2015 年 9 月 14 日

（報道発表資料）

日本電信電話株式会社
国立学校法人　東京大学大学院工学系研究科

世界で初めて、誤り率監視の不要な量子暗号実験に成功

～波束の収縮に基づいた新原理による手法を実証～

日本電信電話株式会社（東京都千代田区、代表取締役社長：鵜浦博夫　以下、NTT）と東京大学大学院工学系研究科（東京都文京区、総長：五神 真）は共同で、光子伝送の誤り率監視を行うことなしに安全性を確保する量子暗号を世界で初めて実現しました。

本成果は、総当たり差動位相シフト(round-robin differential phase shift: RRDPS)方式と呼ばれる量子暗号方式を実験により実証したものです。この結果により、不確定性原理に基づく従来の方式と異なり、波束の収縮（※1）を安全性の原理とした量子暗号を世界で初めて実証することができました。本実験により、従来方式で必須とされてきた送信者と受信者との間での定期的な誤り率監視が不要な量子暗号が実現されたことから、簡便かつ効率の高い量子暗号システムの実現に向けて大きな可能性が広がることが期待されます。

今回得られた成果は、2015 年 9 月 14 日(英国時間)に英国科学誌「ネイチャー・フォトニクス」で公開されます。

本研究の一部は内閣府革新的研究開発推進プログラム（ImPACT）の山本喜久プログラム・マネージャーの研究開発プログラム「量子人工脳を量子ネットワークでつなぐ高度知識社会基盤の実現」の一環として行われました。

１．背景

私たちの生活の中でインターネットの重要性が増している昨今、情報通信のセキュリティの重要性は一層高まっています。近年、通信のセキュリティを確保する究極の技術として、量子力学の原理に基づき秘匿通信を行う量子暗号が注目を集めています(図 1)。量子暗号は、光の量子力学的状態(量子状態)に暗号鍵をエンコードして送信する量子鍵配送(quantum key distribution: QKD)によって 2 者間で共有した秘密鍵を用いて暗号通信を行うものです。QKD により送信された暗号鍵は量子力学の原理に基づき安全であるため、将来いかに技術が進展しても安全な通信を行うことができます。QKD は、既に欧州や日本で大規模なネットワーク実験が行われ、これを用いた TV 会議のデモがなされるなど、既に実用に近い技術に成長しつつあります。

従来の QKD は、例えば情報を光の最小単位である光子の量子状態に載せて運ぶことで、「情報を読むと量子状態が乱れてしまう」というハイゼンベルクの不確定性原理（※2、以下不確定性原理）によりその安全性が守られています。具体的には、暗号鍵の情報を光子の量子状態に載せて伝送するため、途中で第三者が盗聴すると量子状態が壊れ、その結果鍵伝送に誤りが生じます。よって、テストビットを用いて送信者と受信者の間で継続的に鍵伝送の誤り率を観測し、その値により第三者へ漏洩する可能性のある鍵の量を見積もり、その結果を用いて光子伝送により得られた鍵を圧縮することで、安全な鍵を生成します。すなわち、従来の QKD においては、盗聴を監視するために誤り率を常に観測する必要がありました。昨年、今回の発表機関の一つである東京大学のグループら

により、従来の QKD と異なり、その安全性が不確定性原理によらず、波束（量子状態）の収縮に基づく新しい原理の QKD 方式である RRDPS 方式が提案されました(東大、国立情報学研究所のニュースリリース：http://www.t.u-tokyo.ac.jp/epage/release/2014/2014052201.html)。本方式によると、誤り率監視の不要な QKD の実現が期待されるため、実験による検証が待たれていました。

２．研究の成果

今回、NTT 物性科学基礎研究所（以下、NTT 物性研）と東京大学大学院工学系研究科は、RRDPS 方式に基づいて、誤り率監視の不要な QKD を世界で初めて実現しました。

RRDPS 方式は、従来の QKD と異なり、漏洩しうる情報量がはじめから一定の値に抑えられていることを特長とする QKD 方式です(図 2)。具体的には、RRDPS 方式においては、複数の光パルスに光子が存在しうる量子状態を用いて暗号鍵を伝送しますが、漏洩する可能性のある情報量は光パルスの数のみにより決定され、誤り率に依存しません(図 3)。よって、使用した光パルスの数から決まる盗聴の可能性のある鍵の量に応じて、光子伝送により得られた鍵を圧縮することで、誤り率を監視することなく安全鍵を生成することができます。

