東京大学
THE UNIVERSITY OF TOKYO

量子暗号の到達距離を２倍に
―新しい推定手法で盗聴監視の困難を解決―

１．発表者

前田　健人（東京大学大学院工学系研究科物理工学専攻　修士課程２年）
佐々木寿彦（東京大学大学院工学系研究科光量子科学研究センター　助教）
小芦　雅斗（東京大学大学院工学系研究科光量子科学研究センター　教授）

２．発表のポイント

◆難航していたセキュリティの問題を解決し、特殊技術を使わずに量子暗号の到達距離を従来の約２倍に伸ばせることを初めて証明した。
◆生成が困難な特殊な光を用いれば盗聴の痕跡が浮かび上がるはずだが、それをレーザー光だけを用いて厳密に推定する新手法の発案が解決の鍵となった。
◆汎用性の高い新推定手法は、量子暗号だけでなく、光を用いる量子技術開発の促進にも有用と期待される。

３．発表概要：

量子暗号（注１）は、量子力学の性質を利用して、盗聴者の計算能力や技術レベルに依存しない強固なセキュリティを持った通信を可能にする技術です。既存の光通信技術だけで実現できることも量子暗号の特長のひとつですが、その場合には通信距離が 250km 程度までという限界がありました。最近、既存技術だけでこの距離を約２倍に伸ばすアイデアが注目され、世界中の研究者がセキュリティの証明に取り組みましたが、盗聴攻撃の監視にどのくらいの時間を割けばセキュリティが確保できるか、という肝心の部分が未解決でした。

本研究グループは、この新しい量子暗号方式の問題を解決し、証明されたセキュリティのもとで通信を行う具体的な手続きを与えることに初めて成功しました。この方式において、盗聴の痕跡を直接調べるには、量子力学的な特性を持った特殊な光が必要です。それを、レーザー光だけで間接的に推定する新しい手法を考案したことが、解決の鍵でした。この成果により、既存技術でも量子暗号の到達距離を 500km 程度まで伸ばす道が拓けました。また、解決の鍵となった新しい推定手法は汎用性が高く、光を用いる量子技術開発の促進につながると期待されます。

本研究は、内閣府総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム（SIP）「光・量子を活用した Society5.0 実現化技術」（管理法人：量研）ならびに科学技術振興機構(JST)の戦略的創造研究推進事業(CREST)の支援のもとに行われました。

４．発表内容：

《研究の背景》

代表的な量子暗号方式では、１個の光子（注２）に信号を載せて通信することで、量子力学の性質を用いて盗聴を監視しながらセキュリティを確保します。長距離の通信には光ファイバーが用いられますが、光ファイバーは完全に透明という訳ではなく、遠くまで届くのは光のごく一部です。例えば、100km の光ファイバーを通り抜ける光子は 100 個に１個の割合です。このため、既存の技術では 250km 程度が限界で、それを超えるには開発途上の技術（注３）が必要と考えられてきました。

これに対し、昨年５月、英国のグループが、既存技術で長距離通信を達成するためのツインフィールド方式と呼ばれる量子暗号方式を提案しました（東芝のニュースリリース

https://www.toshiba.co.jp/rdc/detail/1805_01.htm）。図１のように、通信したい二人（アリスとボブ）の真ん中に光子を検出する装置を設置し、光パルスをこの装置に向かって送り出します。中央の装置が光子を１個検出すると、その結果を聞いて、アリスとボブは１ビットの乱数を共有できます。検出された光子は、アリスまたはボブから届いたものなので、二人の距離の半分の長さの光ファイバーを通り抜けただけです。それでも二人が乱数を共有できるのは不思議な気がしますが、量子力学の干渉（注４）という性質が使われています。実質的に光ファイバーの距離が半分になるので、二人が 500km 程度離れても通信が可能であることが期待されました。

しかしながら、当初の提案では、盗聴者のあらゆる攻撃、例えば中央の装置を乗っ取るなどの攻撃に対して、セキュリティを確保できるかが不明でした。その後、国内外の８以上のグループがセキュリティの確立を目指しましたが、現実的な時間で完全な監視を行う方法が見つからず、このツインフィールド方式は画竜点睛を欠いた状況が続いていました。

《成果の内容》

今回、本研究グループは、中央の装置と光ファイバーに対してどんな盗聴が試みられても、それを効率よく監視できる手法を明らかにしました。これにより、既存技術の範囲で到達距離を２倍にするという方式が､量子暗号としてのセキュリティを持つことを初めて証明しました。以下に、問題解決のポイントを説明していきます。

量子暗号において、盗聴の痕跡を調べるのは、科学捜査で指紋を探すのに似ています。目には見えない指紋を専用の光源で浮かび上がらせるように、量子暗号では、盗聴検出用の光パルスを通常の通信用のパルスに混ぜ込んで、盗聴の痕跡を調べます。光子に信号を載せる代表的な量子暗号方式では、盗聴検出用の光パルスは、通信用の光パルスと同じ光源を用いて作ることができます。

