平成２８年９月２０日

報道機関　各位

東北大学電気通信研究所
学習院大学理学部物理学科

量子雑音ストリーム暗号と量子鍵配送を組み合わせた高速・大容量秘匿光通信システムを世界で初めて実現

【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。そのような中で情報量は益々増え、やり取りする情報の安全性を確保することが極めて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と学習院大学の平野琢也教授のグループは、QAM（Quadrature Amplitude Modulation：直交振幅変調）と呼ばれるコヒーレントな多値信号を量子雑音の中に隠す QAM 量子雑音暗号伝送技術（QAM/QNSC: QAM/Quantum Noise Stream Cipher）と、単一フォトンに近い極めて微弱なレーザー光で暗号の生成と解読のための鍵を安全に配信する量子鍵配送（QKD: Quantum Key Distribution）技術を組み合わせることにより、極めて安全でかつ高速・大容量な秘匿光通信システムを世界で初めて実現しました。量子暗号伝送において世界最速の単一チャンネル 70 Gbit/s のデータ速度で 100 km の伝送に成功し、その有用性を実証しました。周波数利用効率も 10.3 bit/s/Hz と極めて高いものです。この新暗号技術は 9 月 21 日にドイツ Dusseldorf で開催されるヨーロッパ光通信国際会議（ECOC）で発表されます。

【背景】

情報化社会の発展と共に、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が益々高まっています。現在は安全性の高い通信方式として 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（ソフトウェア暗号）が用いられています。今日の大容量通信の主流は光ファイバ通信ですが、光ファイバ通信にも高い秘匿性が求められています。しかし、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、数理暗号で秘匿化しても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。そのため最近では、原理的に解読を不可能にする物理的暗号化方式（ハードウェア暗号）あるいは秘密鍵を安全に配信する技術（受信した信号の振幅分布の形状変化から盗聴を見破る技術）の研究開発が世界各国で進められています。

【従来の技術】

盗聴者が絶対に解読することの出来ない完全秘匿暗号方式として、今までに BB84（1984 年に提案されている）を代表とする量子鍵配送（QKD: Quantum Key Distribution）が提案されています。QKD では、量子力学の原理（不確定性原理）を利用してまず盗聴を検出できる通信チャンネルを作製し、そのうえで鍵の情報を送受信します。もし、盗聴が検出された場合には、その鍵を破棄して、違うタイミングで再度新たな鍵を送付します。ひとたび送受信者間で安全な鍵が共有出来れば、使い捨て鍵暗号（One time pad 暗号）方式を用いて絶対に安全な暗号通信が可能となります。この QKD システムにおいて、送信者は単一光子あるいは微弱なコヒーレント光の直交する偏光や位相に鍵の情報を乗せて正規受信者へ送付します。例として鍵配送に位相を用いる場合の鍵の割り振り方を図 1 に示します。送信者は、I と Q の直交関係にある 2 つの振幅情報（以降、モードと呼ぶ）のいずれかをランダムに選択し、I モードでは、0 度でビット情報 “1”、180 度で “0” を送り、Q モードでは、90 度で “1”、270 度で “0” を送ります。もし I モードだけで鍵を送付した場合、I モードと同位相の関係にある局発光信号とのホモダイン検出により、鍵が“0”であるか“1”であるか容易に検出することができます。しかし、直交関係にある Q モードの光子が混在する場合には、そのQモードで送付された信号をIモードと同位相の局発光信号で検出すると、Q モードの位相を検出出来ないため、その検出結果は確率 1/2 でランダムに“0”または“1”となります。このような検出の誤りが発生する要因は、直交する I と Q モード間の不確定性にあり、この不確定性の関係が成り立つ 2 つのモードを利用して鍵の情報を送付することで安全な鍵配送を実現しています。さらに、盗聴により単一光子の位相を測定し、測定後になりすまして単一光子を送り出しても、受信時の不確定性により同じ位相を配送することが出来ません。即ち、万が一盗聴されても必ず位相の分布にその痕跡が残り、盗聴されていることを見破ることが出来ます。(この QKD の原理の詳細な説明は補足に譲ります。)