今回得られた成果を用いることで、QKD システムにおいて送信者と受信者の間でテストビットを用いた定期的な誤り率の監視を省略することができるため、QKD システムにおける送受信者間の制御情報の簡略化と、生成された鍵をテストビットとして消費しないことによる鍵生成の効率化を実現できます。また本成果は、不確定性原理によらずに全く新しい原理でどんな盗聴に対しても安全な鍵配送ができることを世界で初めて証明した実験であり、QKD 研究の新たな展開を促すことが期待されます。

【RRDPS 方式による QKD 実験】

① 送信者アリスは減衰レーザー光により生成したパルス間隔 T の 5 連パルスからなる微弱光パケットの各パルスに 0 またはπの位相変調を施した後、光ファイバを介して受信者ボブに送付する。受信者ボブは、総当たり位相差測定を実現するために、光スプリッタ、遅延時間が T, 2T, 3T, 4T の 4 つの遅延干渉計、および光子検出器(※3)からなる測定装置を備えている。光が非常に微弱であるため、4 つの遅延干渉計のうちたまたま光子が到達した一つの干渉計において位相差が検出される(図 4)。

② RRDPS 方式により安全鍵が伝送可能であることを実験的に確認した。アリス-ボブ間の最大伝送損失は 8.7 dB であった。30 km までのファイバ伝送にも成功した(図 5)。

③ 有限長解析(鍵の長さが有限の場合、物理特性の揺らぎが盗聴量の見積もりに影響することを考慮に入れた安全性解析)を行った場合も安全鍵が配送可能であることを実験により確認した。これにより、鍵の長さの有限性を考慮した現実のシステムでも安全な鍵配送が可能であることを示した(図 6)。

３．技術のポイント

(1) RRDPS 方式

今回採用した RRDPS 方式(図 2)においては、アリスは各パルスに存在する光子数の平均値が 1 より十分小さい微弱レーザー光により生成された時間間隔 T の L 個のパルスからなる微弱光パケットに 0 またはπの位相変調を印加し、伝送路を介してボブに送付します。ボブは、遅延時間が T, 2T, … (L-1)T をとることのできる遅延干渉計と、干渉計の 2 つの出力にそれぞれ接続された光子検出器を備えています。干渉計の遅延時間が NT(N は 1 以上 L-1 以下の整数)のとき、N パルス離れたパルス間の位相差が 0 の時検出器 0 で、πの時検出器 1 で光子を検出します。ボブは受信する各パケ

ットに対して遅延時間をランダムに変更して位相差測定を行います。各パケットの光は非常に微弱なので、ボブはパケットあたりせいぜい 1 個の光子しか検出しません。ボブは、受信した各パケットについて(a)光子を検出した時刻(パルスの番号)、(b)どちらの検出器で検出したか、(c)どの遅延時間を選択したか、を記録し、そのうち(a)と(c)を普通の通信回線を用いてアリスに知らせます。アリスはこの情報から(b)の情報を知ることができるので、検出器 0/1 で光子を検出した場合をビット 0/1 と割り振ることで、アリスとボブはランダムなビット列を共有することができます。

この方式が、盗聴者イブのどんな技術によっても破れないことについては、量子力学の原理に基づく厳密な証明を与えることに成功していますが、「波束の収縮」によっておおよその概念を説明可能です（図 7)。波束の収縮とは、測定前は何らかの物理量、たとえば光子の時刻が定まっていない量子状態（波束）が、「どこにあるか測る」という測定により「収縮」して時刻が決まるという性質です。我々には収縮した結果しか見えないため、波束に含まれる情報の一部分しか取り出すことが出来ません。波束の収縮の重要な性質は、測定の仕方によって、波束のどのような種類の情報を取り出したいのかを選べる点です。RRDPS 方式においては、ボブが遅延時間を変えることが測定の仕方を変えていることに、光子がパケット中のどこか一つのパルスで検出されることが波束の一部分の情報が得られたことに、それぞれ相当します。そして、ボブがたくさんの（L-1 種類の）測定を行うことがポイントになっています。イブがたまたまボブと同じ測定を（すなわち、同じ遅延時間での測定を）行い、かつ同じ時刻で光子を検出したときだけ盗聴に成功するため、イブはどうしても偶然に頼らざるを得ません。その成功確率は L だけで決まり、誤り率と無関係です。また、L が大きくなると成功確率が下がるため、盗聴できる情報量がより制限されます。このように、波束の収縮の持つ性質が、RRDPS 方式の安全性の源となっています。

