　職	研究項目	参加時期
L.J. Wang	マックスプランク	Director	量子暗号用光源開発	平成 12 年 11 月～ 平成 18 年 3 月
Z. Lu	マックスプランク	ポスドク	量子情報バッファ開発	平成 16 年 2 月～ 平成 18 年 3 月
Ch. Silberhorn	マックスプランク		量子暗号用光源開発	平成 17 年 1 月～ 平成 18 年 3 月
A. Dogariu	ＮＥＣラボアメリカ	Scientist	量子暗号用光源開発	平成 12 年 11 月～ 平成 16 年 3 月
A. Kuzmich	ＮＥＣラボアメリカ	Scientist	量子暗号用光源開発	平成 12 年 11 月～ 平成 13 年 3 月
J. Fan	ＮＥＣラボアメリカ	ポスドク	量子暗号用光源開発	平成 14 年 8 月～ 平成 16 年 10 月
T. Liu	マックスプランク	ポスドク	量子情報バッファ開発	平成 16 年 6 月～ 平成 17 年 1 月

③小林グループ（光子の絡み合い制御技術）

氏　名	所　属	役　職	研究項目	参加時期
小林　孝嘉	東大理学系研究科	教授	量子情報研究指導	平成 12 年 11 月～ 平成 18 年 3 月
藪下　篤史	東大理学系研究科	助手	量子情報理論	平成 13 年 4 月～ 平成 18 年 3 月
大館　暁	東大理学系研究科	D2	量子情報実験	平成 15 年 4 月～ 平成 18 年 3 月
佐々木秀貴	東大理学系研究科	D1	量子情報実験	平成 14 年 4 月～ 平成 18 年 3 月
三上　秀治	東大理学系研究科	D1	量子情報実験	平成 14 年 4 月～ 平成 18 年 3 月
堀切　智之	東大理学系研究科	D1	量子情報実験	平成 14 年 4 月～ 平成 18 年 3 月
竹野　唯志	東大理学系研究科	M1	量子情報実験	平成 16 年 4 月～ 平成 18 年 3 月
小澤　陽	東大理学系研究科	M1	量子情報実験	平成 16 年 4 月～ 平成 18 年 3 月
福岡　郷介	東大理学系研究科	M1	量子情報実験	平成 16 年 4 月～ 平成 18 年 3 月
Haibo Wang	東大理学系研究科	CREST 研究員	量子情報実験	平成 14 年 7 月～ 平成 18 年 3 月
Yongmin Li	東大理学系研究科	ポスドク	量子情報実験	平成 15 年 6 月～ 平成 18 年 3 月
村尾　美緒	東大理学系研究科	助教授	量子情報実験	平成 14 年 4 月～ 平成 15 年 9 月

平澤　正勝	東大理学系研究科	助手	量子情報理論	平成 14 年 5 月～ 平成 16 年 5 月
藤　貴夫	東大理学系研究科	助手	量子情報実験	平成 12 年 11 月～ 平成 14 年 5 月
井出　俊毅	東大理学系研究科	D3	量子情報実験	平成 12 年 11 月～ 平成 15 年 3 月
柳原　康生	東大理学系研究科	D3	量子情報実験	平成 12 年 11 月～ 平成 15 年 3 月
武井　宣幸	東大理学系研究科	M2	量子情報実験	平成 12 年 11 月～ 平成 14 年 3 月
後藤　隼人	東大理学系研究科	M2	量子情報実験	平成 13 年 4 月～ 平成 15 年 3 月

④広田グループ（量子暗号安全性理論の研究）

氏　名	所　属	役　職	研究項目	参加時期
広田　修	玉川大学工学部	教授	量子暗号物理階層理論	平成 12 年 11 月～ 平成 18 年 3 月
相馬　正宜	玉川大学工学部	助教授	量子暗号の情報理論的特性	平成 16 年 4 月～ 平成 18 年 3 月
山崎　浩一	玉川大学工学部	助教授	量子暗号プロトコル	平成 12 年 11 月～ 平成 18 年 3 月
大崎　正雄	玉川大学工学部	助教授	量子暗号の情報理論的特性	平成 12 年 11 月～ 平成 18 年 3 月
加藤研太郎	中央大学	ＣＯＥ研究員	量子暗号安全性理論	平成 12 年 11 月～ 平成 18 年 3 月
臼田　毅	愛知県立大学	助教授	量子暗号プロトコル	平成 13 年 9 月～ 平成 18 年 3 月

⑤佐々木グループ（量子符号化技術と高感度光子検出技術の研究）

氏　名	所　属	役　職	研究項目	参加時期
佐々木雅英	情報通信研究機構	量子情報Gリーダ	量子回路構成	平成 12 年 11 月～ 平成 18 年 3 月
藤原　幹生	情報通信研究機構	主任研究官	光検出技術	平成 13 年 4 月～ 平成 18 年 3 月
武岡　正裕	情報通信研究機構	研究官	光子状態制御	平成 13 年 4 月～ 平成 18 年 3 月
辻野　賢治	情報通信研究機構	専攻研究員	光子状態制御	平成 16 年 4 月～ 平成 18 年 3 月
北川　晃	情報通信研究機構	専攻研究員	量子情報理論	平成 16 年 4 月～ 平成 18 年 3 月
長田　宏二	情報通信研究機構	専攻研究員	量子情報理論	平成 16 年 4 月～ 平成 18 年 3 月

早瀬　潤子	情報通信研究機構	専攻研究員	光子状態制御	平成 16 年 4 月～ 平成 18 年 3 月
井筒　雅之	情報通信研究機構	上席研究員	光子状態制御	平成 12 年 11 月～ 平成 17 年 3 月
水野　潤	情報通信研究機構	専攻研究員	光子状態制御	平成 12 年 11 月～ 平成 17 年 10 月
長谷川敦司	情報通信研究機構	主任研究官	高速光技術	平成 13 年 4 月～ 平成 16 年 3 月
A. Carlini	情報通信研究機構	STA フェロー	量子情報理論	平成 13 年 4 月～ 平成 14 年 2 月
三森　康義	情報通信研究機構	専攻研究員	光子生成検出技術	平成 13 年 11 月～ 平成 16 年 3 月

5　成果発表等

(1)論文発表　（和文　30 件、英文　167 件）

【富田グループ】

1. 宇佐見康二，南部芳弘，富田章久，中村和夫，“真空揺らぎに感度を持つ光子検出器－量子カウンター－”日本物理学会誌 **60**, pp.363-367.(2005)
2. 田島章雄，南部芳弘，“量子暗号: 実用化技術の開発、PLC による小型化、長距離化への取り組み”OPTONICS，285, 110 (2005)
3. Y. Nambu and K. Nakamura, “Experimental Investigation of a Nonideal Two-Qubit Quantum-State Filter by Quantum Process Tomography,” Phys. Rev. Lett. 94, 010404 (2005).
4. A. Tomita, Y. Nambu, and A. Tajima, “Recent Progress in Quantum Key Transmission,” NEC Journal of Advanced Technology, **2**, No.1 pp. 84-91 (2005).
5. S. Kono, A. Kirihara, A. Tomita, K. Nakamura, J. Fujikata, H. Saito, and K. Nishi: ” Excitonic molecule in a quantum dot: Photoluminescence lifetime measurement of an InAs/GaAs single quantum dot,” to be published in Phys. Rev. B
6. 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)
7. T. Hiroshima, "Majorization Criterion for Distillability of a Bipartite Quantum State", Phys. Rev. Lett. Vol. 91, 057 902 (2003)
8. S. Ishizaka, “Analytical formula connecting entangled states and the closest disentangled state”, Phys. Rev. A 67, 060301(R) (2003)
9. 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)
10. 南部芳弘，“量子チャネルの評価技術”応用物理 **72**, pp.181-185 (2003).
11. S. Ishizaka "Analytical formula connecting entangled states and the closest disentangled state", Phys. Rev. A, Vol. 67, No. 5 (2003).
12. K. Hirose, Y. Meir, and N.S. Wingreen: “Local Moment Formation in Quantum Point Contacts” Phys.Rev.Lett., 90, 026804 (2003).
13. 中村和夫、富田章久、南部芳弘：”量子暗号システムの普及に向けて，量子情報科学とその展開(別冊数理科学)”，サイエンス社，160-166，（2003）.
14. A. Tomita and K. Nakamura: “Balanced, gated-mode photon detector for qubit discrimination at 1550 nm,” Optics Letters **27** (2002) pp. 1827-1829.
15. 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)
16. S. Ishizaka, "The reduction of the closest disentangled states", J. Phys. A: Math. Gen., Vol. 35, No. 38, pp. 8075-8081 (2002).
17. T. Hiroshima, “An entanglement measure based on the capacity of dense coding”, Physics Letters A 301 (2002) 263-268.
18. BaoSen Shi and A. Tomita: “Teleportation of an unknown state by W state”, Phys. Lett., A296 (2002) pp.161-164.
19. 富田章久：”量子暗号”オペレーションズ・リサーチ　5 月号 pp.322-327 (2002)
20. 南部芳弘、富田章久：”光量子暗号システム”電子情報通信学会誌　8 月号　pp.606-612 (2002)
21. 松本啓史、富田章久、今井浩：“大規模量子計算の可能性”　Computer Today 9 月号 pp.11-16 (2002)
22. 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”, Phys. Rev. A66, 0338XX (2002)
23. K. Hirose and N.S. Wingreen: “Ground-State Energy and Spin in Disordered Quantum Dots”, Phys. Rev. B65 193305 (2002).
24. S.M. Cronenwett, H.J. Lynch, D. Goldhaber-Gordon, L.P. Kouwenhoven, C.M.Marcus, K.

Hirose, N.S. Wingreen and V. Umansky: “Low-Temperature Fate of the 0.7 Structure in a Point Contact: A Kondo-like Correlated State in an Open System”, Phys. Rev. Lett. 88, 226805 (2002)
25. Y. Meir, K. Hirose and N.S. Wingreen: “Kondo Model for the 0.7 Anomaly in Transport through a Quantum Point Contact”, Phys. Rev. Lett. 89, 196802 (2002).
26. K. Hirose, N.S. Wingreen and Y. Meir: “Local Moment Formation in Quantum Point Contacts”, Phys. Rev. B (2002) submitted.
27. 広瀬賢二:「半導体ナノ構造への密度汎関数法の応用」固体物理　10 月号　（2002） in press.
28. S. Ishizaka, “The reduction of the closest disentangled state”, submitted to J. Phys. A　Math. Gen.
29. 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).
30. K. Hirose, S.S. Li and N.S. Wingreen, "Mechanisms for Extra Conductance Plateaus in Quantum Wires"　Physical Review B, vol.63, 033315 (2001).
31. K. Hirose, F. Zhou and N.S. Wingreen, "Density-Functional Theory of Spin-Polarized Disordered Quantum Dots",　Physical Review B, vol.63, 075301 (2001).
32. K. Hirose and N.S. Wingreen, "Temperature Dependence Suppression of Conductance in Quantum Wires", Physical Review B, vol.64, 073305 (2001).
33. T. Hiroshima and S. Ishizaka: “Local and Nonlocal Properties of Werner States”, Quantum Communication, Computing, and Measurement 3 (KLUWER ACADEMIC/PLENUM PUBLISHERS, NY), 407 (2001)
34. X.B. Wang, K. Matsumoto, and A. Tomita: “Detecting the Inseparability and Distillability of Continuous Variable States in Fock Space”, Phys. Rev. Lett. 87, 137903 (2001)
35. 富田章久:「光による量子ゲートの実現について」　Computer Today　９月号 p.17 (2001)
36. Y. Nambu: “Restoration of entanglement by Disentanglement Eraser”, Phys. Rev. Lett., submitted. (2001)
37. S. Ishizaka and T. Hiroshima: “Maximally Entangled Mixed States in Two Qubits”, Quantum Communication, Computing, and Measurement 3 (KLIWER ACADEMIC/PLENUM PUBLISHERS, NY), 63 (2001)
38. S. Ishizaka: “Quantum channel locally interacting with environment”, Phys. Rev. A63, 034301-1 – 034301-4 (2001)
39. A. Tomita: “Complete Bell State Measurement with Controlled Photon Absorption and Quantum Interference”, Phys. Lett. A282 331-335 (2001)
40. T. Hiroshima: “Decoherence and entanglement in two-mode squeezed vacuum states”, Phys. Rev. A63, 022305 (2001)
41. 石坂智、中村和夫:「量子コンピュータ概論 ---量子コンピュータは何故速いのか？---」シミュレーション学会誌 vol.19-4 20-26 (2000)
42. T. Hiroshima and S. Ishizaka: “Local and nonlocal properties of Werner states”, Phys. Rev. A62, 044302 (2000)
43. S. Ishizaka and T. Hiroshima: “Maximally entangled mixed states under nonlocal unitary operations in two qubits”, Phys. Rev. A62, 22310 1-4 (2000)
44. K. Nakamura and Y. Nambu: “Quantum Key Distribution Using Two Coherent States of Light and Their Superposition”, Phys. Rev. A62, 012312-1-11 (2000)
45. A. Tomita and O. Hirota: “Security of the noise-based cryptography”, J. Optics B2 705-710 (2000)
46. K .Hirose, F. Zhou, and N.S. Wingreen: “Spin-Density-Functional Theory of Clean and Disordered Quantum Dots”, Proc. 25th Int. Conf. Phys. Semicond., 1349 (2000)

【Ｗａｎｇグループ】

1. J. Fan, A. Migdall, and L. J. Wang,"Efficient Generation of Correlated Photon Pairs in a Microstructure Fiber," *Opt. Lett.* **30,** 3368(2005).
2. J. Fan, A. Dogariu, and L. J. Wang,"Parametric Amplification in a Microstructure Fiber," *Appl. Phys. B, Lasers and Optics*, **81,** 801(2005).

3. J. Fan, A. Dogariu, and L. J. Wang, "Generation of Correlated Photon Pairs in a Micro-structured Fiber," *Opt. Lett.* **30,** 1530 (2005).
4. A. Dogariu, M. Hsu, and L. J. Wang,"Reducing Far-Field Diffraction by Structured Apertures," *Opt. Commun.* **220**, 223 (2003).
5. A. Dogariu, J. Fan, and L. J. Wang "Correlated Photon Generation for Quantum Cryptography," *NEC R&D Journal* **44**, 983 (2003).
6. J. Fan, A. Dogariu, and L. J. Wang,"Amplified Total Internal Reflection," *Optics Express*, **11,** 299 (2003).
7. 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*, **20,** 560 (2003).
8. L. J. Wang, "Causal Filters and Kramers-Kronig Relations," *Opt. Commun.* **213**, 27 (2002).
9. L. J. Wang, C. K. Hong, and S. R. Friberg,"Generation of Correlated Photons via Four-Wave-Mixing in Anomalously Dispersive Optical Fibers," *J. Opt. B* **3**, 246 (2001).

