

「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、冷却ファイバ内自然四光波混合/周期分極反転ニオブ酸リチウム(PPLN)導波路内パラメトリックダウンコンバージョン/シリコン細線導波路内自然四光波混合を利用した時間位置もつれ発生を行なった。また、ファイバーループ内にPPLNを配置した構成による偏波もつれ発生も行なった。さらに、これらにより発生させた量子もつれ光子の長距離ファイバ伝送(～100km)を行なった。特に、時間位相もつれについては、量子秘密鍵生成(over 50km×2)にも成功した。これらはいずれも、世界トップレベルの成果である。

関連技術としては、無中継量子暗号システムに関し、各種プロトコルの提案・評価及びDPS-QKD と呼ばれる独自方式による伝送実験を行なった。特に後者については、距離・鍵生成速度とも世界トップデータ(12bps@200km, 17kbps@105km)を記録している。その他、光子検出技術に関し、波長変換型検出器の開発、性能評価技術の開発、などを行なった。

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. 研究実施内容(文中にある参照番号は 4.(1)に対応する)

◆差動4値位相シフト(DQPS)QKD の提案・実証実験

DPS-QKD 方式は、構成が簡便/高速化に有利/光子数分岐攻撃に強い、などの利点を有するが、連続クリック攻撃と呼ばれる盗聴により伝送距離が制限されることが指摘されていた。これに対し、各パルスの位相を $\{0, \pi\}$ 、 $\{\pi/2, 3\pi/2\}$ のいずれかとして送信することにより盗聴による誤り率を増加させる方法を提案し、安全性解析によりその有効性を示した。さらに、実証実験を行った。

◆DPS 量子秘密共有実験⁶⁾

H17 年度に DPS 方式を量子秘密共有プロトコルに応用するシステムを提案したが、シフト鍵を得る段階に留まっていた。本年度はこれについてさらに詳細な検討を加え、秘密鍵生成条件を明らかにした。さらに、得られた結果に基づいて秘密鍵生成実験を行った。他のプロトコルに比べ、構成が簡便、ファイバ伝送に適している、等の利点を有している。

◆巨視的コヒーレント光 DPS-QKD

前年度まで、光子検出を行わずに秘密鍵を配布する方式として、巨視的2コヒーレント状態を用いるプロトコルを提案・検討してきた。今年度は、過剰雑音の影響についてさらに検討を加え、システム性能評価を行った。長距離化には向かないものの、通常光受信器が使用可能なため、実用システムに適した方式といえる。

◆量子もつれ光子対を用いた 100 km 光ファイバ上の量子鍵配送^{2,11)}

これまでに開発した PPLN 導波路内パラメトリック下方変換による時間位置もつれ光子対源と、米国 NIST 及び情報通信研究機構(NICT)開発による超伝導単一光子検出器を用いて 50km×2 の光ファイバ量子鍵配送実験を行い、0.57bps(誤り率 6.9%)のシフト鍵生成に成功した。これは、ファイバ上の量子もつれ QKD 実験の世界最長記録である。

