長距離・高速大容量な量子雑音暗号伝送をデジタルコヒーレント通信を用いて世界で初めて実現

中沢　正隆
東北大学電気通信研究所 超高速光通信研究分野
〒980-8577 仙台市青葉区片平 2-1-1
Tel: 022-217-5522, Fax: 022-217-5523

＜成果の概要＞

インターネット、携帯電話、光通信などの ICT 技術の発展と共に、高速・大容量な通信システムがグローバルに運用されています。そのようななか、やり取りする情報の安全性を確保することが重要になってきています。

東北大学電気通信研究所の中沢正隆教授のグループは、QAM (Quadrature Amplitude Modulation：直交振幅変調)と呼ばれる多値デジタルコヒーレント光伝送方式に量子雑音を付加し、伝送信号をその雑音の中に隠すことにより、高速・大容量の強力な新たな量子暗号伝送に世界で初めて成功しました。当初の実験では 10 Gbit/s で 160 km 伝送に成功し、その後単一チャネル 40 Gbit/s-480 km の伝送に成功しました。そして、暗号としての秘匿性が従来の量子ストリーム暗号に比べて二乗倍強いことを実証しました。

＜背景＞

情報化社会の進展により、インターネット上での安全な商取引、個人情報の保護、機密情報の漏洩防止など、ネットワークのセキュリティに対する要求はますます高まっています。現在は AES (Advanced Encryption Standard)や公開鍵暗号のように解読に膨大な計算量を要する数理暗号が用いられていますが、今後コンピュータの計算能力が飛躍的に向上すると短時間で解読されてしまう恐れがあります。このため、数理暗号だけでは盗聴の危険性を完全に排除することは困難です。光ファイバは極端な曲げを与えると光が漏洩することから、盗聴者は情報を盗み取ることができる可能性があります。そのため、原理的に解読が不可能な暗号方式の実現に向けて世界各国で研究開発が進められています。

＜従来の技術＞

今まで光量子暗号通信方式として、BB-84（1984 年に提案されている）を代表とする量子鍵を用いた使い捨て鍵暗号（One time pad 暗号）が絶対に解けない完全秘匿暗

号として提案されています。共通鍵を単一光子や微弱なコヒーレント光で伝送することにより安全に鍵を配送することが出来るといわれています。しかし、元の通信文と同じ長さの使い捨ての共通鍵を受信者に配送する必要があり、量子暗号の速度は鍵配送の速度（数 100 kbit/s）で制限されてしまう問題点がありました。また、伝送距離は最大でも 200 km 程度でその時の通信速度は 50 kbit/s 以下でした。一方で、伝送速度を 1 Mbit/s にすると伝送距離は数 10 km 以下でありました。

これに対して光の量子雑音を利用した量子ストリーム暗号（QSC: Quantum Stream Cipher、別名：Y00）が 2000 年に提案されています。この方式は共通鍵を元に生成した擬似乱数を用いて光信号の位相あるいは振幅を多値変調します。そしてそのデータ信号を光の量子揺らぎの中に埋め込むことにより、盗聴者が光信号を正確に受信出来なくしています。変調の多値度を大きくして変調される信号の強度差もしくは位相差を狭めることにより、伝送時に付与される量子雑音がその差より大きくなるように設定してデータを雑音に埋もれさせ、極めて高い安全性を実現しています。

QSC による具体的な通信方法の一例を図 1 に示します。“1”と”0”のディジタル情報を送る場合、通常は光のオン・オフで伝送しますが、QSC では暗号の鍵を使い、決められたルールに従って“1”と”0”を多値信号レベルのいずれかのレベルに割り当てます。図１の例では８値の振幅(0~7)のいずれかのレベルに割り当てています。この光信号には必ず量子雑音が付加されますので（図 1 では灰色で示しています）、雑音の大きさより十分細かく信号レベルを割り当てておくと、受信器でデータ信号は雑音に埋もれて判別できなくなってしまいます。しかし、正規受信者は暗号の鍵をあらかじめ知っていますので、互いに共有する閾値より光パワーが大きいか小さいかという判定方法によって、雑音に埋もれた信号から “1”と “0”を正しく読み取ることが出来ます。一方、盗聴者は鍵がわかりませんので、正しい信号レベルを特定することができず、データを盗み取ることが出来ません。

