量子暗号通信の仕組みと開発動向

後藤（ごとう）　仁（ひとし）

要　旨

現在広く利用されている RSA や AES のような暗号方式は、計算量的に安全な暗号方式と呼ばれ、現実に利用可能な計算能力を最大限投入したとしても、暗号文や秘密鍵を現実的な時間で解読することは困難である。しかし今後、量子コンピューターのように極めて高い計算能力を持つコンピューターが開発されたとき、これらの暗号方式は現実的な時間内に解読することが可能になるといわれている。

こうした中、次世代の暗号として量子暗号が注目を集めている。量子暗号とは、従来の暗号のように式の計算や数字の置換えによって情報を隠すのではなく、量子力学という物理法則の原理により通信途中での盗聴を完全に防ぐ方式であり、量子コンピューターでも解読は不可能である。

もっとも量子暗号は、通信の途中で減衰して消滅したり、観測すると変化してしまったりするような量子 1 個に情報を載せて通信を行うものであり、その通信距離や通信速度には大きな制約が存在する。また、その機能は暗号鍵の共有のみであり、メッセージの暗号化にはバーナム暗号等従来型の暗号を利用する必要がある。量子暗号は、従来の暗号化のイメージと大きく異なった部分があり、それを組み込んで活用する際には、システム全体のリスクを十分に評価したうえで慎重に行うことが必要となる。本稿では量子暗号の元になっている量子力学の概要から量子暗号の原理やその特徴までわかりやすく説明する。

キーワード：暗号技術、量子暗号、BB84、Y-00、量子力学

本稿の作成に当たっては、独立行政法人産業技術総合研究所情報セキュリティ研究センター物理解析研究チーム長の今福健太郎氏ならびに金融研究所スタッフから有益なコメントをいただいた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

後藤　仁　日本銀行金融研究所企画役
（現 システム情報局企画役、E-mail: hitoshi.gotou-1@boj.or.jp）

1. はじめに

次世代の暗号として量子暗号が注目を集めている。量子暗号の一般向けの解説には、「絶対に安全な（盗聴されない）」「破ることが原理的に不可能な」「安全性を物理法則で保証する」といった修飾語を伴って、「究極の暗号」「夢の暗号」として説明されることが多い。その理由としては、「従来の暗号のように式の計算や数字の置換えによって情報を隠すのではなく、量子力学という物理法則の原理により通信途中での盗聴を完全に防ぐ方式」であり、「量子コンピューターが発明されると、従来の暗号方式は無意味になるが、量子暗号は決して破られることはないから」と説明されることが多い。

これに対し技術者向けの説明はやや異なっている。例えば専門誌に載る量子暗号の記事をみると、それらは通信距離や通信速度といった成果を強調する。一例を挙げれば2008年10月9日の記事において、東芝欧州研究所が20 kmの距離で1.02 Mbps、100 kmの距離で10.1 kbpsの通信に成功し、世界最高速度を達成したと報道されている。しかし、そもそも一般の暗号通信であれば通信距離や通信速度といった点が成果にカウントされることはなく、通信速度1 Gbpsの回線暗号化装置や、10 Gbpsイーサネットに対応したVPN装置が既に出荷されている。通信距離に関しては、人工衛星を利用した通信などでは往復約7万kmもの距離があるが、日々何の問題もなく通常の暗号技術を利用して通信が行われている。それと比較して量子暗号通信の成果はあまりに貧弱にみえる。

そこで本稿では既存の暗号通信と比べたときの量子暗号通信の特徴を整理するとともに、なぜこうした限界が存在するのか、そうした限界に甘んじてまで利用するメリットは何なのかについて、わかりやすく説明することとしたい。

2. 暗号

(1) 暗号の機能

通常、暗号の説明では3人の登場人物が出てくる。アリスと呼ばれる情報の送信者、ボブと呼ばれる受信者、そして2人の通信内容を知ろうとしたり偽の情報を送ろうとしたりするイブと呼ばれる盗聴者である（図1参照）。

暗号には、情報を秘密にして隠す守秘機能と、今通信している人が情報を受け取るべき正しい人であることを確認したり、ある文書を作成したのが特定の人であることを確認したりする認証機能の2つがある。守秘機能は、文字通り秘密を守るということであり、アリスがボブに文書を送る際、ボブ以外の者（イブ）がその文書を読むことがないようにする機能である。通常はアリスとボブが予め秘密の情報（鍵）を共有しておき、その情報を用いることでしか内容が読めないように文書を変

