

「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17 年度採択研究代表者

井上 恭

大阪大学大学院工学研究科・教授

## 通信波長帯量子もつれ光子とその応用システム

### § 1. 研究実施の概要

量子もつれ光子は、特異な性質を持つ量子力学的状態として、世界的にその研究が進められている。本研究チームは、量子もつれ光子のファイバ通信への応用技術を開拓することを目的とし、通信波長帯での量子もつれ光子発生技術やその応用システム(主に量子暗号)、及びそれらの関連技術について研究を進めている。

量子もつれ技術に関しては、まず発生に関して、PPLN 内カスケード 2 次非線形過程による時間位置もつれ光子発生、シリコン細線導波路内四光波混合による識別不可能な光子発生、ループ構成 PPLN 偏波もつれ光子発生及びその識別不可能性の実証、などを行った。また、光パラメトリック量子もつれ光源から発生する複数光子対の影響を定量化した。システム実験としては、200km ファイバ伝送実験(世界最長)、正弦波ゲート APD 光子検出器による高速量子もつれ量子暗号実験(従来の 10 倍)、などを行った。

関連技術としては、量子鍵配送(QKD)に関して様々な研究を行った。デコイを使った 2 量子状態プロトコルの提案と無条件安全性証明、単一光子型 DPS(差動位相シフト)QKD の無条件安全性証明、同時光子検出モニター DPS-QKD の提案・性能評価、光前置増幅器を用いる巨視的コヒーレント光 DPS-QKD の性能評価、量子/古典波長多重伝送におけるラマン散乱の影響の定量化、などを行った。

今後は、上記を発展させ、さらに高性能な量子もつれ応用システム技術を実現していく。

### § 2. 研究実施体制

(1)「阪大」グループ(研究機関別)

① 研究分担グループ長:井上 恭(大阪大学、教授)

② 研究項目:量子通信システムの提案・評価

(2)「NTT」グループ(研究機関別)

① 研究分担グループ長:武居 弘樹(NTT、主任研究員)

② 研究項目: 時間位置もつれ光子を用いた量子通信実験・単一光子検出実験

(3)「産総研」グループ(研究機関別)

① 研究分担グループ長:吉澤 明男(産業技術総合研究所、主任研究員)

② 研究項目:偏波に基づく多光子間量子もつれ合い技術の開発

### § 3. 研究実施内容

(文中に番号がある場合は(4-1)に対応する)

#### ◆量子もつれ光子対の 200 km ファイバ伝送実験<sup>6)</sup>

NTT 開発による PPLN 導波路量子もつれ光子源と東芝欧州研究所開発による自己差分回路 InGaAs/InP-APD 単一光子検出器を用いて、量子もつれ光子対の 200 km(100 km x 2)ファイバ伝送実験を行い、明瞭度>79%以上の良好な干渉波形を得た。本結果は、量子もつれ光子対の長距離伝送の世界記録である。

#### ◆正弦波ゲート単一光子検出器を使った量子もつれ光子量子鍵配送の高速実験

日本大学開発による正弦波ゲート APD 光子検出器(ゲート周波数:500MHz)を用いて量子もつれ光子量子鍵配送(QKD)実験を行い、超伝導単一光子検出器を用いた従来実験の約 10 倍の鍵生成率(@短距離)を達成した。さらに、小芦(阪大)提案による「同時計数法」の採用により、100 km 伝送での安全鍵生成を実現した。

#### ◆シリコン細線導波路を用いた識別不可能光子対の発生実験

識別不可能な光子は量子情報通信における不可欠な構成要素である。今回、シリコン細線導波路中の自然放出四光波混合に基づく量子相関光子対源を用いて、独立な 2 光源からの単一光子の Hong-Ou-Mandel 量子干渉実験を行った。明瞭度 66%が得られ、独立光源からの識別不可能光子の発生を確認した。

#### ◆PPLN 導波路内カスケード 2 次非線形光学効果による時間位置もつれ光子対発生実験

PPLN 導波路に 1.5 $\mu$ m 帯の光を入力して波長 780 nm の第二高調波を発生させ、これをポンプ光として、パラメトリック下方変換(PDC)により同一導波路内で 1.5 $\mu$ m 帯量子相関光子対を発生することができる。この手法による相関光子対/時間位置もつれ光子対の発生に初めて成功し

