「量子暗号に３０年ぶりの新原理」

―「読まれたら気づく」から「読めない」手法へ―

１．発表のポイント

◆従来の量子暗号（注1）は、不確定性原理（注3）に基づき、通信路（注2）の雑音量を監視することでセキュリティを確保していたのに対し、監視が不要な全く新しい原理に基づく量子暗号方式を提案

◆特殊な光源は用いず、レーザー光パルス間の干渉効果のみを用いて、雑音耐性を飛躍的に向上し、セキュリティ確保のために費やされる通信量を大幅に削減

◆既存の光通信技術を基に、物理法則に裏打ちされた強固なセキュリティをさまざまな場面で提供する道を拓く成果

２．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。既存の量子暗号方式は全て、盗聴者が盗み見ると変化する通信路（注2）の雑音量を監視することで、不確定性原理（注3）を介して盗聴された情報量を見積るという仕組みに基づいていました。

東京大学大学院工学系研究科の小芦雅斗教授と理化学研究所の佐々木寿彦特別研究員（当時、東京大学大学院工学系研究科　特任研究員）は、国立情報学研究所の山本喜久教授とともに、従来とは全く異なる動作原理に基づく量子暗号方式を提案し、通信路の雑音量を監視せずにセキュリティを確保できることを証明しました。新方式は、基本的に通常のレーザー光源と干渉計の組み合わせ（図１）により実現可能で、盗聴者は何をしても、一定の小さい情報量しか得られません。

本成果は「読まれたら気づく」方式から、「そもそも読まれない」方式への大きな転換です。従来の方式に比べると、監視に関わる手間が省かれ、雑音が大きい通信路でも秘匿通信が可能になります。この成果は、量子暗号の最初の提案以来30年ぶりに、本質的に新しい量子効果の利用法を提唱するもので、暗号にとどまらず、広範囲な発展が期待されます。

本研究は、最先端研究開発支援プログラム（FIRST）ならびに先端光量子科学アライアンス（APSA）の支援のもとに行われました。

３．発表内容：

《研究背景》

量子暗号（注1）は、基本的な物理法則である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のもとで秘匿通信を行う技術です。ハイゼンベルクの不確定性原理（注3）によれば、微弱な光パルスに載った信号を盗聴者が盗み見ると、その行為によって信号が変化するので、通信路（注2）の雑音量が増加したように見えます。そこで、雑音量を監視して、盗聴された情報量を正しく推定することでセキュリティを担保する――これが従来の量子暗号方式全てに共通する動作原理でした。

この従来法の欠点のひとつは、使用している通信路にもともとあった雑音も、盗聴者が引き起こしたと仮定しなければならず、その分だけ効率が低下してしまうことです。単に情報を送るだけの場合でも、通信路のビット誤り率（注4）が増えると送れる情報量は低下しますが、秘匿

通信のためには、ここからさらに盗聴されたと考える分を差し引く必要があります。従来の量子暗号では、雑音が増加すると、想定される盗聴量も増加するので、ビット誤り率が 15%程度になると、全く情報を送れなくなってしまいます。もうひとつの欠点は、通信路の監視の精度の問題です。通信路の監視は、本来の通信の中に、抜き打ち検査を混ぜ込むことで行われます。十分な精度で監視するためには、一定の検査の回数がどうしても必要になります。そのため、たった数百ビットの秘匿通信をしたい、という場合であっても、監視のために最低限百万ビット以上の通信量が必要、という不便さがありました（図２）。

《今回の成果》

今回、小芦雅斗教授らの研究グループが考案した手法は、上に述べた従来の手法とは全く異なる動作原理に基づく新しい量子暗号方式です。特殊な光源を使用する必要はなく、レーザー光源からの微弱光パルスの列に、デジタル光通信でも使用されている差動位相変調（注5）という方式でビット値の情報を載せて送信します。受信者は、遅延回路（注6）を含んだ干渉計を用いてパルスをランダムにずらして重ね、光子検出によりビット値を読み出します（図１）。動作原理は後述しますが、これだけのことで、通信路の監視をせずにセキュリティを確保できることを証明しました。

この方式では、雑音の大きさに関係なく、一定の小さな量しか盗聴できません。つまり、通信路の雑音が増加しても、盗聴されたと考えて差し引く分量は変わりません。その結果、高いビット誤り率の通信路でも、秘匿通信が可能になります。遅延回路により最大127パルス分の遅れが生じる場合、ビット誤り率35%程度でも通信が可能で、遅延を大きくすることでこの限界値をさらに大きくすることも可能です。また、通信路の監視の精度を問題にする必要がないことも特長のひとつで、最低限必要な通信量は千ビット程度で済みます（図３）。