QSC の最大の特徴は、単一光子のような微弱な光ではなく通常の光通信に用いるレーザ光が使えますので、高速・長距離伝送が可能であり、既存の光通信システムと極めて高い親和性を有していることです。既に 10 Gbit/s で数 100 km の伝送が報告されています。しかし、この方式では多値変調は用いるものの、１回の変調において伝送できる信号はその方式上１ビットでありました。

一方、次世代の光通信方式として、QAM (Quadrature Amplitude Modulation)に代表されるように、振幅および位相を多値で変調することにより、１つの信号（シンボル）に多ビットの情報を乗せるデジタルコヒーレント伝送技術が注目されています。この QAM 方式では、光電界の位相と振幅に同時に情報を載せることが出来ます。東北大学

中沢研究室では既に 2048 値のコヒーレント伝送実験にも成功しています。具体的には、図２に示すように、I, Q と呼ばれる２つの直交したチャネルで光の振幅を独立に多値変調し、データ信号を生成します。このことは振幅と位相に独立なデータを与えることと等価です。図２の例では I, Q それぞれを４通りの振幅で変調し、4 x 4 = 16 QAM 信号を生成しています。16 個のシンボル点には 0000 ~ 1111 の 4 ビットの情報を割り当てることが出来ますので、1 つの信号で 4 ビットの情報を送ることが出来ます。従って、QAM の多値数を増やすことによって周波数の利用効率が大幅に拡大し、伝送容量が格段に向上できます。このため最近のコヒーレント通信の中核技術になっています。今回我々は、QAM 方式のプロトコルを QSC に新たに導入することにより、伝送容量の増大と同時に安全性も著しく増強できる画期的な量子暗号方式を世界で初めて実現しました。

＜今回の成果＞

今回我々は、今まで中沢研究室で進めてきている QAM と呼ばれる多値変調を用いたデジタルコヒーレントを量子ストリーム暗号に適用し、10 Gbit/s の 16 値 QAM 暗号を 150 km 伝送する事に世界で初めて成功しました。そして、暗号としての秘匿性が従来の量子ストリーム暗号に比べて二乗倍強いことを実証しました。今回の量子暗号が持つ特徴は以下の通りです。

(1) 光の二重鍵による安全性の増強

従来の QSC 方式では、振幅もしくは位相のみの暗号化で、両者に同時に暗号化は出来ませんでした。言わば 1 次元の暗号と言えます。一方我々は、位相と振幅の両方を同時に独立に暗号化することにより、いわば QSC 方式に二重鍵の機能をもたせ安全性を高める方法を新たに提案しました。振幅と位相へ乗せた暗号の強度は独立にかつ同程度に高いので、両者の積で与えられる全体の暗号強度は二乗倍になります。

その概要を図３に示します。送信者は送りたいデータおよび鍵をシンボルごとに 2 つのブロックに分け、片側を I チャネル、もう片側を Q チャネルに割り当てます（図３(a)の例では緑色が I、青色が Q に対応）。そして I と Q を 90 度位相をずらして足し合わせ、QAM 信号を生成します。この信号に量子雑音が付加されると、信号が I, Q 両方向、即ち 2 次元的に乱されます。しかし正規受信者は I, Q 両方の鍵を持っていますので、I, Q それぞれを正しく受信しデータを完全に復元できます。一方、盗聴者は I, Q どちらか一つでも鍵を持っていないとデータを復元できません。つまり、安全性が二乗倍に向上します。

一例として、鍵の長さを 127（7 段の擬似ランダム系列）とし、I, Q それぞれの振幅を 1024 段階に区切った場合を想定しますと、この暗号をスーパーコンピュータを使って解読するには、従来の QSC でも 83.7 年要しますが、今回の方式では 2.1×10^{27} 年と見積もられ、解読はほぼ不可能となります。

