フォトニックデバイス部門

大阪大学大学院工学研究科
電気電子情報工学専攻　井上　恭

●量子暗号システムの研究

量子暗号とは、量子力学の原理を利用して究極的に安全な暗号通信を実現する技術である。より具体的には、離れた2者に暗号通信のための秘密鍵を供給するシステムであり、量子力学の「不確定原理」あるいは「量子状態の複製不可の定理」により鍵の安全性を保証する。秘密鍵を供給するシステムであるので量子鍵配送（Quantum Key Distribution：ＱＫＤ）とも呼ばれる。本研究室では、独自に考案した差動位相シフト（ＤＰＳ）ＱＫＤと呼ばれる量子鍵配送方式をベースに、改良プロトコルの提案・システム性能評価、あるいはその周辺技術の研究を行っている。この研究テーマに関して、2009年度は、（１）光前置増幅器を用いる巨視的ＤＰＳ－ＱＫＤ方式、（２）ＤＰＳ－ＱＫＤに対する連続クリック攻撃の検知方法、（３）量子チャンネル/古典チャンネル波長多重系におけるラマン散乱光の影響の定量化、などの項目について研究を行った。

1.　はじめに

現在広く用いられている暗号システムの安全性は、暗号化されたデータを解読するのに膨大な計算量を要し実質的には不可能、であることにより保証されている。しかしながらこれは、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あらかじめ共有する必要がある。そこで、バーナム暗号通信のための秘密鍵を光の量子的性質を利用して安全に供給しようというのが量子暗号または量子鍵配送（ＱＫＤ）である。

本事業推進担当者は、この量子暗号に関し、差動位相シフト（DPS）ＱＫＤと呼ばれる独自のプロトコルを提案し、その研究開発を進めている．本方式は、従来方式に比べ、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、などの特徴を有している。以下、これに関し本年度行った研究項目を紹介する。

2.　光前置増幅器を用いる巨視的ＤＰＳ－ＱＫＤ

量子暗号では、通常1光子レベル以下の超微弱な光が送受信される。そのため受信端では、単一光子検出器あるいは微弱光ホモダイン検出器が用いられる。しかしながら、これらの受信器には受信性能や実装面での制約が大きい。そこで、より実際的な量子暗号方式として、比較的パワーの大きいコヒーレント光を送信し通常の光検出器で受信する量子暗号方式について検討した。鍵の安全性確保にはコヒーレント光の量子雑音を利用する。これに関しては、基本方式は以前に提案済みであったが、今年度はより実用に近い光前置増幅受信器を用いた場合のシステム性能（秘密鍵生成レート/伝送距離）を検討した。想定される各種盗聴法について検討し、それぞれについてのシステム性能をシミュレートしたところ、数10kmの鍵配送が可能であることが示された。本方式は装置構成が従来光通信と同じであることが特徴的であり、実際的であるといえる。

3.　ＤＰＳ－ＱＫＤへの連続クリック攻撃検知法

従来のＤＰＳ－ＱＫＤ方式に対しては、連続クリック攻撃と呼ばれる盗聴法が最も強力であり、これにより鍵配送距離が制限されることが知られていた。これへの対抗策として、共光子検出率モニターによる盗聴検知法を考案した。正常時のＤＰＳ－ＱＫＤシステムでは連続パルス列が送受信されるのであるが、連続クリック攻撃を受けると、ひとかたまりのパルス群が間欠的に受信されることになる。そこで、一定時間間隔の複数時間スロットで共に光子が検出される頻度をモニターすることにより、盗聴を検知する。従来の量子暗号ではビット誤り率から盗聴を検知するのが常套手段であったところを、光子検出率を利用する点が特徴的である。実際の

光子検出器の特性（検出効率/雑音特性）を考慮したシミュレーションにより、本方式が有効であることを示した。

4. デコイDPS－QKD

DPS－QKDでは微弱な連続位相変調パルス列が送受信される。この方式の改良版として、振幅の異なるパルス（デコイパルス）をランダムに挿入する方式について検討した。一般に微弱光の位相と振幅を同時には正しく測定することはできず、そのため位相情報が盗聴されると、デコイパルスの振幅が変化する。この振幅変化より盗聴を検知する。これまで2値USD連続クリック攻撃に対して有効であることを示していたが、本年度はさらに、個別一般攻撃、ホモダインなりすまし攻撃、4値USD連続クリック攻撃など、他の盗聴法について検討しその有効性を示した。

5. 量子／古典波長多重伝送系におけるファイバーラマン散乱の影響

量子暗号システムでは、1光子レベルの光を送受信する量子チャンネルと、鍵生成のための後処理情報をやり取りする古典チャンネルが用いられる。通常は両者は別々の伝送媒体で送られるが、同一ファイバ上で波長多重伝送できるとシステム的に効率が良い。しかしながらこの場合、高い光パワーの古典チャンネル光から発生する自然ラマン散乱光が量子チャンネル伝送の障害となることが知られている。但しこれまでは、特定の条件下での影響が検討されているのみであった。

そこで本研究では、量子／古典チャンネル波長多重伝送系におけるラマン散乱光の影響を定量的・体系的に検討した。まず、ファイバで発生するラマン散乱光パワーを各種条件下で測定し、モデル化した。その後、測定結果に基づき、古典チャンネル波長多重時の量子チャンネルの伝送特性をシミュレートし、量子チャンネル伝送が可能である動作条件を定量的に明らかにした。

6. 広ゲート幅APD単一光子検出器

量子暗号システムの基本デバイスである単一光子検出器には、アバランシェフォトダイオード（APD）を高電圧印加状態で用いることが一般的である。但し、連続的に高電圧を加えると誤動作しやすくなりさらには破損するため、一瞬だけ高電圧を印加するゲート動作モードで用いる。この場合、特定の時刻のみでしか光子検出できず、光子検出速度の制限要因となる。また、QKD方式としては連続的に光子検出可能であることが求められるプロトコルもあるのだが、そのような方式にはゲート動作APDは使用できない。

そこで、広い時間幅のゲート電圧を印加する駆動法を試みた。ゲート幅を広げた分だけ光子検出率が上がり、また数パルスに渡っての光子検出が可能となる。実際に回路を試作したところ、所定の性能が得られた。