これまでに多種類の QKD 方式が報告されていますが、中でも単一光子に近い微弱なレーザー光に 4 値の位相変調を与えて鍵情報を送信し、受信側で強い強度の局発光を用いて量子雑音限界のホモダイン検波を行う 4 値 QKD 方式は、光通信用の一般的な素子を用いることが出来る実用性の高い方式です。しかしながら、この QKD と使い捨て鍵暗号を用いた量子暗号方式は大変強力なものである一方で、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、このため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欠点がありました。

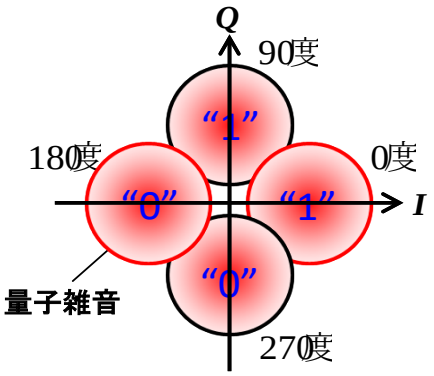


図 1　4 値 QKD 方式の原理

これに対し、東北大学では光信号の位相および振幅を同時に多値で変調する QAM（Quadrature Amplitude Modulation）方式のデータを量子雑音の中に埋もれさせて暗号化す

る量子雑音暗号（QNSC: Quantum Noise Stream Cipher）伝送方式を 2013 年に提案しています。この方式は送信者はあらかじめ用意した共通鍵により生成した擬似乱数を用いて光信号の位相と振幅の両方を多値変調します。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、盗聴者がデータを正確に受信出来なくしています。一方、正規受信者は共通鍵を保有しているため数学的な処理を施すことにより誤りなく情報を受信で出来ます。伝送時には QAM 変調の多値度を大きくして信号間の位相差および振幅差を小さくすることにより、通信システムの量子雑音がそれらより極めて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。

その一例として 16 QAM データを暗号化する様子を図 2 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 2 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。この信号にレーザーや光増幅器からの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。正規受信者は I, Q 両方の鍵をあらかじめ持っていますので、信号処理により I, Q それぞれを正しく受信しデータを完全に復元出来ます。しかし、盗聴者は鍵を持っていないためデータを復元出来ません。