図 1　暗号説明の登場人物

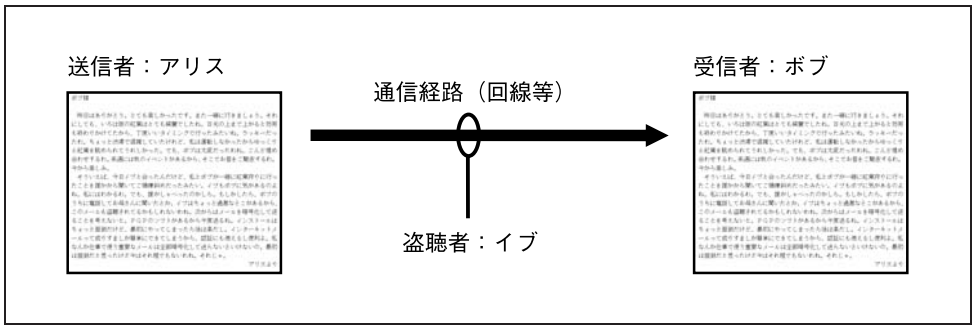
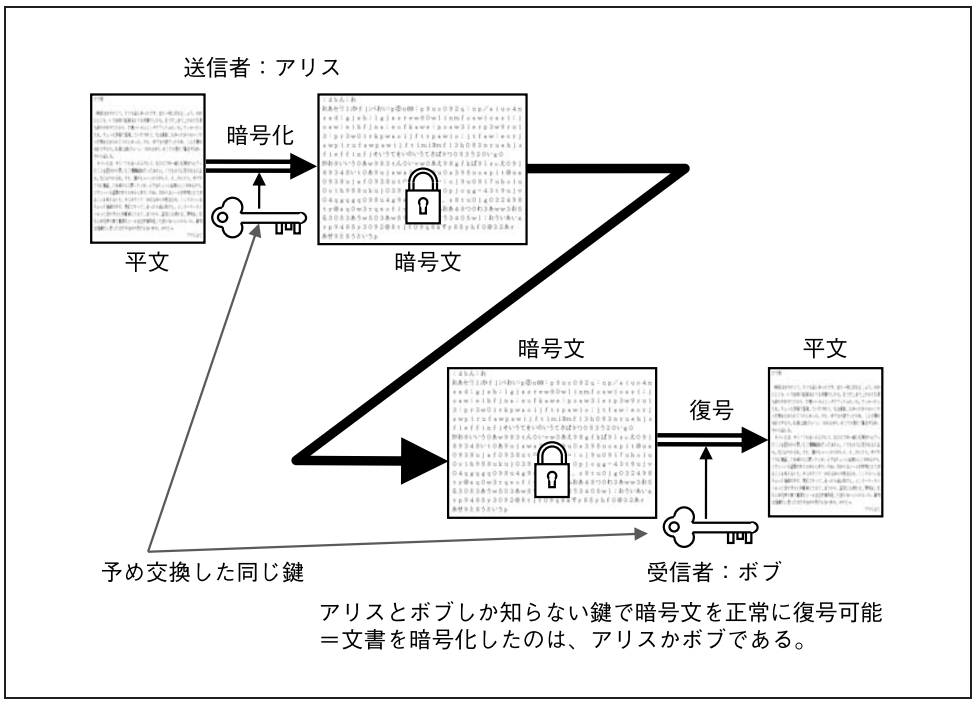


図 2　暗号の認証機能



換（暗号化）してアリスがボブに変換後の文書を送る。ボブは、共有した鍵を用いて受け取った文書を元の文書に逆変換（復号）して読むことができるが、鍵を持たないイブは通信の内容を盗聴しても文書を読むことができないことになる。一方認証は、通信している相手や文書を作成した人が特定の人であることを確認する機能である。鍵で暗号化された文書は、その鍵を持っている人以外は作成することも読むこともできない。つまり、予め特定の相手と共有した鍵によって文書が正常に復号できた場合、それを作成したのは鍵を共有した相手であると確認できることになる。ボブは送られた文書を作成したのは鍵を共有したアリスであることを確認できる（図 2 参照）。

(2) 現代における暗号の重要性

かつて暗号は、軍事や外交における情報の秘匿を主目的として開発されてきた。しかし最近では、インターネットをはじめとするネットワークの普及によって、暗号は、一般個人の日々の生活にも不可欠なものとなっており、生活のさまざまな場面で活用されている。

電子メールを利用して親しい相手と通信する際、その内容を他人に知られたくはない。インターネット・バンキングで利用するIDやパスワードが漏れると、知らないうちにお金を送金されてしまう。また、クレジットカードの番号と有効期限が知られると、それだけで買物ができてしまう。こうした場面では通信の暗号化が有効に活用され、安全性が守られている。

最近の自動車は、鍵についているボタンを押すだけでドアを開くことができる。エンジンをかける際に鍵を差し込まずポケットに鍵を入れておくだけで始動できる車もある。ここでも暗号を利用して自動車と鍵の間で通信が行われ、正当な鍵であることを確認する仕組みになっている。

さらに、近年急速な普及をみせている非接触IC型の乗車券、クレジットカードやいわゆる電子マネーでも暗号技術が活用されている。

もっとも、暗号を利用しているからと無条件で信用することはできない。自動車の鍵については、各国の主要な自動車メーカーが採用しているKEELOQという製品の攻撃に成功したとの報告[1]が暗号技術分野の主要な国際学会の1つであるEUROCRYPT2008においてなされた。この報告によると、50台のパーソナルコンピューターを利用して2日間計算することで内部のキーを解読することができ、それによって各メーカーのマスターキーを知ることができるとしている。また、海外の非接触IC型の乗車券に採用されている製品では、IC部分を削って顕微鏡で観察することにより内部構造を解析し、脆弱性を見つけたとの報告があり、カード偽造の模様を撮影したとされる映像がインターネットで公開された。

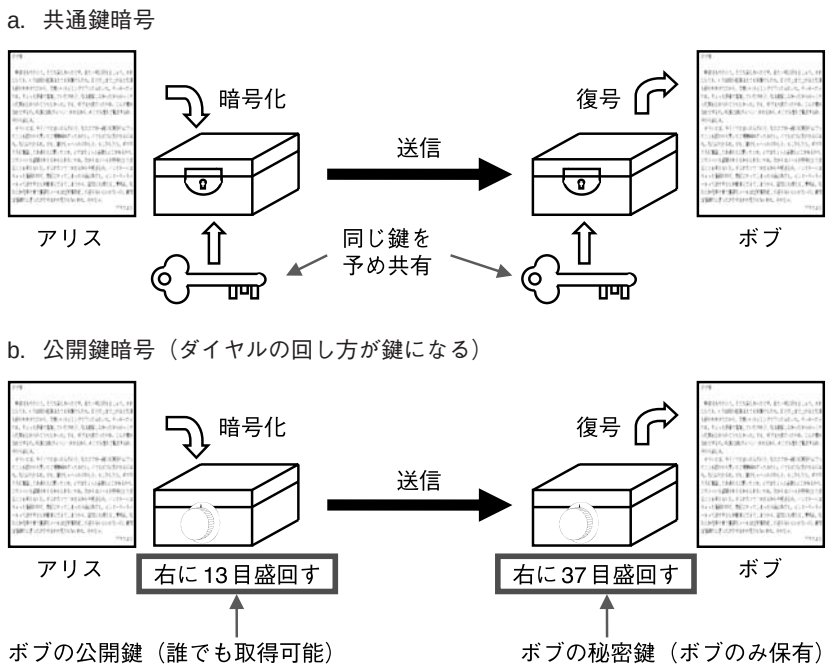
(3) 暗号の種類

暗号にはどのような種類があるのだろうか。古くは紀元前のシーザー暗号から最近の楕円曲線暗号まで暗号の方式にはさまざまなものがあるが、大きく分けると共通鍵暗号（あるいは対称鍵暗号）と公開鍵暗号に分かれる。