(2) 多値 QAM による量子暗号通信の高速化

QSC に QAM 方式を導入することにより、安全性が向上するだけでなく、その伝送速度も大幅に高速化されます。図１の従来の量子ストリーム暗号は１多値変調に付き１ビットの情報しか送れませんでした。一方、図３に示す QAM 方式では、従来のように 1 ビットずつ暗号化するのではなく、1 シンボル（データ）につき複数ビット即ち多ビットを暗号化しています。これによってビットレートが大幅に高速化できます。図３(a)では I と Q 軸で 2 ビットずつ変調し、ビットレートが $2^2 = 4$ 倍高速化されます。

QAM を QSC に導入するもう一つのメリットとして、受信者は QAM 信号を受信するために局発光と呼ばれる参照用の光源を用意しておく必要があり、その位相はデータ信号と正確に同期している必要があります。この位相同期には光 PLL (Phase-locked Loop)と呼ばれる技術が用いられます。ところが、盗聴者は光信号を盗聴しようとしても光の S/N が確保されず、正確な PLL 動作が原理的に実現しません。このためそもそも暗号が雑音の中に混在する信号を受信することができません。

(4) 暗号化装置の開発とその動作実証

本暗号方式の性能を実証するために、QAM 型 QSC 暗号化装置を開発し、ビットレート 10 Gbit/s、伝送距離 160 km の伝送実験を行いました。その構成を図４に示します。今回の実験では 16 QAM 信号を 2.5 Gsymbol/s の速度で生成し、単一チャネルで 2.5 x 4 = 10 Gbit/s のビットレートを実現しています。16 QAM は I, Q がそれぞれ 4 値の振幅で定義されますが、暗号化に際し振幅と振幅の間をさらに 64 分割（合計で 256 分割）しています。これを 160 km 伝送させて受信すると、信号は雑音に埋もれてしまい、鍵を知らない盗聴者には図５(a)のようにランダムに見えます。一方、正規受信者は鍵を使って雑音に左右されずデータを正しく受信できるため、図５(b)のように信号を明瞭に判別することが出来ます。測定の結果、盗聴者は 1 つのシンボル（データ）につき 99.5%の確率で受信に失敗しますが、正規受信者は全く誤り無く受信できることが示されました。最近ではさらなる高速化と長距離化を図り、単一チャネルで 40 Gbit/s-480 km の伝送に成功しています。

＜今後の展望＞

今回のQAM型QSC方式の基本実証ではQAMの多値度を16に設定しましたが、我々の研究グループは通常の QAM 伝送において 2048 値までの超多値化を図り、66 Gbit/s で 150 km の伝送を実現しています。従って、例えば信号の生成速度を 10 Gsymbol/s に高速化し、QAM の多値度を 32 以上に増大させ、さらに偏波多重（２つの直交する偏波を両方伝送に用いる）という技術を用いれば、容易に 100 Gbit/s-150 km を超える伝送が可能になります。更に WDM（Wavelength Division Multiplexing：波長多重）と呼ばれる既存の技術と組み合わせるとテラビット領域の実用性の高い暗号技術が確立できます。

QAM は近い将来長距離・大容量光ネットワークに導入されると予想されており、QAM 型 QSC はその高い親和性から、サイバー攻撃に耐え得るセキュア通信の実現に大きく貢献するものと期待されます。