【小林グループ】

1. H. Wang and T. Kobayashi, “Phase measurement at the Heisenberg limit with three photons”, Phys. Rev. A, 71, 021802, 2005
2. T. Horikiri, H. Sasaki, H. Wang, and T. Kobayashi, “Security and gain improvement of practical quantum-key distribution using a gated single-photon source and probabilistic photon-number resolution”, Phys. Rev. A, 72, 012312, 2005
3. H. Wang, T. Horikiri, and T. Kobayashi, “Polarization-entangled mode-locked photons from cavity-enhanced spontaneous parametric down-conversion”, Phys. Rev. A, 70, 043804, 2005
4. H. Wang, Y. Li, S. Odate, and T. Kobayashi, “Generation of a sub-Poissonian state with quantum high- and low-pass filters”, Phys. Rev. A, 72, 013822, 2005
5. Y. M. Li and T. Kobayashi, “Multi-photon entangled states from two-crystal parametric down-conversion and their application in quantum teleportation”, Opt. Commun., 244, 285-289, 2005
6. Y. Li, H. Mikami, H. Wang, and T. Kobayashi, “Single mode approximation of parametric down-conversion”, Phys. Rev. A, 2005, 063801.
7. 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
8. Y. M. Li and T. Kobayashi, “Four-photon entanglement from two-crystal geometry”, Phys. Rev. A, 69, 020302, 2004
9. A. Yabushita, and T. Kobayashi, “Spectroscopy by frequency-entangled photon pairs”, Phys. Rev. A, 69, 013806, 2004
10. H. Wang, T. Horikiri, and T. Kobayashi, “Polarization-entangled mode-locked photons from cavity-enhanced spontaneous parametric down-conversion”, Phys. Rev. A, 70, 043804, 2004.
11. P. Kumbhakar and T. Kobayashi, “Nonlinear optical properties of Li2B4O7(LB4)crystal for the generation of tunable ultra-fast laser radiation by optical parametric amplification”, Appl. Phys. B, 78, 165-170, 2004.
12. Y. Li and T. Kobayashi, “Four-photon W state using two-crystal geometry parametric down-conversion”, Phys. Rev. A, 70, 014301, 2004
13. P. Kumbhakar, T. Kobayashi, and G. C. Bhar, “Sellmeier dispersion for phase-matched terahertz generation in ZnGeP2”, Appl. Opt., 43, 16, 3324-3328, 2004
14. H. Wang and T. Kobayashi, “Quantum interference of a mode-locked two-photon state”, Phys. Rev. A, 70, 053816, 2004
15. A. Yabushita, T. Fuji, and T. Kobayashi, “Nonlinear propagation of ultrashort pulses in cyanine dye solution investigated by SHG FROG”, Chem. Phys. Lett., 398, 4-6, 495-499, 2004
16. 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
17. 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
18. P. Kumbhakar, S. Adachi, Z.-G. Hu, M. Yoshimura, Y. Mori, T. Sasaki, and T. Kobayashi: "Generation of tunable near UV laser radiation by type-Ⅰ second-harmonic generation in a new crystal, K2A12B207(KABO)", Jpn. J. Appl. Phys., 42,L1255-L1258, 2003
19. H. Goto, H. Wang, T. Horikiri, Y. Yanagihara, and T. Kobayashi: "Nonclassical interference of multimode two-photon pairs with an unbalanced interferometer", Phys. Rev. A reviewing, (2003)
20. 井出俊毅、小林孝嘉、古沢明：“量子テレポーテーション，量子情報科学とその展開(別冊数理科学)“，サイエンス社，168-173, (2003)
21. T. Ide, H.F. Hofmann, T. Kobayashi, and A. Furusawa: "Continuous variable teleportation of single photon states", Phys. Rev. A, 65:012313, (2002)
22. T. Ide, Takayoshi Kobayashi, and H. F. Hogmann: "Gain tuning and fidelity in continuous variable quantum teleportation", Proceedings of Wigner Centennial Conference, p.109.
23. T. Ide, H. F. Hofmann, T. Kobayashi, and A. Furusawa, "Continuous-variable teleportation of single photon states," Phys. Rev. A, 65,012313,2002
24. 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
25. A. Vukics, J. Janszky, and T. Kobayashi, "Nonideal teleportation in coherent state basis," Phys. Rev. A, 66, 023809, 2002
26. H. F. Hofmann, T. Kobayashi, and A. Furusawa, "Information losses in continuous variable quantum teleportation", Phys. Rev. A64, 040301 (2001).
27. 井出俊毅、小林孝嘉、古沢明: "量子テレポーテーション", 数理科学, 39:24--29, (2001)
28. 小林孝嘉、柳原康生: "図解 ナノテクノロジーのすべて", 第 4 章 産業別にみるナノテクノロジー 量子テレポーテーション 頁 122-12, 工業調査会 (2001)
29. A. Yabushita and T. Kobayashi: "Generation and characterization of a source of wavelength division multiplexing quantum key distribution", J. Appl. Phys., submitted.
30. M.I. Stockman, D.J. Bergman, and T. Kobayashi: "Coherent control of nanoscale localization of ultrafast optical excitation in nanosystems", Phys. Rev. A, 69, 054202 (2004).
31. H.F. Hofmann, T. Ide, T. Kobayashi, and A. Furusawa: "Quantum nondemolition measurement of a light field component by a feedback compensated beam splitter," Phys. Rev. A, submitted.
32. H. Goto, H. Wang, and T. Kobayashi, "Multimode squeezed state produced by an optial parametric oscillator," Phys. Rev. A, submitted.
33. A. Vukics,J. Janszky, and T. Kobayashi, "Infinitesimal representation and a generalization of the quantum-scissors device," Phys. Rev. A, submitted.

【広田グループ】

1. O.Hirota, M.Sohma, M.Fuse, and K.Kato, "Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme." Physical Review A, vol -72, 022335, 2005
2. S.J.van Enk and O.Hirota, "Entangled states of light and their robustness against photon absorption" Physical Review A, vol--71, 062322, 2005
3. 広田 修、解読不可能な超高速 Yuen 量子暗号プロトコル、光科学研究の最前線、日本学術会議、2005
4. T.Hiroshima, and O.Hirota, "Continuous variable noise free states in correlated quantum noisy channels," Proc. of QCM&C, ed by S.M.Barnett, AIP, 2004.
5. O.Hirota, K.Kato, M.Sohma, and M.Fuse, "A quantum symmetric key cipher(Y-00) and key generation: Quantum stream cipher part II, " Proc. on quantum informatics in Moscow. 2004.
6. 広田 修、量子暗号の最新動向、情報処理、vol-45, no-11, 2004
7. O.Hirota, K.Kato, M.Sohma, T.Usuda, and K.Harasawa, "Quantum stream cipher based on optical communications, " Proc. on Quantum Commun. and quantum Imaging, SPIE, vol-5551, 2004.
8. 広田 修、光通信ネットワークと量子暗号、電子情報通信学会、論文誌 B, No-4, pp

478-486, 2004
9. T.Hiroshima, and O.Hirota,; Continuous variable noise free states in correlated quantum noisy channels, Proceedings, vol.734, S. M. Barnett, E. Andersson, J. Jeffers, P. Ohberg, and O. Hirota (Eds.), American Institute of Physics, New York, (2004).
10. O.Hirota, K.Kato, M.Sohma, and M.Fuse,; A quantum symmetric key cipher(Y-00) and key generation: Quantum stream cipher part II, Proc. of Quantum Informatics 2004.
11. 広田 修, 量子暗号の最新動向 情報処理、vol-45, no-11, (2004)
12. O.Hirota, K.Kato, M.Sohma, T.Usuda, and K.Harasawa,; Quantum stream cipher based on optical communications, Proc. SPIE, vol-5551, (2004).
13. 広田 修, 光通信ネットワークと量子暗号 電子情報通信学会、論文誌 B, No-4, pp 478-486, (2004)
14. S. Usami, H. Shiraki, T. S. Usuda, and I. Takumi, Construction of quantum error correcting code for specific position errors, Proceedings, vol.734, S. M. Barnett, E. Andersson, J. Jeffers, P. Ohberg, and O. Hirota (Eds.), American Institute of Physics, New York, (2004).
15. K.Yamazaki, Eavesdropping on Key Distribution Scheme based on Shot Noise of Intense Laser Pulses Proceedings, vol.734, S. M. Barnett, E. Andersson, J. Jeffers, P. Ohberg, and O. Hirota (Eds.), American Institute of Physics, New York, (2004).
16. M.Osaki, K.Yamazaki, and M.Ban, Interference of the correlation by beam splitting in YK protocol QKD system Proceedings, vol.734, S. M. Barnett, E. Andersson, J. Jeffers, P. Ohberg, and O. Hirota (Eds.), American Institute of Physics, New York, (2004).
17. 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.
18. 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, pp.320-331, 2003.
19. 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)
20. M. Sohma and O. Hirota: “A Capacity of Channels Assisted by Two-mode Squeezed State”, Physical Review, A68, 022303 (2003).
21. K. Kato and O. Hirota: “Square-Root Measurement for Quantum Symmetric Mixed State Signals”, IEEE Transactionson Information Theory, Dec., (2003).
22. M.Sohma and O.Hirota, “Squeezing is good at low information rate,” Physical Review A, vol.65, no-2, 022319 , 2002.
23. 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).
24. M.Sohma and O.Hirota, “Information capacity formula of quantum optical channels”, Recent research development in Optics I (2001), Research Signpost, Trivandrum, India
25. S. van Enk and O.Hirota, “Entangled coherent state: teleportation and decoherence”, Physical Review A, vol.64, no-2, 022313 (2001).
26. K.Kurokawa and O.Hirota, “Properties of quantum reliability function and its applications to several quantum signals”, Electronics and communications in Japan, Part 3, vol.84, no.9, pp.31-41 (2001).
27. S. van Enk and O.Hirota, “Entangled coherent state: teleportation and decoherence”, Physical Review A, vol.64, no-2, 022313 (2001).
28. 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).
29. 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)
30. 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).
31. A.S. Holevo, M. Sohma, and O. Hirota. “Error exponents for quantum channels with constrained input”, Report on Mathematical Physics vol. 46, no.3, pp.343-358, 2000
32. M. Sohma and O. Hirota, “Binary discretization for quantum continuous channels”, Physical Review A. vol.62, no.5, pp.052312-1-4, 2000
33. A.S. Holevo and O. Hirota, “Quantum Gaussian Channel”, IEEE Proc. ISIT 2000, 2000.
34. O. Hirota, “A foundation of quantum channels with super addictiveness for Shannon information”, Applicable Algebra in Eng. Communication and Computing, vol.-10, no.4/5, pp.401-423, 2000.
35. A. Tomita and O. Hirota: “Security of classical noise-based cryptography”, J. Opt. B, vol.2, no.6, 705-710 (2000)
36. T. Sugimoto and K. Yamazaki: “A Study on Secret Key Reconciliation Protocol “Cascade” ”, IEICE Trans., vol. E83-A, 1987-1991, Oct., (2000)

【佐々木グループ】
1. Y. Mitsumori, A. Hasegawa and M. Sasaki, "Local field effect on Rabi oscillations of excitons localized to quantum islands in a single quantum well," Phys. Rev. B71, 233305/1--4(2005).
2. M. Fujiwara, and M. Sasaki, "Multiphoton discrimination at telecom wavelength with charge integration photon detector," Appl. Phys. Lett. 86(11), 111119/1--3 (2005).
3. M. Takeoka, M. Sasaki, P. van Loock, and N. Luetkenhaus, "Implementation of projective measurements with linear optics and continuous photon counting," Phys. Rev. A71, 022318/1--10(2005).
4. M. Akiba, M. Fujiwara, and M. Sasaki: “Ultrahigh-sensitivity high-linearity photodetection system using a low-gain avalanche photodiode with an ultralow-noise readout circuit,” Opt. Lett. 30(2), 123 (2005).
5. J. Mizuno, K. Wakui, A. Furusawa, and M. Sasaki: “Experimental demonstration of entanglement-assisted coding using a two mode squeezed vacuum state,” Phys. Rev. A71, 012301(2005).
6. 武岡 正裕, 佐々木 雅英: “光量子情報処理入門　第 4 回:量子情報処理プロトコル II「量子暗号」” レーザー研究, Vol33(3),194--200 (Mar. 2005)
7. 武岡 正裕, 佐々木 雅英: “光量子情報処理入門　第 3 回 : 種々の量子情報処理プロトコルと量子計算” レーザー研究, Vol33(1), 57--61 (Jan..2005)
8. M. Fujiwara, and M Sasaki, "Performance of GaAs JFET at a Cryogenic Temperature for Application to Readout Circuit of High-Impedance Detectors," IEEE Transactions on Electron Devuces, 51(12),2042--2047(2004).
9. M. Takeoka, M. Sasaki, P. van Loock, and N. Nutkenhaus, "Quantum State Discrimination with Linear Optics and Continuous Measurement," Quantum Communication, Measurement and Computing, pp67--70(American Institute of Physics 2004).
10. M. Sasaki, "Toward Implementation of Coding for Quantum Sources and Channels," Quantum Information, Statistics, Probability, pp130--143 (Rinton Press 2004).
11. M. Fujiwara and M. Sasaki, "Photon Number Resolving Detector At Telecommunication Wavelength," Quantum Communication, Measurement and Computing, pp40--43 (American Institute of Physics 2004).
12. M. Sasaki, K. Wakui, J. Mizuno, M. Fujiwara, and M. Akiba, "EPR Beams and Photon Number Detector: Toward Synthesizing Optical Nonlinearity," Quantum Communication, Measurement and Computing, pp44--47(American Institute of Physics 2004).
13. A. Kitagawa, and K. Yamamoto:“Analysis for practical realization of number-state manipulation by number-sum Bell measurement with linear optics,” Phys. Rev. A 70, 052311 (2004).
14. A. Kitagawa, and K. Yamamoto:“Analysis for practical realization of number-state manipulation by number-sum Bell measurement with linear optics,” Phys. Rev. A 70, 052311 (2004).
15. K. Nagata, W. Laskowski, M. Wiesniak, and M. Zukowski:“Rotational Invariance as an Additional Constraint on Local Realism,” Phys. Rev. Lett. 93, 230403 (2004).

16. M. Takeoka, M. Fujiwara, J. Mizuno, and M. Sasaki:“Implementation of generalized quantum measurements: Superadditive quantum coding, accessible information extraction, and classical capacity limit,” Phys. Rev. A 69, 052329 (2004).
17. M. Sasaki: “Toward Implementation of Coding for Quantum Sources and Channels,” Quantum Information, Statistics, Probability, pp130--143 (Rinton Press 2004).
18. M. Sasaki, A. Hasegawa, Y. Mitsumori, and F. Minami: “Theory of active dephasing control in qubit arrays”, Journal of Luminescence, vol. 108(1-4)215--219 (2004).
19. A. Hasegawa, T. Kishimoto, Y. Mitsumori, M. Sasaki, and F. Minami: “Multi-wave-mixing of two-dimensional excitons in semiconductors” Journal of Luminescence, vol.108(1-8)211--214(2004)
20. Y. Mitsumori, Y. Ohkubo, A. Hasegawa, M. Sasaki, and F. Minami: “Optical selection rule for hyper-rayleigh scattering in resonance with exiton states in ZnSe” Journal of Luminescence, vol.108(1-4)211--214(2004)
21. 武岡 正裕, 佐々木 雅英: “光量子情報処理入門　第 2 回：量子テレポーテーション” レーザー研究, Vol32(11), 722--726 (Nov.2004).
22. 武岡 正裕, 佐々木 雅英: “光量子情報処理入門　第 1 回：光子対の量子エンタングルメント” レーザー研究, Vol.32(9), 600--603 (Sep. 2004)
23. 佐々木 雅英: “量子情報通信” ITU ジャーナル, Vol.34(1)(Jan. 2004)
24. 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).
25. 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)
26. 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).
27. 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).
28. M. Takeoka and M. Ban, M. Sasaki: "Unambiguous quantum-state filtering" Phys. Rev., A**68**(1) 012307/1--7(2003).
29. 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).
30. 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).
31. 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).
32. 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)
33. 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)
34. 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)
35. 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)
36. 佐々木雅英、武岡正裕 : "量子通信路符号化", 応用物理学、Vol. 72, N0. 2, 169--175 (2003).
37. 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).
38. Masahiro Takeoka, Masahide Sasaki, and Masashi Ban: "Continuous Variable Teleportation as a Quantum Channel" Optics and Spectroscopy, Vol.94, No.5, 734 -- 742(2003)

39. A. Chefles and M. Sasaki: "Retrodiction of generalized measurement outcomes", Phys. Rev. A67(3), 032112/1--12 (2003).
40. Masahiro Takeoka, Masahide Sasaki, and Masashi Ban: "Continuous variable teleportation as a quantum channel", Optics and Spectroscopy, 94 (5), 735--743 (2003).
41. 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).
42. A. Hasegawa and Y. Mitsumori: "Ultrafast electron control of optical device", J. Commun. Res. Lab. vol. 49 (1), 97--103 (2002).
43. 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).
44. M. Sasaki, J. Mizuno, and M. Fujiwara: "Quantum detection circuit for quantum channel coding", J. Commun. Res. Lab. vol. 49 (1), 105--118 (2002).
45. 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).
46. M. Sasaki, M. Ban, and S. M. Barnett, "Optimal parameter estimation of a depolarizing channel," Phys. Rev. A66 022308-1--022308-8 (2002).
47. M. Sasaki and A. Carlini, "Quantum learning and universal quantum matching machine" Phys. Rev. A66 022303-1--022303-10 (2002).
48. 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, N0. 1, 9--21 (2002).
49. 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).
50. 佐々木雅英、水野潤、藤原幹生："量子通信路符号化のための量子検出回路", 通信総合研究所季報 48(1), 101—112 (2002).
51. 武岡正裕、番雅司、佐々木雅英："雑音環境下における非古典的量子状態の連続量量子テレポーテーション", 通信総合研究所季報 48(1), 113—121 (2002).
52. 長谷川敦司、三森康義："光デバイスにおける超高速電子制御", 通信総合研究所季報 48(1), 95—100 (2002).
53. 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, N0. 10(通巻 467) 58--62 (2002).
54. 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).
55. 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).
56. 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).
57. H. Tobioka, Y. Mitsumori, F. Minami, and A. Hasegawa, "Time-resolved three-pulse photon echoes in GaSe," J. Lumin Vol.94－95, p 601－604 (2002).
58. 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).
59. 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).
60. M. Fujiwara, M. Sasaki, and M. Akiba: "Reduction method for low-frequency noise of GaAs junction field-effect transistor at a cryogenic temperature", Appl. Phys. Lett. 80(10), 1844—1846 (2002).
61. Masahiro Takeoka, Daisuke Fujishima, and Fumiko Kannari: "Optimization of ultrashort-pulse squeezing by spectral filtering with the Fourier pulse-shaping technique", Opt. Lett. 26(20), 1592—1594 (2002).
62. 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).

