量子暗号システムの研究

井上　恭

大阪大学大学院工学研究科
電気電子情報工学専攻

概要：　量子力学の原理により、究極的に安全な暗号通信を実現する技術として、量子暗号の研究が進められている。これは、離れた2者に暗号通信のための秘密鍵を安全に供給する技術で、より正確には量子鍵配送（QKD）と呼ばれている。本研究室では、独自に考案した差動位相シフト（DPS）QKDという量子鍵配送方式をベースに、改良プロトコルの提案や各種盗聴を考慮したシステム性能の見積もり、さらには実証実験などを行っている。これまで具体的には、（1）光子検出器を用いない巨視的コヒーレントDPS-QKD方式の提案・システム評価、（2）差動4値位相シフトQKD方式の提案・理論解析・実証実験、（3）デコイパルスを用いるDPS-QKD方式の提案、（4）DPS量子秘密共有システムの提案・実証実験、（5）波長変換型光子検出器を用いるDPS-QKDシステムの偏波無依存化、（6）DPS-QKDにおける光源要求条件の明確化、などを行なってきた。

はじめに

様々な情報が通信ネットワーク上を行き交う高度情報化社会では、通信の秘匿性が重要度を増しており、そのための暗号通信技術が必要とされる。暗号通信の基本構造は、送信者が送信データを秘密鍵により暗号化し受信者がそれを復号化するというものであるが、現在用いられている暗号通信システムは、盗聴者が暗号データを解読するには膨大な計算量が必要であり実際上解読不可能であるように構築されている。しかしながらこれは、実際上不可能というだけで、絶対的な安全性を保証するものではない。

これに対し、物理原則に基づいて原理的に安全な暗号通信システムを提供するのが量子暗号である。暗号通信には、バーナム暗号（またはワンタイムパッド暗号）と呼ばれる方式がある。これは、送信データと同じ長さの秘密鍵を用いて暗号化/復号化を1回のみ行なう方式であり、秘密鍵が漏洩していない限り絶対に安全であることが数学的に証明されている。量子暗号は、バーナム暗号用の秘密鍵を量子力学の原理を利用して離れた2者に安全に供給する技術である。鍵を供給するシステムであるので、より正確には量子鍵配送（Quantum Key Distribution: QKD）と呼ばれる。秘密鍵を絶対安全に供給できれば、それを使って絶対に安全なバーナム暗号通信が可能となる。

量子暗号の最初の提案は、1984年にBennett-Brassardによってなされた。この方式は、提案者の名前と提案年からBB84プロトコルと呼ばれている。その後、E91、B92、BBM92などいくつかの方式が順次提案されてきたが、現在でもなおBB84が量子暗号研究の主流となっている。これに対し筆者は、2002年（NTT在職時）に差動位相シフト（Differential Phase Shift: DPS）と呼ぶ新しい量子暗号方式を提案した。本方式は、従来方式に比べ、構成が簡便で高い鍵生成速度が可能という特徴を有している。提案以来、NTTを中心にシステム実験が進められ、2007年には12bps-200km/17kbps-100km伝送というトップデータを記録している。

本研究室では、このDPS-QKD方式をベースとして、改良プロトコルの提案、各種盗聴を考慮したシステム性能評価、検証実験、などを行なっている。本稿では、そのうちのいくつかを紹介する。

