2002年12月13日

（報道発表資料）

科学技術振興事業団
日本電信電話株式会社

国際共同研究事業における成果について

「単一光子光源を用いた量子暗号伝送実験に成功」

--量子暗号の長距離伝送への適用に期待--

科学技術振興事業団（理事長　沖村憲樹）と日本電信電話株式会社（以下NTT、代表取締役社長　和田紀夫）は相互の協力により、単一光子光源を用いた量子暗号の伝送実験に世界で初めて成功した。この成果は、１２月１９日付の英国科学誌ネイチャーに発表される。

本研究は、科学技術振興事業団の国際共同研究事業、量子もつれプロジェクト（代表研究者はスタンフォード大学教授／ＮＴＴ　Ｒ＆Ｄフェロー、山本喜久氏、及びフランス国立科学研究センターエコール・ノルマル・シュペリオール物理学科長・教授、アロシュ氏）と、さらに、NTT物性科学基礎研究所－スタンフォード大学両者の共同研究に基づき、相互の協力の下で行われたものである。

将来どのような予期せぬ技術革新が起ころうとも、未来永劫にわたって絶対に盗聴されないという夢の暗号方式が現実のものとなりつつある。量子暗号である。量子暗号では、各パルスには単一の光子だけが注入され、その光電界の振動の向き（これを偏波という）を変調して、０または１というビット情報を伝送する。量子暗号の安全性は、盗聴に入った第三者がいかに巧妙な手段で単一光子の偏波状態を測定しようとも、その盗聴の痕跡が測定された単一光子の偏波状態に残り、その痕跡を通して盗聴行為が見つけ出されてしまうことによっている。観測されたことによって状態が変わってしまう現象は、“波束の収縮”と呼ばれ、量子の世界に特有の不思議な現象である。このように、量子暗号の安全性は量子力学の基本原理に基づいているため、その安全性は絶対である。現行の暗号方式の安全性が、現時点でのコンピュータの性能限界、現在知られているアルゴリズムの効率に対して相対的に保障されているのとは際立った違いである。

しかし、この量子暗号には実用技術として重大な欠点があった。半導体レーザに代表される通常の光源から放出される光パルスでは、光子の数を厳密に確定することができない。光子数はポアソン分布している。平均として、各パルスに１個の光子がある、といっても、光子が全く存在しないパルスもあれば、光子が２個以上存在するパルスもある。光子が存在しないパルスはビット情報を伝送できないし、光子が２個以上あるパルスに対しては、第三者が光子１個を秘密裏に抜き取り、その偏波状態を測定しても、残りの光子にはその盗聴の痕跡が残らないので、安全性が破られてしまうのである。これまでに行われた量子暗号の実験では、通常の半導体レーザ光源が使われていたため、この種の問題が常につきまとい、結果として伝送速度と

伝送距離に厳しい制限が生じた。

科学技術振興事業団量子もつれプロジェクトとNTT物性科学基礎研究所は相互の協力により、半導体素子を用いて単一光子を確実に発生する技術を確立し（Phys. Rev. Lett. 86, 1502 (2001); Nature 419, 594 (2002) ）、これを用いて、ベネットとブラサードが1984年に提案したプロトコル（BB84方式）に基づく量子暗号の伝送実験に今回、世界で初めて成功した。

