量子暗号鍵配送用量子もつれ光源技術

荒平　慎　　岸本　直
村井　仁

インターネットに代表される様々な通信ネットワークは我々の生活に必要不可欠なものとなっている。その多大なメリットの一方で、ネットワークを経由して機密情報が盗まれるなど、通信ネットワークの拡大には負の側面も大きい。情報漏えいなど情報セキュリティ上の脅威は、最近のサイバー攻撃の例などで見られるように近年ますます増大している。

情報の秘匿性を確保する一般的な手段は暗号化であり、古来より盛んに研究され実用化されてきた。現在利用されている暗号方式は、解読に要する計算時間が膨大になるために事実上解読が不可能という意味で安全性が保証された方式であり、コンピュータの計算能力向上により解読される危険性を常に有している。

それに対して、自然法則（量子力学）を安全性の基盤におく量子暗号は、解読不可能な究極の暗号を実現でき、スマート社会を支える高セキュリティ技術として高い注目を集めている。我々は、金融・官公・防衛関係などの非常に高い情報セキュリティを必要とする事業分野への適用を目指して、量子暗号通信システムの研究開発を進めている。本稿では、量子暗号技術について概説するとともに、我々が開発を進めている高品質・低雑音・通信波長帯量子もつれ光源の開発状況について報告する。

量子暗号のしくみ

実際の情報暗号化は、鍵情報（暗号鍵）に基いた情報の暗号化／復号化によって実行される。そして暗号通信では、この暗号鍵情報を如何に第3者に知られることなく送受信者で共有するかが重要になる。

暗号通信毎に異なる暗号鍵（共通鍵）を用いる暗号通信方法は使い捨て（ワンタイムパッド）方式と呼ばれ、解読が不可能なことが証明されたほぼ唯一の暗号通信方式である[1)]。しかしながら、暗号通信セッション毎に異なる共通鍵を送受信者が共有するのは非常に困難で、ごく限られた用途にしか使用されてこなかった。

量子暗号の特徴は、共通鍵の共有を高い秘匿性で実現できる点にあり、これとワンタイムパッド方式を組み合わせることで、解読の不安がない、究極の暗号通信を実現することができる。現在、主に開発が進められている量子暗号プロトコルは、①単一光子を用いる方式（BB84方式）、②量子もつれ光子を用いる方式（E91方式、BBM92方式）に大別される[2)]。現在、実用化開発が先行しているのは①の単一光子方式であり、欧州などでは単一光子方式量子暗号通信システムを提供するベンチャー企業が立ち上げられている。

我々が現在開発に注力しているのは②の量子もつれ方式（BBM92方式）である。単一光子方式では、複数の光子が発生した状態（多光子状態）があると光子の一部を取り出した盗聴が可能であり、その対策が必要である。一方、量子もつれ方式では、異なる量子もつれ光子の間の測定結果には相関がないため、上記のような多光子状態を狙った盗聴に耐性がある。また人為的な乱数発生器が不要であるなど単一光子方式よりも高い安全性を確保できる。そのため量子もつれ方式は、より高いセキュリティ及び将来のネットワーク拡張の点から有望であり、次世代量子暗号通信システムとして期待される。

量子もつれを用いた量子暗号システムでは、「量子もつれ」と呼ばれる状態にある2つの光子（光子対）を使って暗号化に使用する共通鍵を配送（共有）する。量子もつれ状態にある光子対は、測定前には不確定な物理状態（重ね合わせ状態）にあるが、観測により一方の光子の状態が確定すると、その瞬間に（観測を待たず）もう一方の光子の状態も確定する。例として光子A、光子Bが偏光量子もつれ状態にあるとき、光子Aが横（H）直線偏光として観測されるとき光子Bも必ずH直線偏光で観測され、また、光子Aが縦（V）直線偏光であったなら光子Bも必ずV直線偏光であるといった確定的な相関関係が得られる。これら光子対の偏光状態は測定前は不確定で、H、Vどちらの偏光状態が観測されるかはそれぞれ確率50%でランダムである。このような偏光相関は二つの光子の間の距離がどれだけ離れていようとも基本的には維持される。その為、例えば光子

