# 量子暗号の安全性

**暗号とは第三者からの盗聴を防ぎながら正規ユーザ間で通信を行うことを目的としたものです．従来の暗号は原理的なレベルでも絶対的な安全を保障するものではありません．本稿では万人は決して自然法則には逆らえないということを利用した，原理的に絶対安全な量子暗号理論について解説します．**

玉木　潔（たまき きよし）†1　/加藤　豪（かとう ごう）†2

NTT物性科学基礎研究所 †1
NTTコミュニケーション科学基礎研究所 †2

## 量子暗号とは

量子暗号は量子鍵配布とも呼ばれ，正規ユーザ間で安全に鍵（共通で正規ユーザ以外には知られていない乱数列）を配布するための手段です．ここでいう「安全」とは，ユーザの装置がある条件を満たしている場合の任意の盗聴に対する安全性を指し，原理的に考えられる最高レベルの安全性のことです．以下では量子暗号の安全性理論について説明し，現実的な装置を用いたうえでの安全性についても触れます．

## ワンタイムパッド

もしあなたがとても親しい友人から次のようなメッセージをメールで受け取ったら，どう思うでしょうか？

「rdlmgvmyroorlmbvm」

このような意味をなさないアルファベットの文字列が送られてきたら，一瞬友人の携帯かPCがウイルスに侵されたことを疑いたくなります．しかし，パズル好きな方ならこれが意味をなす文章であることにもしかしたら気付くかもしれません．これは伝えたい英文を直接打つのではなく，ちょっと分かりにくく加工（暗号化）したものです．暗号化の方法は，伝えたいアルファベットを，MとNを中心にして折り返しの位置にあるアルファベットと対応させることです．例えば，A⇔Z，B⇔Y，C⇔X…といった具合です．このルールに気付くと先ほどの文字列は「iwonbillionyen」となり，これは「I won billion yen」つまり宝くじかなにかで10億円が当たったことを伝える文（平文）を暗号化した文字列（暗号文）だったと分かるわけです．これは単純な例ですが，①暗号化のルールを知っている受信者は，送信者が何を言っているのかがすぐに分かる（送信者と受信者が正しく通信できる），②暗号化のルールを知らない人（盗聴者）がメッセージを見てもすぐには解読できない（盗聴を防ぐことができる），という2つの点で暗号の本質を良く表しています．

具体的に今の例では，アルファベットの対応関係（秘密鍵）をあらかじめ送信者と受信者が共有することで暗号文から簡単に平文をつくることができます．また強度の強い暗号とは，盗聴者が解読に要する時間が長いものを指すと考えるのが自然ですが，秘密鍵を固定する暗号方式は，解読されるまでの時間を永遠に伸ばすことは難しいでしょう．その最大の原因は，メールアドレス，メールのヘッダ情報，送信者や受信者の名前など，ほとんどの通信ではあらかじめ盗聴者に知られている平文情報があることです．この情報と該当する暗号文を使えば，秘密鍵の情報を知ることができ，さらに通信をすればするほど，秘密鍵の情報は漏れてしまいます．そのため最終的には秘密鍵すべてが知られてしまうことになります．

そこでより安全な暗号にするために，秘密鍵を毎回通信のたびに更新するという方法が考えられますが，さらに一歩踏み込んで，1文字ごとに鍵を変えてみてはどうでしょうか？　こうすることによって，あらかじめ知られている平文情報に該当する秘密鍵は見破られてしまいますが，そこで得た知識は秘密鍵のほかの部分の推定には全く役立たなくなり，あらかじめ盗聴者に知られていない平文の安全性は保たれることになります．このように1文字ごとに暗号化の方法を独立に決める方式はワンタイムパッドと呼ばれており，暗号の中でももっとも高い強度を持っています（**図1**）．通常の通信では，すべての情報を0と1というビット値に変換して行うのが普通で，暗号化はあるビットでは0⇔0，1⇔1という対応

