光通信における量子暗号技術

井　上　　恭

Quantum Cryptography in Optical Communications

Kyo INOUE

Quantum cryptography has been intensively studied, which provides a secrete key to two legitimate parties for ciphering/deciphering a message. The unconditional security is guaranteed based on the law of quantum mechanics, where the double properties of light, wave and particle, are used. This article describes quantum cryptography; how it utilizes quantum mechanics and the state of art of the technology.

Key words: quantum cryptography, quantum mechanics, photons, secrete key

「光は波動であり粒子である」というのは，量子力学の根幹的な命題である．量子力学の教科書を広げると，おおむね，空洞放射スペクトルやアインシュタインの光量子説，あるいは1光子レベルのヤングの干渉実験から話が始まっており，量子力学における光の量子性の重要度がうかがえる．ところが，量子力学の工学応用の局面に目を向けると，半導体やレーザーなど，原子系は量子的に取り扱われている一方で，光系は古典的取り扱いで十分，というのがもっぱらである．CCDなどでは光量子が利用されているといえるかもしれないが，波動と粒子の二重性が用いられているわけではない．量子暗号は，「光は波動であり粒子である」という性質を利用したシステムである．工学応用面では出番のなかった光の量子性が，ここにきて役に立つ（かもしれない）ようになってきた，といったところであろうか．ただ，本当に実用化されるのかと問われると，はっきりイエスと答えられないのが正直なところである．本稿では，量子暗号について，量子力学がどのように利用されているか，技術の現状，などを紹介する．

1.　量子暗号とは

量子暗号通信と一般に称されているが，実は量子を使って通信をしているわけではない．暗号通信には，送受信者が同じ秘密鍵を所有し，それを用いてデータを暗号化/復号化する秘密鍵方式とよばれる方法がある．ここで使う秘密鍵を，離れた二者に安全に供給するのが量子暗号システムである．秘密鍵が他者に知れられていないことを保証するのに，光の量子性が利用される．したがって，より正確には，量子鍵配送（quantum key distribution）と呼称される．しかし，これもまた正確ではない．配送というと一方がもっている鍵を他方に送るイメージであるが，光子の送受信をベースにして両者が共通の鍵を作り出すのが量子暗号の実際である．さらにいえば，鍵生成過程で相手が偽者でないことを認証するステップが必要で，そのための秘密鍵をあらかじめ共有していることが前提となる．つまり，認証用秘密鍵を元手に，データ転送用秘密鍵まで増殖させるのが量子暗号システムの機能といえる．

2.　量子暗号の原理

量子暗号の説明は偏波を例になされることが多いが，ここでは1光子のヤングの干渉実験との類似性から，1光子を2パルスに分けたときの位相差を用いる方式について説明する．実際，ファイバー伝送系の実験のほとんどはこちらを採用している．図1にその基本構成を示す．送信側では，1光子を経路長の異なるマッハ・ツェンダー干渉計に通し，時間位置の異なる2パルスとする．1光子が2つに分割されるわけではないが，確率振幅として2つに分かれる．このあたりの事情は，ヤングの干渉実験で1光子がダブルスリットに分かれるのと同じである．ここで，干渉計の一方の経路上に位相変調器を置き，2パルス間の位相差を $\theta_a = \{0, \pi\}\ \{\pi/2, 3\pi/2\}$ の4値のいずれかとして送信す