《本提案の量子暗号方式の動作原理》

この方式が盗聴を防ぐ原理は次のようになります。説明のために、送信者が送り出すパルスに、順に1,2,3,...と番号を付けます（図１）。微弱光なので、ほとんどのパルスについては、受信者も盗聴者も光子は検出できません。たまに光子が検出されると、受信者は、重ねた２つのパルスの位相が同じだったのか違っていたのかがわかるので、それをビット値とします。受信者は、例えば「10パルス分だけパルス列をずらすように遅延回路を設定し、5番と15番のパルスを重ねたところで光子を検出した」と送信者に報告します。送信者は、5番と15番のパルスに自分が与えた位相変調の記録から、受信者の決定したビット値がわかり、これで1ビットの情報が送れたことになります。

日常の常識に照らすと、どのパルスに光子がいたのかは、送信者がパルスを送り出した時に既に決まっていた、と考えたくなるでしょう。しかし、量子力学では、そうではなくて、いろいろな場所に光子がいる可能性の「重ね合わせ」（注7）になっていると考えます。実際、1個の光子の検出で、2つのパルスの位相の相違が判別できるのは、5番のパルスに光子がいた可能性と、15番のパルスに光子がいた可能性とが、どのような重ね合わせになっているかを識別する測定を行っているためと解釈できます。

本提案では、その光子の居場所の可能性が、2か所だけでなくもっとたくさんのパルスに広がっていることを利用しています。受信者が光子を検出して初めて、その多くの可能性の中から、5番と15番という数字が選ばれたと考えることができて、これは波束の収縮（注7）とも呼ばれています。ここで大事なのは、この2つの数字(5,15)が両方ともランダムに決まっているわけではない、という事実です。この2つの番号の差である10は、遅延回路でパルス列をずらす大

きさですから、受信者が好き勝手に決めることができる数字です。10という数字は受信者が選びますが、そのあと、(1,11), (2,12),(3,13),… のどれに波束の収縮が起こるのかは、量子力学の持つ不確実性によってランダムに選ばれます。比喩的に言えば、ケーキの切り分け方は指定できるけれど、切り分けたピースのうちどれが貰えるのかは全くわからない、という状況です（図４）。

ここで盗聴者が通信路に介入して、光子検出を行い、例えば(3,8)のパルス対の位相の相違を知ったとします。この情報は、ほとんどの場合に意味がありません。なぜなら、受信者が偶然パルス列を5パルスずらすことを選ばない限り、(3,8)のパルス対の位相の相違を用いて送受信者がビット値を決めることはないからです。

盗聴者が光子検出を行うタイミングを遅らせた場合はどうでしょうか？盗聴者は送信者からのパルス列を保存しておき、受信者には偽のパルス列を送ります。受信者が例えば(5,15)という数字の組を発表した後で、保存しておいたパルス列を測定するという作戦です。この場合、盗聴者は正しくパルス列を10ずらすことができますが、(1,11), (2,12),(3,13),… のどれに波束の収縮が起こるのかは、量子力学の持つ不確実性によってランダムに選ばれるため、運よく(5,15)に当たることは滅多にありません。

このように、波束の収縮の本質的な不確実性と、受信者自身が波束の収縮のさせ方を選べるという性質が合わさって、盗聴できる可能性が小さく抑えられているのです。実際、上に述べた単純な盗聴法に限らず、物理的に可能なあらゆる盗聴法に対するセキュリティが今回証明されています。

《総括》

今回の成果は、従来の量子暗号である「読まれたら気づく」方式から、「そもそも読まれない」方式への大きな転換です。従来の方式に比べると、監視に関わる手間が省かれ、雑音が大きい通信路でも秘匿通信が可能になります。また、基本的に通常のレーザー光源と干渉計の組み合わせにより実現可能であるため、既存の光通信の技術との親和性も高いといえます。量子暗号が最初に提案されたのは、1984年の論文でした。今回見いだされた動作原理は、この30年の間、誰も気づくことのなかった、本質的に新しい量子効果の利用法だと言えます。今後、この新しい動作原理の理解を深めることで、暗号にとどまらず、広範囲な発展が期待されます。

