「量子情報処理システムの実現を目指した新技術の創出」
平成 15 年度採択研究代表者

井元　信之

（大阪大学大学院基礎工学研究科　教授）

「光子を用いた量子演算処理新機能の開拓」

１．研究実施の概要

本プロジェクトでは５ヶ年を通じ光子を用いた量子演算処理として、４光子の範囲でできる光子間ゲート操作、５光子以上の処理、連続量の情報処理、これらの基礎となるトモグラフィー技術、これらを総合した multiparty quantum computing について理論および実験の両面から追究し、基礎的デモンストレーションを行うとともに、より高度な実現に向けての課題と方向性についての知見を得ることを目的としている。平成 17 年度の研究の経過・成果・今後の見通しは以下の通りである。

多者間量子ネットワークへの展開を考えると、量子チャンネルとしてはノード間調整や active 補償を必要としない方式が望まれる。補助光子の付加およびその線形光学一括測定によって、その条件を満足しつつ位相雑音を除去する方法を考案した(PRL)。この方法によれば、他の系と絡み合いを持つ状態の送信も可能であり、量子暗号の場合には従来の方法で問題になるトロイの木馬攻撃を回避できる。今後は実験を行う。

量子暗号の安全性の理論では、現実的装置を仮定し無条件安全性および現実的盗聴に対する安全性の双方について知見を得、より具体的な安全性条件を明らかにした(PRA)。これにより一つのステップを踏み出したと考えるが、さらに種々提案されている量子暗号方式に対し安全性を理論面から押さえて行きたい

量子情報の性質はまだ解明すべきことが多々ある。その一つとして「補助系がある場合の量子ビットの確率的クローニング」を初めて扱い、補助系との相互作用によりクローニング確率が上がる場合（候補状態が３つ以上ある場合）と上がらない場合（候補状態が２つ以下の場合）があることを証明した(PRA)。

４光子以上の多光子による量子演算については、線形光学素子による量子制御ノットゲートの研究、それを用いた多光子量子回路の実現に向けた研究に取り組み、従来より簡便な方法を開発した(PRL)。類似の成果がクィーンズランド大学、マックスプランク量子光学研究所のグループからも独立にかつ同時に発表され、本成果は一般紙等でも幅広く報道された。この実現により、今後、複数の量子ゲートを用いた量子回路の実現が完全に視野に入ったと考えている。今後は、まず素子のエラー原因を同定し、より量子忠実度の高いゲ

ートの開発にむけた研究を進めると共に、２光子が一方の光路に出力される場合を検出するような素子の研究にも着手したい。一方非線形性を用いたゲートについての解析も行った(PRA)。

また、多光子量子回路の実現に向けて、2002 年に我々のグループの考案した量子もつれ合いフィルタを念頭に検討を進めた。これに関しては、クィーンズランド大学のジェレミ・オブライアン博士と共同して研究を進めている。ほぼその光学系の基本設計を終えた段階である。

単一光子源の開発に関しては、波長 1.55 ミクロンの、伝令信号付き単一光子源の開発に初めて成功した(JOSAB)。これまで報告されてきた伝令付き単一光子源は、通信波長帯域であるが連続光励起のもの（ジュネーブ大学、Magi-Q)、もしくはパルス励起だが可視域のもの（ジョンホプキンス大学）であり、それぞれ前者は量子リピーターなどの複数光子間干渉を用いた研究には使用できない事、後者は長距離通信に用いられない事、といった欠点を持っていた。今後は、より理想的な光子数分布の実現に向けた研究、ならびに、２光子干渉能力の評価などを進めたい。

