2.3.2 量子暗号

井上恭
電気電子情報工学専攻・教授

2.3.2.1 はじめに

情報通信システムが現代社会の基盤として浸透するにつれ，通信の秘匿性・安全性がますます重要になってきている．現在広く用いられている暗号システムは公開鍵方式と呼ばれ，その安全性は暗号化されたデータを解読するのには膨大な計算量を必要とすることにより確保されている．しかしながらこれは，現在の計算機能力では解読困難というだけで，原理的に安全というわけではない．これに対し，バーナム秘密鍵方式と呼ばれる暗号通信方式は，絶対に安全であることが証明されている．ただしこの方式では，同じ秘密鍵を送受信者が共有する必要があり，その秘密鍵をいかに安全に両者に供給するかが大きな問題であった．そこで近年，バーナム暗号通信のための秘密鍵（実体はランダムなビット列）を，量子的物理現象を利用して安全に供給する量子暗号の研究が進められている．鍵の安全性は量子力学の原理により保証されており，これをバーナム暗号通信に適用することにより，究極的に安全な暗号通信が実現される．

量子暗号にもいくつかの方式がある．中でもBB84と呼ばれる方式は，量子暗号として最初に提案されたものあり，広く研究されている．これに対し本事業推進担当者は，差動位相シフト（Differential Phase Shift:DPS）と呼ばれる新しい量子暗号方式を提案し，その研究開発を進めている．本方式は，BB84に比べ，構成が簡便，秘密鍵供給効率が高い，光子数分岐攻撃と呼ばれる盗聴法に強い，などの特徴を有する．今年度はこの量子暗号方式について，（１）波長変換型光子検出器を用いるシステムの偏波無依存化，（２）デコイパルスを用いる改良プロトコルの提案，（３）量子雑音を利用する改良プロトコルの提案，などを行った．以下，DPS方式を説明した後，各項目について述べる．

2.3.2.2 DPS量子暗号方式

図2.3.2.1にDPS方式の基本構成を示す．送信者（慣例的にアリスと呼ぶ）は，レーザからの連続光を光強度変調器により一定間隔の光パルス列とし，各パルスの位相を0またはπでランダムに変調し，それを平均0.1-0.2光子/パルスという光パワーまで弱めて送信する．受信者（慣例的にボブと呼ぶ）は，送られてきた光パルス列を２分岐し，一方に１パルス分の遅延を与えた後，再び合波する．これにより，前後２パルスが重なり合って干渉する．干渉の結果，２パルスの位相差が0なら検出器1が，πなら検出器2が，それぞれ光子を検出する．ボブは，検出器１による光子検出を「０」，検出器2による検出を「１」としてビットを生成する．ただし，送信パワーが平均0.1-0.2光子/パルスなので，光子は稀にしか検出されない．そこでボブは事後に，光子検出時刻をアリスに知らせる．するとアリスは，自分の位相変調データと光子検出時刻を照合することにより，光子検出した検出器を知る，すなわちボブのビットを知る．これにより，アリスとボブは同じランダムなビット列（＝秘密鍵）を得る．

ここでのポイントは，光子の干渉を利用している点である．光子はぽつりぽつりと検出されるのであるが，検出のされ方は波の干渉効果に従っている．光の粒子性と波動性が現われているということである．干渉効果が起こるためには，光子状態が確定していない必要がある（これを量子力学的重ね合わせ状態という）．重ね合わせ状態は観測すると確定状態に変化して干渉効果は消える．そのため，

伝送途中で盗聴が行われると干渉が消滅する．そこで，干渉特性をモニターすることにより盗聴を発見することができる．

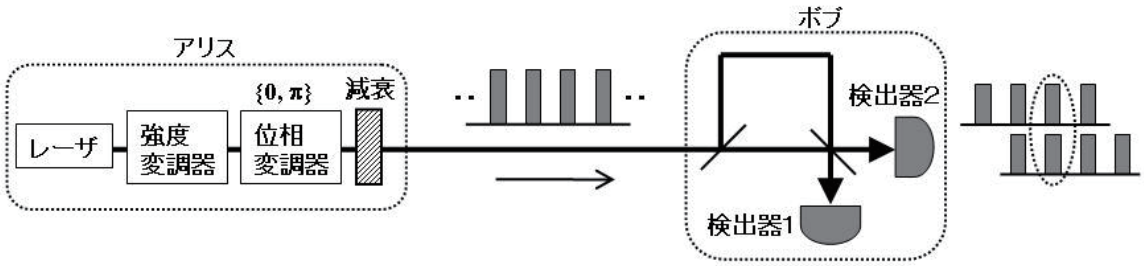

図2.3.2.1 DPS量子暗号方式の基本構成.

2.3.2.3 波長変換型光子検出系を用いるシステムの偏波無依存化

量子暗号システムにおいては，光子検出が大きな課題である．これには通常，APD（アバランシェ・フォトダイオード）が用いられるが，ファイバ通信波長帯用のAPDで光子検出する場合には間欠的にしか動作させられず，鍵生成速度の制限要因となっている．一方，短波長用APDは連続動作が可能である．そこで，通信波長光子を波長変換して短波長APDで検出する光子検出法が研究されているが，波長変換の際に偏波依存性があることが実装上の課題であった．これに対し，送信パルス列を交互に直交偏波変調して光子受信系の偏波依存性を解消する方法を提案し，実証実験を行った．

2.3.2.4 デコイDPS方式

DPS方式のシステム性能（鍵生成速度/伝送距離）を向上させるべく，改良方式を提案した．平均0.1-0.2光子/パルスである送信パルス列に，平均１光子のパルス（デコイパルス）を時々紛れ込ませる．このようにすると，正常時と盗聴時との受信状態との差異が大きくなって盗聴が発見しやすくなり，その結果，システム性能が向上する．シミュレーションにより，伝送可能距離が従来方式の約1.4倍となることが示された．

2.3.2.5 量子雑音利用DPS方式

前記のように，光子検出が量子暗号システムの大きな課題である．そこで，大きなパワーの信号光を送信し，これを通常の光受信器で検出して秘密鍵を生成する方式を提案した．送信光の変調位相は$\pm\delta$とし，$Ae^{\pm i\delta}$という２つのコヒーレント状態が量子雑音のため一部重なるようにδを設定する（図2.3.2.2）．量子雑音のために２状態が完全には識別できないことにより，鍵の安全性が確保される．この方式は，伝送距離は大きくできないが，通常の光受信器が使用可能なため高速動作が期待される．

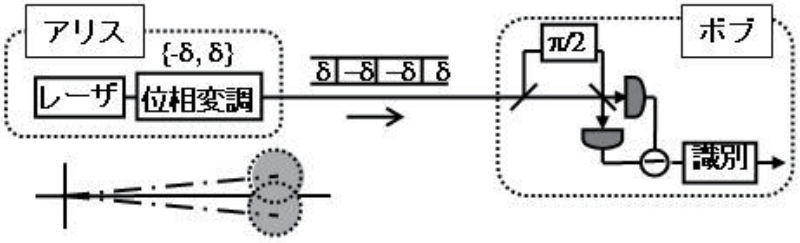

図2.3.2.2 量子雑音を利用するDPS量子暗号方式.