63. 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).
64. 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).
65. M. Sasaki, A. Carlini, and R. Jozsa: "Quantum template matching," Phys. Rev. A64, 022317-1~11 (2001).
66. M. Sasaki, A. Carlini, and A. Chefles: "Optimal phase estimation and square root measurement," J. Phys. Math. Gen. 34, 7017-7027 (2001).
67. S. M. Barnett, C. R. Gilson, and M. Sasaki: "Fidelity and the communication of quantum information," J. Phys. Math. Gen. 34, 6755-6766 (2001).
68. 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).
69. 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).
70. Jun Mizuno, Mikio Fujiwara, Makoto Akiba, Tetsuya Kawanishi, Stephan M. Barnett, and Masahide Sasaki: Optimum detection for extracting maximum information from symmetric qubit sets", Phys. Rev. A65 (1), 012315-1—012315-10 (2001).
71. H. Tobioka, Y. Mitsumori, F. Minami, and A. Hasegawa: "Time-resolved three-pulse photon echoes in GaSe", Journal of Luminescence 94&95, 601—(2001).
72. Y. Mitusmori and F. Minami: "Transient coherent emission from anisotropic semiconductors studied with phase-locked pulse pairs", Journal of Luminescence 94&95, 663—(2001).
73. Y. Mitsumori and R. Kawahara, T. Kuroda, and F. Minami: Ultrafast phase distortion of the transmitted pulse in GaAs quantum wells", Journal of Luminescence 94&95, 645—(2001).

(2)口頭発表（国際学会発表及び主要な国内学会発表）

①招待及び口頭講演（国内学会 192 件、内招待 16 件、国際学会 114 件、内招待 21 件）

②ポスター発表　　（国内学会 1 件）

【富田グループ】

国際学会発表

1. S. Kono, A. Kirihara, A. Tomita, K. Nakamura, K. Nishi, H. Saito, J. Fujikata, and H. Ohashi: "Time-resolved Photoluminescence Measurement of Exciton and Biexciton in an InAs/GaAs Single Quantum Dot," International Quantum Electronics Conference (IQEC), Tokyo, Japan (July 12, 2005)
2. A. Tomita, "Recent development of technologies for quantum communication," #5631-07, Photonics Asia 2004, Beijing, P. R. China (Nov. 9-12, 2004). (Invited)
3. K. Nakamura, "Progress in Quantum Information Technology", The 1st Academia and Industry Workshop on Foresights for Future Infocom, 2004/05/28. (Invited)
4. K. Nakamura, "Quantum Information Technology in NEC", Workshop of Berkeley Quantum Information Center 2004/05/13.　(Invited)
5. K. Nakamura, Y. Nambu, A. Tomita, H. Kosaka and T. Kimura, "Research Activities of Quantum Cryptography in NEC", 量子情報通信と量子ナノデバイスに関する国際シンポジウム 2004/03/12　(Invited)
6. K. Nakamura, "World's longest single-photon transmission in quantum cryptography system using low cost optical fiber", 6th JAPAN-SWEDEN JOINT QNANO WORKSHOP 2003/12/15 (Invited)
7. 宇佐見 康二、南部 芳弘、史 安森、富田 章久、中村 和夫、"Observation of Antinormally-ordered Intensity Correlation of Electromagnetic Field via Stimulated Parametric Down-conversion", 国際ワークショップ「量子力学の非局所性と統計的推測」NQIS、京都産業大学、2003/9/8

8. T. Hiroshima, "Majorization Criterion for Distillability of a Bipartite Qauntum State", QIT-EQIS (2003/9/2/-/3/、Kyoto)
9. O. Hirota, M. Sohma, and T. Hiroshima, "Is Additivity a Fundamental Requirement i Quantum Information Theory?" QIT-EQIS (2003/9/2/-/3/、Kyoto)
10. 石坂 智、"Analytical formula connecting entangled states and the closest disentangled state"、QIT-EQIS (2003/9/2-3, Kyoto)
11. 広瀬賢二、"Local Moment Formation in Quantum Point Contacts" APS March Meeting, Austin (USA), 3 月 5 日 (2003).
12. Yoshihiro Nambu, Koji Usami, Akihisa Tomita, Satoshi Ishizaka, Tohya Hiroshima, Yoshiyuki Tsuda, Keiji Matsumoto, and Kazuo Nakamura, "Experimental investigation of pulsed entangled photons and photonic quantum channels," Proc. SPIE Int. Soc. Opt. Eng. **4917**, 13 (2002). (Invited)
13. A. Tomita, "Quantum information processing with fiber optics," ERATO workshop on Quantum Information science (EQIS2002), Sanjo-Conference Hall, University of Tokyo, Tokyo, Japan (Sep. 7, 2002) (Invited)
14. S. Ishizaka: "Local properties of the closest disentangled and PPT states", ERATO Workshop on Quantum Information Science 2002 (EQIS), Tokyo (Japan), Sep. 6-8, 2002.
15. Bao-Sen Shi and Akihisa Tomita: "A novel way for preparation of Bell state using femtosecond pulse pumped spontaneous parametric down-conversion", ERATO workshop on Quantum Information science (EQIS2002), Sanjo-Conference Hall, University of Tokyo, Tokyo, Japan (Sep.8, 2002).
16. T. Hiroshima: "Locally induced global disorder in quantum composite systems", ERATO Quantum Information Science 2002, Tokyo, Japan, September 6-8 (2002).
17. K. Hirose, Y. Meir, and N.S. Wingreen: "Instability to local moment formation in quantum point contacts", Int. Conf. on Quantum Transport and Quantum Coherence, Tokyo, Japan, Aug.16-19 (2002)
18. K. Hirose and N.S, Wingreen: Stabilization of ground-state minimal spin in disordered quantum dots", The 23rd Int. Conf. on Low Temperature Physics, Hiroshima, Japan, Aug.20-26 (2002)
19. A. Tomita, Y. Nambu, and K. Nakamura, "Quantum Information Processing with Photonic Devices" ICFS 2002 --- The International Conference on Fundamentals of Electronics, Communications and Computer Sciences, Waseda University, Tokyo, Japan. (Mar. 28. 2002). (Invited)
20. Xiangbin Wang, K. Matsumoto, A. Tomita: "Detecting the Inseparability and Distillability of Continuous Variable States in Fock Space", The Fifth Workshop on Quantum Information Processing (QIP 2002), IBM T.J. Watson Research Center, NY, USA. (Jan. 14-17, 2002)
21. Y. Nambu et.al., "Experimental Investigation of Pulsed Entangled Photons and Photonic Quantum Channels, "Photonic Asia 2002, Shanghai, China Oct. 2002 (Invited)
22. Y. Nambu, K. Usami, A. Tomita, S. Ishizaka, T. Hiroshima, Y. Tsuda, K. Matsumoto and K. Nakamura: "Evaluation of Pulsed Entangled States and Quantum Channels", International Symposium on Quantum Computation- Nano Science and Technology for Implementation (ISQC), Odaiba, Tokyo, Mar.12-14 (2002)
23. K. Usami, Y. Nambu, S. Ishizaka, T. Hiroshima, Y. Tsuda, K. Matsumoto, and K. Nakamura, "Restoration of entanglement by spectral filters" ERATO workshop on Quantum Information Science 2001 (EQIS2001) 9/6-9/8 (2001) Tokyo, Japan
24. T. Hiroshima, "Optimal Superdense Coding" EQIS(Erato Quantum Information Science)2001 (2001.9., Tokyo)
25. K. Nakamura: "Toward Practical Quantum Cryptography", 日端量子ナノエレクトロニクスワークショップ、Sweden, Jun. 13-15 (2001). (Invited)
26. K. Hirose and N.S. Wingreen: "Mechanisms for extra conductance plateaus in quantum wires", American Physical Society Meeting, Seattle, USA, Mar. 12-16 (2001).

国内学会発表

1. 河野俊介, "半導体量子ドット分光と量子情報" つくばナノ光量子科学ワークショップ 2005/6/15

2. 富田　章久　“量子情報処理と光量子デバイス”　つくばナノ光量子科学ワークショップ　2005/6/15
3. 田島　章雄，田中　聡寛，前田　和佳子，高橋　成五，竹内　剛，富田　章久，南部芳弘，“高速量子暗号システムの開発”電子情報通信学会　光通信システム研究会 OCS2005-13　2005/5/23
4. 田島　章雄，田中　聡寛，前田　和佳子，高橋　成五，竹内　剛，富田　章久，南部芳弘，“高速量子暗号システムの開発”電子情報通信学会　量子情報技術研究会 2005/5/12
5. 河野　俊介，桐原　明宏，富田　章久，中村　和夫，西　研一，斎藤　英彰，藤方　潤一，大橋　啓之“InAs/GaAs 単一量子ドットの蛍光寿命測定” 応用物理学会 春季応用物理学関係連合講演会　2005/3/31
6. 南部　芳弘，富田章久，田島　章雄，中村　和夫，“単一方向型量子暗号通信システムの開発” 応用物理学会 春季応用物理学関係連合講演会 2005/03/29
7. 田島　章雄，田中　聡寛，前田　和佳子，高橋　成五，竹内　剛，富田　章久，南部芳弘，“高速量子暗号通信システムの開発 (1) ―アーキテクチャ―”電子情報通信学会総合大会　2005/3/21
8. 河野俊介，桐原明宏，富田章久，中村和夫，西研一，斎藤英彰，藤方潤一，大橋啓之，InAs/GaAs 単一量子ドットの蛍光寿命測定，第５２回応用物理学関係連合講演会，2005 年 3 月，埼玉大学
9. 田島　章雄，田中　聡寛，前田　和佳子，高橋　成五，竹内　剛，富田　章久，南部芳弘，“NEC における量子暗号技術への取り組み”東京大学 生産技術研究所 量子暗号研究会　2005/2/22
10. 富田章久，南部　芳弘，田島　章雄，“High Speed/Long Distance Transmission for Quantum Cryptography”　暗号と情報セキュリティシンポジウム (SCIS)　2005/1/25
11. 中村　和夫：「量子情報技術の高度化に向けた光子状態の制御と評価」量子情報処理シンポジウム、一橋記念講堂、12 月 20 日(2004) (招待).
12. 前田　和佳子，田中　聡寛，田島　章雄，高橋　成五，竹内　剛，富田　章久，南部芳弘, “量子暗号鍵配布システムの実用技術の開発” 電子情報通信学会　量子情報技術研究会　2004/12/06
13. 中村　和夫：「量子暗号の基礎と最近の進展」第 42 回茅コンファレンス、宮城蔵王ロイヤルホテル、8 月 23 日(2004) (招待).
14. 中村和夫　「量子コンピュータ開発の現状」2004 年度第２回冷凍部会例会　2004/06/23 (招待).
15. 南部　芳弘、“プロセストモグラフィーによる量子相関チャネルの評価実験(2)”、電子情報通信学会第 10 回量子情報技術研究会 QIT2004-16、学習院大学、2004/05/24-25.
16. 中村和夫　「量子力学の原理による情報処理通信技術の革新へ向けて」　ナノテクノロジー総合シンポジウム　2004/03/15 (招待).
17. 中村和夫　「量子力学の原理が保障する絶対安全な暗号」科学技術振興機構　基礎研究報告会　2004/03/08 (招待).
18. 南部芳弘、“非線形光学による光子対発生と量子通信への展開”レーザー学会学術講演会第 24 回年次大会「先端光分野を切り開く非線形光学技術の現状と展望」シンポジウム（仙台国際センター），S-3 (2004). (招待)
19. 中村和夫　「量子暗号の基礎と最近の進展」日本学術振興会　未踏・ナノデバイステクノロジー研究会 2004/01/29 (招待).
20. 南部 芳弘、”プロセストモグラフィーによる量子相関チャネルの評価実験” 電子情報通信学会第 9 回量子情報技術研究会 QIT2003-85、NTT 厚木センター、2003/12/11-12
21. 廣嶋 透也、"Majorization Criterion for Distillability of a Bipartite Qauntum State" 日本物理学会 2003 年秋季大会（2003/9/20/-/23/、岡山）
22. 石坂 智、”相対エントロピー・エンタングルメントの解析解” 日本物理学会 秋季大会