連続変数量子情報処理については、モード同期パルス光を用いたパラメトリック増幅により 3dB をこえるスクイージングを実現した(Opt. Lett.)。さらに、２つのスクイーズド光を発生し、連続変数エンタングルメントの生成に初めて成功した。また、通信波長帯でのスクイージングでも大きな値を得た。これらは、今後の量子通信の進展に資する結果と考える。同じく連続変数の量子暗号では安全性解析を進める(PRA)とともに、光ファイバーを量子通信路とするプラグアンドプレイ方式と、昨年特許出願を行った自由空間を通信路とする同軸光学系方式の双方で量子鍵配送を実証することができた。プラグアンドプレイ方式では伝送距離 10km を達成し、今後より長距離高速化を目指す。

２．研究実施内容

雑音のある量子チャンネルにおける高忠実度量子通信は、以前 Nature に出版したエンタングルメント抽出法を進化させたもので、信号光子に続けて参照光子を同時に送り、線形光学素子による二つの光子の一括測定により雑音のみ打ち消して元の量子情報を残す方法である。理論的には、信号光子と参照光子を近接させ同じ雑音を受けるようにすることにより、二つの光子が張る拡大されたヒルベルト空間の中にデコヒーレンスの影響を受けない部分空間ができるので、それへの射影を線形光学と光子検出のみを用いて実用に足る成功確率で行うものである。

量子暗号の安全性の理論では、現実的盗聴法として従来「光増幅＋ビームスプリッティング」攻撃が考察されていたが、実は光増幅をパラメトリック増幅で行えば anti-cloning（増幅に伴い発生する共役波）が利用できてしまう。今回はそれも盗聴手段として取り入れることにより、従来よりさらに安全を保証するための条件を明らかにすることができた。

補助系がある場合の確率的クローニングは、従来の二つの理論を組み合わせ、さらに

LOCC(量子情報でよく用いられるパラダイム)的考察を行うことにより理論化に成功した。従来の二つの理論とは、一つは「補助系がある場合の決定論的クローニング」を否定的に解決した Jozsa の定理であり、もう一つは「(補助系がない場合の)確率的クローニング」が可能であることを示した Guo 等の論文である。

４光子以上の多光子による量子演算については、光路干渉計をいっさい不要にしたコンパクトで安定な量子制御ノットゲートの開発に成功した。これは、独自に考案した部分偏光ビームスプリッター(Partially Polarizing Beam Splitter, PPBS)を利用することで、以前我々の考案したシンプルなゲートに含まれていた２つの結合光路干渉計を不要にしたものである。

単一光子源の開発に関しては、波長 1.55 ミクロンの、伝令信号付き単一光子源の開発に初めて成功した(CLEO-Europe 発表)。これまで報告されてきた伝令付き単一光子源は、通信波長帯域であるが連続光励起のもの（ジュネーブ大学、Magi-Q)、もしくはパルス励起だが可視域のもの（ジョンホプキンス大学）であり、それぞれ前者は量子リピーターなどの複数光子間干渉を用いた研究には使用できない事、後者は長距離通信に用いられない事、といった欠点を持っていた。今後は、より理想的な光子数分布の実現に向けた研究、ならびに、２光子干渉能力の評価などを進めたい

連続変数量子情報処理については、パルス光を用いたパラメトリック増幅による連続変数エンタングルメントの生成に初めて成功した。これはパルス光のもつ高い瞬間強度と導波路による光の閉じ込め効果を利用して、シングルパスのパラメトリック増幅でスクイーズド光を発生し、さらに、２つのスクイーズド光を重ね合わせることで連続変数エンタングルメントを発生したものである。２つのホモダイン検出器で直交位相振幅の相関を測定し、量子雑音レベルよりも 0.7dB 小さくなることを確認した。この実験は波長 1.06μｍのピコ秒モード同期レーザーを光源として用いた。通信波長帯のスクイーズド光発生実験では、パルスモードのホモダイン検出で初めて 2dB を超えるスクイージングを観測することができた。また、パラメトリック過程によるプローブ光の減衰も 6dB という大きな値が得られた。