大阪大学工学系研究科電気電子情報工学専攻（〒565-0871 吹田市山田丘 2-1）　E-mail: kyo@comm.eng.osaka-u.ac.jp

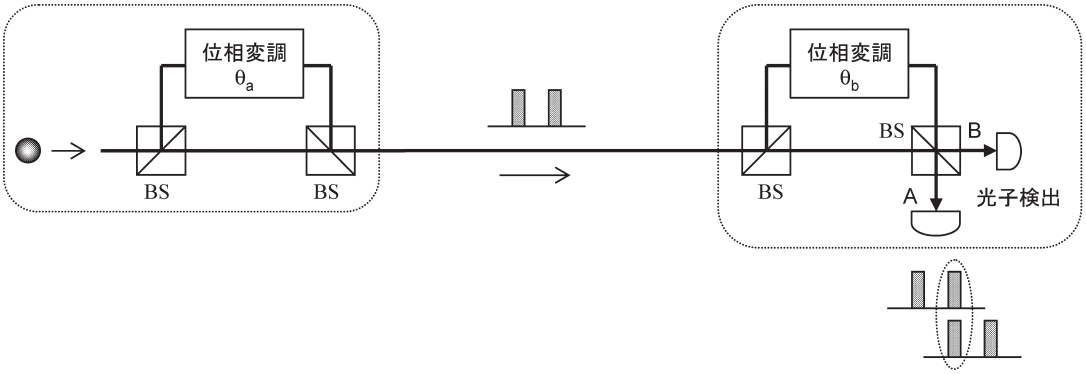

図1　パルス間位相を利用する量子暗号システム．BS：ビームスプリッター．

る．受信側では，受信光を送信側と同様の干渉計に通す．これにより，長経路を通った1番目の確率振幅と短経路を通った2番目の確率振幅が干渉し，位相差に応じて干渉計出力端のいずれかで光子が検出される．確率振幅どうしが干渉するのは，1光子のヤングの干渉実験において，スリットの反対側で干渉が起こるのと同様である．ここで，受信側干渉計の位相変調器は，2経路間に $\theta_b=\{0$ または $\pi/2\}$ の位相差をつけるように動作する．

入力位相差 θ_a に対する干渉計出力端子Aでの光子検出確率は，θ_b に依存して図2のようになる（端子Bは相補的な形）．(θ_a, θ_b) の組み合わせが $(0, 0)$，$(\pi, 0)$，$(\pi/2, \pi/2)$，$(3\pi/2, \pi/2)$ だと，100% の確率で，それぞれ端子A，端子B，端子A，端子B，で光子が検出される．その他の場合，AとBとでの検出確率は50%：50%である．この動作特性を利用して，次の手順により秘密鍵を生成する．(1) 光子送受信後，受信者は検出した光子について，θ_b が0または $\pi/2$ のどちらであったかを送信者に知らせる．(2) 送信者は該当する光子について，θ_a が $\{0, \pi\}$ または $\{\pi/2, 3\pi/2\}$ のどちらであったか（4値のどれであったかではなく）を受信者に知らせる．(3) 位相差が，$\theta_a=\{0, \pi\}$ かつ $\theta_b=0$，または $\theta_a=\{\pi/2, 3\pi/2\}$ かつ $\theta_b=\pi/2$，であったら，送信者は $\theta_a=0$ または $\pi/2$ をビット「0」，$\theta_a=\pi$ または $3\pi/2$ をビット「1」とし，受信者は光子検出@端子Aをビット「0」，光子検出@端子Bをビット「1」とする．これらの場合の光子検出確率は確定的なので，送受信者のビットは同一となる．これを秘密鍵とする．上記以外の場合の送受信結果は無視する．

以上のシステムに対し第三者が盗聴を試みても，光の量子性により成功しない．まず，盗聴者が信号の一部を盗み聞く方法は，送られているのが1光子であることからうまくいかない．盗聴すると受信者には何も届かず，鍵ビットとはならないからである．ただし，弱めたレーザー光を使うシステムにおいては，有限の確率で1パルスに2個以上