（2003/9/20-23、岡山）

23. 河野 俊介、中島 とも子、富田 章久、中村 和夫、石田 真彦、藤方 潤一、横田 均、大橋 啓介、斎藤 英彰、西 研一、”InAs/GaAs 量子ドットの単一ドット分光”, 第 64 回応用物理学会学術講演会、福岡大学、2003/9/1
24. 廣嶋 透也、"Majorization Criterion for Distillability of a Bipartite Qauntum State" 第 8 回量子情報技術研究会（2003/6/30/-/7/2/、札幌）
25. 石坂 智、”Normal vector on entangle-disentangle boundary surface” 第 8 回量子情報技術研究会（2003/6/30-/7-2、札幌）
26. A. Tomita and K. Nakamura: “A balanced gated-mode photon detector for qubit discrimination in 1550 nm,” 第 6 回量子情報技術研究会　QIT2002-33 (2002)
27. 富田、中村 : “ファイバオプティクスによる半古典的量子フーリエ変換”第 7 回量子情報技術研究会　QIT2002-53 (2002)
28. 南部芳弘、宇佐見康二、中村和夫 : “Experimental Study of Photonic Quantum Channel,” 電子情報通信学会 量子情報技術研究会、学習院大学　2002/11/11
29. 石坂智 :「量子コンピュータの基礎と展望」発表、フロンティアプロセス 2002，京都，7/26-27（2002）
30. 南部芳弘､神戸俊之､中村和夫:「異種 4 状態を用いた BB84 量子鍵配付実用システム」、第 6 回量子情報技術研究会、京大会館 5/27-28 (2002)
31. 宇佐見康二（東工大、CREST）、南部芳弘（NEC、CREST）、津田美幸（筑波大、ERATO）、松本啓史（EARTO）、中村和夫（NEC、東工大、CREST）「量子状態トモグラフィーにより推定した２光子偏光状態の忠実度」日本物理学会　第５７年次大会、立命館大学びわこ・くさつキャンパス、2002 年 3 月 24 日～27 日
32. 宇佐見康二（東工大、CREST）、南部芳弘（NEC、CREST）、津田美幸（筑波大、ERATO）、松本啓史（EARTO）、中村和夫（NEC、東工大、CREST）「量子状態トモグラフィーにより推定した２光子偏光状態の忠実度」第６回量子情報技術研究会（QIT６）、京都大学、2002 年 5 月 27 日～28 日
33. 廣嶋 透也、"Coherent information and quantum entanglement"、第 6 回量子情報技術研究会、京都、5/27-28 (2002).
34. 廣嶋 透也、"Dense Coding 通信容量とエンタングルメント測度"、日本物理学会 2002 年秋季大会、愛知、9/6-9 (2002).
35. 南部芳弘、宇佐見康二、津田美幸、松本啓史、中村和夫 「ポンプ光の偏光状態制御による高エンタングルメント EPR パルス光子対の発生」日本物理学会 第５７回年次大会, 立命館、3/24-27 (2002)
36. 南部芳弘、宇佐見康二、中村和夫、「量子プロセストモグラフィーによる光学的デコヒーレンスチャネルの特性評価」日本物理学会 第５７回年次大会，立命館 3/24-27 (2002)
37. 南部芳弘、宇佐見康二，中村和夫，“量子暗号の実用化への展開と将来技術へ向けた評価実験”第 49 回応用物理学関連連合講演会「量子光学の新展開：量子情報通信・処理技術」シンポジウム（東海大学），29p-YM-7 (2002).（招待）
38. 南部芳弘、宇佐見康二、津田美幸、松本啓史、中村和夫、「ポンプレーザのプリコンペンセイションによる高エンタングルメント EPR パルス光子対の発生」電子情報通信学会 第５回量子情報技術研究会, NTT 厚木 11/12-13 (2001)
39. 宇佐見康二、南部芳弘、津田美幸、松本啓史、中村和夫、「量子状態トモグラフィーにより推定した２光子偏光状態の忠実度」日本物理学会第５７回年次大会　3/24-27 (2002) 滋賀県草津市
40. 広瀬賢二, N.S.Wingreen, 「量子ポイントコンタクトでの電子間相互作用効果」日本物理学会，徳島(徳島文理大徳島校), 17aYG-10, 9 月 (2001).
41. 広瀬賢二，N.S.Wingreen, 「乱れた量子ドットのスピン状態理論」日本物理学会，徳島(徳島文理大徳島校), 18pYJ-2, 9 月 2001.
42. 広瀬賢二, Y. Meir, N.S. Wingreen, 「量子ポイントコンタクトでのスピン依存電気伝導理

論」日本物理学会 2002 年秋季大会、春日井市、9/6-9（2002）.
43. 広瀬賢二，K. Burke, Y. Meir, N.S. Wingreen, 「時間依存密度汎関数法による量子ドットの励起スペクトル計算」、日本物理学会秋季大会、春日井市、9/6-9 (2002).
44. 宇佐見康二(東工大)、南部芳弘、石坂智、廣嶋透也、富田章久、中村和夫（ＮＥＣ）、「量子トモグラフィーを用いた２光子偏光状態のエンタングルメントの実験的評価」、日本物理学会第 56 回年次大会、中央大学、平成 13 年３月 28 日
45. 富田章久:“量子通信の夢と現実” フォーラム 量子情報科学 大磯 1/11-14 （2001）(招待)
46. A. Tomita: “Implementation of two-qubit optical quantum gates”, Quantum computation society in KANSAI, Kyoto, Japan (January 22, 2001).
47. 富田章久：“量子暗号の原理と実現法” 応用物理学会 量子エレクトロニクス研究会 1/25-1/27 （2001）(招待).
48. 中村和夫：「量子暗号・量子通信への小規模量子計算の応用について」，東北大学電気通信研究所研究会 「大規模量子コンピュータの実現に向けて」 ９月 27 日 （2001）(招待).
49. 石坂智：「MEM 状態のエンタングルメント回復プロトコル」発表，日本物理学会 2001 年秋季大会，徳島文理大 9/17-20 (2001)
50. 広瀬賢二、N.S. Wingreen: 「量子ポイントコンタクトでの電子間相互作用効果」，日本物理学会 2001 年秋季大会，徳島文理大 9/17-20 (2001)
51. 広瀬賢二、N.S. Wingreen: 「乱れた量子ドットのスピン状態理論」、同上
52. 中村和夫：「量子コンピュータとは？」 自動車技術会、８月 24 日 (2001) (招待).
53. 中村和夫：「量子暗号デバイス技術の展望」 JST 異文化交流会、長野、8/4-6 (2001) (招待).
54. 中村和夫：「量子暗号の基礎とその将来展望」 東京大学ナノリンク研究会、５月 16 日 (2001) (招待).
55. 南部芳弘、宇佐見康二(東工大)、石坂智、廣嶋透也、富田章久、中村和夫：“量子トモグラフィーを用いた２光子偏光状態のエンタングルメントの実験的評価”，日本物理学会第 56 回年次大会、中央大学多摩キャンパス、3/27-30 (2001)
56. 石坂智：”量子テレポーテーションとデコヒーレンス”, 同上
57. 石坂智：”Entanglement and decoherence”, 第２回：量子情報科学セミナー，大磯プリンスホテル 3/12-15 (2001)
58. K. Usami, Y. Nambu, S. Ishizaka, T. Hiroshima, A. Tomita and K. Nakamura: “Evaluation of Entanglement in Photon pairs by Quantum Tomography”, ibid.
59. 富田章久：「量子暗号の原理と実現法」，応用物理学会 量子エレクトロニクス研究会 軽井沢 １月 25 日 (2001)（招待）.
60. 南部芳弘、河野芳江,「ビットコミットメント不可能定理の情報論的説明」，第４回量子情報技術研究会、東工大 11/29-30 (2000)
61. 石坂智、「量子チャンネルの局所デコヒーレンス」、第４回量子情報技術研究会，東工大， 11/29-30 (2000)
62. 廣嶋透也、 ”Optimal dense coding with mixed state entanglement”, 第４回量子情報技術研究会、東工大、11/29-30 (2000)

【Wang グループ】

国際学会発表

１． J. Fan, A. Migdall, and L. J. Wang, 2005 CLEO/IQEC, Conference on Lasers & Electro-Optics Postdeadline Papers “Efficient generation of correlated photon pairs in a microstructure fiber”

２． J. Fan, A. Migdall, and L. J. Wang, 2005 CLEO/IQEC, Conference on Lasers & Electro-Optics Technical Digest “Generation of Correlated Photons with Conjugate Pumps in a Microstructure Fiber”

３． J. Fan, A. Migdall, and L. J. Wang, 2005 Proceedings of SPIE: Quantum Communications and Quantum Imaging III “A microstructure fiber two photon source with conjugate laser pumps”(invited)
４． A. Dogariu, J. Fan, L.J. Wang, G. Leuchs,2004 CLEO/IQEC, Conference on Lasers & Electro-Optics Technical Digest, “Classical and Quantum Correlation of Four-wave Mixing in Micro-Structured Fiber.”
５． A. Dogariu, J. Fan, L.J. Wang, J.A. West, 2003 CLEO/IQEC, Conference on Lasers & Electro-Optics Technical Digest, “Photon-pairs Generation in Micro-structured Fiber.”
６． A. Dogariu, J. Fan, L.J. Wang, 2004 Conference on Physics of Quantum Electronics, Snowbird, Utah, “Correlated photon generation in a photonic crystal fiber.”(invited)

【小林グループ】
国際学会発表

1. P. Kumbhakar, S. Chatterjee, and T. Kobayashi, “Some newly developed crystals for measurement of ultrafast laser pulses by second harmonic generation”, UFO/HFSW2005, The Joint Conference on Ultrafast Optics 5 and Applications of High Field and Shortwavelength Sources 6, Nara, Japan, Sep. 25-30 (2005)
2. T. Kobayashi, H. Wang, Y. Li, and S. Odate, “Application of linear optical networks in quantum optics”, ICAM'05, International Conference on Applied Mathematics, Bandung, Indonesia, 22-26, Aug. (2005) （Invited）
3. T. Horikiri, “Quantum Key Distribution with a Heralded Single Photon Source”, IQEC/CLEO-PR2005, Tokyo, Japan, 11-15, Jul (2005)
4. H. Wang, “Response Characteristic of a Quantum High-/Low-Pass Filter”, IQEC/CLEO-PR2005, Tokyo, Japan, 11-15, Jul (2005)
5. H. Mikami, “New High-Efficiency Source of a Three-Photon *W* State and its Full Characterization Using Quantum State Tomography”, IQEC/CLEO-PR2005, Tokyo, Japan, 11-15, Jul (2005)
6. H. Mikami, Y. Li, K. Fukuoda and T. Kobayashi, “Efficient generation of a three-photon w state”, CLEO/QLS '05, Baltimore, MA, USA, May 22-27 (2005)
7. J. Janszky, J. Asboth, A. Gabris, A. Vukics, M. Koniorczyk, and T. Kobayashi, “Two-mode Schrdinger cats: entanglement and teleportation,” Wigner Centennial Conference, Pecs, Hungary, Jul. 8-12, 2002（Invited）
8. A. Vukics, J. Janszky, and T. Kobayashi, “Nonideal teleportation in coherent-state basis,” Wigner Centennial Conference, Pecs, Hungary, Jul. 8-12, 2002
9. T. Ide, T. Kobayashi, and H. F. Hofmann, “Gain tuning and fidelity in continuous variable quantum teleportation,” Wigner Centennial Conference, Pecs, Hungary, Jul. 8-12, 2002 (Invited)
10. T. Kobayashi and H. F. Hofmann, “Displacement operator representation of quantum transportation”, In 2nd Winter Institute of FQTQO (Foundations of Quantum Theory and Quantum Optics), Calcutta, India, Jan. 2-11 2002. （Invited）
11. T. Ide, H. F. Hofmann, T. Kobayashi, and A. Furusawa, “Continuous variable teleportation of single photon state”, In International Conference in Quatuntum Mechanics(ICQM), Saitama, Japan, November 12-13 2001.
12. H. F. Hofmann, T. Ide, T. Kobayashi, and A. Furusawa, “Information extraction and quantum state distortions in continuous variable teleportation”, In International Conference in Quatuntum Mechanics(ICQM), Saitama, Japan, November 12-13 2001.

国内学会発表

1. 竹野唯志、籔下篤史、堀切智之、小林孝嘉, “広帯域偏光絡み合い光子対の生成”, 日本物理学会, 徳島大学, 9 月 7 -11 日 (2005)
2. 堀切智之、竹野唯志、佐々木秀貴、籔下篤史、王海波、小林孝嘉, “SPDC ゲート 1 光子源を用いた量子鍵配布”, 量子情報技術研究会, NTT 厚木研究開発センター, 5 月 12-13 日 (2005)
3. 三上秀治, 李永民, 福岡郷介, 小林孝嘉, “効率的な三光子 W 状態の生成”, 応用物理学会, 埼玉大学, 3 月 29 日-4 月 1 日 (2005)
4. 大館暁、王海波、小林孝嘉, “３光子を用いた量子限界での位相測定”, 応用物理学会, 埼玉大学, 3 月 29 日-4 月 1 日 (2005)
5. 三上　秀治, 李　永民, 福岡　郷介, 小林　孝嘉, 効率的な三光子 W 状態の生成, 日本物理学会春季大会, 東京理科大学, Mar. 24-27, 2005
6. 堀切智之, 王海波, 小林孝嘉, “パラメトリック下方変換光を用いたゲート 1 光子減の光子数識別による量子鍵配布の安全性およびビットレートの向上”, 日本物理学会, 青森大学, 9 月 12-15 日 (2004)
7. 三上秀治, 李永民, 小林孝嘉, “パラメトリック下方変換を用いた四光子 W 状態の生成”, 日本物理学会, 青森大学, 9 月 12-15 日 (2004)
8. 籔下篤史, 小林孝嘉, “波長多重量子暗号鍵配布光源の開発及びその評価”, 日本物理学会, 青森大学, 9 月 12-15 日 (2004)
9. 三上秀治, 李永民, 小林孝嘉, “パラメトリック増幅された光の量子状態の解析” 日本物理学会, 九州大学、 2004 年 3 月 27-30 日
10. 大舘暁, 佐々木秀貴, 小林 孝嘉, “光ファイバを用いた周波数量子相関” 日本物理学会, 九州大学、 2004 年 3 月 27-30 日
11. A. Yabushita, and T. Kobayashi, “Spectroscopy by frequency-entangled photon pairs,” CLEO/Pacific Rim 2003 年 12 月 15-19 日
12. T. Kobayashi, H.Goto, H. Wang, T. Horikiri, and Y. Yanagihara, “Energy-time correlated photon from an OPO” 日米セミナーQuantum Correlation and Coherence, 八ヶ岳ロイヤルホテル 2003 年 9 月 17-19 日（招待）
13. 小林孝嘉, 「量子テレポーテーションのコヒーレント基底による解析」日本物理学会、東北大学川内ｷｬﾝﾊﾟｽ、Mar. 28-31, 2003
14. 後藤 隼人, 王海波, 柳原康生, 堀切智之, 小林 孝嘉, 「多モード２光子対の時間相関関数」日本物理学会, 東北大学・川内キャンパス, Mar. 28-31, 2003
15. 佐々木秀貴, 小林 孝嘉, 「Kerr 媒質中の伝搬による Schroedinger-cat-like state 発生の解析」日本物理学会, 東北大学・川内キャンパス, Mar. 28-31, 2003
16. H. F. Hofmann, 井手俊樹, 古沢明, 小林孝嘉, “Transfer operator description for continuous variable quantum teleportation”. 日本物理学会, 徳島(徳島文理大徳島校), 9 月 2001. 17pTB-10.

【広田グループ】

国際学会発表

1. O.Hirota, T.Usuda, and M.Fuse, “Quantum stream cipher Part III” International Conference on quantum commun. and quantum imaging in San Diego, Aug. 2005.(Invited)
2. O.Hirota, K.Kato, M.Sohma, and M.Fuse, A quantum symmetric cipher (Y-00), The quantum informatics, in Moscow, 2004.(Invited)
3. T. Tomari, S. Usami, and T. S. Usuda, “A study on optimum quantum decoding for binary linear codes with mixed letter-states”, 2004 International Symposium on Information Theory and Its Applications (ISITA2004), Parma, Italy, Proceedings of ISITA2002, pp.1429-1434, (2004.10).

