基礎講座

量子暗号を用いた秘匿通信

荒平　慎

1．はじめに

インターネットの普及は我々の生活を便利で快適なものにする一方、重要な個人情報・機密情報の漏洩は大きな社会的問題となっています。暗号通信は秘匿通信を実現する方法として古くから研究・実用化されています。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(無意味)になるという意味で安全性が保証された方式です。このような安全性は計算量的安全性と呼ばれ、将来的な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ます(図－１)。

図－１　現在の暗号方式

それに対して、解読不可能な究極の秘匿通信を実現する暗号方式として、量子暗号が最近特に注目を集めています。本稿では量子暗号の基本的な仕組みについて紹介いたします。

2．量子暗号の特徴

一般の暗号通信では、暗号の送受信者が盗聴者の存在を確実に検出することは困難です。そのため盗聴者の存在を前提にして、解読を難しくすることで暗号の安全性を確保しています。それに対して量子暗号は、盗聴者の存在を確実に検出する(できる)ことにより暗号通信の安全性を確保します。

量子暗号においては、暗号通信の送受信者はまず、特殊な粒子(量子力学的粒子)を用いて暗号通信に用いる暗号鍵(秘密鍵)を作成します。その後、この秘密鍵を用いて通常の暗号通信を行ないます。

量子暗号を利用すると、送受信者は暗号セッションごとに異なる秘密鍵(ワンタイムパッド秘密鍵)を共有することができます。また盗聴者がこの秘密鍵を盗もうとした場合、量子暗号では盗聴の痕跡を検出することができます。そして、盗聴が検出されたセッションを破棄することで安全が確認された秘密鍵のみを共有することができます。このようなワンタイムパッド秘密鍵を用いた暗号通信は、解読不可能な暗号通信であることが証明されている唯一の暗号通信方法であり(情報理論的安全性)、これにより量子暗号では解読に用いるコンピュータの計算能力を問わず、安全な暗号通信を可能とします。

このように量子暗号の特徴は、暗号の送受信者が盗聴者に知られずに安全な秘密鍵を共有できる点にあります。そのため量子暗号システムはまた、「量子鍵配送」(Quantum Key Distribution、QKD)システムとも呼ばれています。

3．量子暗号の仕組み

量子暗号で用いる「量子力学的粒子」とは、「重ね合わせ状態」と呼ばれる特殊な物理状態にある粒子です。重ね合わせ状態とは、例えば光子の偏光測定をしたときに、個々の測定において横偏光(H)が観測されるか縦偏光(V)が観測されるかは確率的であり、測定前には定まっていない状態をいいます。サイコロを振ったときに出る目の状況に似ています。

このような粒子について一度測定(観測)をしてしまうと、測定前の状態がどのような状態であったかは測定後には知ることができません(「波動関数の収縮」と呼ばれます)。例えば、測定結果がH偏光であった光子が、測定前に100％の確率でH偏光であったのか、それともH偏光状態を確率50％で含む右・左回り円偏光

状態(R、L)であったのかは、測定後には知ることができません。

これを利用すると、正しい測定方法(測定系)を利用した相手(受信者)にのみ正しい測定結果を送ることができ、異なる測定系を用意した相手(盗聴者)には確率的に誤った結果を生じさせることができます。これはまた、盗聴者が送った信号を受信した正規の受信者は、正しい測定系を用いても確率的に誤った結果を得ることを意味します。

従って送受信者は、測定結果(の一部)を互いに照合し誤り率を測定することで盗聴者の存在を知ることができます。

このような盗聴検出を可能にするためには、理想的には一個の粒子を用いる必要があります。複数の粒子が存在すると、一般の暗号通信の場合と同様に、盗聴者は送受信者には知られずにその一部を盗み出すことで盗聴が可能になるためです。

盗聴が検出された場合、それまでの結果を破棄して、また新たに測定をやり直します。ここまでの過程では、送受信者はまだ伝えたい情報(平文)を送っていないので、この段階で情報が漏洩することはありません。

誤り率が規定値より低く、量子暗号プロトコルが成功した場合、H偏光とV偏光(またはR偏光とL偏光)の測定結果をそれぞれビット「1」、「0」に対応させることで、送受信者は盗聴者の知らないランダムなビット列(ワンタイムパッド秘密鍵)を共有することができ、これを用いて安全な暗号通信が可能となります。

量子力学的粒子としては、通信距離を長くするために光(光子)を利用するのが一般的です。

4．量子暗号プロトコル

量子暗号の基本的な仕組み(プロトコル)は1984年にBennettとBrassardにより発明され(BB84方式と呼ばれます)、その後様々な変形プロトコルが開発されてきました。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 量子もつれ光を用いる方式(E91、BBM92方式)

に大別されます(図－２)。

現在実用化研究が先行しているのはBB84方式であり、プロトタイプ機器の試作や商用アクセス通信網を利用したフィールド試験など、商用化開発が進展しています。

一方量子もつれ光を用いた方式(BBM92方式)はまだ研究レベルに近いですが、BB84方式に比較してより高い安全性を確保できること、また将来的には量子中継技術を利用した長距離伝送が期待できることなどから、次世代量子暗号通信システムとして期待されています。

