東京大学
THE UNIVERSITY OF TOKYO

光波を測る量子暗号のセキュリティ問題を解決
―量子暗号装置の低コスト化へ前進―

１．発表者

松浦　孝弥（東京大学　大学院工学系研究科物理工学専攻　博士課程２年）
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[当時]）
佐々木寿彦（東京大学　大学院工学系研究科物理工学専攻　講師）
小芦　雅斗（東京大学　大学院工学系研究科附属光量子科学研究センター　教授）

２．発表のポイント

◆通常、量子暗号では光の粒（光子）の検出を行うが、替わりに光の波の振幅を測る方法も模索されてきた。しかし、セキュリティを保証する理論が未完成という大きな壁があった。
◆光子を検出すれば得られるはずの盗聴の痕跡を、振幅というアナログな測定結果だけから厳密に推定する新手法を発案し、セキュリティの問題を解決した。
◆光子検出装置に比べ、振幅測定装置は低コストでコンパクトに実現できる。波長多重などの既存の光通信技術との親和性も高く、量子暗号技術の普及の促進が期待される。

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。多くの量子暗号方式では、非常に小さなエネルギーを持つ光子（注２）１個の到来を検知できる光子検出器が使われますが、光の波の振幅を測る別の方式も提案されていました。この光波を測る量子暗号方式は、光子検出器の替わりに、もっと安価な、強い光のエネルギーを測る光検出器で実現できるという利点があります。しかし、光子の検出を行う方法に比べると、セキュリティを保証する理論の進展が遅く、盗聴者がどんな技術を使っても盗聴できないという量子暗号の最大の特長を証明するには、非現実的な装置の仮定が必要でした。

本研究グループは、光波を測る量子暗号方式のセキュリティの問題を解決し、非現実的な仮定を置くことなく、保証されたセキュリティのもとで通信を行う具体的な方法を初めて見出しました。波の振幅というアナログ量から盗聴の痕跡を突き止める新しい手法の考案が解決の鍵でした。この成果により、量子暗号装置の低コスト化、コンパクト化や、光波長多重通信（注３）による大容量化の道が拓けることになり、強固なセキュリティを持つ量子暗号技術の普及に大きく弾みがつくと期待されます。

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》

量子暗号は、量子力学の性質が顕著になる微弱な光を用いて通信することで、盗聴の痕跡を検知しながら通信を行います。既存の数学的な暗号では、今通信した内容が、計算能力が進歩した未来のある時点で解読されてしまうリスクがありますが、それに比べて、量子暗号のセキュリティは、盗聴者の計算能力や技術レベルに依存せず、どんな未来の技術を使っても盗聴できないというとても強固なものです。

代表的な量子暗号方式では、１個の光子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。光を受信する装置には、光子１個の到着を電気信号で報せる「光子検出器」が使われます（図１）。ただ、１個の光子のエネルギーはとても小さいので、それを検知することは容易ではなく、光子検出器は冷却装置なども含んだ高価でかさばるものになりがちです。

一方、通常の光通信では、フォトダイオードという光検出器が使われます。これは、光の強弱を電流の大きさに変換するものです。フォトダイオードは、ある程度強い光を測定するための道具で、光子１個を見分ける感度も精度もありませんが、光子検出器に比べて安価でコンパクトです。コヒーレント光通信では、受信した光を参照レーザー光と干渉させることで、フォトダイオードを使って受信光の波の振幅を測定するホモダイン検波という手法が使われます（図１）。ホモダイン検波では、参照レーザー光がある種の増幅器の役目をしているので、微弱な振幅の変化を検知する能力があります。さらに、特定の波長の光だけを増幅するので、光波長多重通信を行っていても、別の波長の光に邪魔されないという特長があります。

ホモダイン検波はこのように魅力的な特長を持つため、これを用いた量子暗号方式が約２０年前から提案されており、連続量量子鍵配送（注４）と呼ばれています。しかし、光子を用いる量子暗号方式に比べてセキュリティを保証する理論の構築が難しく、未解決のまま残されていました。つまり、「この装置を作って暗号通信すれば、どんな盗聴技術でも破れません」という理論の裏付けができていないという状況でした。

《成果の内容》

今回、本研究グループは、未解決だった連続量量子鍵配送のセキュリティの問題を解決し、「この手続きに従って信号処理を行えば、どんな盗聴技術でも事実上破れない」という証明に成功しました。以下に、問題解決のポイントを説明していきます。