4. N. Takatsu, T. S. Usuda, and I. Takumi, “Property of elementary gates for coherent-state qubits and their applicability to quantum communications”, 2004 International Symposium on Information Theory and Its Applications (ISITA2004), Parma, Italy, Proceedings of ISITA2002, pp.1435-1439, (2004.10).
5. T.Hirotashima, and O.Hirota, Continuous variable noise free states in correlated noisy channel, Conference on quantum communication, measurement and computing, in Glasgow, 2004.
6. T. Mizuno, T. S. Usuda, and I. Takumi, “Effect of entangled inputs on attenuated channel with memory”, ERATO Conference on Quantum Information Science 2004 (EQIS2004), Tokyo, Japan, Proceedings of EQIS2004, pp.134-135, (2004.9).
7. N. Takatsu, T. S. Usuda, and I. Takumi, “Application of quantum gates for oherent-state qubits to quantum communications”, ERATO Conference on Quantum Information Science 2004 (EQIS2004), Tokyo, Japan, Proceedings of EQIS2004, pp.179-180, (2004.9).
8. T. Tomari, S. Usami, and T. S. Usuda, “Relation between structure of codes and their optimum quantum decoding”, ERATO Conference on Quantum Information Science 2004 (EQIS2004), Tokyo, Japan, Proceedings of EQIS2004, pp.185-186, (2004.9).
9. O.Hirota, K.Kato, M.Sohma, T.Usuda, and K,Harasawa, Quantum stream cipher based on optical communications, International Conference on quantum commun. and quantum imaging in Denver, Aug. 2004(Invited)
10. T.S. Usuda, T. Tomari, and S. Usami, ‘Pure’ square-root measurement and its optimality for mixed-state signals, The Seventh International Conference on Quantum Communication, Measurement and Computing (QCMC04), Glasgow, UK, (2004.7).
11. S. Usami, H. Shiraki, T.S. Usuda, and I. Takumi, Construction of quantum error correcting code for specific position errors, The Seventh International Conference on Quantum Communication, Measurement and Computing (QCMC04), Glasgow, UK, (2004.7).
12. Kentaro Kato, "A study on the secrity of Y-00 against collective attacks," Proceedings of the 2003 Workshop on Cryptography and Related Mathematics, Chuo University, 2003
13. K. Kato: Performance of classical binary codes for quantum channels: toward highly reliable quantum communications”, Proc. of the 6th Int. Confer. On Quantum Communication, Measurement, and Computing, ed. By J.H. Shapiro and O. Hirota, pp. 496-499, Rinton, 2003
14. H. Shiraki, S. Usami, T. S. Usuda, and I. Takumi: “Quantum error correcting code for specific position errors and its application”, ERATO Conference on Quantum Information Science 2003 (EQIS2003), Proceedings of EQIS2003, pp.111-112, (2003.9)
15. O.Hirota, “On irreversibility, dilation in conditional isometric process,” ERATO Quantum Information Science, Sept. 2002.
16. O.Hirota, M.Sohma, and K.Kato, “Quasi Bell state; Generation and application to entanglement assisted communication,” Proceedings of Photonics-2002, India, 2002.
17. S. Usami, T. S. Usuda, I. Takumi, and M. Hata, “Error Performance for Binary Code with Mixed Letter States,” 2002 International Symposium on Information Theory and Its Applications (ISITA2002), Xi'an, China, Proceedings of ISITA2002, pp.339-342, (2002.10).
18. M. Osaki, M. Ban: “Unambiguous attack to the quantum key distribution system with two-mode squeezed states”, International Symposium on Information Theory and Its Applications (ISITA’02), Xi’an, PRC, October 7-11, 2002.
19. Y. Hayashi, S. Usami, T. S. Usuda, and I. Takumi, “Quantum coding gain with error probability criterion for binary linear codes,” 2002 International Symposium on Information Theory and Its Applications, (ISITA2002), Xi'an, China, Proceedings of ISITA2002, pp.475-478, (2002.10).

20. Kentaro Kato, ``Performance of classical binary codes for quantum channels," QCM&C-2002, MIT, Cambridge, MA, USA, Jul., 2002.
21. S. van Enk, O. Hirota and H. Mabuchi: “Entangled coherent state and its application to quantum information processing”, QCM&C-02, July, 2002
22. M.Sohma and O.Hirota, “Information capacity formula of quantum optical channels”, Recent research development in Optics I (2001), Research Signpost, Trivandrum, India
23. M. Sohma and O. Hirota: "Information capacity formula of quantum optical channnels", Recent research development in Optics Ⅰ, Research Signpost, Trivandrum, India, (2001)
24. Hirota, “Quntum information theory and its applications to quantum information processing”, Technical digest, CLEO/Pacific Rim 2001, 2001.
25. M. Sohma and O. Hirota, “The Gallager functions and related quantities for quantum Gaussian channel”, IEEE Proc. ISIT 2001, 2001.
26. K. Kato and O. Hirota, “Quantum random coding expornent of symmetric state alphabet”, Proceedings of QCM&C 2000, Kluwer/Plenum Pub. , 2001.
27. O. Hirota and M. Sasaki: “Entangled state based on nonorthogonal states”, Proceedings of QCM&C 2000, Kluwer/Plenum Pub. , 2001.
28. M. Osaki: “Super additivity with mixed letter states”, Proceedings of QCM&C 2000, Kluwer/Plenum Pub. , 2001.
29. K. Yamazaki: “Improvement of Key rate for Yuen-Kim cryptoscheme”, Proceedings of QCM&C 2000, Kluwer/Plenum Pub. , 2001.
30. T.S. Usuda, I. Takumi, R. Nakano, M. Osaki, and M. Hata: “Properties of mutual information for M-ary quantum state signals”, Proceedings of QCM&C 2000, Kluwer/Plenum Pub. , 2001.
31. Eisaku Furukawa and Kouichi Yamazaki, “Application of Existing Perfect Code to Secret Key Reconciliation”, in Conf. Proc. of Int. Symp. on Commun. and Inform. Thech., Nov., Chiang Mai, pp.397-400, 2001.
32. K. Ymamazaki: “Perfect-single-error-correcting binary code for interactive secret key reconciliation. Amsterdam, January 9-12, (2001)
33. A. S. Holevo and O. Hirota: "Quantum Gaussian Channel," IEEE Proc. ISIT 2000, (2000)

国内学会発表

1. 水上勇輝（玉川大）・広田　修（玉川大学術研究所）、 Gbit 光通信量子暗号(Y-00)の keyed randomization の研究、電子情報通信学会全国大会、北海道大学、９月２３日、２００５.
2. 小林洋平（玉川大）・原澤克嘉（日立ハイブリッドネットワーク）・広田　修（玉川大学術研究所）、Gbit 光通信量子暗号(Y-00)用、直接・外部多値強度変調の比較 、　電子情報通信学会全国大会、北海道大学、９月２３日、２００５.
3. 渡部　圭（玉川大）・広田　修（玉川大学術研究所）、Gbit 光通信量子暗号(Y-00)の光増幅中継 、　電子情報通信学会全国大会、北海道大学、９月２３日、２００５.
4. 土本敏之, 泊知枝, 宇佐見庄五, 臼田毅, 内匠逸, DSR による混合状態に対する量子最適検出特性, 第 27 回情報理論とその応用シンポジウム, 20.2, 下呂, vol.1, pp.359-362, (2004.12).
5. 大橋直史, 田中貴峰, 臼田毅, 特定位置量子誤り訂正符号の応用プロトコルのクラス 第 27 回情報理論とその応用シンポジウム, 41.2, 下呂, vol.2, pp.759-762, (2004.12)
6. 土本敏之, 泊知枝, 宇佐見庄五, 臼田毅, 内匠逸, 光通信量子暗号に用いられる信号の量子検出特性, 平成 16 年度電気関係学会東海支部連合大会, 講演論文集, O-260, (2004.9).
7. 大橋直史, 田中貴峰, 臼田毅, 特定位置量子誤り訂正符号を用いた量子プロトコルの考察, 平成 16 年度電気関係学会東海支部連合大会, 講演論文集, O-262, (2004.9).

8. N. Takatsu, T.S. Usuda, and I. Takumi, Application of quantum gates for coherent-state qubits to quantum communications, ERATO Conference on Quantum information Science 2004 (EQIS2004), Tokyo, Japan, (2004.9).
9. T. Tomonari, S. Usami, and T.S. Usuda, Relation between structure of codes and their optimum quantum decoding, ERATO Conference on Quantum Information Science 2004 (EQIS2004), Tokyo, Japan, (2004.9).
10. T. Mizuno, T.S. Usuda, and I. Takumi, Effect of entangled inputs on attenuated channels with memory, ERATO Conference on Quantum Information Science 2004 (EQIS2004), Tokyo, Japan, (2004.9).
11. 田中貴峰, 臼田毅, 量子不均一誤り保護符号, 平成 16 年度電気関係学会東海支部連合大会, 講演論文集, O-271, (2004.9).
12. 田中貴峰, 白木宏幸, 宇佐見庄五, 臼田毅, 特定位置量子誤り訂正符号に対する訂正方法の考察 第 26 回情報理論とその応用シンポジウム, 36.1, 淡路, vol.2,(2003.12).
13. 水野達彦, 宇佐見庄五, 臼田毅, 内匠逸, 記憶のある通信路における Holevo 容量の特性 第 26 回情報理論とその応用シンポジウム, 30.2, 淡路, vol.2, (2003.12).
14. 山田稚佳子, 臼田毅, 相互情報量を最大にする符号語確率分布について 第 26 回情報理論とその応用シンポジウム, 30.3, 淡路, vol.2, (2003.12).
15. 大崎、山崎、番、量子暗号鍵配送におけるスクィズド状態の有効性 第 26 回情報理論とその応用シンポジウム, 30.2, 淡路, vol.2, (2003.12)
16. 石原瞳, 宇佐見庄五, 内匠逸, 臼田毅, 部分対称信号に対する誤り最小検出と SRM について 第 26 回情報理論とその応用シンポジウム, 30.4, 淡路, vol.2, (2003.12).
17. 泊知枝, 臼田毅, 2 元線形符号に対する量子最適復号について 第 26 回情報理論とその応用シンポジウム, 30.5, 淡路, vol.2, (2003.12).
18. 田中貴峰, 白木宏幸, 宇佐見庄五, 臼田毅, 量子ハミング限界を破る量子符号の特性 平成 15 年度電気関係学会東海支部連合大会, 講演論文集, p.187, 373, (2003.10).
19. 山田稚佳子, 臼田毅, 誤り最小復号による符号長 n の相互情報量の特性 平成 15 年度電気関係学会東海支部連合大会, 講演論文集, p.179, 357, (2003.10).
20. 石原瞳, 宇佐見庄五, 臼田毅, 内匠逸, 非対称量子信号に対する SRM の最適性 平成 15 年度電気関係学会東海支部連合大会, 講演論文集, p.186, 372, (2003.10).
21. 水野達彦, 宇佐見庄五, 臼田毅, 内匠逸, Shor のアルゴリズムに基づく量子通信路容量の数値計算 平成 15 年度電気関係学会東海支部連合大会, 講演論文集, p.187, 374, (2003.10).
22. 泊知枝, 臼田毅, 量子状態の分析理論と最適検出問題の関連性について 平成 15 年度電気関係学会東海支部連合大会, 講演論文集, p.188, 375, (2003.10)
23. 広田修, 加藤研太郎, 臼田毅, “光通信による量子鍵配送, ”第 8 回量子情報技術研究会, 北海道大学, ２００３.
24. 広田修, 加藤研太郎, 相馬正, 臼田毅, “光ネットワーク対応の量子ストリーム暗号, ” 第 9 回量子情報技術研究会, NTT 厚木, 2003.
25. 白木宏幸, 宇佐見庄五, 臼田毅, 内匠逸, “m-qubits 情報のセキュアな伝送のための特定位置量子誤り訂正”電子情報通信学会 第 8 回量子情報技術研究会, 札幌, QIT2003-3, pp.13-18, (2003.6-7)
26. H. Shiraki, S. Usami, T. S. Usuda, and I. Takumi, Quantum error correcting code for specific position errors and its application, ERATO Conference on Quantum Information Science 2003 (EQIS2003), Kyoto, Japan, Proceedings of EQIS2003, pp.111-112, (2003.9).
27. 宇佐見庄五, 林祐一, 臼田毅, 内匠逸, 誤り率と情報量の双方の規準に基づく量子利得を持つ 2 元符号の特性 電子情報通信学会 第 8 回量子情報技術研究会, 札幌, QIT2003-46,pp.223-226, (2003.6-7).

28. 広田　修、「量子情報の基礎数理と量子計算」第５回代数幾何・数論及び符号・暗号研究会、１月、２００３。
29. 白木宏幸, 宇佐見庄五, 臼田毅, 内匠逸, 「2-qubits 情報のセキュアな伝送のための量子誤り訂正」, 第 25 回情報理論とその応用シンポジウム, 23.4, 伊香保, vol.2, pp.443-446, (2002.12).
30. 泊知枝, 白木宏幸, 宇佐見庄五, 臼田毅, 「吾妻-番プロトコルに用いられる量子状態の構造分析」第 25 回情報理論とその応用シンポジウム, 23.3, 伊香保, vol.2, pp.439-442, (2002.12).
31. 高津直規, 臼田毅, 内匠逸, 「コヒーレント状態に対する基本量子ゲートに対する考察」第 25 回情報理論とその応用シンポジウム, 35.1, 伊香保, vol.2, pp.643-646, (2002.12).
32. 矢野淳一郎，高津直規，「臼田毅, 2 つの異なる非直交状態の組による擬似ベル状態のエンタングルメント特性」 第 25 回情報理論とその応用シンポジウム, 40.3, 伊香保, vol.2, pp.715-718, (2002.12).
33. 臼田毅, 林祐一, 宇佐見庄五, 「量子復号によるエンタングルメント」第 25 回情報理論とその応用シンポジウム, 40.2, 伊香保, vol.2, pp.711-714, (2002.12).
34. 加藤研太郎，``混合状態からなる２元対称信号に対する量子カットオフレートの特性,'' 第 6 回量子情報技術研究会（QIT6），京大会館，5 月，2002 年.
35. 山崎浩一, "古典雑音に基づく秘密鍵配送の一実現法," 信学会情報理論研究会, 富山大学工学部, 5/20-21, 2002.
36. 白木宏幸, 宇佐見庄五, 臼田毅, 内匠逸, 量子誤り訂正符号を用いた量子情報のセキュアな伝送の考察, 2002 年電子情報通信学会総合大会, 講演論文集 基礎・境界, SA-4-2, pp.454-455, (2002.3).
37. 大崎正雄，番雅司, 2 モードスクィズド状態を用いた暗号鍵配送方式への攻撃 2002 年電子情報通信学会総合大会，SA-4-5，pp.460-461, (2002).
38. 古川英作, 山崎浩一, 既存完全符号の秘密鍵系列の一致への適用法, 信学会 2002 年総合大会，早大大久保キャンパス, 3/17-30, 2002.
39. 菊池克俊, 山崎浩一, 対話型秘密鍵系列の一致のための完全符号, 信学会 2002 年総合大会, 早大大久保キャンパス, 3/17-30, 2002.
40. O. Hirota: “On irreversibility, dilation in conditional isometric process”, ERATO workshop on Quantum Information Science 2002. Sept. 2002
41. 大崎正雄，”番雅司，２モードスクィズド状態を用いた暗号鍵配送方式への攻撃”, 電子情報通信学会総合大会，早大，2002 年 3 月.
42. 臼田毅, 内匠逸, 畑雅恭, 多元対称信号に対する量子通信路容量の超加法性 第 24 回情報理論とその応用シンポジウム, T-D-1-2, 神戸, vol.2, pp.501-504, (2001.12).
43. 高津直規, 臼田毅, 内匠逸, Schrodinger cat 状態に対する 1-qubit ゲートの特性解析 第 24 回情報理論とその応用シンポジウム, T-D-3-2, 神戸, vol.2, pp.687-690, (2001.12).
44. 林祐一, 宇佐見庄五, 臼田毅, 内匠逸, 古典線形符号による誤り率規準に基づく符号化の量子利得について 第 24 回情報理論とその応用シンポジウム, F-D-1-3, 神戸, vol.2, pp.783-786, (2001.12).
45. 宇佐見庄五, 臼田毅, 内匠逸, 畑雅恭, 2 元混合状態量子符号の復号誤り率について 第 24 回情報理論とその応用シンポジウム, F-D-1-4, 神戸, vol.2, pp.787-790, (2001.12).
46. 白木宏幸, 宇佐見庄五, 臼田毅, 内匠逸, 量子情報のセキュアな伝送のための量子誤り訂正符号の検討 -- 吾妻-番プロトコルの改良 -- 第 24 回情報理論とその応用シンポジウム, F-D-2-1, 神戸, vol.2, pp.859-862, (2001.12).
47. 加藤研太郎, 古典－量子通信路における符号化法についての一考察, 第 24 回情報理論とその応用シンポジウム, 神戸, 2001 年 12 月.

