プレスリリース
平成 26 年 10 月 24 日

量子鍵配送に関する新理論を確立

～鍵生成速度についての原理的な限界を解明～

【ポイント】

■量子鍵配送の 1 パルスあたりの鍵生成レートに原理的な限界があることを解明
■量子鍵配送プロトコルの改良により、1パルスあたりの鍵生成レートを現状の約 10 倍程度向上可能
■鍵生成レート向上により、行政・産業・医療機関ネットワーク等での量子鍵配送の実用化研究開発が加速

独立行政法人情報通信研究機構（NICT、理事長: 坂内 正夫）は、レイセオンBBNテクノロジーズ社（米国）及びルイジアナ州立大学（米国）と共同で、現在実用化が進められている 2 地点間の量子暗号[*1]における新理論を確立し、量子鍵配送[*2]の 1 パルスあたりの鍵生成レート[*2]の原理的な限界を世界で初めて解明しました。量子暗号は、コンピュータによる解読が絶対不可能とされる究極的な暗号通信として、実用化が期待されている新しい技術です。今回の成果は、鍵生成レートが量子鍵配送プロトコルの改良により、現在の更に 10 倍程度まで向上できる可能性を示すとともに、その将来的な限界を明らかにしました。これらは、これからの研究開発の指針を与えるものであり、このことにより、今後の研究開発の加速が大きく期待されます。

なお、本成果は、英国科学電子ジャーナル「*Nature Communications*」（英国時間 10 月 24 日（金）午前 10:00）に掲載されます。

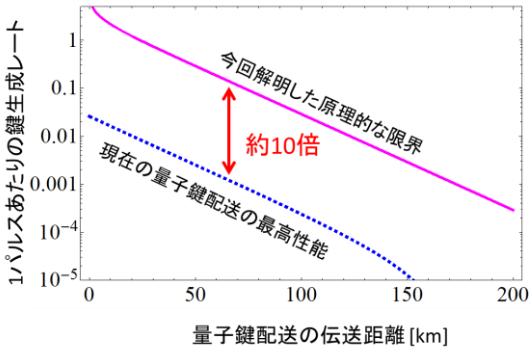
【背景】

量子暗号は、量子鍵配送とワンタイムパッド暗号化から成り、将来開発される可能性のある、いかなる高速な計算機を使っても解読できない究極的な暗号として実用化が期待されている技術です。量子暗号の技術開発課題として、量子鍵配送の鍵生成速度の向上が挙げられています。鍵生成速度は、デバイスの性能や波長多重数で決まる「1 秒当たりの光子パルス[*3]の生成数」と、鍵生成方式（量子鍵配送プロトコル）によって決まる「1 パルスあたりの鍵生成レート」の 2 つの性能により決まります。これまで、1 パルスあたりの鍵生成レートをできるだけ大きくするために、様々な量子鍵配送プロトコルが提案されてきましたが、実用的な 2 地点間の量子鍵配送プロトコルは、いずれも光ファイバーの伝送損失に対して、鍵生成レートが指数的に減衰してしまう性質を持っていました。

【今回の成果】

今回、量子鍵配送について、量子情報理論[*4]に基づく新しい理論を確立し、この鍵生成レートの伝送損失に対する指数的な減衰は、個々の量子鍵配送プロトコルによらない普遍的な原理であることを解明しました。また、その原理的限界は、現在実現している量子鍵配送プロトコルにおける 1 パルスあたりの鍵生成レートの 10 倍程度であることも明らかにしました。

このことは、現在の鍵生成レートが、量子鍵配送プロトコルの更なる改善により、10 倍程度まで向上できる可能性を示すとともに、どのようなプロトコルでも超えられない限界も同時に明らかにしたもので、今後、新しい量子鍵配送プロトコルの開発を進める上で重要な指針を与える成果です。