共通鍵暗号は、暗号化と復号に同一の鍵もしくは一方の鍵から他方の鍵を簡単に求めることが可能な鍵を利用する暗号方式をいう（図3a参照）。代表的な共通鍵暗号には、DES、AES、Camellia、MISTY1などがある。ビデオや音声の通信を暗号化するストリーミング暗号も共通鍵暗号の一種である。

1 http://www.iacr.org/conferences/eurocrypt2008/sessions/SebastianIndesteege_20080414.pdf

図 3　暗号の種類



公開鍵暗号は、暗号化に使う鍵と復号に使う鍵が異なり、一方の鍵を公開することができるようにしたものである（図 3 b 参照）。一方の鍵から他方の鍵を求めることは非常に困難（不可能ではないが、求めるには何万年もかかる）であり、片方を公開しても問題ない。代表的な公開鍵暗号には、RSA 暗号、エルガマル暗号、楕円曲線エルガマル暗号等があり、大きい 2 つの素数を掛け合わせた数の因数分解問題、離散対数問題など数学的に解くことが難しい問題を利用している。

共通鍵暗号は同一の鍵をアリスとボブが共有する必要がある。1 対 1 の通信では特に問題となることはないが、通信する相手が複数の場合、鍵の共有が大きな問題となってしまう。同じ鍵を異なる相手との通信で使用するわけにはいかないため、100 人の相手と通信する場合は 100 通りの鍵を作成して共有する必要がある。100 人が任意の相手と相互に通信する必要がある場合には、ネットワーク全体における鍵の総数は $100 \times 99 \div 2$ で、約 5,000 の鍵を安全にやりとりすることが必要となる。誰でもいつでも参加できるというインターネットの特性上、予め鍵を交換した先としか暗号通信を行うことができないとなると非常に不便である。何万人、何十万人のユーザーを抱える Web サイトにおいては、それだけの数の鍵を予めユーザーと交換しておく必要があるが、それは現実的ではない。しかも、繰り返し通信を行う場合には、ずっと同じ鍵を使うわけにはいかないため、定期的に鍵を変更する必要が

あり、そのたびに大きな手間がかかってしまう。

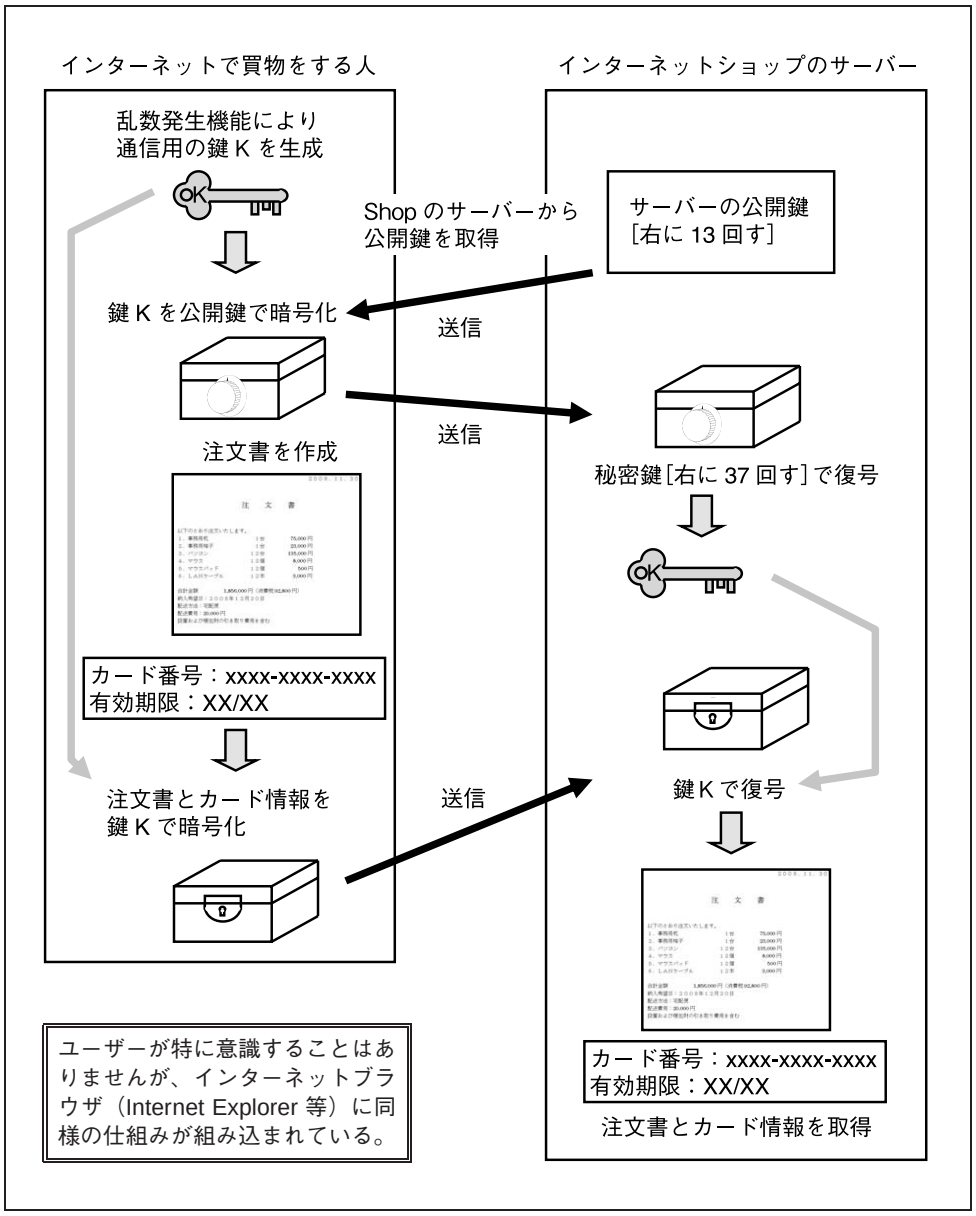
さらに、共通鍵暗号で認証を行おうとすると、いろいろと問題が出てくる。ある人が自分が作った文書であることを証明するためには、証明する相手ごとに鍵を取り替える必要があり、同一の物を多くの人に配付する場合（例えば、ある企業が作成したプログラムであることを利用する者全員に対して証明しようとするような場合）には、多大な手間がかかる。