連続変数の量子暗号では、光ファイバーを量子通信路とするプラグアンドプレイ方式と、昨年特許出願を行った自由空間を通信路とする同軸光学系方式の双方で量子鍵配送を実証することができた。プラグアンドプレイ方式の伝送距離は 10km であり、平均パワーの増加と共に過剰雑音が増加する傾向が見られた。自由空間の伝送距離は最大で 5m であり、今後長距離化を進めたい。

３．研究実施体制

井元グループ

①研究分担グループ長：井元　信之（大阪大学大学院基礎工学研究科、教授）

②研究項目：多者間光子情報処理の研究

概要：4 光子の number-state 展開トモグラフィー、雑音性チャンネルを介した量子通信、エンタングルメント性質、4 光子 Wigner 分布関数トモグラフィー、連続量量子暗号安全性、controlled-U ゲート、マルチパーティーコンピューテーション実験発案。全体とりまとめ。

竹内グループ

①研究分担グループ長：竹内　繁樹（北海道大学･電子科学研究所、助教授）

②研究項目：多光子量子演算ゲートの研究

概要：５光子以上のゲート実現と量子回路、テレポーテーション的リピーター、制御 NOT の新提案および実現、単光子状態発生およびフォトンカウンティング技術発展、マルチパーティコンピューテーションへ多光子およびフォトンカウンティング技術。

平野グループ

①研究分担グループ長：平野　琢也（学習院大学、教授）

②研究項目：ホモダイン量子情報処理の研究

概要：パルス光スクイーズド光やエンタングルメントの効率的な発生およびパルス毎のホモダイン検出、連続変数を用いた光の量子ゲート、単一光子と連続変数とのハイブリッドな量子情報処理、PPLN waveguide 中のパラメトリック増幅、連続変数の量子暗号における空間伝送の実現、マルチパーティコンピューテーション実験へ連続変数技術。

４．主な研究成果の発表（論文発表および特許出願）

（１）　論文（原著論文）発表

井元グループ:

○ Ryo Namiki, M.Koashi and N.Imoto,” Cloning and optimal Gaussian individual attacks for a continuous- variable quantum key distribution using coherent states and reverse reconciliation”,Physical Review A,73,pp. 032302, 2006/3/2.

○ Koji Azuma, J.Shimamura, M.Koashi and N.Imoto, “Probabilistic cloning with supplementary information”, Physical Review A,72, pp.032335, 2005/9/28.

○ T. Yamamoto, M.Koashi and N.Imoto,” Faithful Qubit Distribution Assisted by One Additional Qubit against Collective Noise”, Physical Review Letters, 95, pp.040503, 2005/7/22.

竹内グループ：

○ R. Okamoto, H. F. Hofmann, S. Takeuchi and K. Sasaki, “Demonstration of an optical

quantum controlled-NOT gate without path interference", Phys. Rev. Lett., 95, 21, pp. 210506/1-4 (2005).

○ R. Okamoto, S. Takeuchi and K. Sasaki, "Detailed analysis of a single-photon source using gated spontaneous parametric downconversion", J. Opt. Soc. Am. B, pp.22, 11, pp.2393-2401 (2005).

○ H. Oka, S. Takeuchi and K. Sasaki, "Optical response of two-level atoms with reflection geometry as a model of a quantum phase gate", Phys. Rev. A, 72, pp.013816/1-7 (2005).

平野グループ

○ Ryo Namiki and Takuya Hirano: "Security of continuous-variable quantum cryptography using coherent states": Decline of postselection advantage", Physical Review A, vol. 72, No. 2,024301 (Aug. 2005).

○ T. Hirano, K. Kotani, T. Ishibashi, S. Okude, T. Kuwamoto: "3 dB squeezing by single-pass parametric amplification in a periodically poled KTiOPO4 crystal", Optics Letters, vol. 30, Issue 13, (July, 2005).

（２） 特許出願

H17 年度出願件数：0 件 (CREST 研究期間累積件数：2 件)