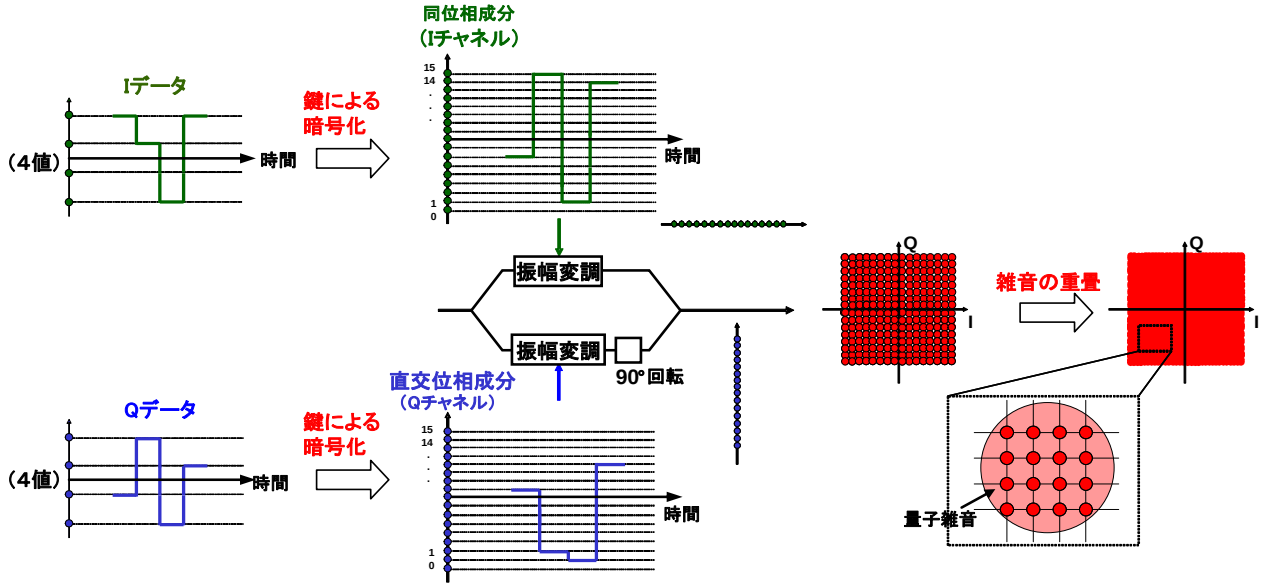


図２　QAM 型 QNSC 方式による暗号化の原理

QAM 型 QNSC 方式では、データ信号として 2^N QAM を用いることで、1 つの信号で N ビットの情報を送ることが出来る利点があります。従って、多値度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、伝送容量を大幅に増大出来ます。このため QAM 方式は今日のデジタルコヒーレント通信の主流となっています。これまでに我々は QNSC 方式により 10~40 Gbit/s のデータ速度で 480 km の伝送を実現しています。QNSC 方式は共通鍵を送受信者間で予め共有する方式です。しかし、この鍵を最初から共有するとその管理も含め盗難などの問題がないわけではありません。

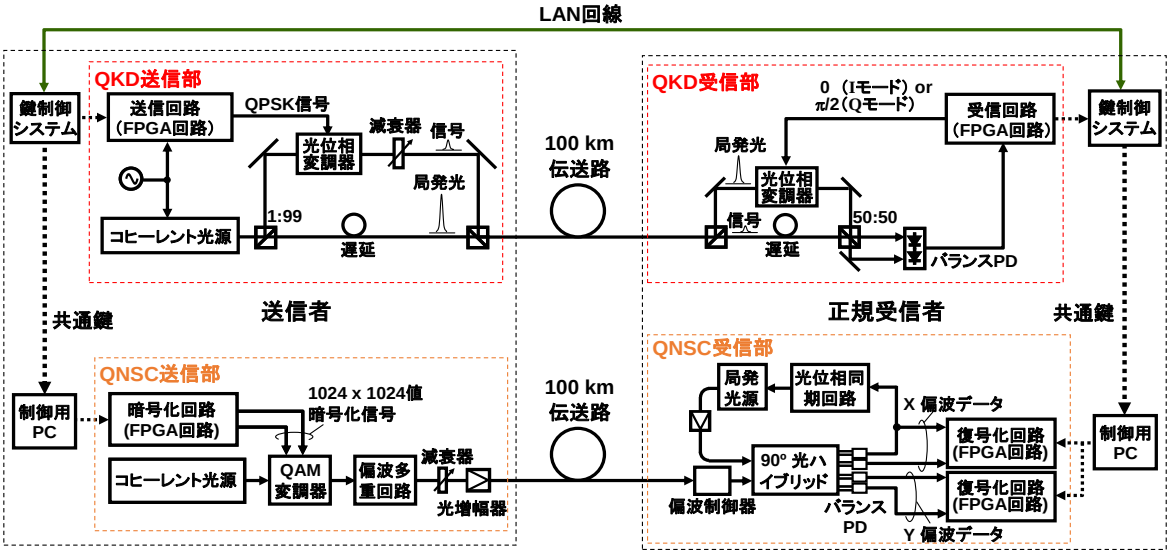
そこで今回、QAM/QNSC 方式においてこの共通鍵のみを QKD 方式で On-line 伝送することにより絶対に盗聴されない安全な鍵をある時間に持ち合うことにより、安全性を飛躍的に向上させる方式を考案しました。