た。これにより相関光子対源の簡便化が可能となる。

#### ◆PPLN 内 PDC による四光子偏波もつれ発生と量子干渉実験

経路内に PPLN 導波路を備えた偏波ビームスプリッタ付ファイバループにより、安定な偏波もつれ光子対源を構成し、2つの独立な光源を用いて偏波型の Hong-Ou-Mandel 量子干渉実験を行った。明瞭度 75% が得られ、独立光源からの識別不可能光子の発生を確認した。

#### ◆光パラメトリック量子もつれ光源の測定における複数光子対の影響の理論解析<sup>7)</sup>

パラメトリック下方変換や四光波混合などの自然パラメトリック過程に基づく量子もつれ発生源を用いた各種測定における複数光子対発生の影響を理論的に明らかにした。

#### ◆デコイを使用する二状態暗号の提案とその無条件安全性証明<sup>9)</sup>

単一光子の非直交2状態を用いる B92-QKD は、盗聴者が USD と呼ばれる測定法により2状態を確率的に識別することが可能であることから、長距離伝送は不可とされていた。これに対し、デコイ状態の使用により長距離化を可能とする方式を提案した。USD はデコイと信号を識別することができないため、従来方式における問題が解決される。方式提案とともにその無条件安全性証明を行った。

#### ◆単一光子を用いた DPS-QKD の無条件安全性証明<sup>10)</sup>

微弱コヒーレント光を用いる DPS (差動位相シフト) QKD は、構成が簡便で実用向けの QKD 方式であるが、無条件安全性は証明されていない。その証明の前段階として、単一光子 DPS-QKD の無条件証明を行った。証明は、送受信装置に制限を設けたうえで、考察システムと等価なエンタングルメント蒸留プロトコルを考え、そこでの受信者の測定をフィルター+Z 基底測定と分解し、そして盗聴操作とそれによるビットエラーとを関係付ける、という手法で行った。この手法により、無条件下における盗聴量を求めることに成功した。

#### ◆巨視的コヒーレント光 DPS-QKD

振幅の大きいコヒーレント光を用いる DPS 量子鍵配送方式は、従来の光受信器が使用可能であるため、実用向きの QKD システムと言える。これに関し、通常の光通信で一般的である光前置増幅器付き受信器を用いた場合のシステム性能評価を行った。このようなシステムでは、光増幅器雑音が主な雑音源となる。典型的な盗聴法であるビームスプリット攻撃及びインターセプトリセンド攻撃について考察した結果、伝送距離は数 10km となることが分かった。

#### ◆同時光子検出モニター DPS 量子鍵配送

DPS 量子鍵配送方式に対するもっとも強力な盗聴法として、連続クリック攻撃が知られている。これへの対策として、同時光子検出率モニター法を考案した。DPS-QKD では等確率で光子を

含むパルスが連続的に受信機へ到達するが、連続クリック攻撃が行われると、光子を含む数パルスが間欠的にやってくることになる。そこで、一定間隔の2時刻でともに光子が検出される回数を計数することにより、連続クリック攻撃を検知する。シミュレーションによりその有効性を示した。

#### ◆量子/古典波長多重伝送における自然ラマン散乱の影響

量子鍵配送では、量子状態を転送する量子チャンネルと基底情報や誤り訂正・秘匿性増強情報をやり取りする古典チャンネルが用いられる。システムの実用化のためには両者が同一ファイバ上で波長多重伝送することが有効であるが、その場合、古典チャンネル光から発生する自然ラマン散乱光子が障害となる。そこで、量子/古典チャンネルを波長多重した時のラマン散乱の影響を定量的に評価した。まずラマン散乱発生効率を測定し、その結果に基づいて量子チャンネルへの影響が軽微で納まる古典チャンネル光パワーを定量化した。