Aが地球にあり光子Bが月にいても、光子Aの偏光が決まると光子Bの偏光も同時に確定される。

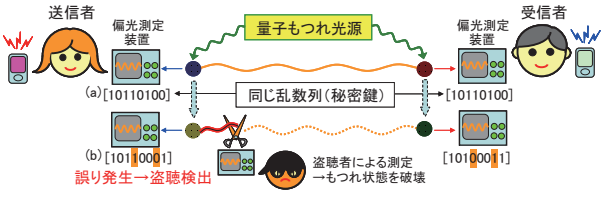

図１　量子もつれを用いた量子暗号（量子鍵配送）

この偏光相関を用いることで、暗号通信に用いる共通鍵を距離の離れた送信者と受信者が共有できるようになる。すなわち、H偏光をビット「1」、V偏光をビット「0」として送信者と受信者がそれぞれ到来してくる光子の偏光測定を繰り返せば、この二人は毎回異なる同じ乱数列を共有することが出来る（**図 1(a)**）。この乱数列をワンタイムパッド暗号通信の共通鍵に利用するのが量子もつれを用いた量子暗号システムである。

この暗号通信方式の特徴は、共通鍵共有プロセスにおいて盗聴者の存在を検出できる点にある。盗聴者が量子もつれ状態にある光子の偏光測定をした場合、量子もつれ状態が破壊されて結果、正規の送受信者が共有した乱数列に誤りが生じる（**図 1(b)**）。この誤りを検出することで盗聴者の存在を検出できる。実際の量子暗号システムでは、共有化された共通鍵の一部を盗聴探知に用いることで共通鍵の秘匿性を確保している。この特徴は今日用いられている暗号システムにおいて盗聴の検知がリアルタイムにできないために重大なセキュリティ事故を引き起こしていることの解決につながる。

以上のように、量子暗号システムで実際に量子力学を利用しているのは共通鍵配送（共有）の部分であり、そのため、この暗号通信システムは厳密には量子鍵配送（Quantum Key Distribution）システムと呼ばれている。

量子鍵配送で共有化された安全な共通鍵とワンタイムパッド暗号方式を用いれば、盗聴者による解読の心配のない暗号通信が可能となる。実際の暗号文の暗号化・送信・復号化は古典的な信号処理回路と通信網を利用して実現することができる。

実際の量子暗号通信システムでは、検出器などで発生する雑音のために、盗聴者が存在しなくても信号誤りが発生する。これに対しては誤り訂正など適切な鍵蒸留プロセスを実行することで対応が可能である。おおよそ11%程度の誤り率までは盗聴者の知りえない安全な共通鍵を共有できることが理論的に示されている[3]。このような信号処理技術を併用することで現実的な量子暗号通信システムの実現が可能となる。

量子もつれ状態は、例えば電子のスピン状態などを利用して実現できる。また例に挙げたような光の量子もつれ状態（量子もつれ光）を用いると、低損失な光ファイバ通信網を利用することで都市間に相当する通信距離での共通鍵共有と暗号通信が可能となる。

高品質量子もつれ光源の開発

量子暗号システムでは、光子1個程度の非常に微弱な光（通常の光通信の十万分の一～百万分の一程度）を送受信するため、量子暗号システムを構成する量子もつれ光源、ならび単一光子検出器としては、十分に低い雑音特性が要請される。特に低損失・低雑音な量子もつれ光源の開発は量子暗号システムの通信距離や共通鍵生成レートを決定するため特に重要である。また、既存システムとの整合を考えると、一般の光通信で用いられる1.5μm波長帯で動作することも重要である。

