Q 量子鍵配送について教えてください

A

量子鍵配送とは

量子鍵配送は信頼された2者に対して「暗号鍵」を供給する方式の1つです．量子鍵配送では，量子力学の原理を利用して，盗聴が検知できる通信チャネルを形成し，そのうえで暗号鍵の情報を送受信します．もし，盗聴が検知された場合には，その暗号鍵を破棄して，別のチャネルで再度送付します．ひとたび2者間で安全な暗号鍵が共有できれば，ワンタイムパッド（使い捨て鍵）方式と呼ばれる暗号方式を用いることにより，インターネットなどの通信回線を使って絶対的に安全な暗号通信が可能となります．

量子鍵配送システム

量子鍵配送システムの簡単な構成を**図1**に示します．慣例に従って，送信者をアリス，受信者をボブ，盗聴者をイブと呼ぶことにします．通信チャネルの形成には，光の粒である光子を利用することが一般的です．アリスは，光子の偏光や位相に鍵ビットの情報を載せてボブに送付します．ボブは，アリスから送られてきた光子の偏光や位相を測定し，鍵ビットの情報を読み出します．これを繰り返すことによって暗号鍵の伝送を行います．もし，イブが途中で盗聴を行うとアリスが送付した光子の状態が変化してしまうため，アリスが送付した鍵ビットの情報と違う情報がボブに伝わってしまいます．アリスとボブは，時々鍵の情報を公開し合い，盗聴が行われていないかをチェックしているため，暗号鍵の不整合から盗聴に気づくことができます．

BB84プロトコル

次に，具体的な量子鍵配送プロトコル（手順）を紹介します．ここでは，BB84と呼ばれる量子鍵配送プロトコルを紹介します．これは，BennetとBrassardにより1984年に提案されたプロトコルで，もっともポピュラーな方式です．光子の偏光を利用した場合を例にとって，簡単に説明します．BB84プロトコルでは，**図2**のように光子の4つの状態を利用します．ここでは，偏光の縦，横，右回り，左回りの4つを使います．アリスは，上記の4つの状態のうち1つをランダムに選択して，その偏光の光子をボブに送付します．ボブは，4つの状態を同時に判別することはできないため，縦もしくは横が判別できる直線偏光検出系，右回りもしくは左回りが判別できる円偏光検出系のいずれかをランダムに選択して，検出を行います．アリスが，縦もしくは横偏光の光子を送付して，ボブが直線偏光検出系で検出した場合には，偏光状態が判定できます．すなわち正しいビット情