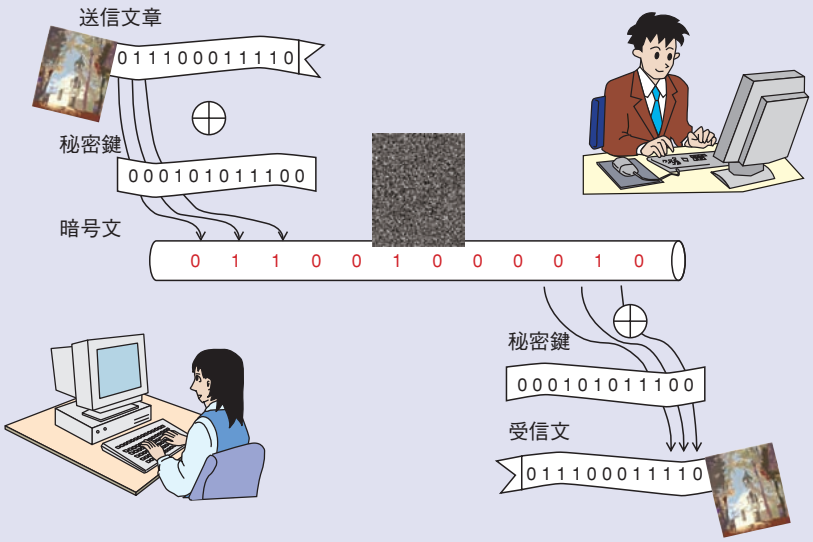


図1　秘密鍵を使った暗号通信

関係を採用し，あるビットでは0⇔1，1⇔0とし，前者の対応関係を秘密鍵のビット値0で指定し，後者を1で指定することにします．すると，ワンタイムパッドの秘密鍵は送信者と受信者が共有するビット値の乱数列ということになります．安全性のために重要なのは，平文と同じ長さの秘密鍵を使うことと，一度使った秘密鍵は二度と使わないことです．結果としてワンタイムパッドは①の条件を満たすとともに，解読は原理的に不可能であり，したがって②の条件を満足します．

それでは，ワンタイムパッドを実現するために，盗聴者に知られずに秘密鍵を送信者と受信者とで毎回共有するにはどうすればよいのでしょうか？この秘密鍵共有をするにあたって，盗聴者が完全にアクセスできる通信路を使わざるを得ないのですが（ただし送信者と受信者はお互い認証ができる，つまり第三者と通信をしていないことを確認できるとします．これは認証プロトコルと呼ばれる暗号で達成できます），もし送信者と受信者が秘密鍵を自由に増やすことができれば，ワンタイムパッドは非常に強力な暗号になります．普通に考えると，盗聴者は送信者が送るすべての情報を得ることができるので，この秘密鍵の共有は不可能に思えます．しかし，後に説明する極めて微弱な光（光子）が持つ奇妙な性質と事後選択を用いることにより，受信者が得た情報に対して盗聴者が持つ情報量を少なくすることができ，この情報の非対称性をうまく利用して秘密鍵を増やすことが可能になります．この秘密鍵増幅の方法を量子暗号と呼びます．つまり量子暗号とは，直接暗号通信をする手段ではなく，後の暗号通信のために必要な秘密鍵を安全に配布する便利な手段です．

## 量子力学

ここでは，量子暗号を理解するうえで必要な量子力学について，簡単に説明したいと思います．量子力学は，一般に非常に微小な粒子の振る舞い方を予言する原理のことです．その原理の1つに，「粒子は排他的な状態を同時にとれる」というものがあります．これは，1つの粒子が複数個所に同時に存在できることを意味しており，1つの粒子が1カ所だけに存在していることを常識だと思っている我々からすると非常に奇妙に思えます．この原理は粒子の重ね合わせの状態と言いますが，このとき粒子がどこにいるかを観測すると，どこか1カ所に粒子は出現しますが（これを状態の収縮と言います），どこに出現するのかを確実に予想することは不可能で，確率的にしか予想できません．さらに2つの粒子がそれぞれ複数個所の重ね合わせの状態をとっているときには，ある場所の存在確率は強め合い，ある場所では弱め合います．これは波の干渉と全く同じで，干渉は位相というものによって決まるので，重ね合わせ状態では波と同様に粒子は位相を持っています．この性質を粒子の波動性と呼びます．つまり，量子力学によると粒子は粒でありかつ波でもあるのです．

それでは我々が目にする1つの粒子が同時に複数個所に存在しないのはなぜなのでしょうか？　それは，その粒子がほかの光に照らされたり，空気中のチリや分子と衝突することによって，常に位置が観測されている状況，つまり状態は常に収縮しているので1カ所に存在している，と説明できます．ここで人間が実際に観測をしようがしまいが関係なく，反射光や衝突した粒子に，大きな粒子の位置情報が含まれていることが重要で，この情報が収縮を引き起こします．

## 量子暗号プロトコル

次に量子暗号プロトコルを説明したいと思います．プロトコルというのは手順のことで，送信者と受信者が使う装置は物理が仮定するモデルどおりに動くことを前提とします．

プロトコルではまず，送信者は1つの光子を光ファイバ内の位置1，位置2，位置3，…位置Nという複数の位置に同時に存在する状態を生成します．光ファイバ内の光の進む速さは一定なので位置情報はタイムスロット情報になります．さらに，N－1個のタイムスロット間の位相に送信者がつくったN－1個のビット値乱数の情報を載せます．具体的にはビット値0を位相0に，ビット値1を$\pi$に対応させます．