48. 加藤研太郎：SITA ワークショップ講演”量子符号”, 第 24 回情報理論とその応用シンポジウム，神戸，2001 年 12 月.
49. 加藤研太郎, エンタングルメント復号を持つ古典－量子通信路の符号化, 電子情報通信学会量子情報技術研究会，NTT 厚木，2001 年 11 月.
50. 大崎正雄，番雅司，２モードスクィズド状態を用いた量子暗号鍵配送方式 第 24 回情報理論とその応用シンポジウム, pp.867-870, (2001).
51. 山崎浩一：量子暗号鍵配送系のための誤り訂正符号，信学論総合大会，基礎・境界チュートリアル講演，立命館，(2001）
52. 山崎浩一：量子暗号，信学論ソサイエティ大会，基礎・境界チュートリアル講演，電通大，（2001）

【佐々木グループ】

国際学会発表

1. M. Takeoka, M. Sasaki, and N. Luetkenhaus, "Implementation of binary projection measurement with linear optics and photon counting," EQIS2005, National Museum of Emerging Science and Innovation, Tokyo, Japan, 28 Aug (2005).
2. M. Fujiwara, and M. Sasaki, "Development of a Charge Integration Photon Detector for telecom-band," EQIS2005, National Museum of Emerging Science and Innovation, Tokyo, Japan, 27 Aug (2005).
3. J. Ishi-Hayase, K. Akahane, N. ayamamoto, M. Kujiraoka, J. Inoue, K. Ema, M. Tsuchiya, and M. Sasaki, "Coherent Dynamics of Excitons in Stack of Self-assembled InAs Quantum Dots at 1.5 μm Waveband," The 15th International Conference on Dynamical Processes in Excited States of Solids, Shanghai, China, 3 Aug (2005).
4. M. Takeoka, and M. Sasaki, "Discrimination of binary orthogonal states with linear optics and continuous photon counting," IQEC and CLEO-PR, Nihon Toshi Kaikan, Tokyo, Japan, 15 Jul (2005).
5. M. Fujiwara, and M. Saskai, "Performance of a Charge Integration Photon Detector for telecom-band," IQEC and CLEO-PR, Nihon Toshi Kaikan, Tokyo, Japan, 14 Jul (2005).
6. M. Takeoka, M. Sasaki, P. van Loock, and N. Luetkenhaus, "Quantum state discrimination via linear optics and photon counting," European Quantum Electronics Conference (EQEC2005). Munich, Germany, 15 June (2005).
7. M. Takeoka, "Implementation of projective measurements with linear optics and continuous photon counting," Workshop on quantum information processing with linear optics(QUIPROLO II), Bristol, England, 30 March (2005).
8. M. Sasaki, "EPR beams and photon number detector for non-Gaussian operations with continuous variables," (Invited talk) ESF-JSPS Frontier Science Conference Series for Young Researchers, Kanagawa, Japan, 15 March (2005).
9. M. Takeoka, M. Sasaki, and P. van Loock, "Design of POVMs with linear optics and continuous measurement," Photonics Asia 2004, Beijing, China, 11 November. (2004).
10. A. Kitagawa, K. Yamamoto, K. Nagata, M. Takeoka, and M. Sasaki: “Quantum state engineering with entangled squeezed states and photon number detector,” Photonics Asia 2004, Beijing, China 11 Nov. (2004).
11. M. Sasaki, A. Hasegawa, T. Kishimoto, J. Ishi-Hayae, and F. Minami," Decoherence suppression of semiconductor excitons by bang-bang control," EQIS'04, Tokyo, Japan, 5 September (2004).
12. M. Takeoka, and M. Sasaki, "Implementing quantum measurement with restricted tools: Information theoretical analysis," EQIS'04, Tokyo, Japan, 4 September (2004).
13. J. Hayase, and T. Ishihara, "Room temperature polariton photoluminescence in a two-dimensional array of inorganic c-organic hybrid-type quantum-wells," ICPS 2004, Arizona, USA, 29 July (2004).
14. M. Fujiwara, and M. Saskai: “Photon number resolving detectors at telecommunication wavelengths,” QCMC 2004, Glasgow, UK, 25 July (2004).
15. M. Fujiwara, M. Sasaki, and M. Akiba: “Performance of a GaAs JFET at cryogenic temperature for faint light detection system,” SPIE 2004, 22 June (2004).

16. M. Takeoka: “Discrimination of quantum states with linear optics and continuous photon counting,” Xth International Conference on Quantum Optics, Minsk, Belarus, 1-3 June (2004).
17. K. Hirosawa, H. Furumochi, A. Tada, F. Kannari, and M. Takeoka: “Ultrashort-pulse squeezing with microstructured fibers and spectral filtering,” CLEO/IQEC, San Francisco, USA, 18 May (2004).
18. M. Sasaki: “EPR beams and photon number detector for non-Gaussian operations with continuous variables,” ESF-JSPS Frontier Science Conference Series for Young Researchers, Kanagawa, Japan 15 March (2004).
19. M. Sasaki: “Coding Technologies for Quantum Communications”, International Symposium on Quantum Info-Communications and Related Quantum Nanodevices, Mita Kaigisho Auditorium, Tokyo, Japan, 12 March(2004). (Invited).
20. M. Fujiwara, and M. Sasaki: “Development of a Photon Number Resolving Detector in Telecommunication Wave Band” International Symposium on Quantum Info-Communications and Related Quantum Nanodevices, Mita Kaigisho Auditorium, Tokyo, Japan, 11 March(2004).
21. J. Mizuno, M. Sasaki, K. Wakui, and A. Furusawa: “Quantum Dense Coding Using 2-Mode Squeezed States” International Symposium on Quantum Info-Communications and Related Quantum Nanodevices, Mita Kaigisho Auditorium, Tokyo, Japan, 11 March(2004).
22. M. Sasaki: “Small Scale Quantum Computing for Quantum Communications—From theory to experiment—”**,** Japan German Colloquium 2004 on Quantum Optics, organized by JSPS and MPG Wildbad Krueuth,Germany, 10 February(2004). (Invited)
23. J.A.Vaccaro, Y. Mitsumori, S.M.Barnett, E. Andersson, A.Hasegawa, M.Takeoka, and M.Sasaki: “Quantum data compression”, Stochastic Altorithms: Foundations and Applications Hatfield, September (2003). (Invited)
24. Y. Mitsumori, J.A. Vaccaro, S. M. Barnett, E. Andersson, A. Hasegawa, M. Takeoka, and M. Sasaki: "Implementing quantum noiseless coding using linear optics" EQIS'03, Kyoto, Japan, 5 September (2003).
25. M. Sasaki, A. Hasegawa, Y. Mitsumori, and F. Minami: "Theory of active dephasing control in qubit array" The International Conference on Dynamical Processes in Excited States of Solids(DPC '03), Christchurch, New Zealand, 4 August(2003).
26. Y. Mitsumori, Y. Okubo, A. Hasegawa, M. Sasaki, and F. Minami: "Optical selection rule of hyper Rayleigh scattering in resonance with excitonic wave function in ZnSe" The International Conference on Dynamical Processes in Excited States of Solids(DPC '03), Christchurch, New Zealand, 4 August(2003).
27. A. Hasegawa, T. Kishimoto, Y. Mitsumori, M. Sasaki, and F. Minami: "Multi-wave-mixing of two dimensional excitons in semiconductors" The ernational Conference on Dynamical Processes in Excited States of Solids, Christchurch, New Zealand, 4 August(2003).
28. H.Sekiguchi, K. Ikeda, F. Minami, J. Yoshino, Y. Mitsumori, H. Amauchi, T. Nagao, and H. Sasaki: “Photon Bottleneck effects in InAs/GalnP Quantum dots”, The International Conference on Dynamical Processes in Excited States of Solids(DPC '03), Christchurch, New Zealand, 4 August(2003).
29. Y. Mitsumori, H. Maruki, A. Hasegawa, F. Minami, M. Sasaki："Exciton Rabi Oscillation in Semiconductor Quantum Dots" The 10th International Workshop on Femtosecond Technology FST 2003 TB-3July 17 (2003). (Invited)
30. M. Takeoka and M. Sasaki, M. Ban: "Design of an optimal quantum receiver for interferometric sensing device" European Quantum Electronics Conference 2003 (EQEC 2003), Munich, Germany, June 22-27 (2003).
31. A. Carlini and M. Sasaki: "CPTP mappings, repeaters in lossy quantum channels, and state-dependent quantum cloning", ERATO workshop on Quantum Information Science 2002 (EQIS'02), Sanjo-Kaikan, Tokyo, JAPAN, September 5--8, (2002).
32. M. Sasaki and M. Takeoka: "Quantum channel coding -Theory and Experiment-", ERATO workshop on Quantum Information Science 2002 (EQIS'02), Sanjo-Kaikan, Tokyo, JAPAN, September 5--8, (2002). (Invited)
33. Y. Mitsumori, H. Maruki, A. Hasegawa, F. Minami, M. Sasaski: "Photon echoes form GaAs quantum dots", 26th International Conference on the Physics of Semiconductors (ICPS26), Edinburgh, UK, P218, July 28-- Aug. 2 (2002).

34. A. Hasegawa, T. Kishimoto, Y. Mitsumori, Y. Sasaki, and F. Minami: "Temporal behavior of Quantum Interfered Polarization between Two Excitons", 26th International Conference on the Physics of Semiconductors, Edinburgh, England, P44, July 28-- Aug. 2 (2002).
35. M. Sasaki, M. Fujiwara, M. Takeoka, and J. Mizuno: "Quantum decoder for single photon communication", The Sixth International Conference on Quantum Communication, Measurement, and Computing (QCMC'02), MIT, Massachusetts, USA, July 22--26, (2002).
36. M. Takeoka and M. Sasaki: "Two-frequency-mode entanglement generation inside an optical pulse by a nonlinear fiber and spectral pulse shaping", The Sixth International Conference on Quantum Communication, Measurement, and Computing (QCMC'02), MIT, Massachusetts, USA, Jul. 22--26, (2002).
37. M. Takeoka, M. Ban, and M. Sasaki: "Continuous variable teleportation as a quantum channel", The IXth International Conference on Quantum Optics (ICQO'2002), Raubichi, Belarus, May 14--17, (2002).
38. S. Matsuura, M. Akazaki, Y. Sozaki, H. Kaneda, T. Nakagawa, M. A. Patrashin, M. Shirahata, M. Fujiwara, T. Doi, Y. Hibi, T. Hirao, M. Kawada, H. Nagata, H. Shibai, T. Watabe, M. Noda: “Current status of the detector development for the Far-Infrared Surveyor (FIS) on ASTRO-F”, Far-IR, Sub-MM and MM Detector Technology Workshop, 1—3 April 2002, Monterey, California, USA, 2-03, (2002).
39. S. Matsuura, Y. Isozaki, M. Shirahata, M.A. Patrashin, H. Kaneda, T. Nakagawa, M. Fujiwara, M. Kawada, H. Shibai, T. Hirao, T. Watabe: “Monolithic Ge:Ga two-dimensional array detector for the FIS instrument on the ASTRO-F satellite”, SPIE Astronomical Telescopes and Instrumentation: Space Telescopes and Instruments, 24—28 August 2002, Hilton Waikoloa Village Hotel, Waikoloa, Hawaii USA, 4850-129, (2002).
40. 武岡 正裕（通信総研），藤島 大輔（慶応大），大野 公久（慶応大），神成 文彦（慶応大） "Optimization of ultrashort pulse squeezing in a nonlinear fiber by using the Fourier pulse shaping technique" 17th Interdisciplinary Laser Science Conference 2001/10/17, Long Beach, California.
41. 武岡 正裕（通信総研），藤島 大輔（慶応大），坂田 丞（慶応大），神成 文彦（慶応大） "Optimization of Ultrashort Pulse Squeezing in Nonlinear Fibers by an Initial Pulse Shaping" CLEO/Pacific Rim 2001、2001/07/17、幕張
42. 飛岡 秀明（東工大），三森 康義（通信総研），南 不二雄（東工大），長谷川 敦司（通信総研） "Time-resolved three-pulse photon echoes in GaSe" International Conference on Dynamical Processes in Excited States of Solids 2001/07/02、Lyon.
43. 藤島 大輔（慶応大），武岡 正裕（通信総研），神成 文彦（慶応大） "The optimization control of soliton squeezing in nonlinear fibers using a pulse shaper and a spectral filter" Quantum Electronics and Laser Science Conference (QELS 2001) 2001/05/06, Baltimore, Maryland.

国内学会発表

1. 佐々木 雅英、「スクィーズド光と光子数測定に基づく量子情報処理」第 10 回光波シンセシス 研究会「量子情報のための光波シンセシス」
   東京大学 生産技術研究所（東京）、6 月 24 日（2005）.
2. 武岡 正裕, 佐々木 雅英、「線形光学素子と光学測定による直行 2 量子状態の識別」第 12 回量子情報技術 研究会、NTT 厚木研究開発センタ（神奈川）、5 月 13 日(2005).
3. 藤原 幹生, 佐々木 雅英 :「通信波長帯 charge integration, photon detector(CIPD)の性能」日本物理学会第 60 回年次大会、東京理科大学 野田キャンパス、3 月 27 日(2005).
4. 鈴木 重成, 辻野 賢治, 神成 文彦, 佐々木 雅英 :「光源のパルス化が及ぼす単一光子スクィーズド状態測定への影響」日本物理学会第 60 回年次大会、東京理科大学 野田キャンパ ス、3 月 27 日(2005).
5. 北川 晃, 和久井 健太郎, 武岡 正裕, 佐々木 雅英 :「非ガウス型測定を用いたスクイーズド状態の操作とデンスコーディングへの応用」第 11 回量子情報技術研究会、京都大学、12 月 7 日(2004).

6. 武岡 正裕, 和久井 健太郎, 佐々木 雅英、「量子符号化：原理実証から非ガウス制御の実現に向けて」第 11 回量子情報技 術研究会、京都大学、11 月 11 日(2004) (招待講演)
7. 早瀬 潤子, 長谷川 敦司, 岸本 直, 三森 康義, 南 不二雄、佐々木 雅英、「多光波混合による励起子のデコヒーレンス制御」日本物理学会 2004 年秋季大 会、青森大学、9 月 13 日(2004).
8. 廣澤 賢一, 多田 睦, 古用 博人, 神成 文彦, 武岡 正裕, 佐々木 雅英、「超短パルスレーザのフォトニッククリスタルファイバ伝搬による周波数モー ド間量子相関形成」平成 16 年度電気学会東京支部連合研究会光・量子デバイス研究会 東京電機大学、9 月 10 日(2004).
9. 佐々木 雅英 :「光ガウス状態の非ガウス的制御と量子符号化」第 42 回茅コンファレンス、宮城蔵王ロイヤルホテル、8 月 23 日(2004) (招待).
10. 武岡 正裕, 佐々木 雅英, Peter van Loock, Norbert Luetkenhaus :「線形光学素子と連続 測定を用いた量子状態の識別」第 10 回量子情報技術研究会、学習院大学、5 月 24 日(2004).
11. 岸本 直, 長谷川 敦司, 三森 康義, 佐々木 雅英, 南 不二雄 :「半導体中の励起子のデコヒーレンス制御」日本物理学会第 59 回年次大会 九州大学（福岡）、3 月 29 日(2004).
12. 廣澤 賢一, 多田 睦, 古用 博人, 神成 文彦, 武岡 正裕 :「フォトニッククリスタルファイバーを用いたフェムト秒パルス光子数スクィージング」応用物理学会春季講演会 東京工科大学、3 月 28 日(2004).
13. 三森 康義, 長谷川 敦司, 佐々木 雅英, 南 不二雄 :「半導体量子ドットの励起子ラビ振動」量子情報通信と量子ナノデバイスに関する国際シンポジウム 三田共用会議所（東京）、3 月 11 日(2004).
14. 武岡 正裕, 佐々木 雅英 :「量子情報通信の基本問題と最近の発展」日本学術振興会 未踏・ナノデバイステクノロジー第１５１委員会 伊東（静岡県）、1 月 30 日(2004)
15. 水野 潤, 和久井 健太郎, 古澤 明, 佐々木 雅英 :「2 モードスクイーズド状態を用いた通信路に関する性能評価」電子通信情報学会 電子情報技術時限研究専門委員会 第 9 回量子情報技術研究会 NTT 厚木研究開発センター講堂, 12 月 12 日(2003)
16. 佐々木雅英, 中村和夫 :「量子情報通信 ー限りなく早く、そして絶対安全にー 」第 105 回 通信総合研究所研究発表会 丸の内ビルディング(東京)11 月 19 日（2003）.
17. 武岡 正裕, 番 雅司, 佐々木 雅英 :「量子状態フィルタリングのための最適量子測定」日本物理学会 2003 年秋季大会 23pTF-3, 岡山大学(岡山), 9 月 23 日(2003)
18. 岸本 直, 長谷川 敦司, 三森 康義, 佐々木 雅英, 南 不二雄 :「２次元半導体における多光波混合２」日本物理学会 2003 年秋季大会 岡山大学(岡山), 9 月 22 日(2003)
19. 和久井 健太郎, 水野 潤, 古澤 明, 佐々木 雅英 :「2 モードスクイーズド状態を用いた通信路に関する性能評価」日本物理学会 2003 年秋季大会 21pTF-15 岡山大学（岡山）, 9 月 21 日(2003)
20. 藤原 幹生, 佐々木 雅英 : 「通信波長帯光子数識別器のための積分型読み出し回路の信頼性評価実験」日本物理学会 2003 年秋季大会 21pTF-6, 岡山大学（岡山）, 9 月 21 日(2003)
21. 三森 康義, 長谷川 敦司, 南 不二雄, 佐々木 雅英 :「半導体量子アイランド中の励起子四光波混合 II」日本物理学会秋の分科会 岡山大学（岡山）, 9 月 20 日(2003)
22. 三森 康義, 長谷川 敦司, 南 不二雄, 佐々木 雅英 :「量子ドットの光学的ラビ振動」物質材料機構ナノマテリアル研究所 つくば市（茨城）8 月 18 日(2003)
23. 三森義康, 丸木浩代, 長谷川敦司, 南不二雄, 佐々木雅英 「Exciton Rabi Oscillation in Semiconductor Quantum Dots」FST 2003 フェムト秒テクノロジー国際ワークショップ 幕張（千葉)7 月 17 日（2003）
24. 佐々木 雅英, 長谷川 敦司, 三森 康義, 岸本 直, 番 雅司, 内山 智香子, 南 不二雄 :「Non-linear optical Spectroscopy for Decoherence in Quantum Dot Array」QIT8 北海道大学 学術交流会館, 6 月 30 日(2003)