研究成果

まず、基本となるDPS量子鍵配送について説明しておく。図1は、DPS-QKDの基本構成である。送信者は、$\{0, \pi\}$でランダムに位相変調したコヒーレントパルス列を平均1光子／パルス未満（例えば0.2）まで減衰させて送信する。受信者は、受信したパルス列を1ビット遅延干渉計に通して前後のパルスを干渉させる。干渉の結果、パルス間位相差が0ならば検出器Aで、πならば検出器Bで、それぞれ光子が検出される。ただし、平均1光子／パルスであるので、光子検出される時刻は稀かつランダムである。光パルス列送受信後、受信者は送信者に光子検出時刻を通知する。送信者は、光子検出に対応するパルスについて、自身の変調位相差が0ならばビット「0」を、πならばビット「1」を生成する。一方受信者は、検出器Aによる光子検出事象をビット「0」、検出器Bによる光子検出事象をビット「1」とする。このようにして生成したビットは、送受信者で同一となる。これを秘密鍵とする。このシステムにおいては、伝送信号光パワーが平均1光子／パルス未満であるがために、盗聴者は全ての位相差を読み取ることはできず、したがって鍵ビットを得ることができない。これにより、生成した秘密鍵の安全性が確保されている。

＜巨視的コヒーレントDPS量子鍵配送＞

上記DPS-QKDでは、単一光子検出により鍵ビットを生成していた。しかし現実には、光子1個の検出は容易ではなく、QKDのシステム性能（鍵生成速度、伝送距離）は概ね光子検出器によって制限されている。また、APDを冷却して使用するなど高度な実装技術が必要である。そこで、光子検出に拠らない量子鍵配送方式を考案した。基本的な装置構成は図1と同様であるが、送信者の変調位相は微小値$\pm\delta$とし、送信光パワーを受信側で通常の光検出器で検出可能なレベルとする。ここで、位相がδと$-\delta$の2つの信号状態は、コヒーレント光に不可避に備わっている量子雑音により、複素振幅空間上で一部が重なり合うように設定する（図2a参照）。一方受信者は、光子検出器を通常の光検出器に置き換え、さらに2つの光検出器からの検出信号を差動検波する。送信2状態が図2aのように重なり合っているため、差動検波の出力信号分布は位相差$\{0, \pm 2\delta\}$に対応する信号レベルを中心に拡がった形状となる（図2b参照）。受信者は、この信号分布に対し図2bに示すように閾値$\pm d$を設定し、dより大きい信号からビット「1」を、$-d$より小さい信号からビット「0」を生成する。そして、送信者に閾値を越えた時間スロットを通知する。一方送信者は、閾値を越えた時間スロットについて、変調位相差が2δならビット「1」、-2δならビット「0」とする。これにより送受信者は共通のビット列を得ることができ、これを秘密鍵とする。本システムにおいては、送信2状態が量子雑音により一部重なり合っているために、盗聴者は伝送状態を完全に識別することはできず、したがって完全な鍵ビットを得ることができない。そのため、安全な鍵配送が可能となる。

本システムでは、光子検出器ではなく通常の光受信器を用いて秘密鍵を生成しているため、従来量子暗号方式よりも高い実用性が期待される。

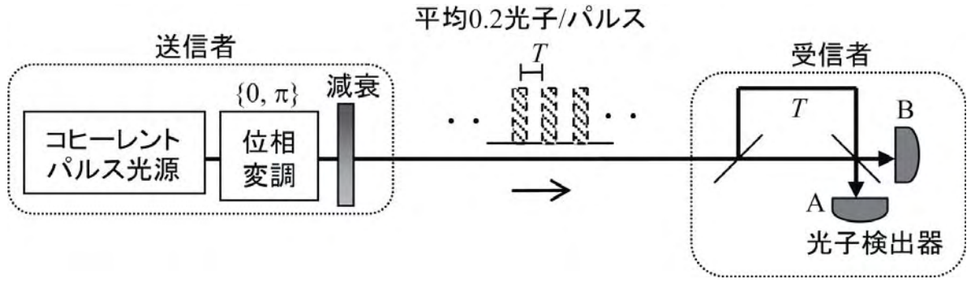

図1　差動位相シフト量子鍵配送の基本構成

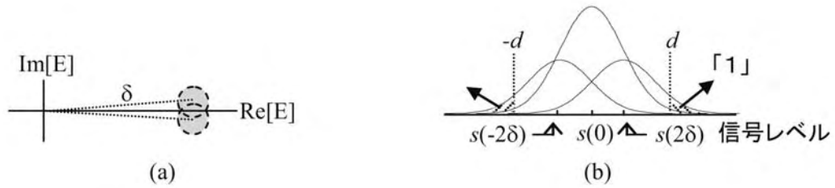

図2　巨視的コヒーレントDPS量子鍵配送における送信信号状態(a)と復調信号分布(b)