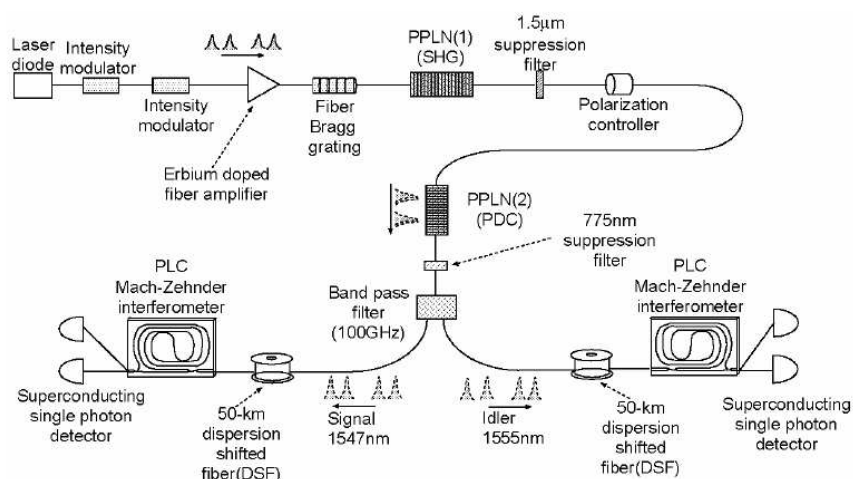


図1. 量子もつれ光子対を用いた量子鍵配送実験系

◆量子もつれ交換実験²⁾

これまでに開発した光ファイバ内四光波混合による時間位置もつれ光源を用いて、独立なもつれ光源から識別不可能な光子対を発生することに成功した。この識別不可能性を利用して、量子もつれ交換により、独立した光源から出力された2光子を「もつれさせる」実験に成功した。本実験は、2者の中間に配置されたノードにおける量子測定により2者間に量子もつれを生成するものであり、初歩的な「量子情報のリレー」を実現したといえる。

◆シリコン細線導波路による偏波もつれ発生と時間位置もつれ光子対の明瞭度向上^{1, 12)}

前年度報告したシリコン細線導波路内四光波混合による量子もつれ光子対発生をさらに発展させる実験を行った。まず、偏波ビームスプリッタ・ループ構成を用いて偏波もつれ光子対を発生

させ、明瞭度 83%以上の二光子干渉波形を観測した。また、時間位置もつれ光子対の発生について、導波路と光ファイバの結合効率を増大し、かつ系の安定性を向上することにより、95%以上の明瞭度を持つ二光子干渉波形を得た。

◆周波数上方変換を用いた周波数識別可能性の消去¹⁰⁾

光子の識別不可能性は量子情報通信にとって非常に重要であるが、このためには2光子の属性が全て同じでなくてはならない。今回、周波数上方変換技術を用いて、本来は識別可能である波長の異なる2光子を波長変換し、識別不可能な光子とする実験を行った。ファイバ内四光波混合により発生させた2光子を波長変換し、変換後の2光子により Hong-Ou-Mandel 型量子干渉実験に行なったところ、非古典的なくぼみを観測した。本実験は、波長の異なる光子を用いた複数の量子情報システムを結合するための基本技術として今後の展開が期待される。

◆閾値検出器を用いる BB84-QKD の無条件安全性証明⁸⁾

QKD の無条件安全性証明の手法として、もつれ蒸留プロトコルに帰着させる方法が広く用いられているが、そこでは光子数を識別できる検出器を仮定していた。これに対し、光子状態からキュービット状態への数学的な写像を構築し、その写像プラス光子検出という仮想的な実験系が現実的な閾値型検出器と等価であることを示し、実際的な BB84-QKD 系の無条件安全性を証明した。

◆PPLN 内 PDC による偏波もつれ発生の広帯域化とファイバ伝送実験^{4, 5, 7, 13)}

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構成により、安定的に偏波もつれ光子対を発生させた。短尺導波路(1mm)を採用することで 1525-1580nm の範囲内でパルス励起時のもつれ忠実度 85%と CW 励起時のもつれ忠実度 95%を確認した(図2)。また、全長 82km と 132km のファイバによる偏波もつれ伝送実験を行い忠実度 85%と 62%を確認した。

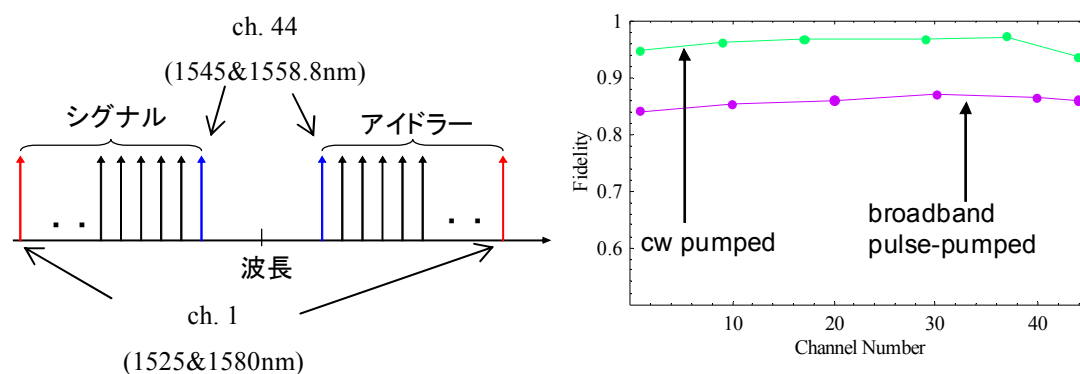


図2. 広帯域偏波もつれ光子対発生

3. 研究実施体制

(1)「阪大」グループ

- 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

- ①研究分担グループ長:武居 弘樹 (NTT 物性科学基礎研究所、主任研究員)
- ②研究項目:時間位置もつれ光子対を用いた量子通信実験

(3)「産総研」グループ

- 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

4. 研究成果の発表等

(1) 論文発表 (原著論文)