一方、ツインフィールド方式では、量子力学の干渉の性質を利用するために、光の波としての性質（波の振動のタイミング）に信号を載せて通常の通信を行います。この場合、盗聴を検出するには、シュレーディンガーの猫状態（注５）と呼ばれる非常に特殊な光が必要になってしまうのです。つまり、既存の技術で距離を伸ばそうとして導入した工夫のせいで、盗聴監視に開発途上の技術が必要になったという訳です。

これに対し、本研究グループは、非常に単純なアイデアで解決を試みました（図２）。レーザー光源だけで簡単に作れる光パルスを２種類用意して、それぞれを照らしたデータを採ります。この２つのデータを引き算すると、特殊な光を照らした時に似たデータ、つまり盗聴の痕跡が浮かび上がるという仕掛けです。考え方は単純ですが、「似たデータ」という部分を「どんな盗聴攻撃をされても見逃がさない」という厳密な推定手法の理論として定式化できたことが、問題解決のポイントでした。

《総括》

本研究成果により、既存の技術を用いて量子暗号の到達距離を500km程度まで伸ばせるという期待に確固たる理論的な裏付けが得られました。解決の鍵となった新しい推定手法は、レーザー光だけで効率よく盗聴行為を監視する可能性を広げるもので、完璧ではない光源や検出器を用いた量子暗号に適用することにより、近距離用の量子暗号方式の低コスト化にも寄与すると考えられます。更には、特殊な光を扱うデバイスを低コストで検査するなどの応用も考えられ、光を用いる量子技術開発の今後の促進につながると期待されます。

５．発表雑誌：
雑誌名：「*Nature Communications*」（オンライン版 2019 年 7 月 17 日掲載）
論文タイトル： Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit
著者：Kento Maeda, Toshihiko Sasaki, Masato Koashi*

６．問い合わせ先：
東京大学　大学院工学系研究科　光量子科学研究センター／光量子科学連携研究機構
教授　小芦　雅斗（こあし　まさと）

＜広報に関すること＞
東京大学大学院工学系研究科　広報室

７．用語解説：
注１：量子暗号
量子暗号は、量子力学の性質を使って、盗聴者に知られないようにしてランダムなビット列を送信者と受信者に配布します。このビット列は秘密鍵と呼ばれ、秘密鍵があればすぐに秘匿通信が可能になります。このような仕組みのため、量子鍵配送、またはイニシャルで QKD とも呼ばれています。

注２：光子
光は電磁波とも呼ばれ、振動する波が光速度で伝わっていくものだと考えられていますが、非常に微弱な光は、光子と呼ばれる粒が弾丸のように光速度で走っているような振る舞いも見せます。波の性質と粒子の性質を兼ね備えるのは、量子力学の大きな特徴です。

注３：開発途上の技術
量子もつれを持った光を生成する光源、光の量子状態を保存する量子メモリ、光子を吸収せずにその存在を検知する量子非破壊測定などの技術は、実験室レベルで開発が進んでいますが、十分な精度で高速に動作するデバイスとして完成するのはまだ先の話です。

注４：干渉
「波」は山と谷が交互にやってくる現象ですが、ふたつの波が重なると、山と谷の重なり具合の関係に依存した様々な現象が起こり、波の干渉と呼ばれます。今回の例では、アリスとボブがビット値に応じて山と谷のタイミングを選んでいるため、光子の検出の際に干渉が起こり、二人のビット値の関係（同じか違うか）が測定結果に現れます。
光子は１個なのに、二人のビット値の関係がわかってしまうのは、量子力学における干渉の不思議さの一つです。計算の問題にこの現象をあてはめると、2 回計算しないとわからなそうなことが 1 回の計算でわかることに相当しますが、これは量子コンピュータが高速に計算できる原理のひとつです。

注５：シュレーディンガーの猫状態
オーストリアの理論物理学者シュレーディンガーが量子力学の不条理さを指摘するために、猫の生死を重ね合わせた状態を例として使いました。光の場合には、山と谷がちょうど正反対の波を重ね合わせた状態が、光が強くなるとシュレーディンガーの例に似てくることから、一般にシュレーディンガーの猫状態と称されます。この状態の光は、半透鏡で二つにわけるだけ