(2)　光スプリッタと複数の遅延干渉計による総当たり位相差測定の実装

図 2 のような遅延時間を動的に変更可能な遅延干渉計を低損失かつ高い位相安定度で実現するのは容易ではありません。この課題を克服するために、今回の実験では受動素子のみで遅延時間をランダムに切り替えることのできる図 4 の系を用いて総当たり位相差測定を実装しました。この系は、光スプリッタ、遅延時間が T, 2T, 3T, 4T の 4 つの遅延干渉計、および光子検出器からなります。光が非常に微弱であるため、パケットに含まれている光子は多くの場合高々1 個です。光スプリッタに入力された光子はランダムに 4 つの経路に振り分けられ、4 つの遅延干渉計のうちのどれか一つの干渉計に送られることで、干渉計の遅延時間をランダムに変更するのと等価な動作を低損失かつ高い位相安定度で実現しました。

４．今後の展開

今回の実験では実験系の制約上、遅延時間は 4 通りに制限されていましたが、RRDPS 方式では遅延時間の数を増やすと伝送距離、ビットレートなどの性能が飛躍的に向上することが予測されています。NTT 研究所では、RRDPS 方式の次世代の QKD 方式としての可能性を探るべく、NTT 研究所の強みである光導波路技術を用いて、100 程度の遅延時間を任意に選択できる総当たり位相差測定を実装し、性能向上を図るなどの基礎研究を行っていきます。また、東京大学大学院工学系研究科では、ImPACT 研究開発プログラムの一環と して、今回実証された新原理に基づく量子暗号方式が潜在的に持つと考えられる、短いセッションでの高効率性、雑音に対する耐性などの特性を追求し、量子セキュアネットワーク構築を目指していきます。

【論文掲載情報】

H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, “Experimental quantum key distribution without monitoring signal disturbance,” Nature Photonics (2015) (DOI:

10.1038/nphoton.2015.173).

【用語解説】

※1　測定における波束の収縮

量子力学では、測定のたびに測定結果が変わり、予想がつかないということが起こります。例えば光子のいる場所の測定の場合、測定する前は、光子の場所を特定できず、波のように広がっていると考えますが、光子の場所を測定すると、ある特定の場所に光子が出現したように見え、これを波束の収縮と呼びます。どの場所に出現するのかは、測定するまで誰にもわかりません。このように、量子力学は、本質的な不確実性をもっています。

※2　ハイゼンベルクの不確定性原理

物質や光がどのような性質を持つのかを知るために観測を行うと、いかに優れた測定器を使っても、観測された対象がその観測行為の影響を受けて変化してしまう、という量子力学の性質です。

※3　光子検出器

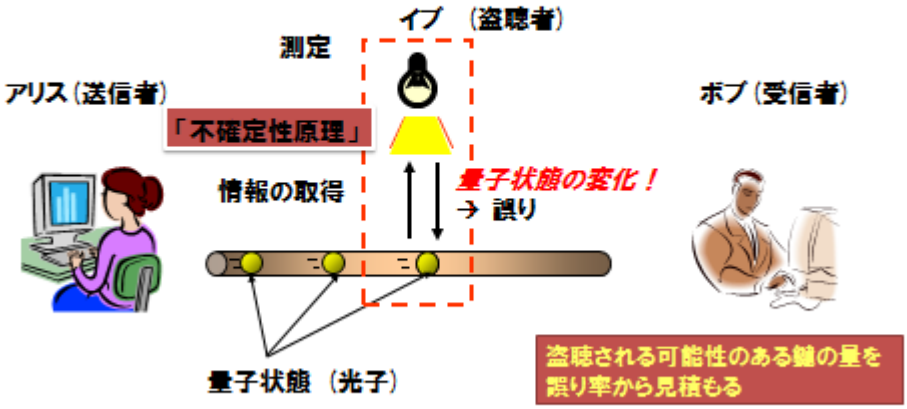
通常の光検出器は多数個の光子を含む比較的強い光のみ検出しますが、光子検出器はたった一つの光子でも検出できる装置です。