25. 藤原 幹生, 秋葉 誠, 佐々木雅英 :「通信波長帯光子数識別器のための InGaAs pin photodiode 低温特性評価実験」日本物理学会 第 58 回年次大会　30pXB-12, 東北大学（宮城）, 3 月 30 日(2003)
26. 佐々木雅英, 三森 康義, J.A.Vaccaro, S.M. Barnett, E. Andersson, 長谷川敦司, 武岡 正裕:「量子情報源符号化の実験的検証について」日本物理学会 第 58 回年次大会 30pXB-14, 東北大学（宮城）, 3 月 30 日（2003）
27. 武岡 正裕, 藤原 幹生, 水野 潤, 番 雅司, 佐々木 雅英: "干渉計測のための量子最適受信機の設計", 日本物理学会 第 58 回年次大会 30pXB-13, 東北大学(宮城), 2003 年 3 月 28--31 日。
28. 長谷川敦司, 岸本直, 三森義康, 佐々木雅英, 南不二雄　「２次元半導体における多光波混合」日本物理学会　第 58 回年次大会　29aYE-9, 東北大学(宮城), 3 月 29 日(2003)
29. 三森康義, 吉野淳二, 宮島俊紀, 関口洋義, 南不二雄　「Submonolayer-InAs 量子構造の光学特性評価」第 50 回応用物理学関係連合講演会　29p-ZE-9, 神奈川大学(神奈川), 3 月 29 日(2003)
30. 三森義康, 丸木浩代, 長谷川敦司, 南不二雄, 佐々木雅英　「半導体量子ｱｲﾗﾝﾄﾞ中の励起子四光波混合」日本物理学会　第 58 年回次大会　29aYE6, 東北大学(宮城), 3 月 29 日(2003)
31. 三森康義, 大岩顕, T.Slupinski, 樫村之哉, 丸木浩代, 南不二雄, 宗片比呂夫:「III-V 族強磁性半導体の光スピン注入磁化反転」第 50 回応用物理学関係連合講演会　28p-ZH-8, 神奈川大学(神奈川), 3 月 28 日(2003)
32. 佐々木雅英: 「量子コンピュータが開く通信の未来」第 4 回量子コンピュータサロン、（財）新機能素子研究開発協会、2003 年 2 月 7 日。
33. 三森康義、長谷川敦司、佐々木雅英 :「半導体量子ドットにおけるコヒーレンスとラビ振動」筑波大学物理学科物理学コロキウム，11 月 29 日（2002）
34. 秋葉誠, 藤原幹生, 佐々木雅英 :「GaAs JEET を使用したリセット回路」日本天文学会, 10 月 9 日（2002）
35. 丸木浩代，南不二雄，長谷川敦司，三森康義，佐々木雅英 :「半導体量子アイランド中の励起子分極のラビ振動Ⅱ」日本物理学会秋の分科会，9 月 9 日（2002）
36. 岸本直，南不二雄，長谷川敦司，三森康義 :「位相緩和とエネルギー緩和」，日本物理学会秋の分科会，9 月 8 日（2002）
37. 平岡 卓爾, 米澤 英宏, 山崎 淳之介, 和久井 健太郎, 武井 宣幸, 青木 隆朗, 古澤 明, 水野 潤, 藤原 幹生, 佐々木 雅英:「直交位相成分スクイーズド光の生成 II」, 日本物理学会 2002 年秋季大会 9aXF-5, 中部大学(愛知), 9 月 6--9 日 (2002).
38. 米澤 英宏, 平岡 卓爾, 山崎 淳之介, 和久井 健太郎, 武井 宣幸, 青木 隆朗, 古澤 明, 水野 潤, 藤原 幹生, 佐々木 雅英:「直交位相成分スクイーズド光の生成 I」, 日本物理学会 2002 年秋季大会 9aXF-4, 中部大学(愛知), 9 月 6--9 日 (2002).
39. 武岡 正裕, 藤原 幹生, 水野 潤, 佐々木 雅英:「量子符号化利得の原理実証」, 日本物理学会 2002 年秋季大会 9pXE-7, 中部大学(愛知), 9 月 6--9 日 (2002).
40. 三森康義, 長谷川敦司, 佐々木雅英:「半導体量子ドットにおけるコヒーレンスとラビ振動」,量子情報技術研究会北海道地区第 15 回研究会, 北海道大学(北海道), 6 月 13 日 (2002).
41. 佐々木 雅英, 武岡 正裕:「量子符号化 ; 理論と実験」, 量子情報技術研究会北海道地区第 15 回研究会, 北海道大学(北海道), 6 月 13 日 (2002).
42. 三森康義, 丸木浩代, 長谷川敦司, 南不二雄, 佐々木雅英:「半導体量子ドットにおけるコヒーレンスとラビ振動」, 第 6 回量子情報技術研究会(QIT6) 17, 京都大学(京都), 5 月 27--28 日 (2002).
43. 佐々木 雅英, 水野 潤:「量子情報通信の基礎」第 49 回応用物理学関係連合講演会(2002 年春季) 29p-YM-4, 東海大学(神奈川), 3 月 27--30 日 (2002).

44. 三森康義, 樫村之哉, 大岩顕, 守谷頼, T. Slupinski, 南不二雄, 宗片比呂夫:「(Ga,Mn)As 系薄膜の光誘起スピン-キャリアダイナミクス」, 第 49 回応用物理学関係連合講演会 (2002 年春季) 29a-p10-9, 東海大学(神奈川), 3 月 27--30 日 (2002).
45. 藤原幹生, 秋葉誠, 佐々木雅英「極低温動作 GaGa JFET の高ゲート入力インピー ダンスにおける性能」第 49 回応用物理学関係連合講演会（2002 年春）29a-YK-4　平成 14 年 3 月 29 日　東海大学.
46. 長谷川 敦司（通信総研）, 岸本 直（東工大）, 三森 康義（通信総研）, 南 不二雄（東工大）, 佐々木 雅英（通信総研）「量子ビートの位相操作１　ートランジェントグレーティングー」日本物理学会第 57 回年次大会 、平成 14 年 3 月 27 日、立命館大学
47. 岸本 直（東工大）, 長谷川 敦司（通信総研）, 三森 康義（通信総研）, 佐々木 雅英（通信総研）, 南 不二雄（東工大）「量子ビートの位相操作２　ー時間分解フォトンエコーー」日本物理学会第 57 回年次大会、平成 14 年 3 月 27 日、立命館大学
48. 三森 康義（通信総研）, 丸木 浩代（東工大）, 長谷川 敦司（通信総研）,南 不二男（東工大）, 佐々木 雅英（通信総研）「半導体量子アイランドにおける励起子分極のラビ振動」日本物理学会第 57 回年次大会、平成 14 年 3 月 27 日、立命館大学
49. 丸木 浩代（東工大）, 三森 康義（通信総研）, 長谷川 敦司（通信総研）, 佐々木 雅英（通信総研）, 南 不二男（東工大） 「半導体量子アイランドにおける励起子の位相緩和とエネルギー緩和」日本物理学会、平成 14 年 3 月 27 日、立命館大学
50. 武岡 正裕（通信総研）, 佐々木 雅英（通信総研）, 藤島 大輔（慶応大）, 神成 文彦（慶応大） 「光ファイバによる超短パルス光子数スクイージングの最適化と周波数モード間エンタングルド状態生成の提案」日本物理学会第 57 回年次大会 、平成 14 年 3 月 24 日、立命館大学
51. 藤島 大輔（慶応大）, 武岡 正裕（通信総研）, 神成 文彦（慶応大）「フェムト秒パルス波形整形器を用いた非線形ファイバ光子数スクイージングおよび量子相関の最適化制御」電子情報通信学会技術研究報告 (レーザ・量子エレクトロニクス) 、平成 13 年 6 月 15 日、機械振興会館
52. 秋葉誠, 藤原幹生, 佐々木雅英「極低温動作 GaAs J-FET の高入力抵抗下における特性評価」, 日本天文学会春季大会 W54a, 茨城大学(茨城), 3 月 28 日(2002).
53. 武岡 正裕（通信総研）, 番 雅司（日立基礎研）, 佐々木 雅英（通信総研）「連続量テレポーテーションと量子状態の非古典性」第５回 量子情報技術研究会、平成 13 年 11 月 12-13 日、NTT.
54. 中村和夫、佐々木雅英、「量子暗号・量子通信への小規模量子計算の応用について」東北大学電気通信研究所共同利用プロジェクト研究会「大規模量子コンピュータの実現に向けて」（仙台市）2001 年 9 月 27 日、28 日
55. 水野 潤, 藤原 幹生, 秋葉 誠, 川西 哲也, Barnett Stephen M., 佐々木 雅英 "Optimum detection for extracting maximum information from symmetric qubit sets" 日本物理学会 2001 年秋季大会 18aTB-12, 徳島文理大学(徳島), 9 月 17--20 日（2001）.
56. 丸木浩代、三森康義、細谷剛、南不二雄、長谷川敦司 :「半導体量子アイランド中の励起子移送緩和」, 日本物理学会 2001 年秋季大会 17pRE-10, 徳島文理大学(徳島), 9 月 17--20 日（2001）.
57. 水野 潤, 藤原 幹生, 秋葉 誠, 川西 哲也, Barnett Stephen M., 佐々木 雅英 "Optimum detection for extracting maximum information from symmetric qubit sets" 日本物理学会 2001 年 秋の分科会　18aTB-12　平成 13 年 9 月 18 日 徳島大学
58. 丸木 浩代（東工大）, 三森 康義（通信総研）, 細谷 剛（東工大）, 南 不二雄（東工大）, 長谷川 敦司（通信総研）「半導体量子アイランド中の励起子位相緩和」日本物理学会２００１年秋季大会、平成 13 年 9 月 18 日、徳島大学
59. 藤原幹生, 秋葉誠, 佐々木雅英「極低温動作 GaAs J-FET の低周波ノイズ削減手法」第 62 回応用物理学会学術講演会（2001 年秋）13p-ZF-6 平成 13 年 9 月 13 日愛知工業大学.

60. 藤島 大輔（慶応大）, 武岡 正裕（通信総研）, 神成 文彦（慶応大）「波形整形器を用いた非線形ファイバーでの光子数スクイージング最適化制御」第 62 回応用物理学会学術講演会 、平成 13 年 9 月 11 日、愛知工業大学.
61. 佐々木雅英、A. Carlini, A. Chefles: 「N個の有限次元量子系に対する最適位相評価」日本物理学会 2001 年春季大会（中央大学）、27aYN-10. (2001).
62. 佐々木雅英 :「量子通信の基礎理論」量子エレクトロニクス研究会「量子情報処理」(軽井沢), 2001.1.25

(3)特許出願　　※委託契約に基づく研究機関からの出願

特願 2004-242676(2004.8.23)

(4)受賞等

①受賞

【小林グループ】

平成 17 年　5 月　国際時間分解振動分光学会賞　　小林　孝嘉
平成 17 年　10 月　松尾財団学術賞受賞　　小林　孝嘉
平成 17 年　10 月　台湾交通大学栄誉教授称号　　小林　孝嘉

②新聞報道

【富田グループ】

1. 日本工業新聞(2002 年 5 月 24 日) 「量子暗号用の光子受信感度 10 倍のシステム開発」
2. 日本経済新聞（2004 年 3 月 12 日)「世界最長の 150Km 単一光子伝送に成功」
3. 日本経済新聞(2004 年 9 月 27 日) 「１００ｋｂｐｓの暗号鍵生成レートを実現」

【小林グループ】

1. 日刊工業新聞　（2005 年 9 月 8 日）「量子もつれ合い効率生成」
2. 科学新聞　（2005 年 9 月 16 日）「量子暗号開発へ一歩―小林東大教授ら成功―」

【佐々木グループ】

1. 日本経済新聞、2003 年 5 月 25 日
「太陽系外とも光通信可能　通総研　量子技術で実内実験　衛星探査　範囲広がる」
2. 日経産業新聞、2003 年 11 月 26 日
「量子の手法活用情報を圧縮・復元　総務省が実験成功」
3. 科学新聞、2003 年 12 月 5 日
「通信総研　量子効果による情報圧縮操作　世界初の原理実証成功」
4. 電波タイムズ、2003 年 12 月 1 日
・記事「CRL が正解で初めて実証　量子情報源符号化」
・コラム「記者席」「スタート台に立った量子技術　量子暗号は 5 年以内に実用化」

6　研究期間中の主な活動

(1) ワークショップ・シンポジウム等

年月日	名称	場所	参加人数	概要
H13.10.15 -16	量子絡み合い制御に関する研究会	つくば国際会議場	22 人	研究進捗報告と研究計画の摺り合わせ、研究協力可能性探索等
H14.4.22 -23	ERATO 今井Ｐｊ．＆CREST 中村チーム合同研究会	つくば国際会議場	35 人	相互交流をより深める
H14.9.25 -27	量子絡み合い制御に関する研究会	玉川大学	29 人	研究進捗報告と研究計画の摺り合わせ、研究協力可能性探索等
H15.4.22 -24	CREST 中村チーム全体集会	通信総合研究所	21 人	中間審査へ向けた総合討論
H16.9.14 -15	CREST 中村チームミーティング	東京大学	12 人	成果報告と研究提案を議論する