そこで考案されたのが公開鍵暗号だ。この方式では片方の鍵は誰でも入手できるように公開する。実際の通信の流れをみてみよう。まずボブ（受信者）は、自分との通信に利用する鍵の一方を公開する（この鍵を公開鍵と呼ぶ）。もう一方の鍵は誰にも知られないようにボブが保管する（この鍵を秘密鍵と呼ぶ）。ボブと通信したいアリスは、公開されているボブの公開鍵を入手し、それで文書を暗号化してボブに送るが、復号は公開鍵と対になった秘密鍵でしか行えないので、秘密鍵を持っているボブのみが復号して文書を読むことができる。公開鍵から秘密鍵を導き出すことは非常に困難（事実上不可能）であるため、ボブ以外が文書を読むことはできない。逆にボブがアリスに暗号文を送りたい場合、ボブはアリスの公開鍵を利用して文書を暗号化する。この方式であれば、お互いに通信する人が100人の場合でも、鍵の個数は100個で済み、さらに人数が増えたとしても管理する鍵は人数と同じ数で済む。また通信したいときに公開されている鍵を取得することができるので、管理負担は小さくできる。Webサイトのユーザーが何十万人いようと、サイトは1個の秘密鍵を管理しておけば済む。また、現在広く使われている公開鍵暗号方式であるRSA暗号では、逆に秘密鍵で暗号化して公開鍵で復号することもできるため、これを利用すると文書の認証にも使うことができる。

これだけをみると、公開鍵暗号の方が優れた暗号のようにみえるが、公開鍵暗号には暗号化および復号の際の計算量が大きく時間がかかるという問題点がある。このため、大量のデータの暗号化を行う用途には向いていない。そこで、現在では両方を組み合わせて利用している。具体的には、データ通信は共通鍵暗号で行い、共通鍵暗号で利用する鍵を公開鍵暗号で暗号化して送るという方式が一般的である。

Aさんがインターネット上のサーバーに、注文書とクレジットカード番号を暗号化して送る場合をみてみよう（図4参照）。まずAさんは、共通鍵暗号による通信で使う鍵Kを作る（乱数発生プログラムにより乱数を作って鍵とする）。次に、そのサーバーがインターネット上で公開している公開鍵を入手し、その公開鍵で先ほど作った鍵Kを暗号化してサーバーに送る。その後、鍵Kを利用して共通鍵暗号で注文書とクレジットカード番号を暗号化してサーバーに送る。サーバー側では、自分の秘密鍵で最初に届いた暗号文を復号してAさんが作成した鍵Kを得、その鍵Kを利用して次に届いた文書を復号して注文書とクレジットカード番号を得ることができる。

図４　インターネットショップでの買物



(4) 認証とハッシュ関数

認証とは、今通信している人が、情報を受け取るべき正しい人であることを確認したり、ある文書を作成したのが特定の人であることを確認したりすることである。

通信電文や文書が特定の鍵で暗号化されていれば、相手が暗号化を行うことができる者であると確認できる。共通鍵暗号であれば、予め鍵を交換した相手であると

確認できるし、公開鍵暗号であれば、本人しか知らない秘密鍵の持ち主であると確認できる。また、文書が作成者以外の者によって改変されていないことの証明にも活用できる。

認証においても共通鍵暗号を利用すると鍵の管理が大変になるため、この場合も公開鍵暗号がよく使われる。もっとも、同方式は大量のデータを暗号化するのには向いていない。そこで、暗号化にかかる時間を節約するために暗号技術を応用して作られたハッシュ関数というものを利用する。これは、長い文書から一定の計算に従って短いデータ（ハッシュ値）を作成する関数で、元の文書の長さにかかわらず一定の長さのハッシュ値が作られる。元の文書を変更すると、このハッシュ値が大きく変わり、似たようなデータから同じハッシュ値が作られることがないようになっている。なお、同一のハッシュ関数を使い同じ文書のハッシュ値を計算すると必ず同じ値が得られる。

このハッシュ関数を利用して元の長い文書からハッシュ値を計算し、公開鍵暗号の秘密鍵でハッシュ値を暗号化して元の文書と一緒に相手に渡す。受け取った相手は送り主の公開鍵で復号して得られたハッシュ値と、文書から計算したハッシュ値を比べ、同じであれば、作成した相手が秘密鍵の持ち主であり、また渡される途中で文書が改変されていないことを確認できる（図 5 参照）。

なお、広く使われているハッシュ関数である SHA-1 において、ハッシュ値の衝突（異なる文書から同じハッシュ値が計算されること）が起きる文書の組を、効率的に見つけることができる攻撃方法がみつかり（Wang, Yin, and Yu [2005]）、米国立標準技術研究所（NIST）は 2011 年以降 SHA-1 を米国連邦政府の情報システムにおいて使用しない方針を発表している。また、わが国においては、政府認証基盤（GPKI）および商業登記認証局で利用するハッシュ関数について、SHA-1 から、より安全性が高い SHA-256 への移行が必要である旨が内閣官房情報セキュリティセンターによって示され、2013 年度を目途に移行にかかる検討が進められるとの方針が発表されている（内閣官房情報セキュリティセンター［2008］）。