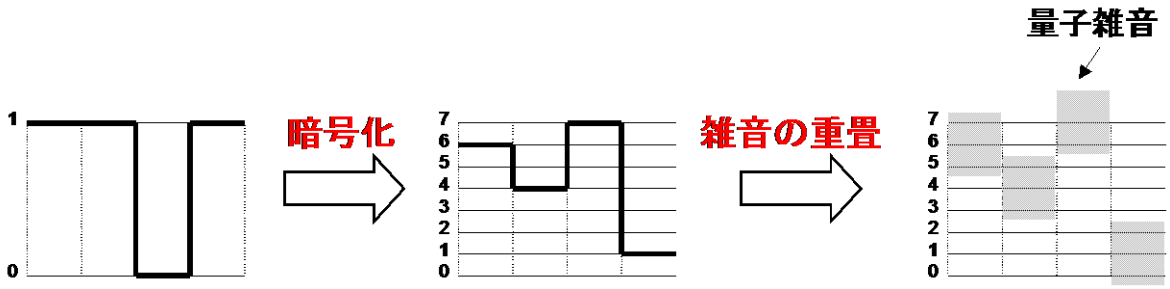


図１　従来の１次元量子ストリーム暗号(Y00)による暗号化の原理

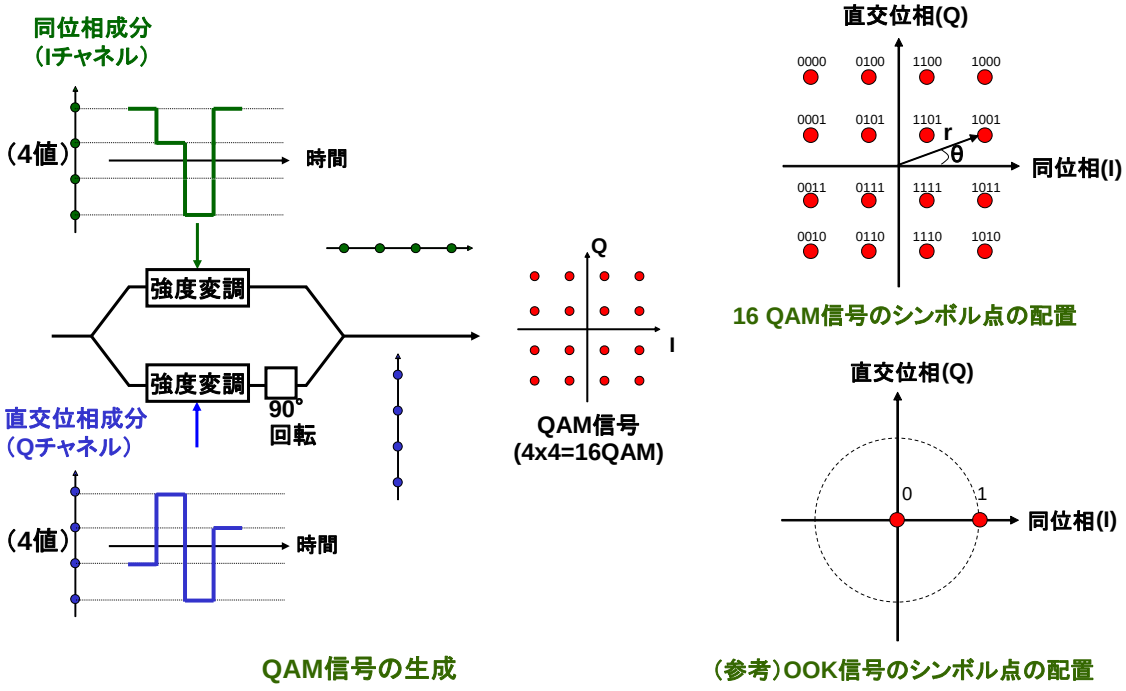


図２　QAM 方式の原理

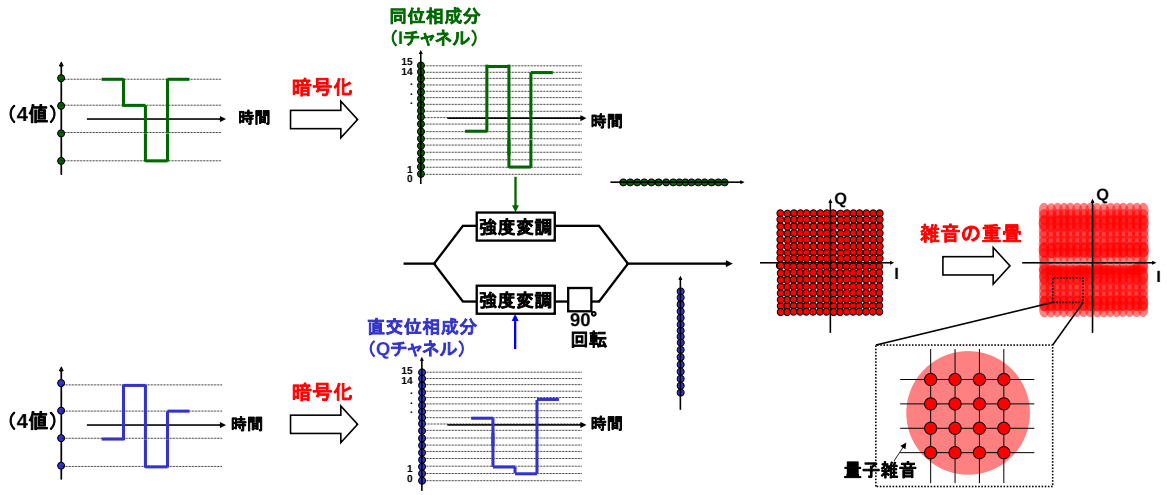


図３　QAM を用いた２次元量子ストリーム暗号方式による暗号化の原理