連続量量子鍵配送の理論的な難しさは、受信者のホモダイン検波の測定結果がアナログ量だということに原因があります。光の波の振幅の測定結果は、例えば 0.874 だったり、1.3929 だったり、測定のたびに千差万別の数字が出てきます。一方、光子検出器の測定結果は、光子が到着したか、しなかったかの２種類しかありません。この違い（図１）が、盗聴の痕跡を調べようとする際に大きく関わってきます。

まず、光子検出器を用いる従来型の量子暗号では、例えば光子検出器を２台用意して、盗聴がない場合には光子が必ず一方の検出器に到着するように設計します。こうすると、もう一方の検出器が光子を検出したら、それは本来起きてはいけない「エラー」であり、直ちに盗聴の痕跡になります。そのため、エラー検出の数が全検出数の何パーセントに相当するのかを調べれば、その「エラー割合」がそのまま盗聴の度合いを表す数値になる、という単純な図式です。

これに対し、ホモダイン検波を用いる連続量量子鍵配送（図２）では、測定結果がアナログ量であるため、この値が出れば即それは盗聴の痕跡なのだ、というはっきりとした結論は出せません。盗聴がない場合には必ずこの測定結果になる、という設計は不可能で、エラーなのかどうかを白黒つけることができないのです。このアナログの数値をどのように信号処理すれば盗聴の度合いを知ることができるのか、というのが研究者を悩ませてきた問題です。これまでに提案されてきた手法では、通信を無限に長い時間続けたら、とか、光の波の振幅の測定を無限の精度で実現できたら、などの実現不可能な仮定のもとでしか、盗聴の度合いを厳密に知ることはできませんでした。

今回の解決のポイントは、ラゲールの陪多項式という数学の道具を使ったある公式の発見です。ホモダイン検波で得られた数値をこの公式に代入してから平均値を計算すると、上に書いた「エラー割合」に相当する値が得られるというものです。高価な光子検出器を使って測定していた「エラー割合」を、安価なフォトダイオードを使って測定する方法を見出したとも言え

ます。この手法により、従来型の量子暗号のセキュリティ理論のテクニックをそのまま使うことが可能になり、非現実的な仮定を一切せずに、「どんな盗聴技術でも事実上破れない」ことの証明に初めて成功しました。

《総括》

本研究成果により、セキュリティの最後のピースが埋まり、安くてコンパクトで大容量という特長を持つ連続量量子鍵配送が実現可能な技術となりました。どんな未来の技術を使っても盗聴できないという強固なセキュリティを持つ量子暗号技術の普及の促進が期待されます。

５．発表雑誌：

雑誌名：「*Nature Communications*」（オンライン版 2021 年 1 月 13 日掲載予定）
論文タイトル：Finite-size security of continuous-variable quantum key distribution with digital signal processing
著者：Takaya Matsuura, 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　附属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

量子暗号では、量子力学の性質を使って、盗聴者に知られていないランダムなビット列を送信者と受信者に配布します。このビット列は鍵と呼ばれます。鍵さえあれば、秘密にしたいメッセージを簡単に安全に送ることができます。このように、鍵を配布することが肝心なので、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：光波長多重通信

光の「色」の違いは、光波の山と次の山の間隔である波長で決まっています。一本の光ファイバーに異なる色（波長）の光を同時に通すことで、大容量の通信を行うのが光波長多重通信です。この通信手法では、ある波長に載せた情報を取り出す際に、他の波長の光が邪魔にならないような工夫が必要ですが、ホモダイン検波はこの点で特定の波長の信号だけを取り出す能力に優れています。

注４：連続量量子鍵配送

受信者がホモダイン検波のようにフォトダイオードを用いる場合、測定結果は電流の大きさというアナログ量（連続量）になります。そのため、このような受信方式の量子暗号（量子鍵配送）方式は、連続量量子鍵配送（CV-QKD）と呼ばれています。これに対して、光子検出器を用いる方式は、測定結果が光子を検出したか否かのデジタル量（離散量）であることから、離散量量子鍵配送（DV-QKD）と呼ばれることがあります。