量子鍵配送の鍵生成レートの限界と伝送距離

【今後の展望】

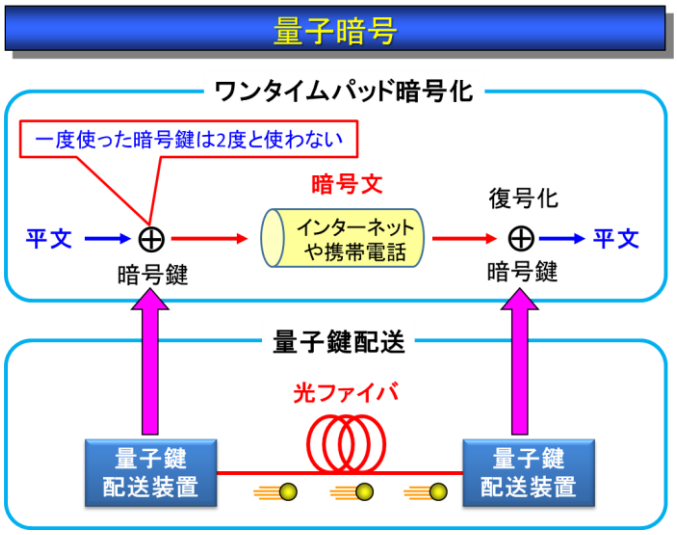
今後は、本成果で明らかとなった鍵生成レートの理論限界に近づく、より優れた量子暗号プロトコルの開発に取り組みます。同時に、1 秒当たりの光子パルスの生成数の向上に向けて、デバイス開発や波長多重化なども進めていきます。

一方、鍵生成速度及び伝送距離の限界は、従来の 2 地点間の量子暗号を超える新しい技術革新により、抜本的に超えることができます。それには、送受信者の間に量子的な中継器を置く量子中継技術[*5]や、量子暗号の物理的安全性の条件を少し緩和することで、鍵生成レートを大きく向上させる新しい物理レイヤ暗号技術[*6]などの実現が不可欠です。これらの技術は、まだ理論的・実験的に発展途上であり、実現には長期間の研究開発を要しますが、こうした基礎的な研究にも積極的に取り組んでいきます。

＜用語解説＞

*1 量子暗号

量子暗号は、「量子鍵配送」による暗号鍵の共有と、それを用いた「ワンタイムパッド暗号化」から構成される。

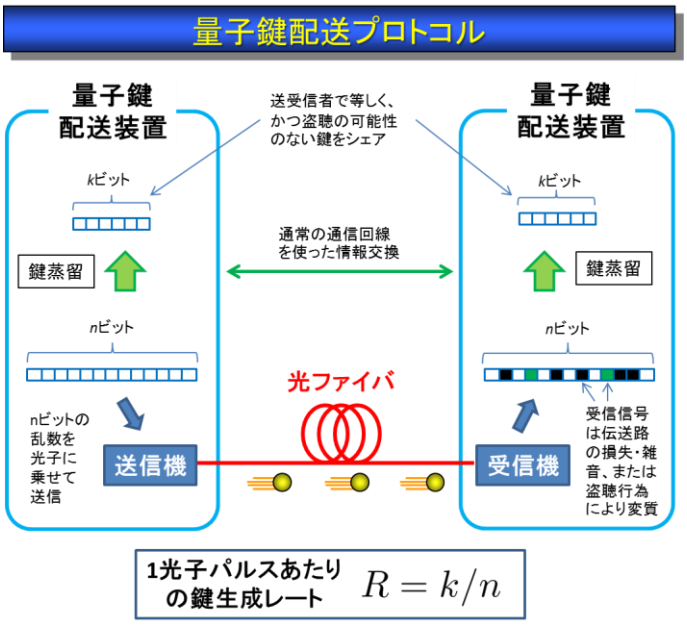


量子鍵配送では、送信者が光子を変調（情報を付加）して伝送し、受信者は届いた光子一個一個の状態を検出し、「鍵蒸留」と呼ばれる情報処理により、盗聴の可能性のあるビットを排除して、絶対安全な暗号鍵（暗号化のための乱数列）を送受信者間で共有する。変調を施された光子レベルの信号は、測定操作をすると必ずその痕跡が残る（ハイゼンベルクの不確定性原理）ため、この原理を利用して盗聴を見破る。

ワンタイムパッド暗号化では、送信情報のデジタルデータを、それと同じ長さの暗号鍵（0と1のランダムなビット列）と足し算することで暗号化し、復号は更にもう一度足し算をすることで行う。パッドとは暗号鍵を意味する。一度使用した乱数列は二度と使わないというのがワンタイムパッドの規則である。ワンタイムパッド暗号は、解読が絶対的に不可能であることがシャノンにより証明されている。