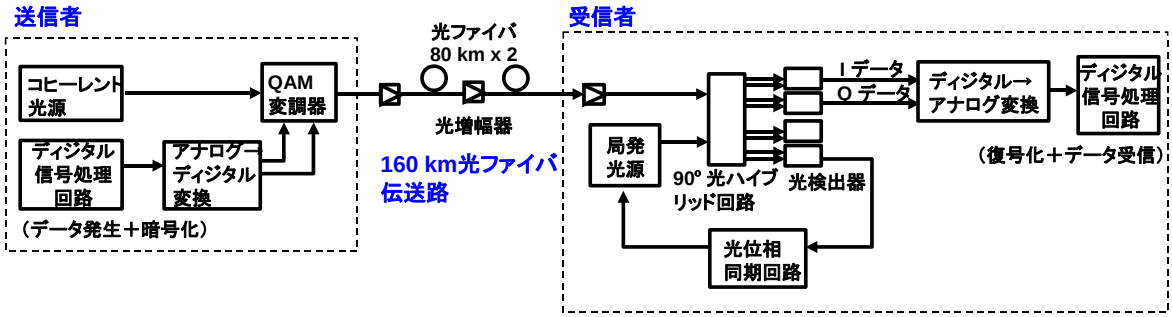
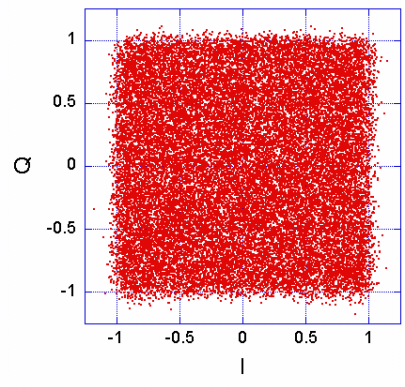
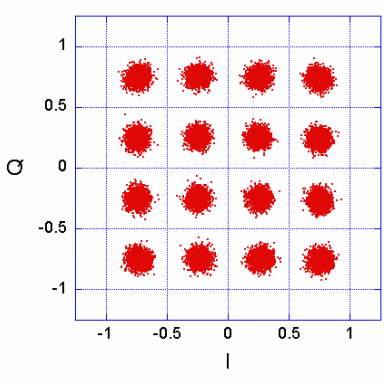


図４　16 QAM を用いた 10 Gbit/s-160 km 量子ストリーム暗号伝送の実験系



(a) 盗聴者が受信する16 QAM信号



(b) 正規受信者が受信する16 QAM信号

図５　盗聴者および正規受信者が受信する QAM 信号