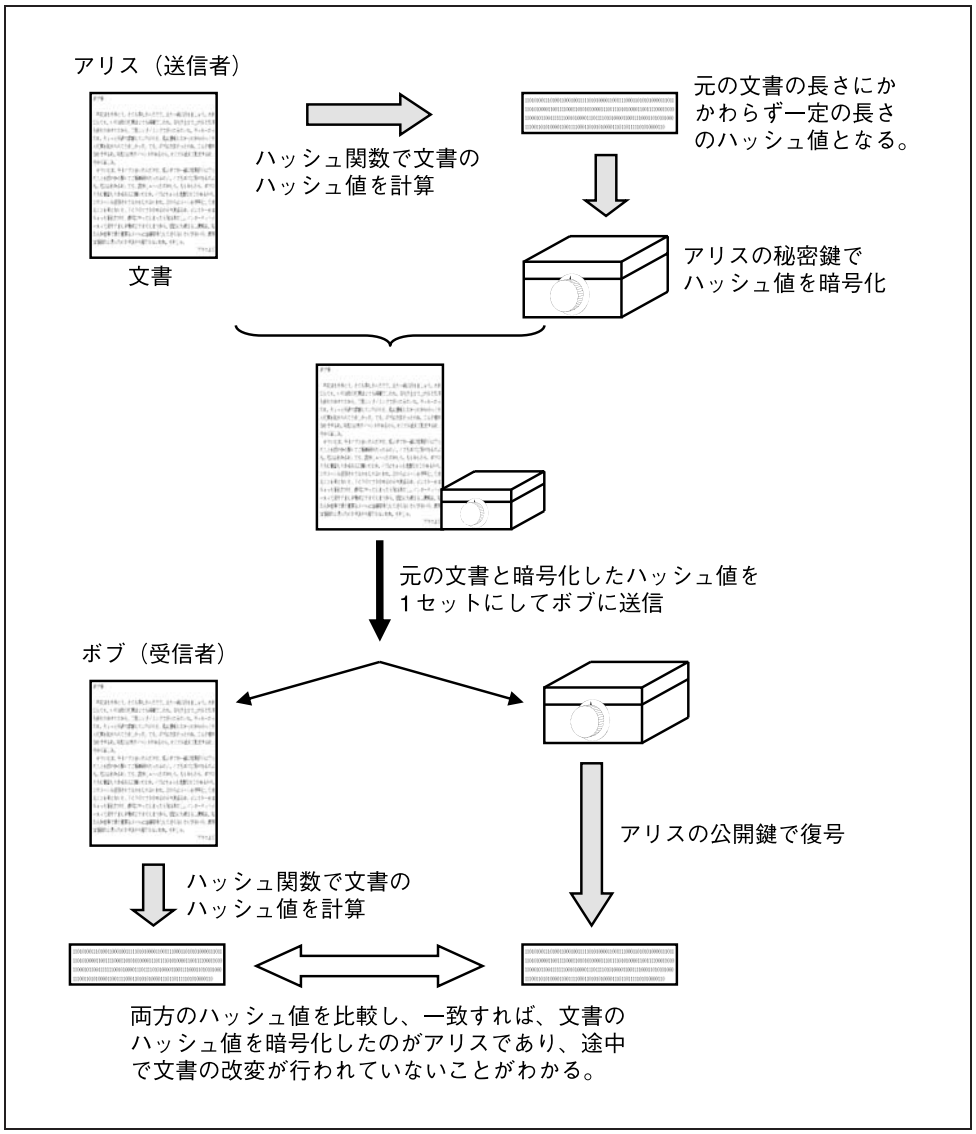
(5) 絶対に破られない暗号

暗号の歴史は新暗号の開発とその解読のいたちごっこであり、それは現在も続いている。特に、近年におけるコンピューターの処理能力の増大は目覚ましいものがあり、非常に安全性が高いと思われていた暗号が 10～20 年で陳腐化するといった事態も生じている。

われわれが暗号を利用するほとんどのケースでは、こうした陳腐化のリスクは許容範囲内であり、例えば電子政府推奨暗号リスト[2]に掲載されている暗号方式を利用すれば十分秘密を守ることができると考えられる。しかし、長期的な安全性が求め

2 http://www.cryptrec.go.jp

図５　ハッシュ関数による認証



られる極めて高いセキュリティを要求する情報では、何年経過しても安全性が低下しないような暗号方式による暗号化が望ましいケースもあろう。

加えて暗号方式の移行問題もある。暗号が大型コンピューターから IC カードの中のチップにまで入り込んでいる現代においては、暗号の安全性が低下したからといって、システムの中に組み込まれている暗号方式を入れ替えることは容易ではない。そのシステムを使っている全員が一斉に暗号方式を変更する必要があるためである。例えば、現在何千万枚も発行されている IC カード型乗車券や携帯電話に組み込まれた乗車券の中で使っている暗号を一斉に取り替えることを想像してほしい。

この問題は、「暗号アルゴリズムの2010年問題」として注目されている。今後は、さまざまな機器等に組み込まれた暗号方式を必要に応じて更新できるようにする仕組みが必要になる。

では、絶対に破られない暗号はあるのだろうか。実は、非常に単純だが、絶対に破ることができない暗号がある。「暗号を解読する」とは、「暗号化に用いられる鍵を知る」こととほぼ同義だが、暗号を解読する側は、同じ鍵が何度も使われたり、一定の決まりに従って鍵が変更されたりすることを頼りに暗号を解読する。これを裏返すと、「鍵が十分ランダムで、同じ鍵が2度と使われることがない暗号は破ることができない」ことになり、例えば「送る電文と同じ長さのランダムに生成した鍵を用意し、一度使った鍵は2度と使わない」ことにより、解読が不可能になる。何度も電文を送り合う場合でも毎回新しい鍵（これまでに利用した鍵と一切関係のない鍵）を使い、同じ鍵は2度と使わない。