ですぐ量子もつれ状態が作れてしまうなど、特殊な性質を持った光で、十分な精度で高速に生成するのは簡単ではありません。

８．添付資料：

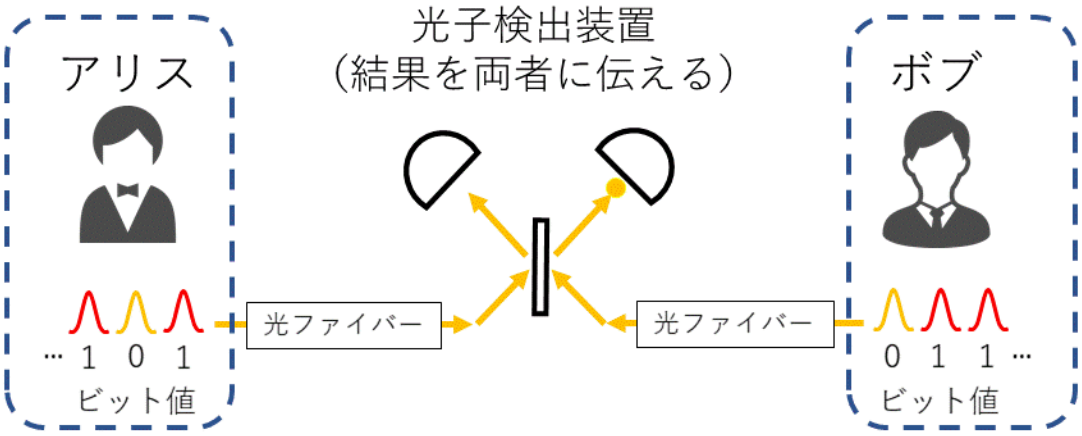

図１：ツインフィールド方式の基本的な仕組み

アリスとボブは、それぞれビット値（0 か 1）をランダムに選び、それに応じて光パルスの波の振動のタイミングを選んで中央に送ります。中央の装置は、両側から届いた 2 つのパルスを半透鏡で重ね合わせて光子を検出します。検出器は 2 つあり、どちらが光子を検出したかによって、アリスとボブの選んだビット値が同じか違うかがわかります。違うとわかった場合はボブがビット値を替えます。すると、光子が検出されるたびに、アリスとボブはランダムな共通のビット値を手にできます。ただし、盗聴行為の監視には何か別の手立てが必要になります。アリスとボブが 500km 離れていても、光子は、250km の光ファイバーを潜り抜けて中央にたどり着けば検出されます。これが、従来の量子暗号に比べて到達距離を約 2 倍にできると期待される理由です。

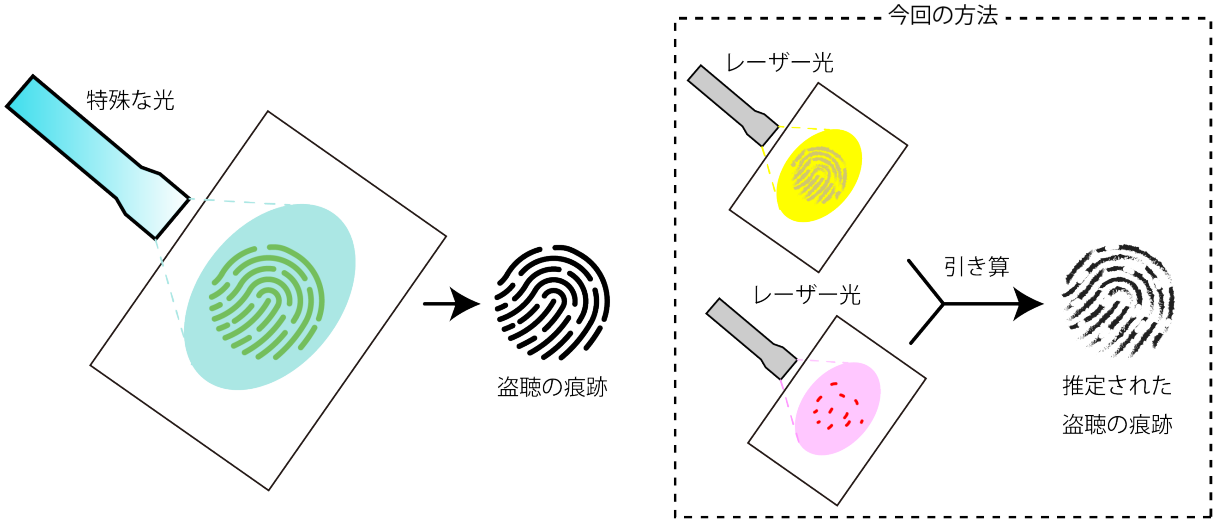

図２：新しい推定手法のイメージ

盗聴の痕跡を直接浮かび上がらせるには、レーザー光源では作れない特殊な光が必要です。そのような光を実際に作る替わりに、新手法では、レーザー光源で作ったパルスを光ファイバーに通して得られたデータを２種類作り、引き算をします。どのような盗聴攻撃でも、この引き算した結果に痕跡が現れることを数学的に証明できます。