NEWS RELEASE
NTT
日本電信電話株式会社

2005年6月14日

単一光子を量子暗号として光スイッチ経由で配送に成功

－アインシュタインをも悩ませた単一光子での干渉現象を応用－

日本電信電話株式会社(ＮＴＴ；本社：東京都千代田区、代表取締役社長：和田紀夫)は、誰かに盗聴されると壊れてしまうほど微弱な単一光子を、光ネットワークにおいて量子暗号として実用化する可能性を世界ではじめて実証しました。この成果は、ＮＴＴと米・スタンフォード大学が共同開発した独自の量子暗号方式と、ＮＴＴが開発した光子をコントロールできる光スイッチ(交換機)を組み合わせることで可能になりました。量子暗号は次世代の暗号方式の切り札になると見られており、情報伝達の安全性を飛躍的に高めるものと期待されています。

ちなみに２００５年は世界物理年※1でもありますが、今回の実験では、かのアインシュタインをも悩ませた「干渉が起こらないはずの単一光子でも、自分自身と干渉をおこし、あたかも干渉があったかのように振る舞う」量子効果を利用しています。最新の物理学でもどうしてこのような干渉が起きるのかは解明されていませんが、今回、この量子効果が暗号技術に応用可能なことを世界で初めて実証することができました。

＜開発の背景＞

例えば、極秘情報や金融データなどは万が一の事故のために必ずバックアップする必要があります。そのためには、専用の光ファイバ回線を直結して煩雑にデータをやり取りする必要がありました。今後は、こうしたバックアップが必要な情報の対象がもっと広がり、一般の企業や個人ユーザにも拡大していくと見られています。そうした際、ユーザとバックアップセンタ間にそれぞれ専用線を引くことはコスト的にも難しく、インターネットなどの汎用回線を使わざるを得なくなるとみられています。

そこで、インターネットで秘密の情報をやり取りする際に、暗号をかけて解読されないようにする仕組みの必要性が生じました。現行では、公開鍵方式と呼ばれる暗号システムが一般に広く使われています。この方式は、だれかが情報を盗聴して解読しようとしているかもしれないが、それを解くには1億年もかかるようにしておくことで、事実上解読は不可能であるとの前提に立っています。しかし近年、コンピュータ処理能力の向上などにより解読に要する時間

が大幅に短縮されるにつれ、暗号の桁数を増やして対処するという、いたちごっこの状況が続いています。

これに替わる次世代の暗号と考えられているのが「量子暗号」技術です。この技術は、その状態を観測することで、量子という外部環境にデリケートな状態(量子状態)が壊れてしまうという現象を利用しています。すなわち、秘密鍵の情報を量子状態にして伝送すると、盗聴者が盗聴した(観測した)時点で量子状態が壊れてしまいます。盗聴者は全く同じ量子状態を作り出すことはできないので、受信側では秘密鍵が盗聴されていることを検知できる仕組みです。

この量子暗号を使うことで、上記のいたちごっこの状況を脱することが可能になりますが、単一光子という非常に微弱な信号と、通常の光伝送で使われている信号を同じネットワークに流すことができなければなりません。また、交換機を通過する場合、光の信号を電気に変えて電気的にスイッチングしたのでは、量子暗号の信号は伝送できません。それは、電気に変えた瞬間に量子状態が壊れてしまうからです。したがって、電気に変えることなく経路を制御できなくてはなりません。幸い、ＰＬＣの光スイッチは、信号を光のままで経路の制御が可能です。しかし、単一光子のように非常に微弱な信号でも通常の光信号と同じように制御が可能なのか確認されていませんでした。

＜実験の内容＞

今回の実験では、インターネットなどのオープンな光ネットワーク環境で、<1>単一光子でも干渉現象が起きること、<2>多対多間で交換機能を果たす光スイッチ内部で経路を制御でき、なおかつ微弱な単一光子と並行して大量の強い光データ伝送が可能なことを実証しました。

まず、<1>の干渉現象ですが、１つの光源からのレーザ光など強い光を並列する２つのスリットを通すと、それぞれのスリットから出た光が干渉して濃淡ができます(図１ａ)。１つのスリットの前に屈折率の異なる媒体を置くと、媒体を通った光の感じる長さが変わるので、干渉縞が変化します(図１ｂ)。今回使用する光スイッチはこの原理を用いたプレーナ光波回路(PLC) ※2となっています。