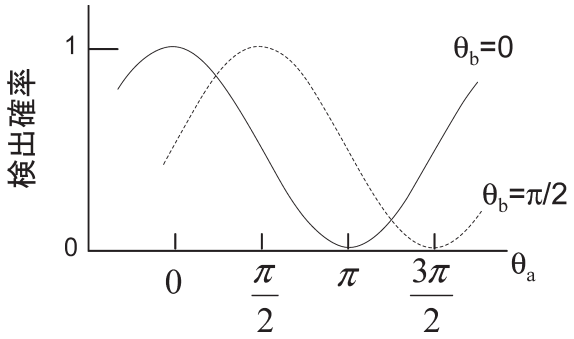

図2　受信側干渉計の出力特性．

の光子が存在し，それから情報が一部漏洩しうる．これに対しては，プライバシー増幅というソフト的手法により対処する．さらに手のこんだ盗聴法としては，伝送中の信号を測定し，測定結果に基づいた偽装信号を受信者に送る方法が考えられる．しかしながらこの場合，送られているのは1光子なので，測定できるのは1回限りである．1回の測定では，$\{0, \pi/2, \pi, 3\pi/2\}$ の4値すべてを識別することはできない．例えば，位相差0の干渉計を使えば $\{0, \pi\}$ は特定できるが $\{\pi/2, 3\pi/2\}$ は識別不可である．したがって，ある割合で不確定な偽装信号を送ることになり，送受信者が正規の手順で秘密鍵を生成すると両者で一部不一致が生じる．そこで，テストビットを照合することにより盗聴行為が露呈する．逆にいうと，不一致がなければ盗聴されていない鍵ということになる．このように，1光子であることにより盗聴を予防しつつ干渉効果を使って鍵ビットを生成しており，光の二重性を巧みに利用したシステムとなっている．（なお一般には，波動関数の重ね合わせ原理や観測による状態の収縮などから量子暗号を説明するのが正統的であり，量子もつれを使う量子暗号にはこちらの説明法が必要であるが，ここではわかりやすい説明を採用した．）

図1の構成を実際に動作させようとすると，干渉計の安

定性が問題となる．これの解決法として，光を送受信間で折り返し伝送し，2パルスの通過経路を同一とすることにより自動的に位相差ゆらぎを補償する「プラグアンドプレイ」[1]とよばれるシステムが提案されている．これまで行われたファイバー伝送実験のほとんどは，この構成を採用している．

また，上記以外にも，光通信で研究されている光DPSK（差動位相シフトキーイング）を量子暗号に応用した方式が提案・実証されている[2]．導波路干渉計を用いて安定な一方向伝送が実現されており，高効率，光子数分岐盗聴に強い，などの特長を有している．

3. 技術の現状

量子暗号実験には，従来の光通信用部品がおおむね利用可能である．光源としては，1パルスに1光子のみを発する単一光子光源が理想であるが，通常は極度に減衰させたレーザー光が使用される．一番の課題は光子検出器である．アバランシフォトダイオードを光子検出時だけ高バイアスにして用いるが，バイアスを高くし過ぎるとダークカウント（光子がないのにアバランシが起こる現象）による誤動作が起こり，バイアスが低いと検出効率が低下する．また，バイアスをかける繰り返し周波数が高いと誤動作が連鎖する現象が起こる．現状では，量子効率＝10%，ダークカウント率＝10^{-5}/ゲート，繰り返し周波数＝数MHz，が典型的な値であり，量子暗号システムの性能（特に鍵生成レート）はほとんど光子検出器の性能で制限されている．

システム実験としては，伝送距離＝数十km，鍵生成レートが数kbpsより小さいものが，屋外実験を含め各種報告されているが[*1]，生成した鍵の安全性の条件がまちまちで単純な数値比較はできない．最もポピュラーな弱レーザー光使用BB84方式（BenettとBrassardが1984年に提案した方式）の場合，真に安全な鍵が生成できる限界は約50 kmとされている．DPSK方式だと，光子数分岐盗聴に強いことから100 km程度（上限は未解明）までは可能である．

単に光子を送受信するシステムでは50〜100 km程度の伝送距離が限界であるが，量子もつれ光子対という特殊な光子を用いると，量子中継あるいは量子リレーとよばれる方法により，さらなる長距離化が可能である．ただし，これに関しては，初歩的な実験が報告されている段階で，実際に長距離伝送実験を行うには至っていない．

以上，量子暗号について述べた．最後に，実用システムへの応用の可能性であるが，よくわからないというのが正直なところである．実現されている性能（伝送距離，鍵生成レート）がまだ不十分ということもあるが，これは今後向上する可能性もあるだろう．それよりも，閉空間であるファイバー伝送路内の光信号を盗聴から守るという需要があるかどうかがよくわからない．特に，量子暗号研究では，将来いかなる技術革新があっても絶対に安全，という謳い文句のもとに，とても現実にはありえない盗聴技術も検討対象とされている．究極を追求するというスタンスの研究であり，それが世の中に出て行くのか，いまのところ不明である．

文　献

1) A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden and N. Gisin: “ “Plug and play” systems for quantum cryptography,” Appl. Phys. Lett., **70** (1997) 793–794.
2) T. Honjo, K. Inoue and H. Takahashi: “Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer,” Opt. Lett., **29** (2004) 2797–2799.

(2005年7月2日受理)

[*1] 光産業技術振興協会2004年度光技術動向調査報告書2.8章（http://www.oitda.or.jp/main/technology/technology0502.pdf）.