用いられた素子は、量子ドットと呼ばれる厚さ４ナノメートル（１ナノメートルは１０億分の１メートル）、直径２０ナノメートルの円板状のInAs半導体微細構造を発光領域としている。この量子ドットを、GaAsとAlAsという２種類の半導体からなる３次元の光マイクロキャビティの中央に閉じ込める（図１）。素子の作製には、分子線エピタキシーと呼ばれる結晶成長技術と、電子ビーム露光とドライエッチングを組み合わせた微細加工技術が用いられた。パルス光をこの量子ドットに照射し、その中に複数の電子－ホール対を光励起で注入する。各電子－ホール対は、次々と光子を放出して消滅するが、この時、最後に残った電子－ホール対は、いつもある決められた波長の光子を放出する。この波長を持つ光子は量子ドットの中に最後に残された電子－ホール対によってのみ発生される。従って、この特定の波長を持つ光子を光波長フィルターで選択的に取り出すことにより、各励起パルス当り、必ず光子１個を発生させることができる。このような光子の放出過程は自然放出と呼ばれ、通常は全くランダムな方向へ放出される。単一光子を決められた方向へ取り出し、量子暗号伝送へ有効に使うために、量子ドットは３次元光マイクロキャビティ内に埋め込まれている。この場合には、自然放出は１つのキャビティモードへのみ選択的に起こるため、決められた方向へ単一光子を有効に取り出すことができる。

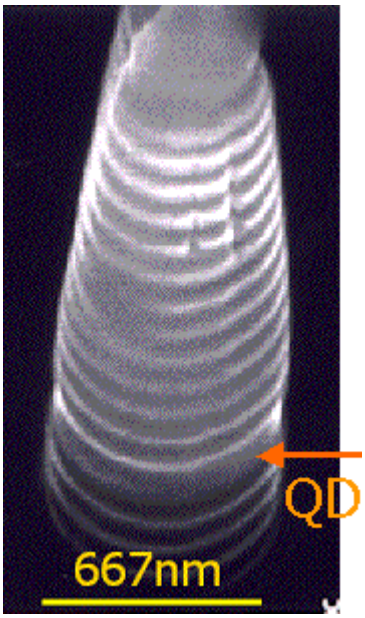
量子暗号伝送システム実験は図２(a)に示す構成で行なわれた。送信者（アリス）は上述した原理に基づいて単一光子を１３ナノ秒（１ナノ秒は１０億分の１秒）毎に発生し、その偏波状態を、水平直線偏波、垂直直線偏波、右回り円偏波、左回り円偏波の４つのうちからいずれか１つに設定する。どの偏波に設定するかは、アリスのコンピュータが発生する乱数によって決定される。アリスはこの乱数を保持しておく。受信者（ボブ）は、この単一光子と５０％－５０％ビームスプリッタで２径路に分離し、一方で水平か垂直かの直線偏波の検出を行ない、他方では右回りか左回りかの円偏波の検出を行なう。光子は１つしかないので、結局は、この４つの偏波の一つだけに相当する検出器が光子を検出する。この量子伝送が終わった後、アリスとボブは偏波状態が円偏波だったか、直線偏波だったかだけの情報を公開し合う。この情報は第三者に漏れてしまうが、例えば、直線偏波のうち、水平、垂直のどちらだったかは二人だけが知っている。二人の偏波基底が一致した時のみ、右回り（水平）ならば０、左回り（垂直）ならば１というビットを鍵として残す。この後、部品、伝送路の不完全さによるビット誤りをなくすための誤り訂正を行ない、その過程で第三者にリークしたビット情報をなくすためのプライバシー増幅という作業を行なって、最終的な鍵が生成される。

図２(b)には、単一光子光源を用いた量子暗号と通常の半導体レーザ光源を用いた量子暗号の伝送速度対伝送損失の理論値と実験値がプロットしてある。今回用いられた単一光子光源は、単一光子を伝送路へ送出する効率が１％、２個以上の光子がパルスに存在する確率は、通常の半導体レーザに比べ約１／１０であった。これにより、通常の半導体レーザを用いた方法に比べて、伝送損失で５dBも大きな値まで許容できることが分かった。