４．発表雑誌：

雑誌名：英国科学雑誌「Nature」[2014 年 5 月 22 日（英国時間）]
論文タイトル：
Practical quantum key distribution protocol without monitoring signal disturbance
著者：Toshihiko Sasaki, Yoshihisa Yamamoto, Masato Koashi*
DOI 番号：10.1038/nature13303

５．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
教授　小芦　雅斗

６．用語解説：

注１：量子暗号

量子暗号では、通常、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：通信路

送信者から受信者へと信号が伝わる経路を指します。光通信では、光ファイバ回線が代表的ですが、地上と衛星を結ぶ通信では、大気中を光が進んでいく部分が通信路になります。

注３：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。

注４：ビット誤り率

0 か 1 か、という 1 ビットの値を受信者に届ける場合に、間違った値が届いてしまう割合を指します。何も通信せずに、受信者が 0 か 1 かを当てずっぽうで決めても、50%は正しい値になるので、ビット誤り率が 50%になると、情報が何も伝わっていないことになります。逆に、通信路のビット誤り率が 50%未満であれば、何らかの情報を届けることができます。

注５：差動位相変調

パルスの光波の振動のタイミングは、位相と呼ばれる角度を使って表すことができます。2 値の位相変調の場合、各パルスの位相を、0°または 180°に設定して送信します。受信側では、2 つのパルスを干渉計で重ねて測定することで、その 2 つパルスが同じ位相を持つか、異なる位相を持つかを判別することができます。なお、微弱光の場合、測定しても何も検出されない場合があり、その時は位相の情報は得られません。

注６：遅延回路

光が迂回する経路を設けることで、干渉計の上側を通ったパルス列の到着が遅れるようにします。その結果、図 1 の下図のように、異なる番号のパルスどうしが干渉します。何パルス分だけ離れたパルスどうしを干渉させるのかは、迂回する経路を切り替えることで、受信者が選択します。

注７：測定における波束の収縮

量子力学では、状態が完全にわかっている対象を測定する場合でも、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。

７．添付資料：

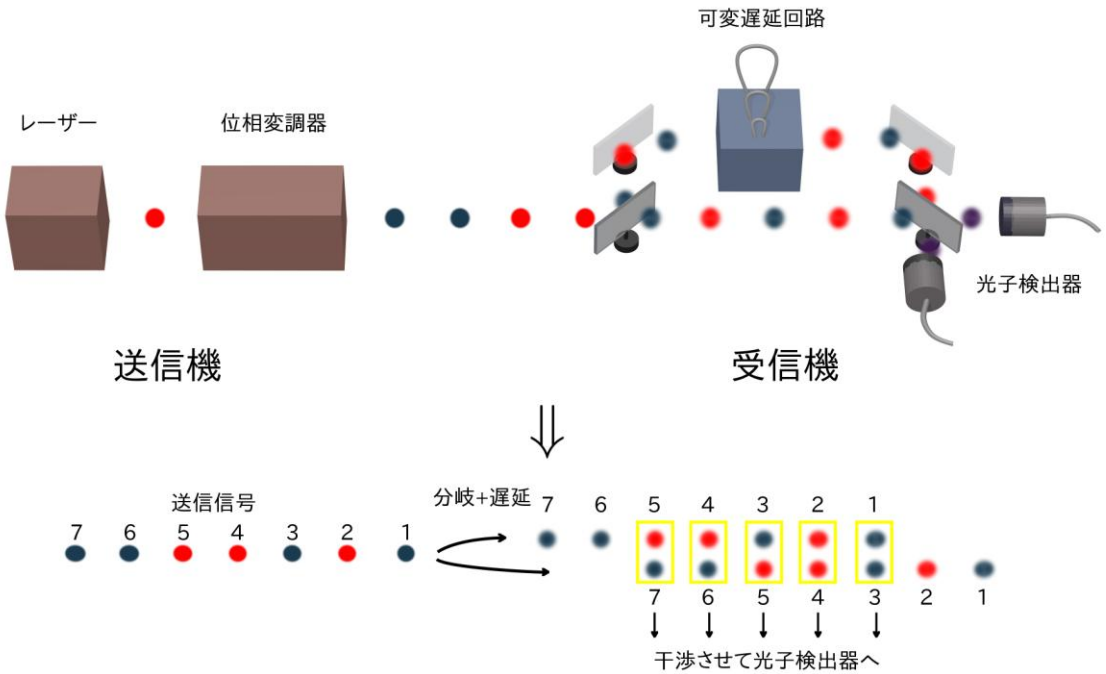

図１：本提案の量子暗号方式の概念図。位相変調器により、各パルスに２種類の印をつける。実際には、位相という量を２種類切り替えるが、図では赤と青の色で表している。受信側では、ハーフミラーで光を分岐し、遅延の大きさを選んで再び重ねて干渉させる。重ねたパルスの位相（色）が同じか異なるかによって、２台の光子検出器のどちらに光子が向かうかが決まる。従って、光子が検出されれば、対応する２つのパルスの位相（色）の相違がわかるので、これをビット値とする。受信者は、その２つのパルスの番号を公開する。送信者は、全てのパルスの位相（色）を記録しているので、公開されたパルスの番号から、受信者の決めたビット値がわかる。