## § 4. 成果発表等

### (4-1) 原著論文発表

#### ● 論文詳細情報

1. B. Miquel(NTT) and H. Takesue(NTT), “Observation of 1.5  $\mu\text{m}$  band entanglement using single photon detectors based on sinusoidally gated InGaAs/InP avalanche photodiodes,” *New J. Phys.*, Vol. 11, 045006 (2009.4),  
doi:10.1088/1367-2630/11/4/045006
2. Q. Zhang(Stanford U.), H. Takesue(NTT), T. Honjo(NTT), K. Wen(Stanford U.), T. Hirohata(Hamamatsu Photon.), M. Suyama(Hamamatsu Photon.), Y. Takiguchi(Hamamatsu Photon.), H. Kamada(NTT), Y. Tokura(NTT), O. Tadanaga(NTT), Y. Nishida(NTT), M. Asobe(NTT) and Y. Yamamoto(Stanford U.), “Megabits secure key rate quantum key distribution,” *New J. Phys.*, Vol. 11, 045010 (2009.4)  
doi:10.1088/1367-2630/11/4/045010
3. Y. Iwai(Osaka U.), T. Honjo(NTT), K. Inoue(Osaka U.), H. Kamada(NTT), Y. Nishida(NTT), O. Tadanaga(NTT), and M. Asobe(NTT), “Polarization-independent, differential-phase-shift, quantum-key distribution system using upconversion detectors,” *Opt. Lett.*, Vol. 34, No. 10, pp. 1606–1608 (2009.5)  
doi:10.1364/OL.34.001606
4. H. Takesue(NTT) and B. Miquel(NTT), “Entanglement swapping using telecom-band photons generated in fibers,” *Opt. Express*, Vol. 17, No. 13, pp. 10748–10756 (2009.6)  
doi:10.1364/OE.17.010748
5. H. Takesue(NTT) and Y. Noguchi(Osaka U.), “Implementation of quantum state

- tomography for time-bin entangled photon pairs,” *Opt. Express*, Vol. 17, No. 13, pp. 10976–10989 (2009.6) doi:10.1364/OE.17.010976
6. J. F. Dynes(Toshiba), H. Takesue(NTT), Z. L. Yuan(Toshiba), A. W. Sharpe(Toshiba), K. Harada(NTT), T. Honjo(NTT), H. Kamada(NTT), O. Tadanaga(NTT), Y. Nishida(NTT), M. Asobe(NTT), and A. J. Shields(Toshiba), “Efficient entanglement distribution over 200 kilometers,” *Opt. Express*, 17, No. 14, pp. 11440–11449 (2009.7) doi:10.1364/OE.17.011440
  7. H. Takesue(NTT) and K. Shimizu(NTT), “Effects of multiple pairs on visibility measurements of entangled photons generated by spontaneous parametric processes,” *Opt. Commun.*, Vol. 283, No. 2, pp. 276–287 (2009.7) doi:10.1016/j.optcom.2009.10.008
  8. K. Tamaki(NTT), N. Lutkenhaus(U. Waterloo), M. Koashi(Osaka U.), and J. Batuwantudawe(U. Waterloo), “Unconditional security of the Bennett 1992 quantum-key-distribution scheme with a strong reference pulse,” *Phys. Rev. A*, Vol. 80, No. 3, 032302 (2009.9) doi:10.1103/PhysRevA.80.032302
  9. M. Lucamarini(U. Camerino), G. Di Giuseppe(U. Camerino), and K. Tamaki(NTT), “Robust unconditionally secure quantum key distribution with two nonorthogonal and uninformative states”, *Phys. Rev. A*, Vol. 80, No. 3, 032327 (2009.9) doi:10.1103/PhysRevA.80.032327
  10. K. Wen(Stanford U.), K. Tamaki(NTT), and Y. Yamamoto(Stanford U.), “Unconditional security of single-photon differential phase shift quantum key distribution”, *Phys. Rev. Lett.* Vol. 103, No. 17, 170503 (2009.10) doi:10.1103/PhysRevLett.103.170503
  11. K. Harada(NTT), H. Takesue(NTT), H. Fukuda(NTT), T. Tsuchizawa(NTT), T. Watanabe(NTT), K. Yamada(NTT), Y. Tokura(NTT), and S. Itabashi(NTT), “Frequency and polarization characteristics of correlated photon-pair generation using a silicon wire waveguide,” *IEEE J. Sel. Top. Quantum Electron.*, Vol. 16., No. 1., pp. 325–331 (2010.1) doi:10.1109/JSTQE.2009.2023338
  12. K. Tamaki(NTT) and G. Kato(NTT), “Quantum circuit for the proof of the security of quantum key distribution without encryption of error syndrome and noisy processing”, *Phys. Rev. A*, Vol. 81., No. 2., 022316 (2010.2) doi:10.1103/PhysRevA.81.022316

#### (4-2) 知財出願

- ① 平成21年度特許出願件数(国内 8件)
- ② CREST 研究期間累積件数(国内 25件)