一方，受信者はこの位相の情報を読み取る測定を行います．この測定はビームスプリッタと呼ばれる光学素子と，1つの光子という微弱な光をとらえることができる単一光子検出器を用いて行われます．ここで重要なことは，送信者は1つの光子しか送っていないので，検出器は一度しか光を検知しない，つまりN－1個ある位相情報のうち1つの位相情報しか読み出せないということです．そして，どこの位相情報を読み出せるかは，送信者，受信者を含めて誰にも予想できないので，同一のビット値を共有するために受信者は測定後どこのタイムスロット間の位相情報の読み出しに成功したかを電話などで送信者に伝えます．すると送信者は該当する位相情報のみを残すことによって，送信者と受信者は1ビットの秘密鍵を共有することになります．この通信を何回も繰り返せば，多くの秘密鍵を送信者と受信者が共有できることになります．

## 盗聴できるのか？

では盗聴者の立場に立ってこの秘密鍵の情報を得ることを考えてみましょう．盗聴者は受信者と全く同じ測定をすることにより，送信者が送った情報のうち1ビットの情報を得ることができます．ところが，そのほかのビットの情報は全く分からないので，受信者に光子を送るときにどのような状態の光子を送って良いのか分かりません．仕方がないので情報を得たビット以外の位相を当て感で設定して受信者に送ったとしましょう．たまたま盗聴者が情報を得た位相を受信者も読み出すと，これは盗聴成功ということになりますが，前述のように受信者がどの位相情報を読み出すのかは，盗聴者も含めて誰にも制御できません．このことは，受信者は盗聴者が当て感で設定した位相情報を読み出す可能性が常に存在し，さらにこの位相情報は送信者が送った情報と食い違う（ビットエラー）可能性も常に存在することを意味しています．したがって，送信者と受信者が多数回通信を行うと，このビットエラーは非常に高い確率で生じます．このことを利用して，送信者と受信者は盗聴を検知できます．具体的には，秘密鍵を構成する多数のビットをランダムに抽出して答え合わせをします．もし，間違い（エラー）が一定の割合以下であるなら秘密鍵として採用し，そうでない場合は残りの秘密鍵は盗聴されていると判断し，捨てることにします．この割合は量子鍵配送の理論によって求められる数値で，エラーの割合がある数値以下の場合は，盗聴者がどんなに巧妙な攻撃を行おうが，送信者と受信者は通常の電話線などを使った情報交換と情報処理により安全な鍵に変換できることが知られています．盗聴者の能力に制限を設けないこの安全性のことを無条件安全性と言います．

## その他の暗号方式

今まで説明した暗号方式は，差動位相シフト量子暗号と呼ばれています．これまでの説明では単一光子源を仮定しましたが，レーザからの光を弱めた光でも通信を行うことができます．この種の量子暗号では受信者がビット値情報を検出するので離散変数量子暗号と呼ばれています．その一方，強い参照光や複数の光検出器を使い，その出力の差分という連続的な値を検出結果とする連続変数量子暗号という方式もあります（**図2**）．連続量の場合，常温でも比較的効率良く量子力学的効果が観測できるところに特徴がありますが，安全性理論の発展は離散変数型と比べてやや遅れています．

## どのような意味で安全なのか

次に量子鍵配送がどのような安全性を与えてくれるのかについて触れます．

前項で盗聴について説明しましたが，盗聴が発覚するのはあくまで確率的なものです．盗聴しているにもかかわらずそれが発覚しない確率というのは非常に小さいですが常に存在します．例えば盗聴者が盗聴に成功したタイムスロットの情報を，受信者もことごとく得る確率は0ではなく，この意味で，量子暗号は完全に安全な秘密鍵をつくれるわけではありません．しかし量子暗号の理論によると，どんなに進んだ技術を使って盗聴が試みられようと，生成した鍵が情報漏れを起こすなど，