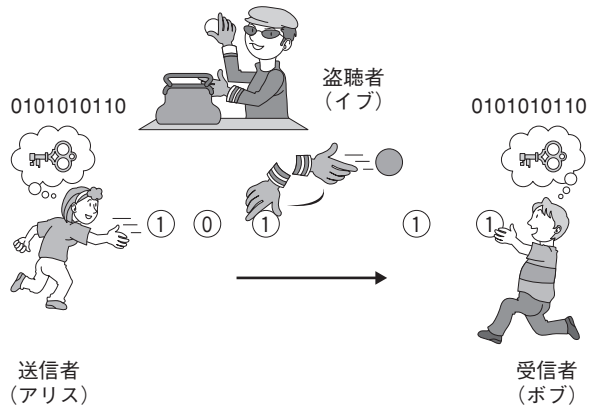

図1　量子鍵配送システムの構成

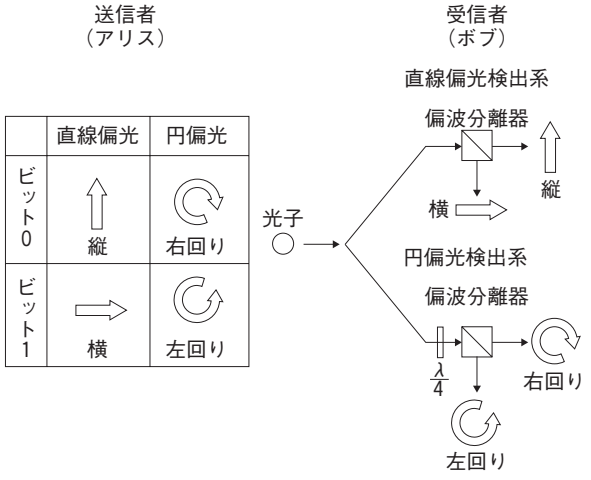

図2　BB84プロトコル

報が送れます（これを観測基底が一致した場合と呼びます）．しかし，円偏光検出系で検出した場合には，アリスの送出した偏光状態は判別できません（これを観測基底が一致しなかった場合と呼びます）．アリスが右回りもしくは左回り偏光の光子を送付した場合も同様です．そして，ボブは光子を受信した後，どちらの検出系を用いたかをアリスに伝えます．アリスは，それに対して基底が一致していたか否かを回答します．基底が一致していた場合には，鍵ビットの情報の伝送に成功します．しかし，一致していない場合には，鍵ビットの情報は伝送できないので，その光子に関する情報は破棄します．上記を繰り返すことにより，暗号鍵の伝送が可能になります．

ここで，イブの盗聴について考えてみます．イブの戦略としては，アリスから送られてきた光子を横取りして，鍵ビット情報を盗み，同じ状態の光子をボブに送れば盗聴成功となります．しかし，イブもボブと同じように検出方法を選択しなければなりません．このため，イブの盗聴は50％の確率でしか成功せず，50％の確率で偏光状態の異なる光子をボブに送ることになります．この誤った偏光の光子が鍵ビットの不一致を誘発することになり，盗聴が発覚します．以上がBB84と呼ばれるプロトコルです．

ここでは，光子の偏光を用いた例を使って簡単に説明しましたが，伝送路としてよく使われる光ファイバ中では通常，偏光状態は保持されないため，偏光に鍵ビット情報を載せる方法は，光ファイバ伝送には向きません．そこで，光ファイバを伝送路に用いた量子鍵配送では，光子の偏光ではなく位相に鍵ビットの情報を載せることが一般的です．

差動位相シフト量子鍵配送

最後に，NTTの提案する新しい量子鍵配送方式である差動位相シフト量子鍵配送方式を紹介します．この方式では，光パルス列の位相差が一部しか読み出せないということを利用しています．**図3**に構成図を示します．アリスは，0もしくはπのランダムに位相変調した光パルス列を10パルスに1光子程度しか含まない程度まで減衰して送出します．ボブは，1パルス分（1ビット分）の遅延を持った干渉計を用いて，各パルス間の位相差を検出します．ボブは，検出できた位相差の情報から鍵ビットを生成します．そして，アリスには検出できた時刻だけを伝えます．アリスは，ボブからの時刻情報と自らの変調情報から鍵ビット列を生成します．この方式は，簡便な構成でファイバ伝送に適していること，暗号鍵生成効率が高いことなどから，注目を集めています．

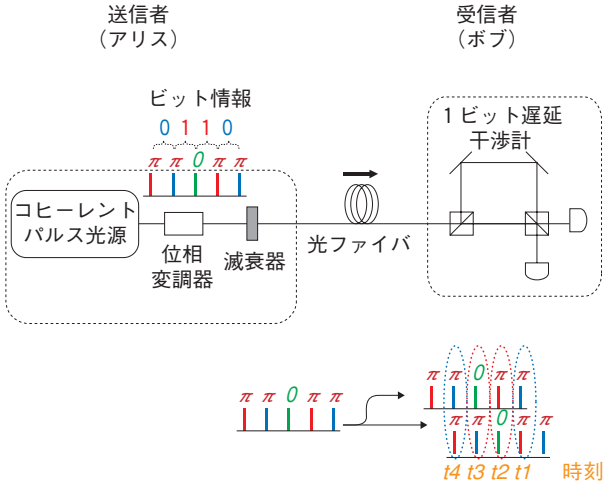

図3　差動位相シフト量子鍵配送

今後の展開

これまでに，光子1個の状態を利用した量子鍵配送実験が，広く行われてきており，成功を収めてきました．しかし，この方法では伝送路のロスなどにより，伝送距離に限界があります．このため，伝送距離を伸ばすためには，中継技術の開発が必須です．量子鍵配送では，古典光通信におけるアンプを用いた中継などは原理的に行えません．このため，量子相関のある光子対を用いて中継を実現する方法があり，今後はこれらの分野が盛んになると思われます．

このコーナで取り上げて欲しい質問をE-mailで編集部までお寄せください．
●(社) 電気通信協会内　NTT技術誌事務局　E-mail　jimukyoku@tta.or.jp