*2 量子鍵配送と鍵生成レート

量子鍵配送は、光子パルスを送信・検出（受信）する量子通信と、送受信したビット列から情報処理により安全な鍵を取り出す「鍵蒸留」から成る。



送信者は、まず n ビットの乱数列を準備し、光子を使ってその情報を受信者に送る。受信者は、これを測定し受信するが、受信された n ビットのビット列は、伝送路の損失で一部が欠落したり、雑音や盗聴者の盗聴行為などによって、一部のビット情報が、送信者が送ったものとは異なるものになってしまう可能性がある（ビット誤り）。

鍵蒸留は、そのような不完全なビット列から、安全かつ誤りのないビット列を取り出す情報処理であり、光子の失われたビットなどを排除する「ふるい落とし」、送受信者が共有したビット列間の誤りを直す「誤り訂正」、さらに、盗聴された可能性のあるビットを排除する「秘匿性増強」などのいくつかのアルゴリズムから構成されている。この鍵蒸留により、最終的に、送受信者間で共通かつ盗聴可能性のない安全な k ビットの乱数列、すなわち、鍵を共有することができる。一般的に鍵の長さ k は、最初に準備した乱数列 n に比べ非常に短いものとなる。

鍵生成レートは、このときの割合、すなわち、k/n であり、これは、光子の物理的な生成・変調・測定方法と、鍵蒸留のアルゴリズムの性能によって決まる。鍵生成レートが大きい（1 に近い）ほど、効率よく鍵を生成できる量子鍵配送プロトコルであるといえる。

*3 光子パルス

量子力学によれば、光は“波”の性質と“粒子”の性質を併せ持っている。光の粒子は、「光子」と呼ばれ、これ以上分割することのできない光のエネルギーの最小単位である。例えば、光通信で通常用いられる 1.5 ミクロンの波長では、1 光子のエネルギーは、約 1,000 京分の 1（1 京は 1 の後に 0 が 16 個ついた単位）ジュールという極めて小さな値になる。

光子パルスとは、パルス信号内に光子が平均して一個程度もない超微弱な光信号パルスである。

***4 量子情報理論**

現在のデジタル通信の最も基本的な理論であるシャノン情報理論と、光子等の物理的性質を最も正確に表す量子物理学を合わせた理論。

現在の情報通信システムは、電磁気学や光学などの古典物理学に基づいて設計されているが、量子情報理論の発展により、情報操作の原理を量子物理学まで拡張すれば、従来不可能だった新機能、例えば、盗聴不可能な暗号通信(量子暗号)や究極的な低電力・大容量通信(量子通信)が可能になることがわかっている。

***5 量子中継**

2 地点間量子暗号の限界を超えた超長距離量子暗号を実現するためには、送受信者の間で量子的な相関を持つ光子(量子もつれ光子)をシェアする必要がある。数百 km 以上離れた 2 地点間で、光ファイバーを使って量子もつれ光子をシェアするためには、減衰した信号を中継する必要があるが、通常の光通信で用いられる中継増幅器は使うことができず、量子中継という新しい中継技術が必要になる。

量子中継では、伝送されてきた光子を保存する量子メモリや、伝送により劣化した量子もつれを純粋化する量子回路などの要素技術が必要となる。これらの技術の実現は、難易度が非常に高く、現状ではまだ確立していない。しかし、その実現に向けた基礎研究は、世界中で急速に進んでいる。

***6 物理レイヤ暗号**

電波、光等の信号の送受信過程や伝送路で発生する物理的な雑音を利用して、盗聴者の計算能力によらない安全性(情報理論的安全性)を実現する暗号方式の総称。量子暗号も、光の量子力学的性質を利用した物理レイヤ暗号の一種である。

量子暗号では、究極の安全性を実現するため、盗聴者は物理的に許されるあらゆる盗聴手段(例えば、量子コンピュータや量子メモリなど、現在の技術ではまだ実現していない未来の技術もすべて含めた盗聴手段)が仮に実行可能であったとしても、安全な鍵を生成できるよう設計されているが、その代償として、鍵生成速度や距離に厳しい制限が課される。一方、盗聴者の盗聴手段に妥当な制限を課すことで、情報理論的安全性を確保しつつ、速度や距離を著しく向上した新しい物理レイヤ暗号を実現できる可能性があり、その研究が進められている。

＜掲載論文＞

掲　載　誌: *Nature Communications* (Nature Publishing Group), DOI: 10.1038/ncomms6235
U　R　L: http://www.nature.com/naturecommunications/
掲載論文名: Fundamental rate-loss tradeoff for optical quantum key distribution
著　者　名: M. Takeoka, S. Guha, and M. M. Wilde