量子もつれ光は、非線形光学媒体中で生じる自然パラメトリック変換（Spontaneous Parametric Down Conversion、SPDC）と呼ばれる現象を用いて発生する。SPDCは励起光子が波長や時間、偏光などの相関を持つ相関光子対に変換される現象であり、これと光干渉計を組み合すことで量子もつれ状態を実現できる。

量子もつれ光源としてはこれまでに、短波長の固体レーザを利用した大型な実験装置や、低雑音化のために極低温（-200℃）へ冷却した装置が開発されていたが、これら大型の光源システムは商用システムへの応用が難しく、コストと性能の両面を満足する実用的な量子もつれ光源の実現はいまだ不十分であった。

図 2（a）は我々が開発を進めている通信波長帯量子もつれ光源の構成図である。非線形光デバイスとして、低損失・高効率を特徴とする周期分極反転$LiNbO_3$（Periodically Poled $LiNbO_3$、PPLN）導波路と呼ばれる特殊な光デバイスを独自開発している[4]。また我々は、単一のPPLN導波路中で非線形光学現象を2回生じさせる、カスケード非線形方式（カスケード光第2高調波（Second Harmonic Generation、SHG）/SPDC方式（**図 2（b）**）を新規開発することにより、商用光通信部品を用いて1.5μm波長帯で常温動作する高品質・低雑音量子もつれ光源を実現した[5]。

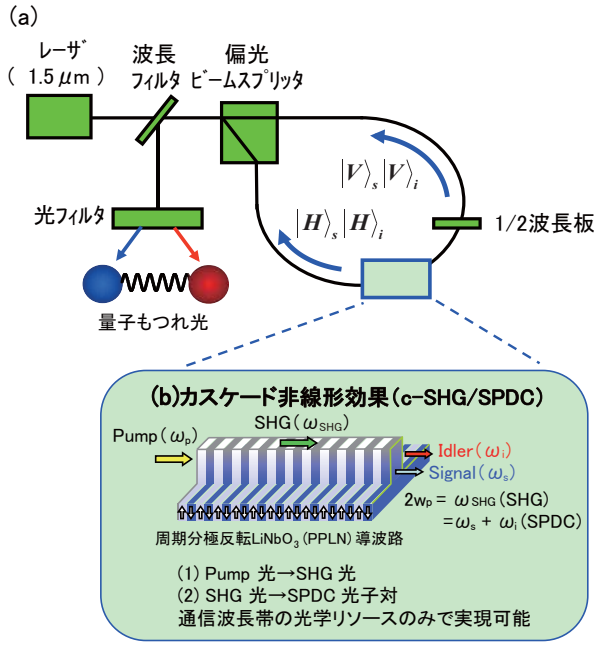

図 2　(a) 通信波長帯量子もつれ光源の構成図
(b) PPLN 導波路を用いたカスケード SHG/SPDC 法

PPLN導波路デバイスを偏光ビームスプリッタで構成した光ループ光路内に挿入し、波長1.5μm帯のレーザ光で双方向励起する。励起光強度を適度に設定すると、光ループから出力されるSPDCによる光子対は、時計回りの励起光によって生じたH偏光のSPDC光子対と、反時計回りの励起光によって生じたV偏光のSPDC光子対との重ね合わせ状態となり、量子もつれ光が発生する。

本方式の特徴は全光学系を商用光通信部品で構成できることで、従来光源のように短波長光源など特殊な光学部品を必要とせず、小型・簡易な構成で信頼性の高い光源開発が可能となる。また、PPLN導波路デバイスの有する高い光学非線形性のために、室温動作においてもラマン散乱など雑音光子を十分抑制でき、低雑音で高品質な量子もつれ光を発生することができる。

図 3は発生させたSPDC光子対の信号／雑音比に相当するCAR（同時カウント／偶発カウント比）を他の量子もつれ光源の文献値と比較した結果である。開発した量子もつれ光源のCARは最大で約4100[5]と世界最高水準にあり、従来光源に比べて2〜3桁程度高い値が得られた。このことは、本光源を用いることで信号誤り率が低い量子鍵配送が実現可能であることを意味している。