1. H. Takesue, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, Y. Tokura, and S. Itabashi, “Generation of polarization entangled photon pairs using silicon wire waveguide,” Opt. Express, Vol. 16, No. 8, pp. 5721-5727 (2008.4)
2. Q. Zhang, H. Takesue, S. W. Nam, C. Langrock, X. Xie, B. Baek, M. M. Fejer, and Y. Yamamoto, “Distribution of time-energy entanglement over 100 km fiber using superconducting singlephoton detectors,” Opt. Express, Vol. 16, No. 8, pp. 5776-5781 (2008.4)
3. M. Curty, K. Tamaki, and T. Moroder, “Effect of detector dead times on the security evaluation of differential-phase-shift quantum key distribution against sequential attacks,” Phys. Rev. A, Vol. 77, 052321 (2008.5)
4. H. Lim, A. Yoshizawa, H. Tsuchida and K. Kikuchi (Univ. Tokyo), “Stable source of high quality telecom-band polarization-entangled photon-pairs based on a single, pulse-pumped, short PPLN waveguide”, Opt. Express, Vol. 16, No. 17, pp. 12460-12468 (2008.8)
5. H. Lim, A. Yoshizawa, H. Tsuchida and K. Kikuchi (Univ. Tokyo), “Distribution of polarization-entangled photon-pairs produced via spontaneous parametric down-conversion within a local-area fiber network: Theoretical model and experiment”, Opt. Express, Vol. 16, No. 19, pp. 14512-14523 (2008.9)
6. K. Inoue, T. Ohashi, T. Kukita, K. Watanabe, S. Hayashi, T. Honjo, H. Takesue, “Differential-phase-shift quantum secret sharing,” Opt. Express, vol. 16, no. 20, pp. 15469-15476 (2008.9).

7. H. Lim, A. Yoshizawa, H. Tsuchida and K. Kikuchi (Univ. Tokyo), “Broadband source of telecom-band polarization-entangled photon-pairs for wavelength-multiplexed entanglement distribution”, Opt. Express, Vol. 16, No. 20, pp. 16052-16057 (2008.9)
8. T. Tsurumaru and K. Tamaki, “Security proof for quantum-key-distribution systems with threshold detectors,” Phys. Rev. A, Vol.78, 032302 (2008.9)
9. H. Shibata, T. Maruyama, T. Akazaki, H. Takesue, T. Honjo, and Y. Tokura, “Photon detection and fabrication of MgB2 nanowire,” Physica C, Vol. 468, pp. 1992-1994 (2008.9)
10. H. Takesue, “Erasing distinguishability using quantum frequency up-conversion,” Phys. Rev. Lett., 101, 173901 (2008.10)
11. T. Honjo, S. W. Nam, H. Takesue, Q. Zhang, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, B. Baek, R. Hadfield, S. Miki, M. Fujiwara, M. Sasaki, Z. Wang, K. Inoue, and Y. Yamamoto, “Long-distance entanglement-based quantum key distribution over optical fiber,” Opt. Express, Vol. 16, No.23 , pp. 19118-19126 (2008.11)
12. K. Harada, H. Takesue, H. Fukuda, T. Tsuchizawa, T. Watanabe, K. Yamada, Y. Tokura, and S. Itabashi, “Generation of high-purity entangled photon pairs using silicon wire waveguide,” Opt. Express, Vol. 16, No. 25, pp. 20368-20373 (2008.11)
13. H. Lim, A. Yoshizawa, H. Tsuchida and K. Kikuchi (Univ. Tokyo), “Wavelength-multiplexed distribution of highly entangled photon-pairs over optical fiber”, Opt. Express, Vol.16, No.26, pp. 22099-22104 (2008.12)

(2) 特許出願

平成 20 年度 国内特許出願件数 : 1 件 (CREST 研究期間累積件数 : 17 件)