【今回の成果】

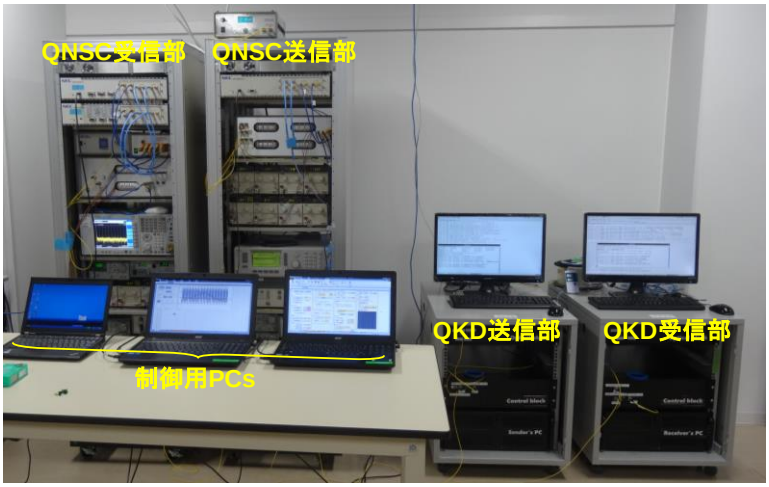
具体的には、今まで東北大学中沢研究室で開発してきた QAM 型 QNSC 方式と、学習院大学平野研究室で開発してきた 4 値 QKD 方式を組み合わせることにより、高速・大容量かつ極めて安全な秘匿光通信システムを世界で初めて実現しました。そして、共通鍵を 1 秒毎に更新しながら単一チャンネル 70 Gbit/s の高速暗号データを 100 km 伝送することに成功しました。この研究成果は 2016 年 9 月に開催されるヨーロッパ光通信国際会議で発表される予定です。今回開発した秘匿光通信システムの特徴は以下の通りです。

(1) 既存の光通信システムを利用している

19 インチラックサイズの可搬な QAM 型 QNSC 装置および 4 値 QKD 装置を開発し、それらを組み合わせて伝送速度 70 Gbit/s、伝送距離 100 km の秘匿光通信システムを構築しました。そのシステム構成およびシステム全体の概観写真を図 3 (a)および(b)に示します。図 3 (a)において QAM 型 QNSC 装置と 4 値 QKD 装置にはいずれも送信用光源としてコヒーレント光源を配置し、受信部では局発光とのホモダイン検波回路を用いています。本システムは市販の一般的な光通信用デバイスを用いているため、既存の光通信システムと同等に取り扱えます。



(a)



(b)

図 3　QAM 型 QNSC 装置と QKD 装置を組み合わせた 70 Gbit/s-100 km オンライン秘匿光通信システム (a)システム構成, (b)概観写真

(2) 共通鍵の更新と多値度切り替え動作による高い安全性

今回の実験では、4 値 QKD 装置により 200 bit/s 以上の鍵生成速度で共通鍵を 100 km 配信しています。この鍵は QKD 方式により高い安全性が確保されています。一方で、QAM 型 QNSC 装置では、QKD とは別の 100 km 伝送路を用いて 70 Gbit/s の高速データを送信しています。盗聴者はいずれか一方の伝送路から仮に情報を検出することに成功したとしても、鍵もしくはデータのいずれかしか手に入れることが出来ず盗聴が困難となります。QAM 型 QNSC 装置の送・受信部では、4 値 QKD 装置で配信した共通鍵を利用して擬似乱数列を生成し、それらの乱数列をもとにそれぞれ暗号化・復号化を行っています。ポイントは、共通鍵の生成速度は 200 bit/s 以上と極めて低速ですが、それでも充分な程低速な毎秒 63 ビットずつの共通鍵を用いて I と Q データ用の 2 つの擬似乱数列を発生させていることです。これにより 1 秒当り 2^{63}-1（=9.2 x 10^{18}）ビットの安全性が担保された乱数列を I および Q データの暗号化に利用することが出来ます。