(2) 招聘した研究者等

氏　名（所属、役職）	招聘の目的	滞在先	滞在期間
Charles H. Bennett (Fellow, IBM Watson Research Lab.)	講演、共同論文構成打ち合わせ	玉川大学学術研究所	13/3/9～ 13/3/16
Christopher A. Fuchs (Researcher, Bell Lab. Lucent Technology)	講演、共同論文構成打ち合わせ	玉川大学学術研究所	13/3/9～ 13/3/16
Benjamin Schumacher (Professor, Dept. of Physics, Kenyon College)	講演、共同論文構成打ち合わせ	玉川大学学術研究所	13/3/9～ 13/3/16
Norbert Lutkenhaus (Project Leader, MagiQ Technologies, New York)	講演、共同論文構成打ち合わせ	玉川大学学術研究所	13/3/9～ 13/3/16
Steven van Enk (Researcher, Bell Lab. Lucent Technology)	講演、共同論文構成打ち合わせ	玉川大学学術研究所	13/3/9～ 13/3/16
John A. Smolin (Researcher, IBM Watson Research Lab.)	講演、共同論文構成打ち合わせ	玉川大学学術研究所	13/3/9～ 13/3/16
Richard Jozsa (Professor, Dept. of Computer Science, Univ. of Bristol, UK)	共同研究と講演	情報通信研究機構　量子情報技術グループ	13/4/17～ 13/4/29
Erika Andersson (Marie Curie Research Fellow at the Univ. of Strathclyde)	共同研究と講演	情報通信研究機構　量子情報技術グループ	13/11/18～ 13/12/3
Alexander Kholevo (Professor, leading scientific researcher at Steklov Mathematical Institute, Russian Academy of Sciences	研究指導と討論	玉川大学学術研究所	16/1/25～ 16/2/7

7　結び

量子情報技術の中でも最も実用に近い量子暗号技術をより広い応用へと展開するには量子中継など、量子絡み合いに関する多様な要素技術の総合的な底上げが不可避であり、これは量子情報全体の技術レベルアップにも繋がる。本研究ではこれらの要素技術の高度化に注力すると共に、量子暗号の実用化促進、また将来の量子中継を含むシステムへ展開する為、量子暗号のシステム実証についても追加テーマとして取り組んだ。

量子絡み合い光源技術については、短パルス励起やフォトニック結晶ファイバを用いた高効率光子対源、さらに３光子の量子絡み合い光源にも成功した。量子通信路での量子状態の制御・変換技術については、量子操作の評価技術、単一量子ドットの分光と低温・強磁場環境での近接場顕微鏡開発、さらに量子情報源符号化と量子通信路符号化技術でシャノン限界を超える世界初の実証実験を実現し、理論でも量子絡み合いのコヒーレント状態への拡張や量子絡み合いの定量化と劣化の回復に関する成果を得た。受信部での量子状態の検出技術については、従来に比べて１桁以上の低ノイズ・高感度な単一光子検出器、誘導放出過程を用いた真空に感度を有する光子検出技術、光子数識別器などの開発に成功した。これらの要素技術の多くは、いずれも世界トップクラスの成果であり、広範な量子情報の基盤技術のレベルアップに大きく貢献し、目標は充分に達成したと言える。

また、量子暗号システムの実証実験については、上述の高性能単一光子検出器を用いた世界最長 150㎞の単一光子伝送、量子絡み合い光子対の片方の受信信号を伝令信号とした量子暗号システム、多値強度変調方式を用いたコヒーレント光通信による新量子暗号システムの開発に成功した。これらの成果は量子暗号の実用化促進、将来システムへの布石、また相補的システム技術の提供となるもので、追加テーマの目標を達成していると言える。

今後、要素技術についてはさらに高度化を進め、量子中継技術として集積するに足るレベルに引き上げることが重要である。特に量子状態の制御・変換技術については、一層の技術的飛躍を実現する必要がある。これは光を用いた量子コンピュータにも繋がる技術であり、今後の重要な課題である。量子暗号のシステム実証に関しては、ユーザ側でのセキュリティニーズの高まりとシステム側での使い易さ（コスト、伝送距離・ビットレートなども含む）の向上によって、市場の立ち上がりが左右され、今後、技術的にもシステムトータルのレベルアップが求められる。

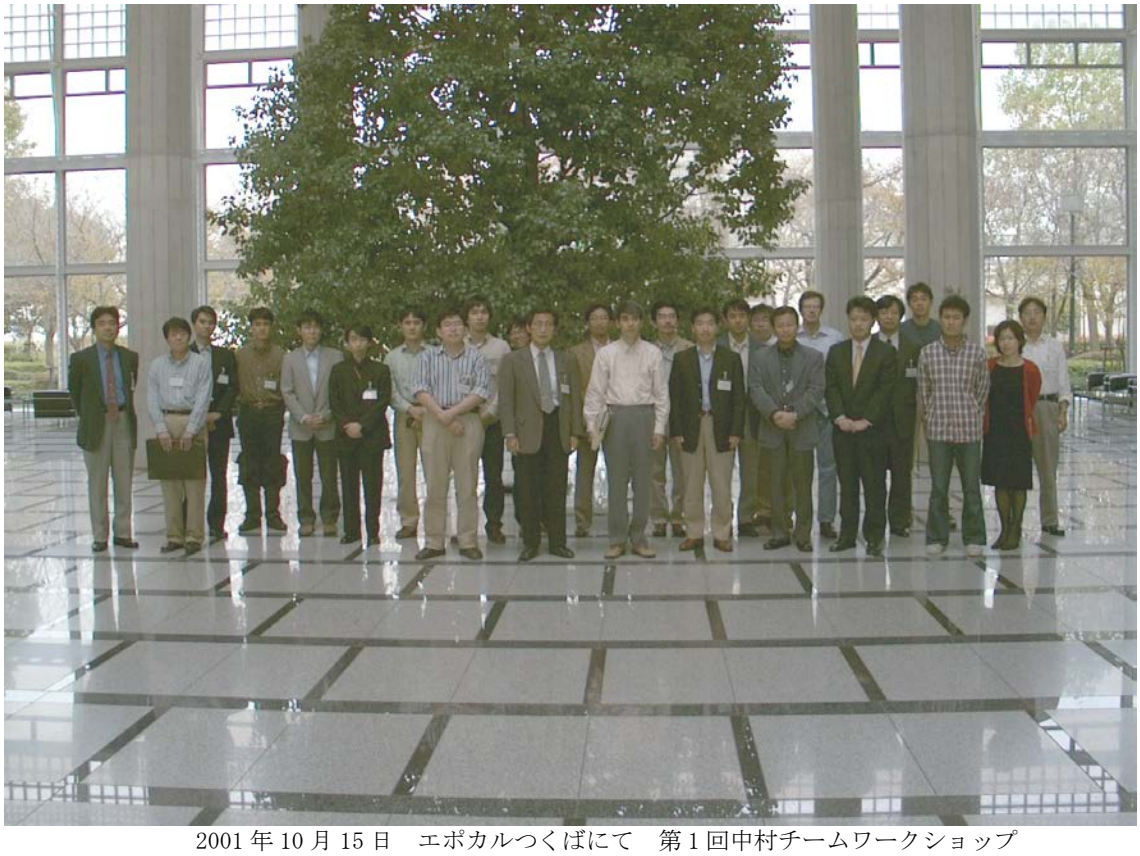
本チームの運営に関して、同じ目標について候補となる技術が複数ある場合でも、一つに絞る事はせず、敢えて並行して開発する道を選択した。これは量子情報技術が黎明期であり本命技術を定めるには時期尚早で、並行開発は量子情報技術全体のレベルアップには効果的であること、さらには将来的なユーザに対して目的に応じた技術的選択肢を複数用意しておくことは好ましいことと考えた為である。そのことが一因

でもあるが、チーム内のグループ間連携においては、比較的緩やかな運営を行った。

研究費の面では、費目の自由度の向上など、従来に比べて格段に良くなっているが、本研究の技術的困難さと比較すると資金の点では十分ではないと言える。今後、本分野への継続的な国の資金的援助を切望する。人材的には本チームから次代を担う若手研究者を日本国内外に輩出できたことは本プロジェクトの重要な成果として誇りに思う次第である。

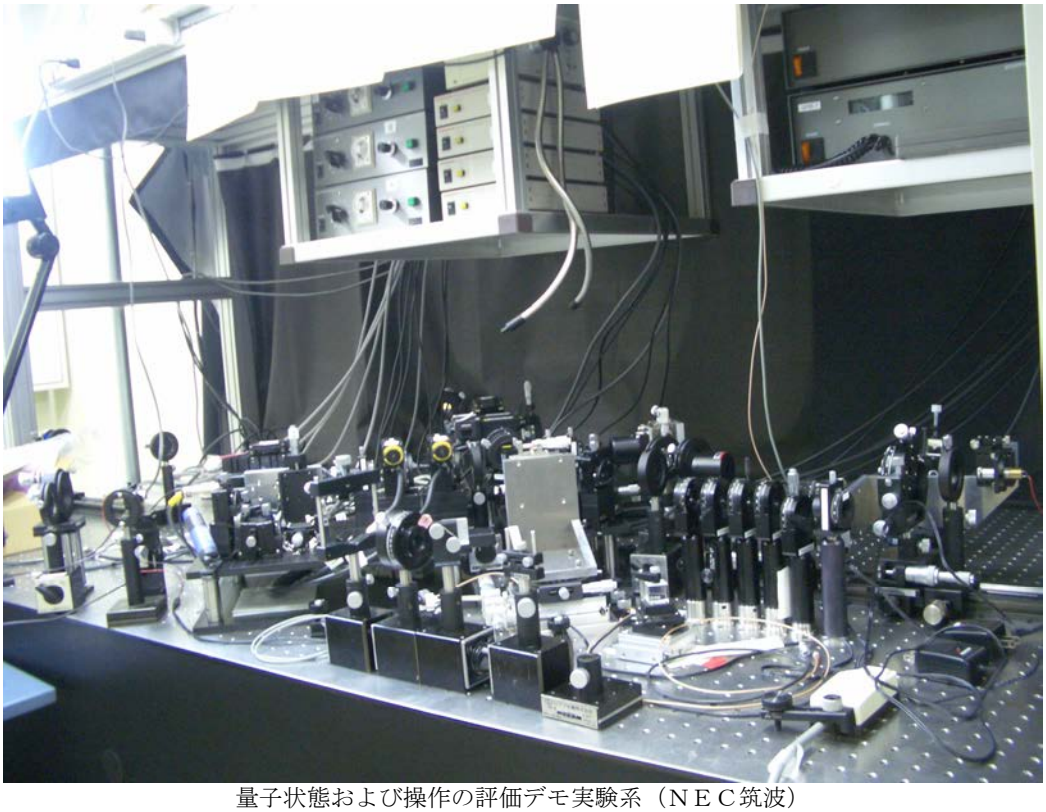
最後に、本プロジェクトを通じて、研究総括の菅野先生、領域アドバイザーの先生方から有益な御助言を頂けたことは、本チームの運営上、非常にプラスとなった。また本チームの遂行に際し、日頃、種々の事務業務を御担当頂いた JST 本部、本領域事務所の技術参事、事務参事を初めとするスタッフの方々には、心から感謝の意を表する次第である。

写真

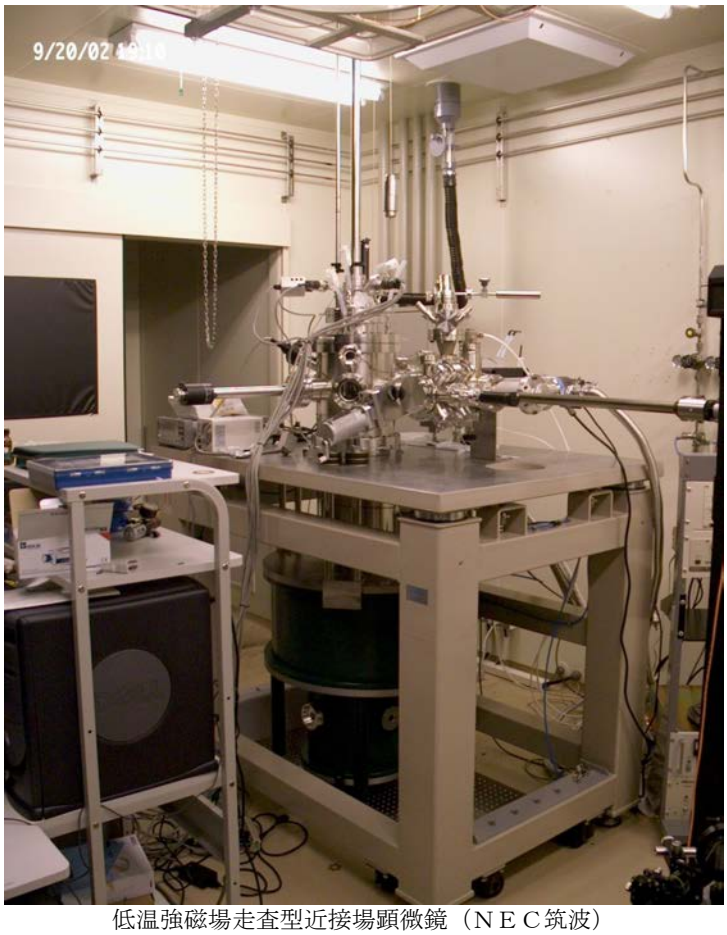


2001 年 10 月 15 日　エポカルつくばにて　第 1 回中村チームワークショップ

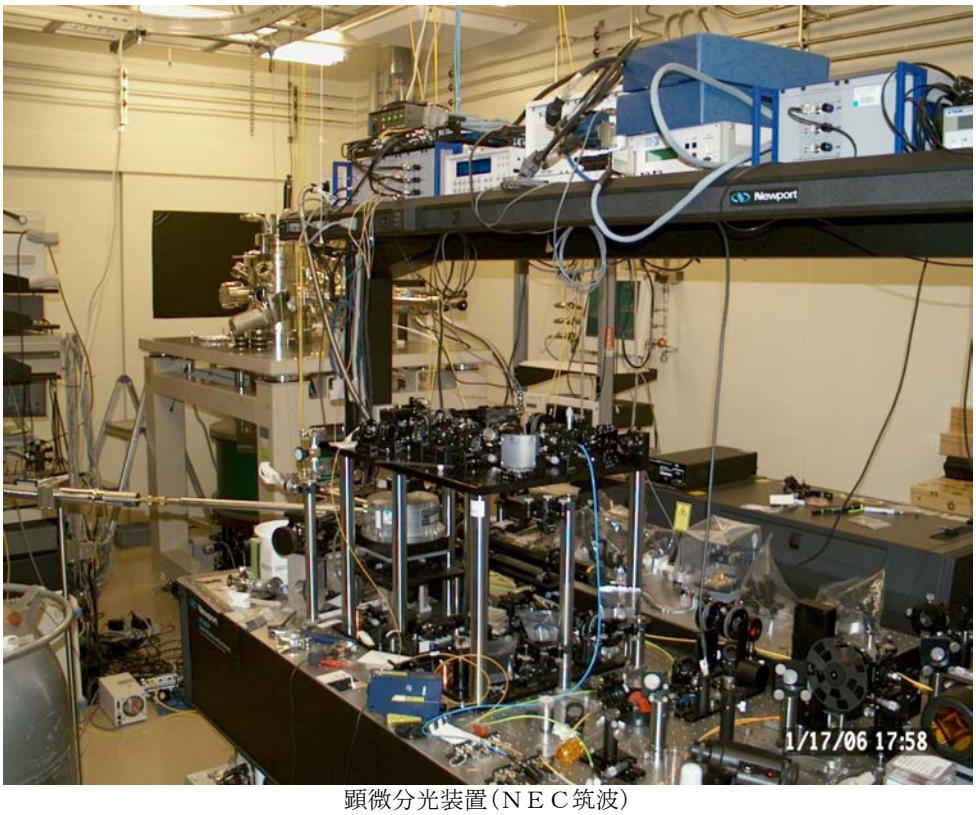
2001 年 10 月 15 日　中村研究代表の講演



量子状態および操作の評価デモ実験系（ＮＥＣ筑波）



低温強磁場走査型近接場顕微鏡（ＮＥＣ筑波）



顕微分光装置（ＮＥＣ筑波）