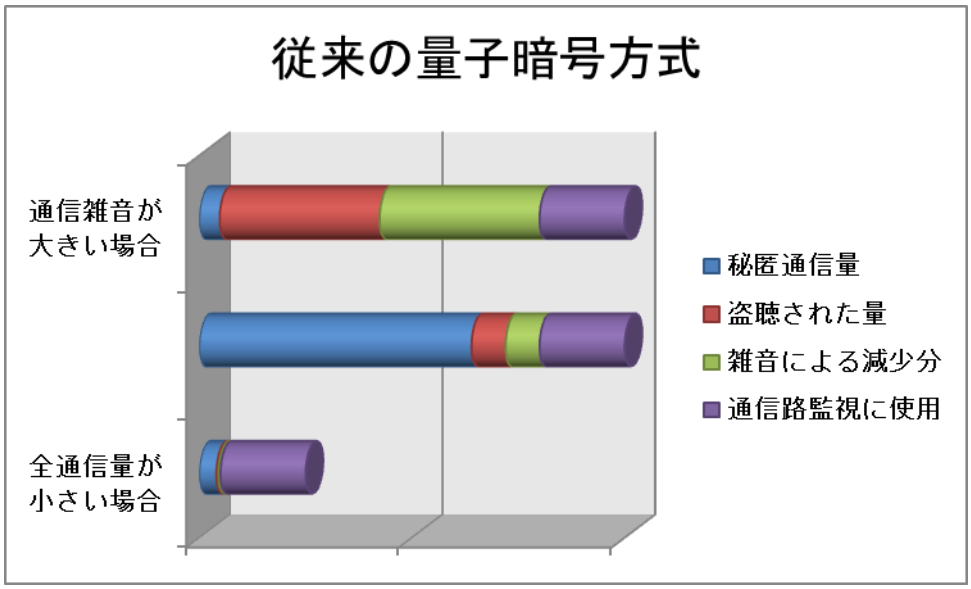

図２：従来の量子暗号方式で得られる秘匿通信量。盗聴量の推定の精度を確保するために一定量の通信路監視が必要になるため、全通信量が小さいと秘匿通信ができなくなる。また、通信路の雑音が大きくなると、想定される盗聴量も増加するため、秘匿通信量が急激に低下する。

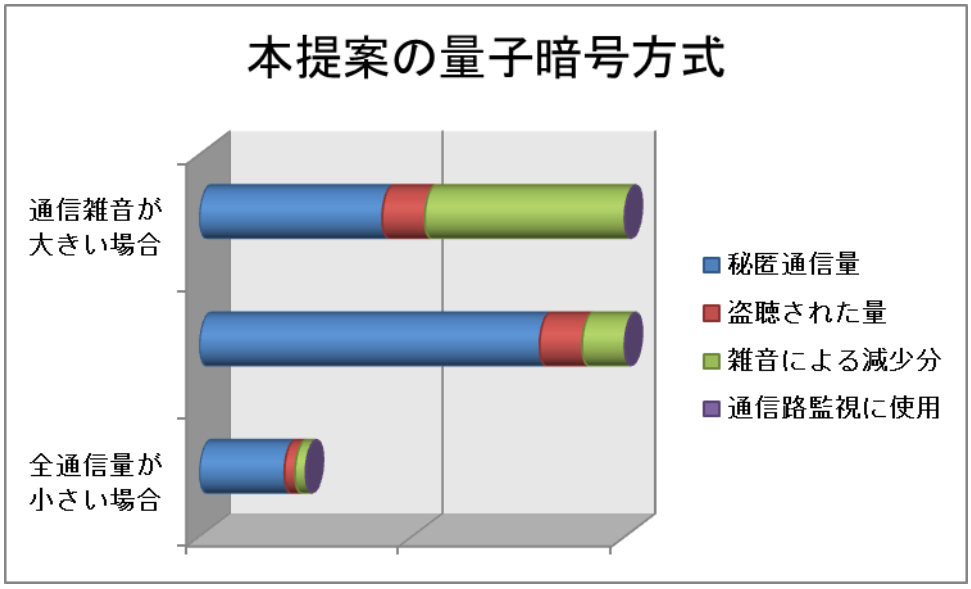

図３：本提案の量子暗号方式で得られる秘匿通信量。通信路監視が不要なため、全通信量が比較的小さい場合でも秘匿通信が可能である。また、通信路の雑音が大きくなっても、盗聴され得る大きさは不変であるため、秘匿通信量が急激に低下することはない。