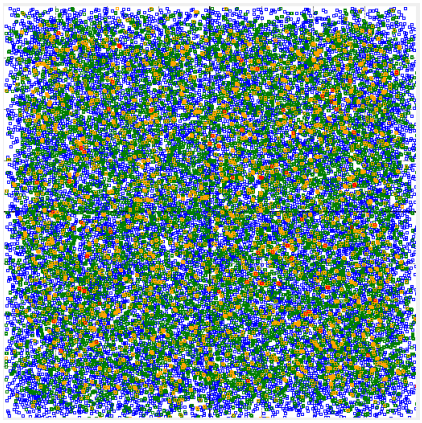
今回の QAM 型 QNSC 装置は 10 ビットで暗号化した I と Q データを 5 Gsymbol/s の速度で生成しています。そのため、それらデータの暗号化に必要な 1 秒当りの乱数列のビット数は高々5 x 10^9 x 10 = 5 x 10^{10} であり、この値は 4 値 QKD を利用して生成した乱数列のビット数 9.2 x 10^{18} と比べ十分小さいものです。従って、本システムでは常時 QKD 装置により高い安全性を保ちながら QAM 型 QNSC 装置による高速伝送を行うことが出来ています。

さらに、QAM 型 QNSC 装置では、適応等化の技術により QAM データの多値度を 4 から 128 値の範囲で任意に切り替えるように設計しました。このときデータの伝送速度は多値度に応じて 10～35 Gbit/s の範囲で切り替わります。この多値度の情報も QAM データとともに暗号化された状態で受信部へ配信され、この情報を元に送・受信者間の同期動作を実現しています。QAM データの多値度をランダムに切り替えることにより、暗号化・復号化のプロセスをランダムに出来るため、盗聴をより極めて困難なものにすることが出来ます。

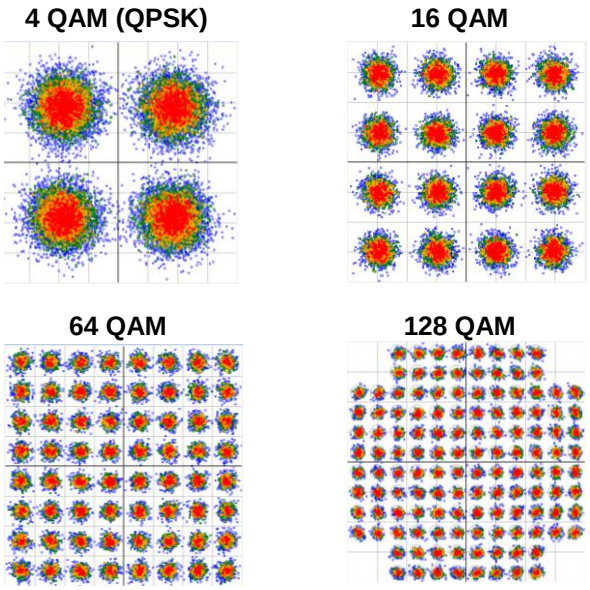
実測例として、4～128 QAM データを 100 km 伝送させた後の復号化前後における復調信号を図４(a)および(b)に示します。I および Q データはそれぞれ 10 ビットずつの多値度（1024 x 1024 値）で変調されているため、信号が雑音に埋もれてしまい、共通鍵の情報を持たない盗聴者には図４(a)のようにランダムに見えます。一方、正規受信者は共通鍵を用いて元の QAM データを復元し、図４(b)に示すように信号を明瞭に判別することが出来ます。図４(a)に示す復号化前の信号の中には、図４(b)に示す 4～128 QAM のいずれかのデータが埋もれていますが、その多値度情報も QAM 型 QNSC 方式により暗号化されているため、盗聴者はどのような変調方式で暗号化された信号であるのかを識別することすら出来ません。