研究
事業推進担当者のシーズと実績

＜差動4値位相シフト量子鍵配送＞

DPS-QKD方式は、構成が簡便である反面、安全性はBB84方式よりいく分劣っている。そこで、BB84のコンセプトをDPSに持ち込んだ改訂プロトコルを考案した。差動4値位相シフト（Differential Quadrature Phase Shift: DQPS）量子鍵配送と呼ぶ方式である。基本的な装置構成は図1と同様であるが、送信者の変調位相は{0, π/2, π, 3π/2}のいずれかとし、受信者はそれを位相差0またはπ/2の遅延干渉計で受信する。このようにすると、変調位相差が{0, π}かつ干渉計位相差が0、または変調位相差が{π/2, 3π/2}かつ干渉計位相差がπ/2、のときにどちらの検出器が光子検出するかは確定的となり、そうでない場合には確率的となる。そこで信号伝送後、送信者は変調位相差が{0, π}であったか{π/2, 3π/2}であったか、また受信者は干渉計位相差が0であったかπ/2であったか、を相手に通知する。そして、お互いの位相差が確定的な光子検出である組み合わせの場合に、|変調位相差0またはπ/2、検出器Aによる光子検出|をビット「0」、|変調位相差πまたは3π/2、検出器Bによる光子検出|をビット「1」、としてビット値を生成する。これにより、同一の秘密鍵ビット列を得る。

このプロトコルでは、信号伝送時には干渉計位相差が不明な分だけ盗聴成功確率が低くなり、これにより鍵の安全性が向上する。本方式について理論解析を行い、従来DPS-QKDよりもシステム性能が向上することを示した。また実証実験を行い、実装可能であることを示した。

＜DPS量子秘密共有＞

量子鍵配送は2者に秘密鍵を供給するシステムであるが、これの展開形として量子秘密共有と呼ばれるシステムがある。3者間（あるいはそれ以上）で秘密鍵を共有するシステムで、その際、第1の参加者には完全な鍵を、第2/第3の参加者には部分鍵を供給する。第1参加者が暗号化したデータを第2/第3参加者は単独では復号できず、両者が協力したときのみ復号可能であるように仕組まれている。

従来、量子秘密共有としては量子もつれを用いたものやBB84プロトコルを応用したものが知られていたが、本研究ではDPS-QKD方式を量子秘密共有に適用したプロトコルを考案した。そして、各種盗聴を考慮したシステム性能評価を行い、実証実験を行った。本方式は、従来方式に比べ構成が簡便であり速い鍵生成速度が可能、などの特徴を有している。

＜DPS-QKDにおける光源要求条件＞

DPS-QKDではコヒーレントパルス光源を用いている。これは、受信側遅延干渉計で前後のパルスを干渉させる際に所望の干渉結果が得られるようにするためであるが、どの程度のコヒーレンシー（可干渉性）が必要であるかは明確ではなかった。そこで、DPS-QKDで用いる光源に求められる要求条件について、理論と実験の両面から検討した。その結果、良好な伝送特性が得られる光源スペクトル線幅は、遅延干渉計のFSR(Free Spectrum Range)の0.07%以下であることを明らかにした。

最後に

本研究室では、絶対的に安全な暗号通信を実現する技術として量子暗号、特にオリジナル提案方式である差動位相シフト量子鍵配送を中心に研究を進めてきた。これまでいくつかの成果を得てきたが、まだまだ検討不足であり、今後ともさらに研究を深めていく予定である。

研究
事業推進担当者のシーズと実績