具体的な暗号化の方法は極めて簡単で、送るデータと鍵に対して排他的論理和と呼ばれる計算をするだけで済む。排他的論理和とは、桁上がりを無視した1桁の二進数の単純な足し算だ。二進数の1と1を足すと、桁上がりが発生して答は10になるが、排他的論理和では上の桁の1を捨てて答を0にする。排他的論理和を $\oplus$ で表すとすると、2つの数において、

$$0 \oplus 0 = 0, \quad 1 \oplus 0 = 1, \quad 0 \oplus 1 = 1, \quad 1 \oplus 1 = 0,$$

となる。

暗号化されたデータを復号するには、以下のように再度鍵との排他的論理和を計算する。

$$\text{データ} \oplus \text{鍵} = \text{暗号文},$$

$$\text{暗号文} \oplus \text{鍵} = \text{データ}.$$

この暗号方式はバーナム暗号もしくは、ワンタイムパッド暗号と呼ばれ、鍵は1回限りの使い捨てとなるため、イブは過去に用いられた暗号文や平文から鍵を推測することができない。

共通鍵暗号は、考えうる全ての鍵の組合せを試すことで原理的には解読が可能であるほか、各共通鍵暗号方式のアルゴリズムに依存した攻撃法（ショートカット・メソッドと呼ばれる）が適用可能となるケースもある。また、RSA暗号は公開鍵 n（2つの素数の積）を、2から n の平方根までの素数で順に割り算してみることで素因数分解でき、秘密鍵を求めることが可能であるほか、数体ふるい法等、より高速での素因数分解を可能とする手法も適用できることが知られている。もっとも、こうした攻撃法を実際に使用し、現実に利用可能な計算能力を最大限投入したとしても、暗号文や秘密鍵を現実的な時間で解読することは困難とみられている。こうした暗号は「計算量的に安全な暗号」と呼ばれる。一方バーナム暗号は、コンピュー

ター資源（能力、時間）を無制限に使えたとしても鍵を知らない限り解読することはできず、「情報理論的（情報量的）に安全な暗号」と呼ばれている。ただし、バーナム暗号では、送ろうとするデータ以上の長さの鍵が必要となるため、鍵をどのように共有するかが問題となる。送ろうとするデータ以上の長さの鍵を安全に相手に届けることができるのであれば、わざわざ暗号を使わなくとも同じ方法で文書を届ければよい。

(6) 暗号の鍵

上記の議論でもわかるとおり、鍵をどのように共有するのかということはシーザー暗号の時代から現在の最新暗号まで変わらない大きな問題である。アリス（送信者）とボブ（受信者）は、同じ鍵もしくは対になっている鍵を用いて文書の暗号化と復号を行う。この鍵がイブ（盗聴者）に知られると暗号はたちまち解かれてしまうため、鍵を安全に受け渡し、管理することは暗号利用の要であり非常に負担の大きい作業である。何とか鍵を共有することなく秘密の手紙をやりとりすることはできないものだろうか。

物理的に紙に書かれた手紙であれば、解決法がある。アリスがボブに手紙を送る場合、南京錠とそれを付けられる箱があれば、南京錠の鍵を相手に渡さなくても、常に箱に鍵がかかった状態のまま手紙を送ることができる。その方法は以下のとおりである。

まずアリスは箱に手紙を入れ、南京錠をかけてボブに送る。受け取ったボブは、その箱にさらに自分が用意した南京錠をかけてアリスに送り返す。2 つの鍵がかかった箱を受け取ったアリスは、自分がかけた南京錠を自分が持っている鍵で外し、ボブに送る。ボブは自分がかけた南京錠を自分で外して手紙を手にすることができる。こうすると、箱は必ず鍵がかかった状態でやりとりされ、しかも鍵を相手に渡す必要もない。

これと同様のことを絶対安全といわれるバーナム暗号でもやってみよう。まず送りたい文書 X をアリスが作った鍵 a で暗号化してボブに送る。ボブは自分が作った鍵 b でさらに暗号文を暗号化し、アリスに送り返す。アリスは鍵 a で電文を復号してボブに送り、ボブが鍵 b で復号するとアリスが送った文書を読むことができる。式でみてみよう。

バーナム暗号で使われる排他的論理和を $\oplus$ の記号を使って表すことにする。排他的論理和には次の性質がある。

$$\alpha \oplus \alpha = 0, \tag{1}$$

$$0 \oplus \alpha = \alpha \oplus 0 = \alpha, \tag{2}$$

$$\alpha \oplus \beta = \beta \oplus \alpha, \tag{3}$$

$$(\alpha \oplus \beta) \oplus \gamma = \alpha \oplus (\beta \oplus \gamma). \tag{4}$$

表 1　α と β の排他的論理和

α	β	$\alpha \oplus \beta$
1	1	0
1	0	1
0	1	1
0	0	0

表 2　排他的論理和の結合関係

α	β	γ	$\alpha \oplus \beta$	$\beta \oplus \gamma$	$(\alpha \oplus \beta) \oplus \gamma$	$\alpha \oplus (\beta \oplus \gamma)$
1	1	1	0	0	$0 \oplus 1 = 1$	$1 \oplus 0 = 1$
1	1	0	0	1	$0 \oplus 0 = 0$	$1 \oplus 1 = 0$
1	0	1	1	1	$1 \oplus 1 = 0$	$1 \oplus 1 = 0$
1	0	0	1	0	$1 \oplus 0 = 1$	$1 \oplus 0 = 1$
0	1	1	1	0	$1 \oplus 1 = 0$	$0 \oplus 0 = 0$
0	1	0	1	1	$1 \oplus 0 = 1$	$0 \oplus 1 = 1$
0	0	1	0	1	$0 \oplus 1 = 1$	$0 \oplus 1 = 1$
0	0	0	0	0	$0 \oplus 0 = 0$	$0 \oplus 0 = 0$