(3) 多値 QAM によるデータ速度の高速性

今回の実験では最大で 128 (=2^7) 値の QAM 信号を 5 Gsymbol/s の速度で生成し、それを偏波多重して伝送しています。その結果、単一チャネルで 5 x 7 x 2 = 70 Gbit/s のビットレートを実現しています。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 7 ビットを暗号化し、その結果、伝送距離 100 km で世界最高速のデータ速度を実現することに成功しました。その周波数利用効率は 10.3 bit/s/Hz であり、伝送容量と距離の積は 7 Tbit/s・km に達します。



(a)



(b)

図４　100 km 伝送後に異なる時間に復号化した 4~128 値 QAM 信号
(a)復号化前（盗聴者），(b)復号化後（正規受信者）

【今後の展望】

今回の QAM 型 QNSC と 4 値 QKD を統合した秘匿光通信システムでは、信号の生成速度は 5 Gsymbol/s でありますが、暗号化および復号化回路を 10 Gsymbol/s に増大させることで容易に 100 Gbit/s 以上のデータ速度が実現出来ます。また WDM（Wavelength Division Multiplexing：波長多重）と呼ばれる既存の大容量化技術と組み合わせるとテラビット領域の暗号技術が容易に実現出来ます。一方、伝送距離は QKD 方式により 100 km に制限されていますが、複数台の QKD 装置を配置して量子鍵を多中継配信することにより、数 100 km の長距離伝送が実現可能です。

今日では QAM 方式を用いた 100 Gbit/s デジタルコヒーレント伝送技術は商用システムへの導入が始まっています。今回開発した秘匿光通信システムは、この光伝送システムそのものであり、光通信の流れとの整合性が高く、サイバー攻撃に強い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。

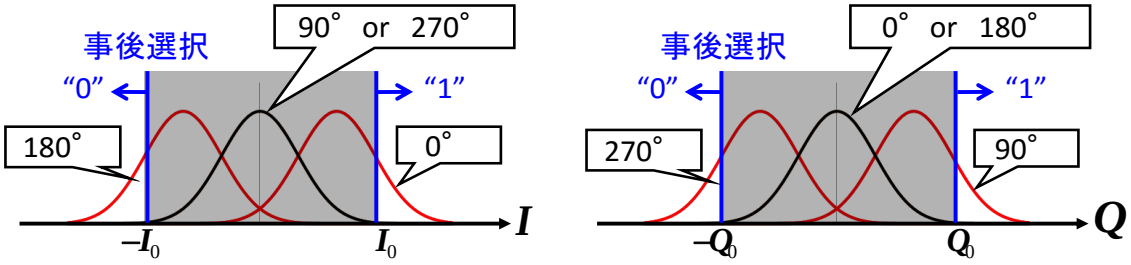
【QKD の動作原理にする補足】

今回の実験で使用した 4 値 QKD 方式を例にとり、QKD の動作原理について補足します。QKD システムの送信部では、図 1 に示すように、I と Q の直交関係にある 2 つのモードのいずれかをランダムに選択し、I モードでは、0 度でビット情報 “１”、180 度で “0” を送り、Q モードでは、90 度で “１”、270 度で “0” を送ります。送信者がどちらのモードを選んだかは、この時点では送信者以外はわかりません。正規受信者は I もしくは Q モードのいずれかに同位相の関係にある局発光源を用意し、ランダムにその位相を変えながら受信した信号とのホモダイン検波を行います。たまたま送信者と正規受信者が用いたモードが一致すれば、送信者が送ったビットと正規受信者の受け取ったビットは同一になります。しかし、二人の選んだモードが異なる場合には、正規受信者が受信するビットの値はランダムに決まるため、二人が同一のビットを共有できるとは限りません。そこで正規受信者はこのような送受信をある程度行った後で、毎回どちらのモードで送受信したかを送信者と電話などの通常の回線を用いて照らし合わせます。このやり取りは正規受信者と盗聴者の持っている情報が異なるため盗聴されても構いません。そのやり方で送信者と正規受信者の間でモードが一致した部分だけを採用すれば、両者で同一の秘密鍵を共有できることになります。これを「モード照合」と呼びます。