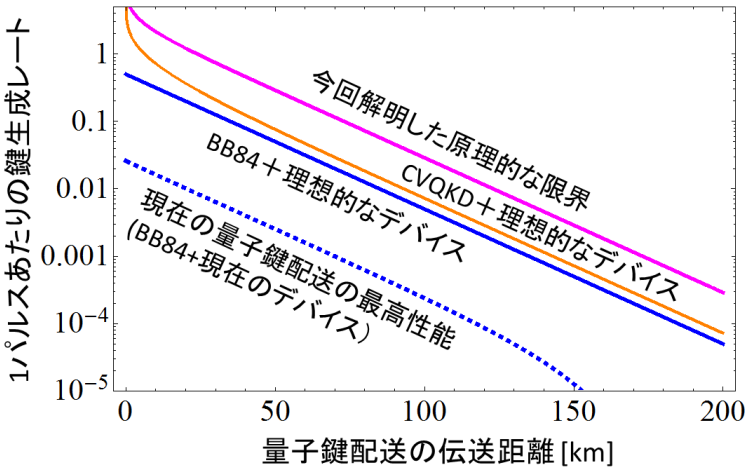
＜ 本件に関する 問い合わせ先 ＞
未来 ICT 研究所
量子 ICT 研究室
武岡 正裕
Tel: 042-327-7471
Fax: 042-327-6629
E-mail: takeoka@nict.go.jp

＜ 広報 ＞
広報部 報道担当
廣田 幸子
Tel: 042-327-6923
Fax: 042-327-7587
E-mail: publicity@nict.go.jp

補足資料

鍵生成レートの「原理的な限界」とは

通常、量子鍵配送の鍵生成レートは、用いる量子鍵配送プロトコル（送信側が送る光の量子状態制御、受信側の測定法、鍵蒸留の方式など）を決めると、計算により求めることができます。一方、今回の成果である鍵生成レートの「原理的な限界」とは、どのような量子鍵配送プロトコル、つまり、送受信者があらゆる量子状態の光や測定法、鍵蒸留法などを使っても絶対に超えられない限界です。【今回の成果】で示した「量子鍵配送の鍵生成レートの限界と伝送距離」の図を再掲し、以下に、その意味をもう少し詳しく説明します。



量子鍵配送の鍵生成レートの限界と伝送距離

デバイス性能による鍵生成レートの向上

上図の一番下側の青い点線で示した「現在の量子鍵配送の最高性能」は、正確には、「現在の最高性能の光子制御・検出デバイスを、現在最も標準的な BB84 という量子鍵配送プロトコルに実装した場合の性能」といえます。ここで、現在の最高性能の光子制御・検出デバイスは、今後の技術開発により更なる性能の向上が期待できます。今後、デバイスの開発が進み、仮に、一切のデバイスの不完全性がなくなったとします。その場合の鍵生成レートは、青い実線で示され、青い点線と比べると、デバイス性能の向上による鍵生成レートの向上がまだ見込めることがわかります。

より良いプロトコルによる鍵生成レートの向上

BB84 というプロトコルが、2 地点間の量子暗号で最上のプロトコルかどうかという点について、実際には、BB84 以外にも様々なプロトコルの提案がなされており、例えば、CVQKD というプロトコルでは、仮に、デバイスが完璧に動作するとすれば、オレンジ色の線の鍵生成レートを達成できることが知られています。

最終的な限界

将来、もっと格段に優れたプロトコルが提案される可能性が期待できます。しかし、赤紫色の線で示した「今回解明した原理的な限界」は、今後、いかなるプロトコルが考案されたとしても、絶対に超えられないという鍵生成レートの最終的な限界、つまり、2 地点間量子暗号のある種の普遍的な限界を示しています。

今後の期待

「今回解明した原理的な限界」は、飽くまで「最終的な」限界です。実際には、現実の鍵生成レートとはまだ 10 倍以上の差があるため、今後もデバイス性能の向上などにより、一層の量子暗号の高速化が期待できます。

また、今回の限界は、光子を送る通信路が 1 回線（1 波長）であると仮定したときのものです。実用上は、従来の光通信と同様、波長多重などの回線を増やす技術を活用すれば、量子暗号システム全体の速度を更に向上させることができます。