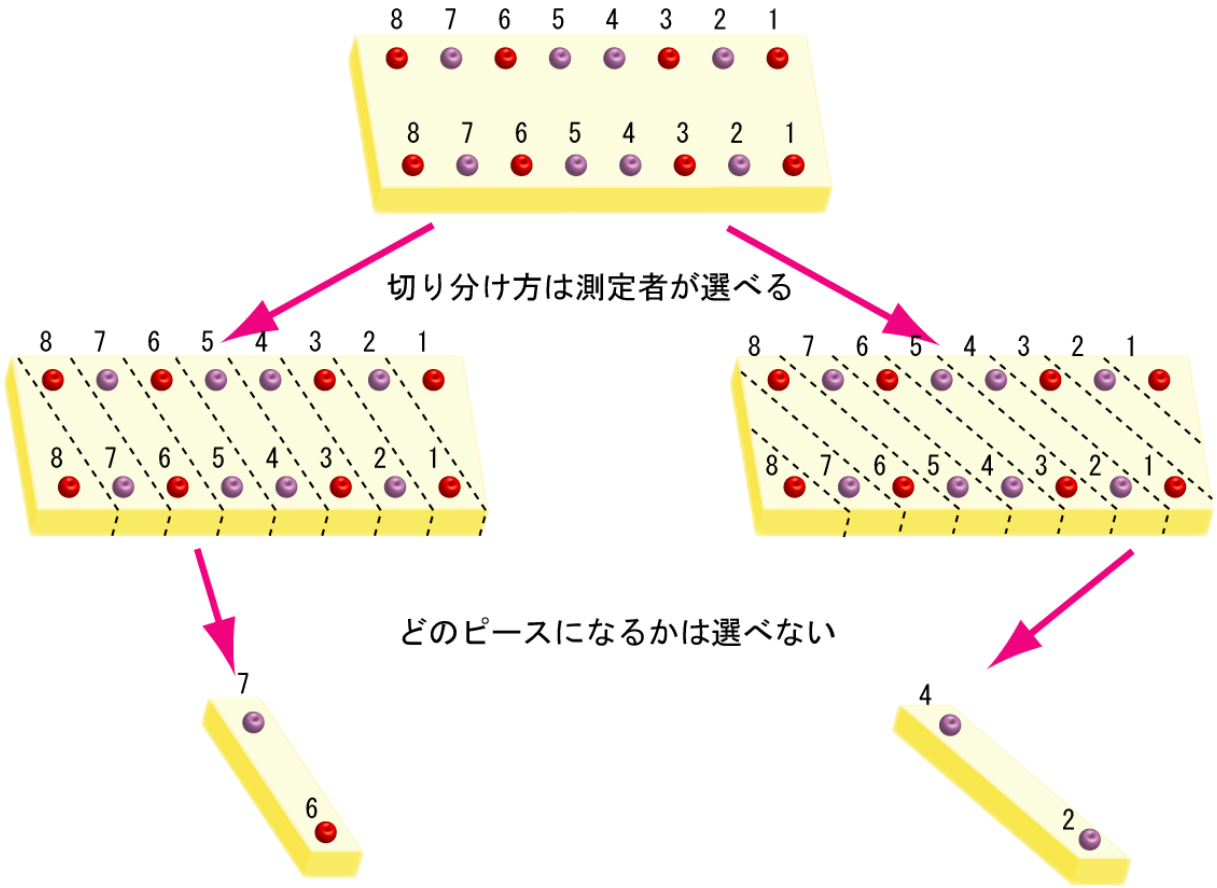

図４：本提案で用いられる微弱光信号の性質。受信者は、流れて来た信号を単に受け取るのではなく、得たい情報に応じて切り分け方を自由に指定できる。どのピースが最後に得られるのかは指定できない。切り分け方は自由なので、はじめから特定の形のピースが流れて来たと解釈することはできない。