＜本件に関する問い合わせ先＞
日本電信電話株式会社
先端技術総合研究所　広報担当

東京大学
東京大学大学院工学系研究科
光量子科学研究センター長・教授
小芦　雅斗

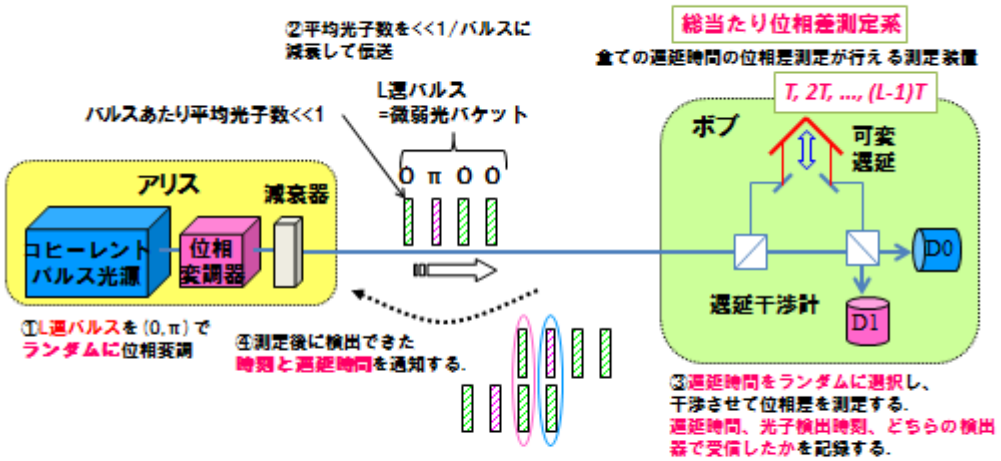
図1：従来の量子鍵配送（QKD）

QKD: 暗号通信のための「鍵」を離れた2者間で安全に共有する



従来のQKD：不確定性原理を利用したQKD→盗聴すると誤りが出る

図2：RRDPS方式



⑤検出時刻と遅延時間よりアリスはボブがどちらの検出器で受信したかがわかる→秘密鍵

図3: RRDPS方式はなぜ安全か

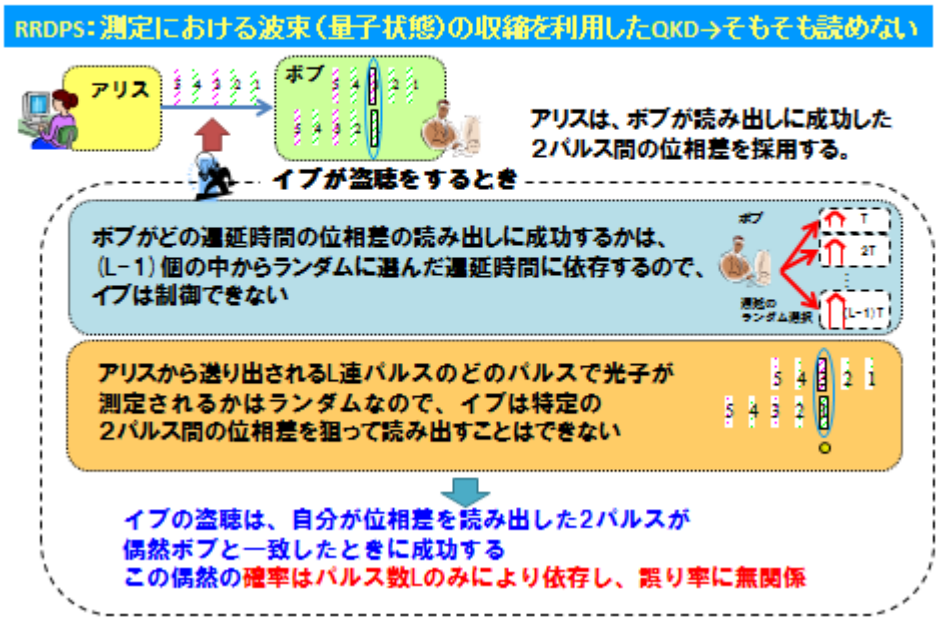
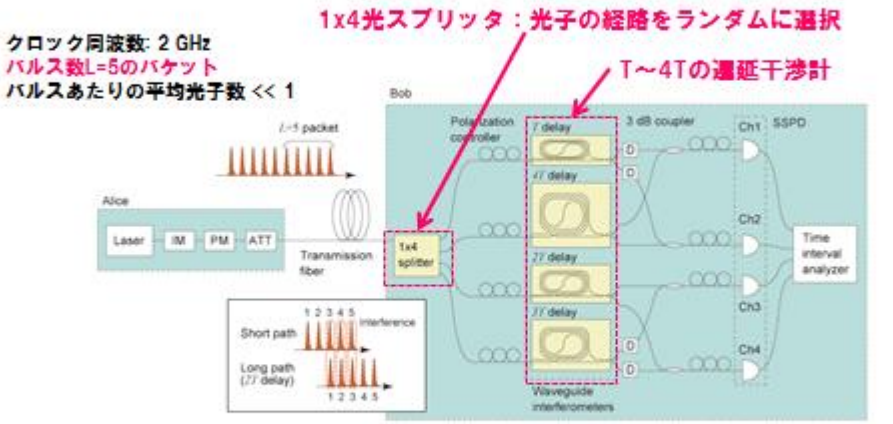