８．添付資料：

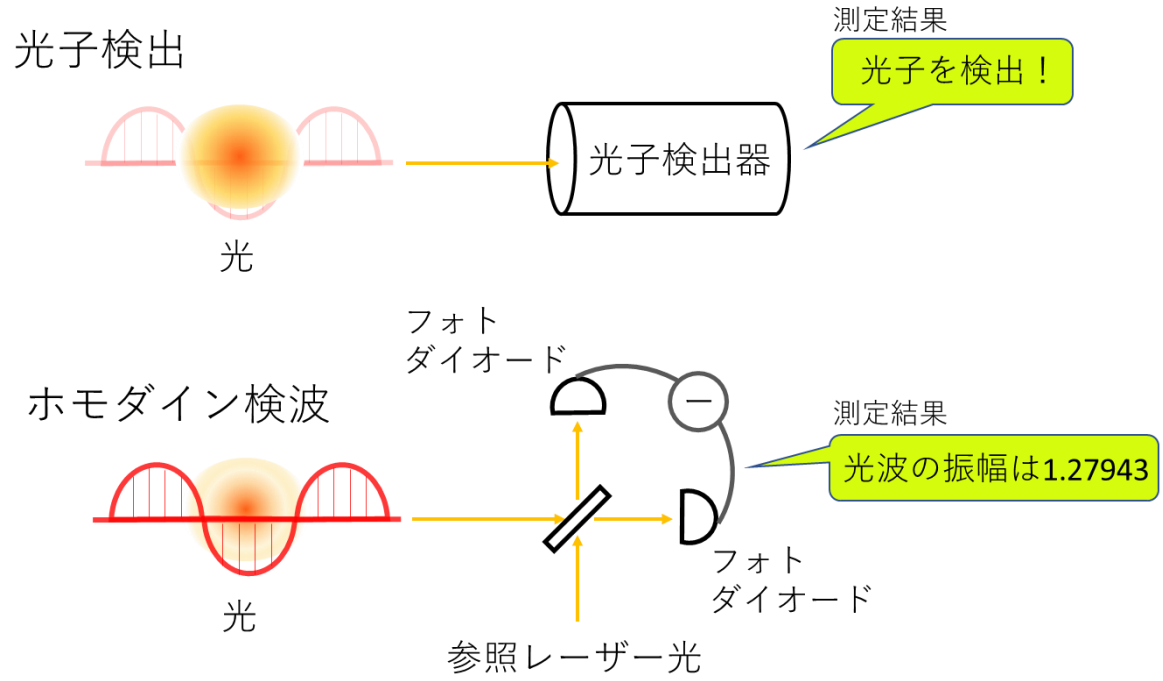

図１：光子検出とホモダイン検波

光は粒としての性質と波としての性質を合わせ持っています。光子検出器は、粒としての性質を測る測定器で、光子の到着を検出して電気信号を出します。ホモダイン検波は、波としての性質を測る手法で、参照レーザー光とフォトダイオードを用いて、波の振幅に比例した電気信号を出力します。光子検出の結果は、光子を検出したか否かの２種類しかありませんが、ホモダイン検出の結果は、振幅の大きさを表すアナログ量です。

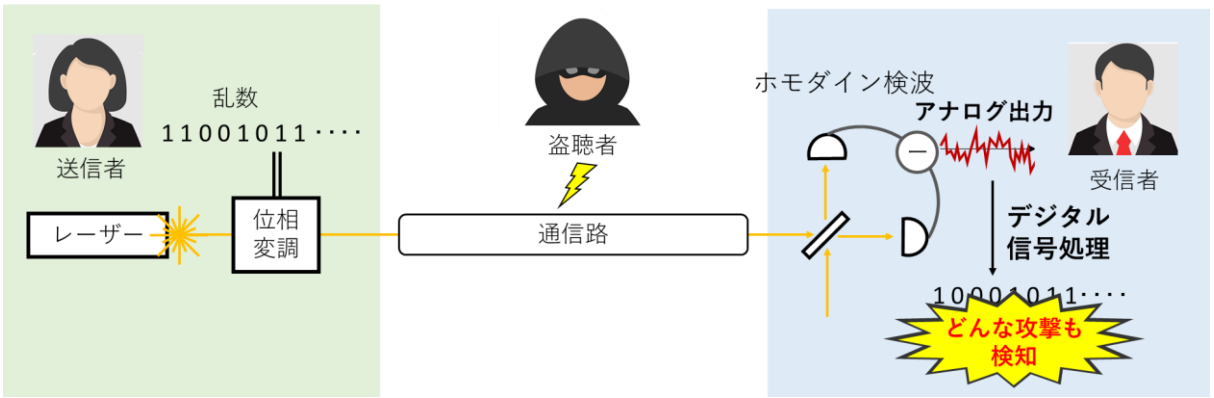

図２：連続量量子鍵配送

連続量量子鍵配送では、送信者が乱数に従って光の波の振幅を変化させ、受信者に送ります。受信者はホモダイン検波によって波の振幅を測定することで、送信者の乱数を受け取ります。この乱数を途中で盗聴しようとすると、量子力学の性質により、その影響がホモダイン検波の出力に現れますが、この出力がアナログ量であるために、そこからどうやって盗聴の度合いを厳密に推定すれば良いのかというのが長年の課題でした。