5．量子暗号を実現するデバイス

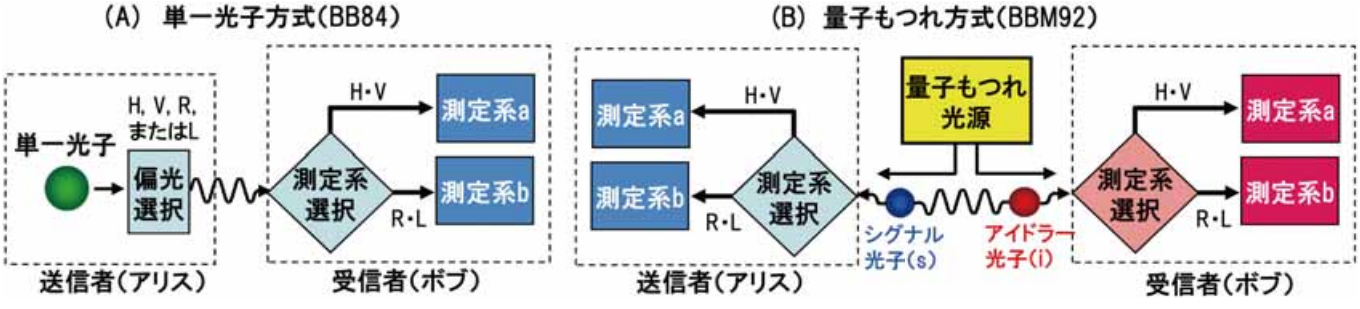
量子暗号を実現するためには、単一光子もしくは量子もつれ光を発生する単一光子源、量子もつれ光源、ならびに単一光子を検出するための単一光子検出器の開発が必要不可欠になります。量子暗号通信においては、盗聴を防ぐために１パルスあたりの平均光子数は１以下(通常、0.1個／パルス程度)としますので、使用する光源・検出器としては、十分に低い雑音特性を有したものが必要となります。

また通信距離を延ばすためには、光ファイバを通信チャンネルとして用いるのが望ましく、使用波長としては、一般の光通信と同様、1.51m帯が最も好適です。

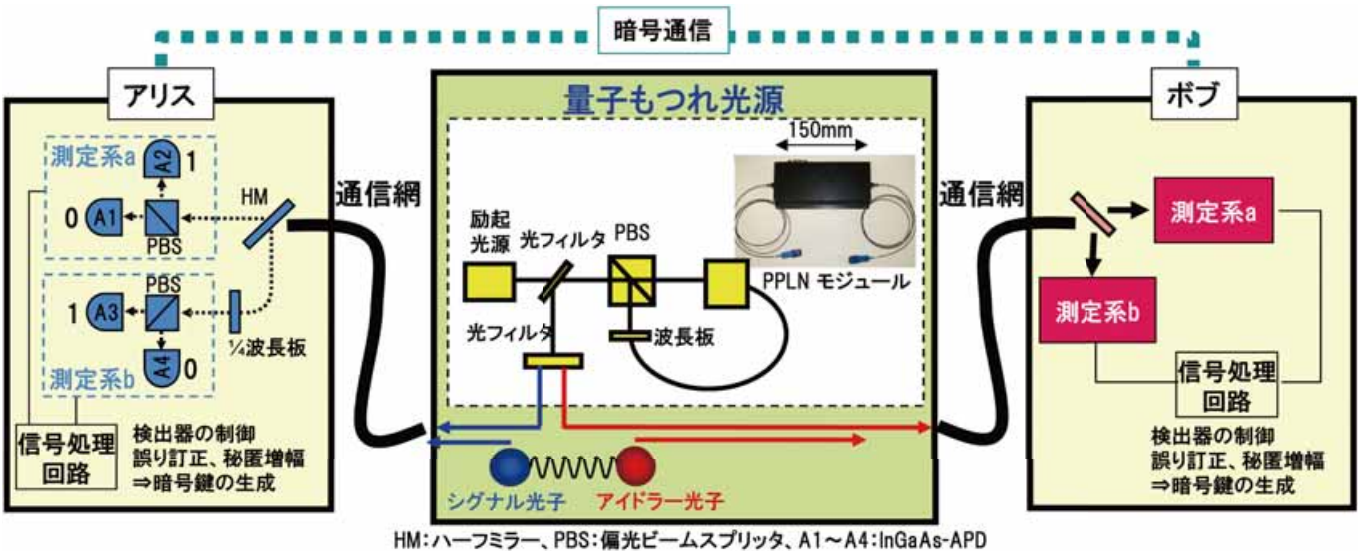
単一光子源としてはレーザ光を極弱い強度に減衰させた擬似的な単一光子源が多くの実証実験で使用されています。また最近では、より理想に近い単一光子源として、量子ドット光源などが研究されています。

また量子もつれ光源としては、特殊な光デバイス中で生じる、自然パラメトリック変換と呼ばれる非線形光学効果が利用されています。

単一光子検出器については、半導体素子を用いたもの、超伝導素子を用いたものなどが研究されています。一般の光通信でも使用されてい



図－２ 量子鍵配送プロトコル (A)単一光子方式 (B)量子もつれ光方式



図－３　量子もつれ光を用いた量子暗号通信システム

るInGaAsアバランシェフォトダイオード(APD)もまた、単一光子検出器として多くの実証実験で利用されています。

これらの光源、検出器を用いて、現在のところ数十km～200km程度の伝送実験の報告がなされています。

量子暗号は最先端の光デバイス開発を必要とする先端技術ですが、一方で、量子暗号はまたユーザの多種多様なニーズを満足するために情報通信システムが提供するサービスの一環でもあります。従って一般の光通信の場合と同様に、これらを実現する上でのコストや信頼性もまた、実用化へ向けた重要なファクタとなります。

量子暗号通信システムの構成例として、量子もつれ光源を用いた量子暗号通信システムの構成例を図－３に示します。

６．おわりに

秘匿通信の重要性は今後もますます高まっていくものと予想されます。量子暗号技術は解読不可能な暗号通信を実現するほぼ唯一の暗号通信方式として、欧米や他のアジア諸国でも研究開発が活発化しています。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ます。

（あらひらしん：沖電気工業(株)）