これらが成り立つことは表 1 および表 2 をみればわかる。

バーナム暗号は、文書 X に対して鍵 a を作用させて暗号文を作成し、再度鍵 a を作用させると元の文書に戻る。式で表すと以下のとおりとなる。

$$a \oplus (a \oplus X) = X. \tag{5}$$

なお、X、a は 1 ビットの情報であり、通常の文書を考える場合は添字を付けて X_i、a_i と表す必要があるが、以下では添字を省略する。(4) と (1) および (2) を使って左辺を計算すると X となり、この式が成り立つことがわかる。$(a \oplus X)$ が暗号文になり、これに、さらに鍵 a を作用させると X に戻る。この記号を使うと先ほどのアリスとボブのやりとりは、

$$b \oplus [a \oplus \{\underline{b \oplus (a \oplus X)}\}], \tag{6}$$

と書くことができる。なお下線は説明のために付したものであり、式の計算とは関係がない（以下同じ）。$(a \oplus X)$ が、アリスがボブに送った暗号文。それにボブの鍵 b でさらに暗号化した $\{b \oplus (a \oplus X)\}$ が、ボブがアリスに送った暗号文になる。これを受け取ったアリスは自分の鍵 a で復号を行い、$[a \oplus \{b \oplus (a \oplus X)\}]$ をボブに送る。ボブはこれを b で復号するという仕組みである。(4) と (3) を使って (6) の下線部を置き換えると、次のように変形できる。

$$b \oplus [\underline{a \oplus \{a \oplus (b \oplus X)\}}]. \tag{7}$$

下線部は (4)、(1) および (2) より $(b \oplus X)$ に等しいので、

$$b \oplus (b \oplus X) = X, \tag{8}$$

が成り立ち、ボブはアリスの文書を受け取ることができた。

一見、アリスとボブが鍵を共有することなく暗号通信を行え、バーナム暗号を使うため、安全性にも問題がないように思える。しかし、よくみると落とし穴があることがわかる。ボブがアリスに送り返した暗号文である $\{b \oplus (a \oplus X)\}$ をアリスは a で復号し、$a \oplus \{b \oplus (a \oplus X)\}$ をボブに送るが、上記 (7) の下線部のとおり、これは $(b \oplus X)$ に等しい。イブが盗聴によって得た $\{b \oplus (a \oplus X)\}$ と $(b \oplus X)$ の排他的論理和を計算すると、

$$\begin{aligned}
\{b \oplus (a \oplus X)\} \oplus (b \oplus X) &= b \oplus a \oplus X \oplus b \oplus X \\
&= b \oplus a \oplus b \oplus X \oplus X \\
&= a \oplus b \oplus b \oplus X \oplus X \\
&= a \oplus 0 \oplus 0 \\
&= a,
\end{aligned}$$

となり、(1)〜(4) を適用するとアリスの鍵である a に等しくなる。このため、最初にアリスがボブに送った暗号文 $a \oplus X$ も盗聴していたイブは、鍵 a を使って復号し、文書を読んでしまうことができる。箱と南京錠ではうまくいった方法ではあるが、バーナム暗号では成り立たない。

バーナム暗号以外でも、共通鍵暗号で暗号通信を行う場合には、何らかの情報を受け渡し、秘密裏に共有することが必要になる。インターネットでは公開鍵暗号で共通鍵暗号の鍵を暗号化して送る方法がよく利用される。現在最も使われている RSA 暗号は、桁数が大きい 2 つの素数を掛け合わせて積を求めることは比較的容易であるが、与えられた積から元の素数を計算（素因数分解）することは極めて難しいという性質を応用して鍵の安全性を確保しており、秘密の鍵を相手に送る必要がないという便利な暗号である。しかし、コンピューターの処理能力や素因数分解アルゴリズムの手法は日進月歩で進化しており、既に 1024 bit RSA 暗号については、公開鍵を素因数分解することで秘密鍵を入手する攻撃に対する耐性が十分ではないと認識されつつある。「CRYPTREC Report 2006」では、「法パラメータのサイズが 1024 ビットの IFP（$n = pq$ 型素因数分解問題）を 1 年間の計算によって完了させるためには、10^{15} FLOPS から 10^{17} FLOPS の処理能力を持つ計算機が要求され、高性能なスーパーコンピュータが過去の成長率を続けて成長した場合に、そのレベルに到達する

時期は、……2010年～2020年の間と推定することができた」としている（独立行政法人情報通信研究機構・独立行政法人情報処理推進機構［2007］）。また、将来登場するであろう量子コンピューターを利用すると、素因数分解が簡単に行えるようになるといわれており、そのときには現在のコンピューターを前提とした計算量的に安全な暗号は使えなくなる可能性が高い。

こうしたことから、より安全な通信を実現するために、絶対に盗聴できないことが理論的に証明されている通信（暗号）が求められている。盗聴されることがなければ、暗号を解かれることもない。そこで注目を浴びたのが量子暗号だ。従来の暗号は、数学的な計算等により情報を隠して盗聴を防いでいるが、量子暗号は非常に小さな粒子である量子の振舞いを応用するという物理学的な方法により情報の盗聴を防ぐものであり、従来とは全く異なった考え方に基づいた暗号方式といえる。