図２(c)には、このようにして作成された鍵を使って、アリスがボブへ実際に暗号通信を行な

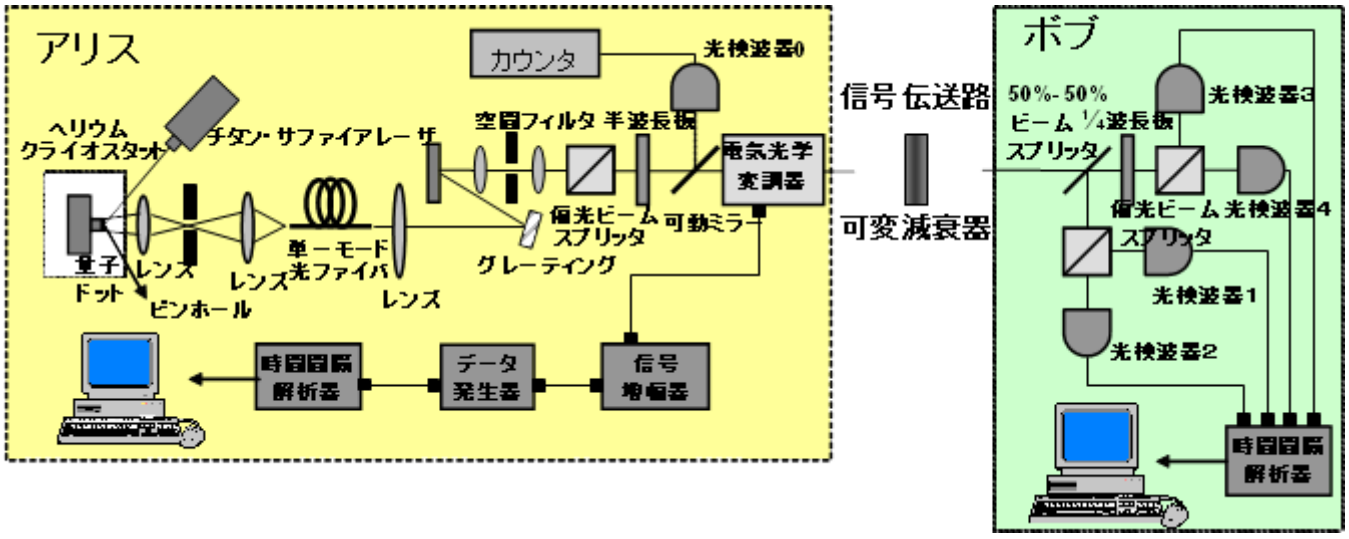
った結果が示されている。アリスは送信したい情報（スタンフォード大学メモリアル教会）と彼女の鍵を用いて暗号文を作成した。暗号文は第三者には単なる雑音と写るが、ボブは彼の持っている鍵を用いて、この暗号文からオリジナルな情報を再生することができた。このような暗号通信はone time padと呼ばれ、絶対に盗聴されないことが知られている。

研究グループでは、単一光子光源の効率を１０%へ、２個以上の光子がパルスに存在する確率を通常の半導体レーザの１／１００に減少することにすでに成功している（Phys. Rev. Lett. 掲載予定）。これにより、４５dBの伝送損失を許容できるシステムの実現が将来的には可能と見ており、最大４０dBの伝送損失を持つ人工衛星を介した超長距離の衛星通信量子暗号システムの実現にメドをつけたいとしている。



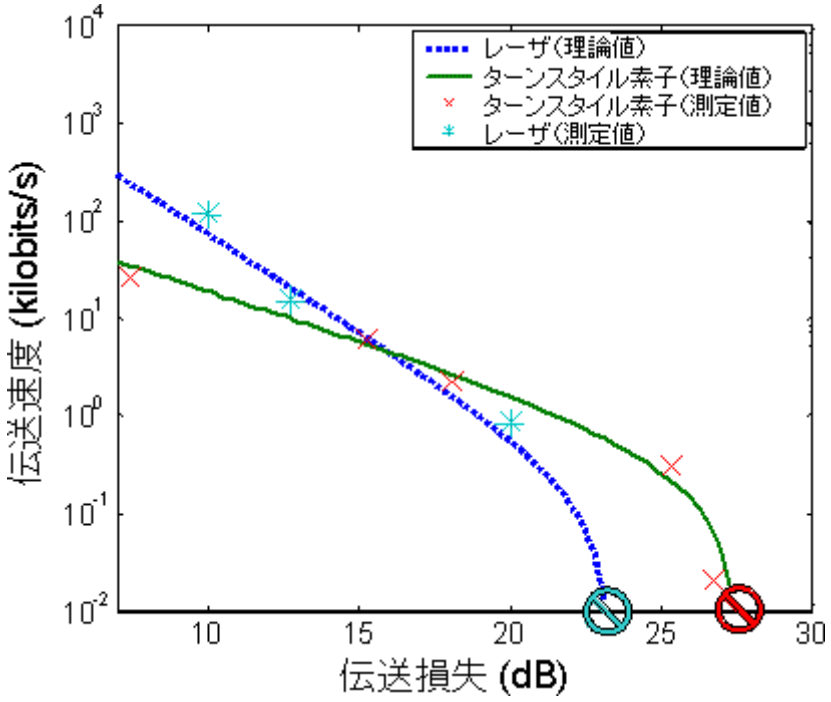
単一光子光源のSEM写真。
単一量子ドットが３次元光マイクロキャビティに閉じ込められている。