次に、盗聴者を発見する方法について説明します。盗聴者もモード情報を知りませんので、正規受信者と同様に読み出し誤りが避けられません。また、盗聴の事実を送信者と正規受信者に察知されないためには、読み出した光子を正規受信者に再送信する必要がありますが、盗聴者の読み出しが誤っていた場合には、その誤った情報をそのまま正規受信者に送ることになります。このような場合、正規受信者と送信者間での「モード照合」に誤りが特に増えることになります。もしこの様な食い違いが見られた場合には盗聴が受けた可能性があると判断してそのビットを捨てます。

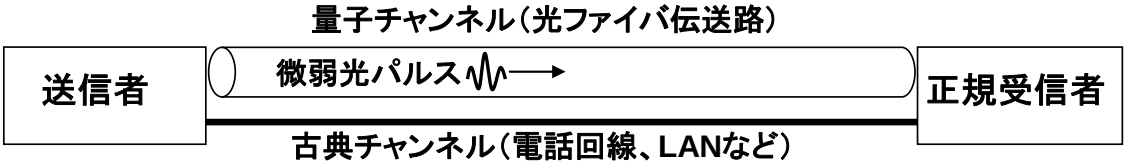
さらに、盗聴者に比べて正規受信者の読み出しの誤り率を低減し、正規受信者が優位に立てる仕組みとして、「事後選択」（Post-selection）方式を採用しています（図５）。正規受信者が、0 度と 180 度（I モード検出時）もしくは 90 度と 270 度（Q モード検出時）の閾値判定を行う際に、図５に示すように識別が容易な確率分布の少ないデータのみを事後選択します。これにより正規受信者は、自分に都合の良いデータを誤りなく事後選択出来ますが、盗聴者は受信者の選んだデータを総べて推測しなければなりません。その結果、正規受信者よりも盗聴者が誤る確率が大きくなり正確な情報を得られません。

QKD による鍵配信では、微弱な光を送る量子チャンネルに加え、電話や LAN 回線などの古典チャンネルを用いた信号処理技術が重要な役割を果しています（図６）。その古典的な信号処理として、先に述べた正規受信者がどのモードを選択して受信したのか送受信者間で照合する「モード照合」、誤り率を低減するための「誤り訂正」、さらには正規受信者が受信した信号に付与された雑音分布の形状より盗聴された可能性のある割合を算出し、その分量の鍵を削除して使用しないようにする「秘匿性増強」の 3 つの手法を用いています。



(a) (b)

図５　受信部における事後選択を用いた閾値判定の様子
(a) I モードを選択した場合, (b) Q モードを選択した場合



量子チャンネル・・・微弱光を送受信し、ビット情報を送受信者間で共有する。その際、観測（盗聴）されると状態が変わる量子力学的性質を利用して盗聴を検知する。

古典チャンネル・・・モード照合、誤り訂正、秘匿性増強のための情報を送受信する。盗聴は自由であるが改ざんができない性質を持つ通信路。

図６　QKD 方式で利用する 2 つの通信路の役割

問い合わせ先

東北大学　電気通信研究所
教授　中沢　正隆
電話　022-217-5522
E-mail　nakazawa@riec.tohoku.ac.jp

学習院大学　理学部物理学科
教授　平野　琢也
電話　03-3986-0221
E-mail takuya.hirano@gakushuin.ac.jp