図１の(ｃ)、(ｄ)は光スイッチの模式図ですが、２つに分かれた光が再度結合する部分で干渉が起こり、一方の導波路だけに光が進むようになっています。経路を変えたいときには、分かれている部分の一方の温度をかえて屈折率を変化させます。すると、屈折率をかえた導波路を通った光の感じる長さがかわるので、干渉の状態が変化して別の出口へ光が出てくるようになります。

さて、量子暗号で使うために光源のパワーを極端に弱くして、1個の光子が時間をおいて出てくるようにした場合、光子は、光スイッチの中央部にある二つに分かれた経路のどちらか一方しか通らなくなります。この結果は、有名な１光子でのヤングの干渉実験から推察できます。干渉縞を映し出すスクリーンの代わりに感光版を置いておきます。光子１つ１つはスリットを抜けて感光版にランダムなスポットをつくっていきますが、時間が経ってたくさんの光子が

スポットをつくると、その形はパワーの強いときの二つのスリットから同時に来る光が作る干渉縞と一致します(図２)。屈折率の異なる媒体を１つのスリットの前に置けば、同じように干渉縞は変化します。これと同じことがPLCの光スイッチで観測されました(図３)。

次に<2>の光スイッチの実験では、導波路構造を用いた干渉型(PLC-MZ)光スイッチを単位として構成された８×８マトリクススイッチを(最小単位の交換機として)使用しました。フォトニックネットワークにおいてすでに適用されている光スイッチと同一原理となっています。最初に単一光子レベルのパルスを光スイッチの１つに入力し、出力ポートで受光できることを確認しました。そしてスイッチを切り替えることにより、別のポートへ信号が切り替わることを確認しました(図４)。次に、同じマトリクススイッチに通常の光伝送で使われている強度の光パルスを別のポートから入力しました。構造上、２つの光はスイッチの途中で交差していますが、量子暗号の受光側に漏れ光除去用のフィルタを挿入すれば、両者独立に並行して動作することが確認されました(図５)。

今回使われた量子暗号は、ＮＴＴと米・スタンフォード大が共同で考案した差動位相シフト方式※3 と呼ばれるもので、

- 高速で安定した一方向伝送
- 受けた光子は無駄にせずすべて利用するので従来法の２倍の鍵の生成速度
- 従来の往復伝送で生じる散乱ノイズがない

などの特徴を持っています。

今回１５ｋｍの光ファイバの途中に光スイッチを挿入して量子暗号を伝送した結果、エラー率※4 ６％で1秒間に約２ｋビットの鍵生成速度を実現しました。この数値は絶対安全な鍵を作るのに十分な値となっています。

さらに、スイッチ内部で大容量の情報伝達と量子暗号が共存できたことにより、本スイッチがインターネットなどの汎用商用ネットでも、単一光子からなる量子暗号信号を伝送可能である事を実証しました。

＜今後の展開＞

今回の成果では、伝送距離が１５ｋｍでの実証ということで利用方法が限定されますが、今後は受光器を改良し、より高速でより遠距離での伝送が可能になるよう、システムの高度化の検討を進めていきます。また、将来の一般ユーザを含めた光ファイバネットワークにおいて広範に量子暗号を適用し、秘匿性を高めたネットワークの実現に向け、研究開発を進めます。

＜用語解説＞

※1　世界物理年：

アインシュタインが光電効果の理論、ブラウン運動の理論、特殊相対性理論

という三つの革命的な論文を発表した１９０５年から百年経たことを記念する年。

※2　プレーナ光波回路(PLC)：
　シリコン基板上などに、光の通るコア部とそれを囲むクラッド部からなる光導波路を形成し、その導波路模様により様々な光機能回路を実現するもの。

※3　差動位相シフト方式：
　ＮＴＴとスタンフォード大で開発した量子暗号プロトコル。従来の光パルスを折り返すPlug&Play BB84方式に比べて一方向の伝送が可能で、セットアップがシンプル、鍵生成効率が高いなどの特長を有する。

※4　エラー率：
　システムの物理的問題により生じるデータの誤り率。これが１０％程度以下であればエラー訂正アルゴリズムにより誤りを最終的にゼロにできる。

・図１　ヤングの干渉実験と光スイッチ
・図２　１光子でのヤングの干渉実験
・図３　１光子レベルでもスイッチング可能
・図４　光マトリクススイッチを経由した量子鍵配送実験(1)
・図５　光マトリクススイッチを経由した量子鍵配送実験(2)

＜本件に関する問い合わせ先＞
ＮＴＴ先端技術総合研究所
企画部　情報戦略担当
為近、甕(もたい)
Tel: 046-240-5152
E-mail: st-josen@tamail.rdc.ntt.co.jp

NTT ニュースリリース