図１



量子暗号システム実験系

図２．（ａ）



単一光子光源を用いた量子暗号と通常の半導体レーザ光源を用いた量子暗号における伝送速度対伝送損失

図２．（ｂ）

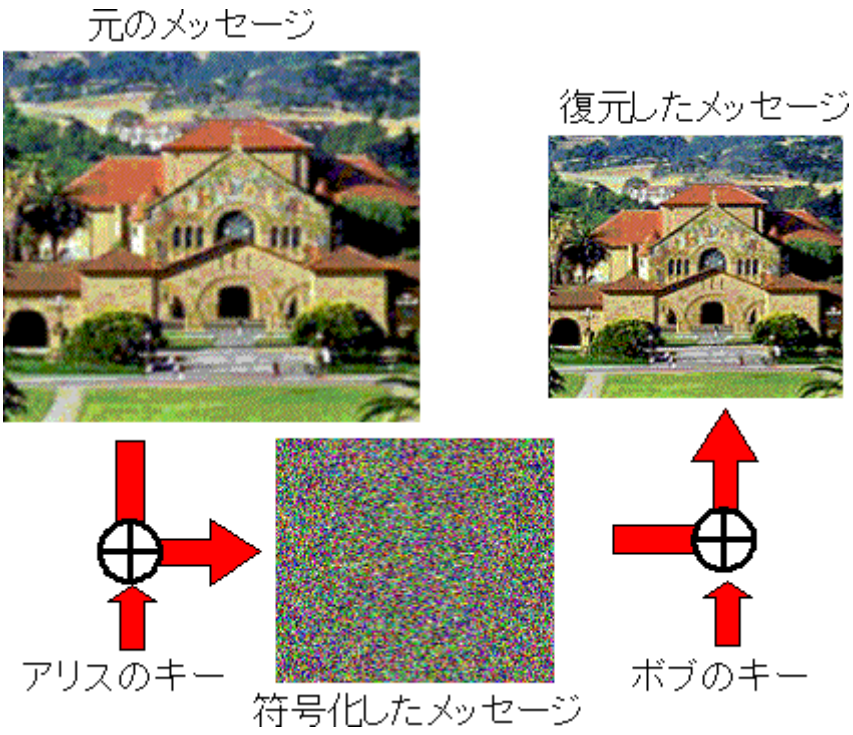


図２．（ｃ）

本件の問い合わせ先：
（１）科学技術振興事業団　国際共同研究事業「量子もつれプロジェクト」
代表研究者：山本喜久
メールアドレス：yamamoto@loki.stanford.edu
TEL：1-650-725-3327
FAX：1-650-723-5320

（２）科学技術振興事業団　国際室
調査役　鈴木寿春
TEL：048-226-5630
FAX：048-226-5751

（３）NTT先端技術総合研究所　企画部
澤木美奈子、甕（もたい）礼史
メールアドレス：st-josen@tamail.rdc.ntt.co.jp
TEL：046-240-5152
FAX：046-270-2365