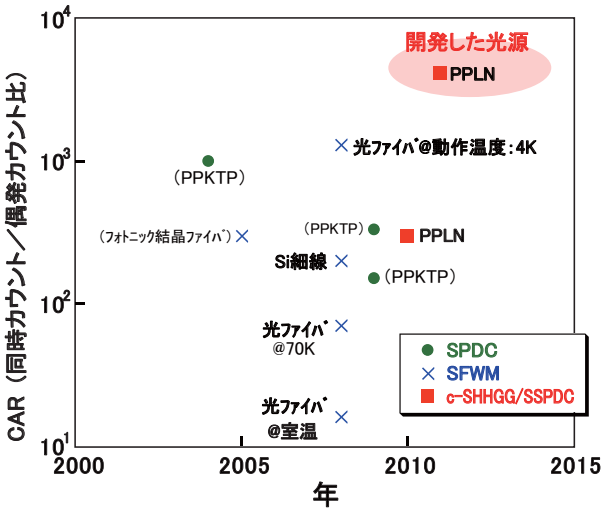

図 3　CAR の比較結果
SPDC：通常 SPDC 方式、SFWM：自然 4 光波混合方式、
c-SHG/SPDC：カスケード SHG/SPDC 方式（本方式）
PPKTP：周期分極反転 $KTiOPO_4$（KTP）結晶

さらに、生成させた量子もつれ光子対を光ファイバ伝送する試験を実施した。**図 4**は通常シングルモード光ファイバ伝送後の明瞭度の変化である。

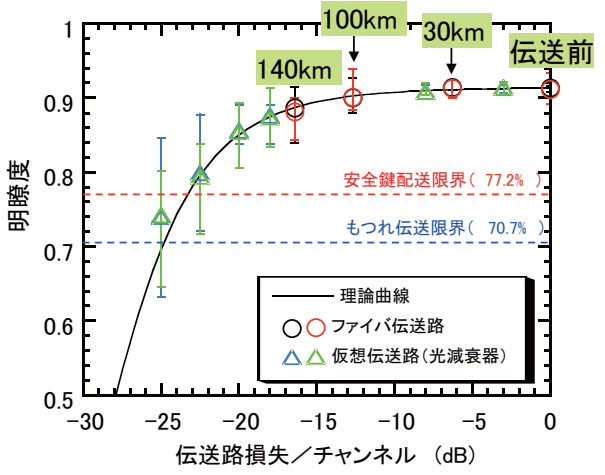

図 4　シングルモードファイバ伝送実験結果

なおこの実験では光子対をそれぞれ同じ長さで別々のシングルモード光ファイバ上を伝送させており、横軸は各ファイバチャンネル当りの伝送損失である。ファイバ伝送140km（各70km、伝送路損失：-16.4dB／チャンネル）後においても安全な秘密鍵配送を可能とする限界値（77.2%）を超える明瞭度が得られた[6]。光減衰器を利用した伝送損失のみを考慮した仮想伝送路の

実験（図中の三角）からは、200km長（伝送損失：約-23dB／チャンネル）程度までの伝送が可能であることが示唆される。このことから通常の光ファイバ通信環境で都市間の伝送に相当する量子暗号通信が可能な性能を実証した。

まとめと今後の課題

量子もつれ光を用いた量子暗号（量子鍵配送）システムについて概説し、我々が開発を進めている高品質・通信波長帯量子もつれ光源の開発状況について報告した。通信波長帯量子もつれ光源は最近ではシリコン細線を利用した小型光源の開発なども報告されており[7]、従来の大型の実験装置というイメージから脱却して、商用機器開発へ向けた取り組みが着々と進められている。