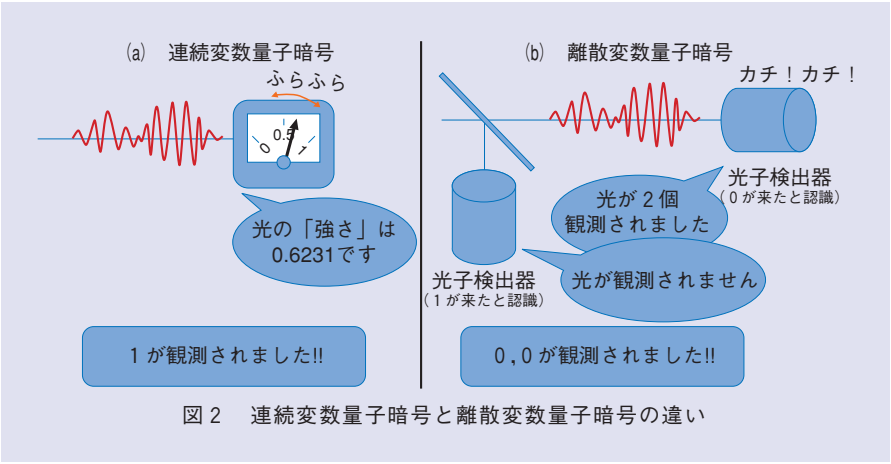


図2　連続変数量子暗号と離散変数量子暗号の違い

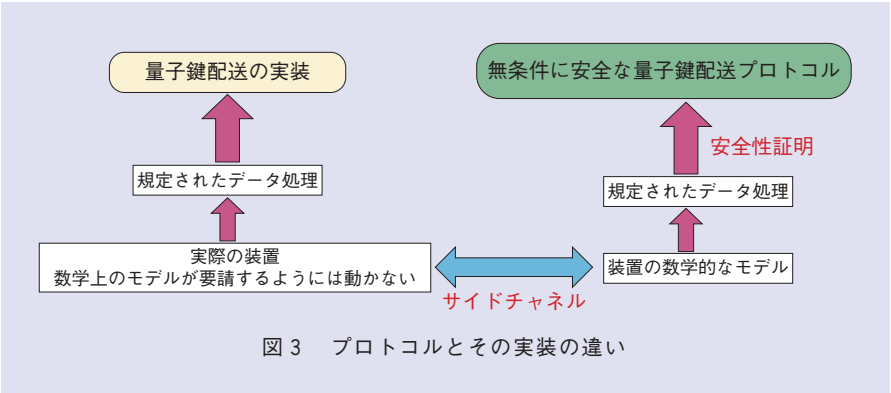


図3　プロトコルとその実装の違い

完全な鍵との違いが露呈する確率を送信者と受信者は好きなだけ小さくすることができます．さらに言うと，この理想的な状況と現実との状況がどの程度原理的に見分けることが可能か，という確率そのものを安全性の尺度としています．実際のデータ処理の能力を考えるとこの確率を$10^{-6}$くらいにするのが現実的だと思われますが，これは100万回通信してそのうち1度だけエラーが起こる確率で，ほとんどすべての通信ではこの数値で十分だと思われます．完ぺきに安全な秘密鍵の場合は，鍵のサイズが1メガビット程度なので，この確率は$2^{-10^6}$となりますが，ここまで小さい確率を求めるのは非現実的といえるでしょう．これはあたかも宇宙の年齢の中でたった一度の情報漏れを心配するようなものです．

最後に装置の不完全性について触れたいと思います．量子暗号プロトコルの冒頭でも述べましたが，プロトコルでは送信者と受信者が使う装置は物理が仮定するモデルどおりに動くことを前提としています．しかし，実際の装置は数学モデルに厳密に従うとは限りませんし，意図していない情報漏れがあります．装置の性質の厳密な解析は不可能なので，そのような情報漏れを完全に防ぐことは不可能です．この種の情報漏れはサイドチャネルと呼ばれており，量子暗号に限らず，すべての通信に存在するものです（**図3**）．

最近，雑誌などで「量子暗号のハッキングに成功」なる記事を目にすることがありますが，これはあくまでサイドチャネルを利用したまでで，量子暗号プロトコルそのものを破ったわけではない，ということに注意が必要です．このようなサイドチャネルの研究は量子暗号の実装の安全性を向上させるうえで必要不可欠なものであり，今後さらなるサイドチャネルの探索とその対策についての研究が必要となってきます．

量子暗号は通信距離が約50～100 kmとやや短く，通信速度も遅いという欠点がありますが，従来の暗号が理論上でも達成できなかった無条件安全性を達成できるという大きなメリットがあります．サイドチャネルに対しての研究を継続的に進めれば，非常に強度の強い暗号が実装されることは間違いないと期待されています．

量子暗号理論のもう少し詳しい説明は以下のサイトの解説記事等で見ることができます．
http://www.uqcc2010.org/index.html

（左から）玉木　潔/ 加藤　豪

量子暗号の使用用途は今のところ限定的ですが，将来あっと驚く使われ方をされるかもしれません．量子暗号は今まで達成できなかった無条件安全性を有するのですから使わない手はないと思います．

◆問い合わせ先
NTT物性科学基礎研究所
量子光物性研究部
量子光制御研究グループ
TEL　046-240-3417
FAX　046-240-3494
E-mail　tamaki.kiyoshi@lab.ntt.co.jp