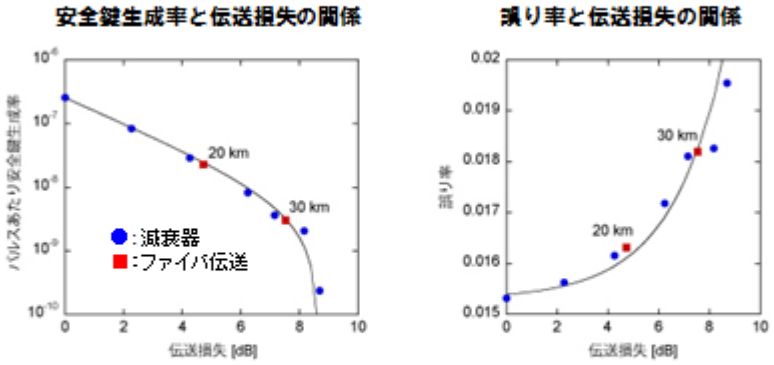
図4：総当たり位相差測定の実装



受動素子を用いてT～4Tの遅延干渉計をランダムに選択する仕組みを実装

→　低損失、高い位相安定度

図5：鍵配送実験結果



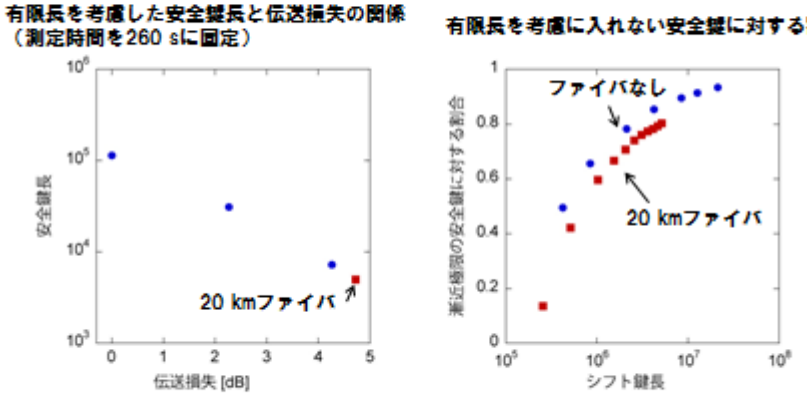
RRDPSプロトコルの原理確認実験に成功（安全鍵生成を初めて実現）
性能：30 kmのファイバ伝送を達成。最大伝送損失は～9 dB。

※鍵の長さの有限性による情報漏洩量の揺らぎを考慮に入れない安全性評価

図6：鍵の長さの有限性を考慮した安全性解析

現実のQKDシステムでは必ず鍵の長さは有限 → 情報漏洩量見積もりの揺らぎ（安全鍵生成に「失敗」する可能性）

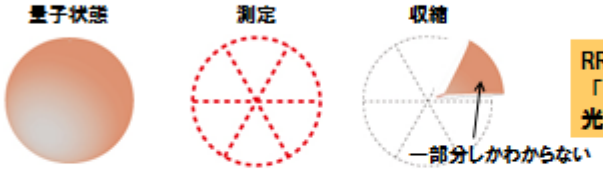
鍵の長さの有限性を考慮しても安全な鍵の長さを計算した



鍵の長さの有限性を考慮した現実のシステムでも
安全な鍵配送が可能であることを確認

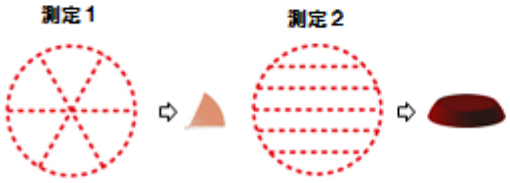
図7：波束の収縮

1．波束の収縮とは、測定前は（たとえば光子の場所が）定まっていない量子状態（波束）が、
測定によって「収縮」して光子の場所が決まるという性質。測定すると、一部分しかわからない



RRDPS方式では、
「どれか一つのパルスでのみ
光子が観測される」ことに相当

2．どのように量子状態を「切るか」は測定する人が選べる



RRDPS方式では、
「ボブが遅延時間をランダムに
選択する」ことに相当