単一光子方式、量子もつれ方式のいずれの量子暗号システムも、その技術課題のひとつとして通信距離の長距離化があげられる。通信距離は伝送路損失でほぼ制限され、光ファイバ環境下でも100km～200km程度が現在の限界である。長距離通信のためには量子中継器が必要とされる。量子中継器は基礎研究の段階で実用化はまだ遠い将来のことと考えられるが、量子もつれは量子中継器を実現するための重要な要素技術の一つであり、その点からも小型・安定で高品質な量子もつれ光源は今後の量子情報通信システムの分野で重要な役割を担うものと考えられる。

量子暗号システムは欧米や他のアジア諸国でも活発な研究開発がなされており、今後も実用化へ向けた精力的な研究開発が続けられるものと期待される。

■参考文献

1）C. E. Shannon, Bell system Technical Journal, 28-4, 656-715 (1949).

2）量子暗号プロトコルの詳細については、佐々木雅英, 松岡正浩監修,"量子情報通信", オプトロニクス社,　平成18.11.5第1版第1刷発行　などを参照

3）N. Lütkenhaus, Phys. Rev. A61, 052304-052313 (2000).

4）T. Kishimoto et al., Photon. Technol. Lett. 23, 3, 161-163 (2011).

5）S. Arahira et al., Opt. Exp. 19, 17, 16032-16043 (2011).

6）S. Arahira et al., Opt. Exp. 20, 14, 15336-15346 (2012).

7）N. Matsuda et al., Sci. Rep. 2, 817 (2012).

●筆者紹介

荒平慎：Shin Arahira. 研究開発センタ ネットワーク・端末技術研究開発部

岸本直：Tadashi Kishimoto. 研究開発センタ ネットワーク・端末技術研究開発部

村井仁：Hitoshi Murai. 研究開発センタ ネットワーク・端末技術研究開発部

TJPO【基本用語解説】

共通鍵

暗号化／復号化に同じ暗号鍵を使用する方式を共通鍵方式と呼ぶ。異なる暗号鍵を利用する方式は非対称鍵方式と呼ばれ、RSA暗号などの公開鍵方式がこれに相当する。

光子

光は波（電磁波）としての性質と粒子（素粒子）としての性質を有する。粒子としての光を光子と呼ぶ。

自然パラメトリック変換（Spontaneous Parametric Down Conversion、SPDC）

光学非線形光デバイス中で生じる非線形光学過程によって、1個ないし複数個の励起光子が消失し、それと同時に、1組の光子対（相関光子対）が新たに発生する現象。この光子対は常に対となって同時生成し、その観測される物理量（波長や偏波など）に距離に依らない相関（非局所的相関）がある。

PPLN導波路

自発分極の向きを周期的に反転させた構造を有する$LiNbO_3$結晶を用いた導波路型光デバイス。位相整合の実現により高い非線形光学効果を得ることが出来、また、導波路構造による高い光閉じ込め効果により、非線形光学効果を高効率化できる。光ファイバ等の非線形媒体に比べ、ラマン散乱などによる雑音光子の発生が少ないなど、高い信号／雑音比を実現するうえで有望なデバイス。

CAR（同時カウント／偶発カウント比、Coincidence-to-accidental ratio）

SPDCによって生じる光子対は常に同時に発生し、その発生時間差はゼロである。ゼロ以外の発生時間差をもつ検出結果は雑音光子など無相関な光子の発生を意味する。CARは時間相関ヒストグラムを測定した時の遅延時間ゼロの時とそれ以外の時の検出比であり、光子対の品質を評価する指標になる。一般の光通信における信号／雑音比に相当する。

明瞭度

量子もつれ光子の性能指数の一つ。光子対の「もつれあい」程度の大小を表す。理想的には100%であり、雑音光子の存在などにより劣化する。安全な量子鍵配送（誤り率11.4%以下）を実現するには明瞭度としておおよそ77.2%以上が必要である。