3. 量子力学の世界

量子暗号の元となっている量子力学の世界はどのようなものであろうか。ここからは、量子力学の対象になるような小さな粒の不思議な性質について話を進める。

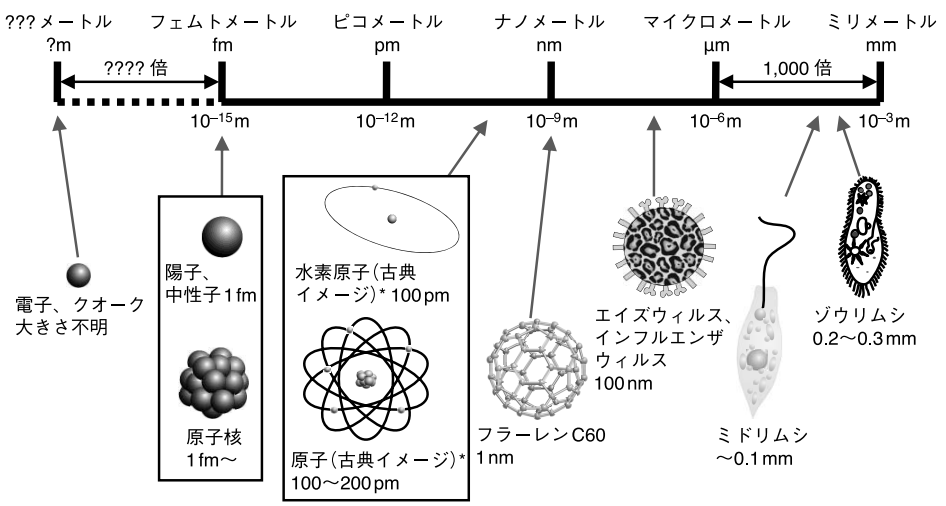
(1) 小さな粒

物質は、どんどん分解していくと、分子、原子に分解でき、さらには電子や陽子、中性子などに分解できるということは、一般の常識でもある。陽子、中性子、電子などは、ある大きさを持った粒子だと考えられており、陽子・中性子の大きさはおよそ1fm（1フェムトメートル）程度である[3]。f: フェムトとは、1,000兆分の1を表す単位で、アラビア数字で書くと、小数点の後に0が14個も並ぶ（0.000000000000001m）。エイズウィルスやインフルエンザウィルスが100nm（ナノメートル：10億分の1メートル）、ナノテクノロジーが対象としている世界でも、集積回路（LSI）の線幅が50nm（0.00000005m）程度、カーボンナノチューブやフラーレンで1nm（0.000000001m）程度であるので、さらに6～7桁も小さいことになる（図6参照）。

一方、電子は陽子よりもさらに小さいと考えられているが、小さすぎて大きさを測ることができない。通常大きさを測るためには、測る対象よりも小さなものをぶつけて、跳ね返り方から調べるが、現代の科学では電子の大きさを測れるようなものが知られていないためである（そもそも電子の大きさを測れるようなものは存在しないのかもしれない）。

3 もっとも、ここからが粒子、ここからが空間というような明確な区切りがあるわけではなく、その境界は曖昧である。ある観測を行ったときにそこから論理的に計算される大きさと思っていただきたい。

図 6　大きさの比較



備考：* 印の図は、ラザフォードやボーアによる古典的イメージの原子モデル。現在は原子核の周りに電子の雲が存在するイメージで描かれることが多い。

（2）不思議な粒

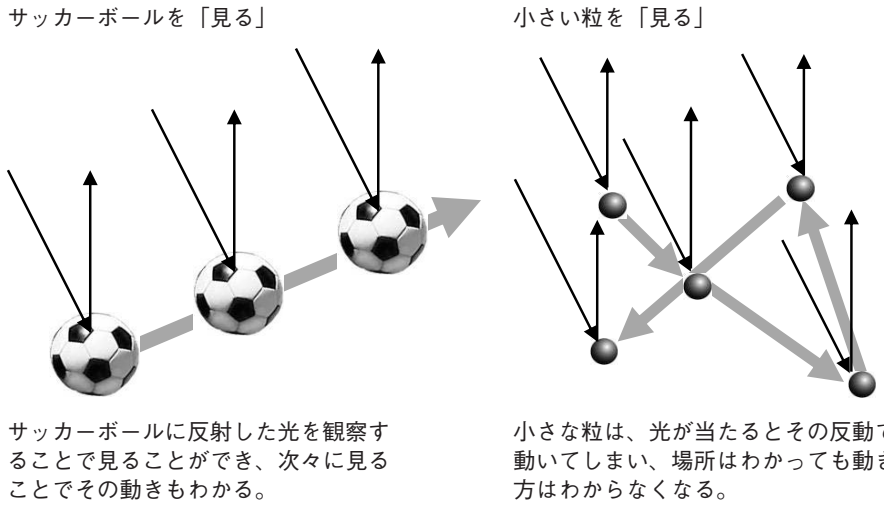
こうした電子のような粒子は、一般的にわれわれが知っている粒子とは大きく異なった性質を持っている。

粒子の性質を知ろうとするとき、まずはその粒子がどこにあるのか（位置）、どの方向にどの位の速さ（速度）で動いているのかを「見る」（観測する）ことが第 1 歩である。

ところで、「見る」というのはどういうことであろうか（図 7 参照）。サッカーボールを見るにはサッカーボールに光を当て、跳ね返ってきた光を観測する（目で見る、あるいは写真に撮る）ことが「見る」ということである。動いている場合でも次々に「見る」ことにより、その速度を知ることができる。

小さな粒子でも「見る」ためには、サッカーボールを見る場合と同じように光を粒子に当て、跳ね返ってきた光を観測する必要がある。しかし、ここでちょっと困ったことが起きる。サッカーボールのような物であれば、いくら光を当ててもびくともしないが、電子のように極めて小さな粒子の場合は、そうはいかない。光を当てるとぶつかった反動で粒子が動いてしまう。跳ね返ってきた光を観測することにより、粒子の位置（光が粒子にぶつかった位置）はわかる。しかし、粒子は光とぶつかって動いてしまったため、次の瞬間にどこにあるのかはわからなくなる。つまり、その速度がわからなくなってしまう。

図７ 「見る」とは



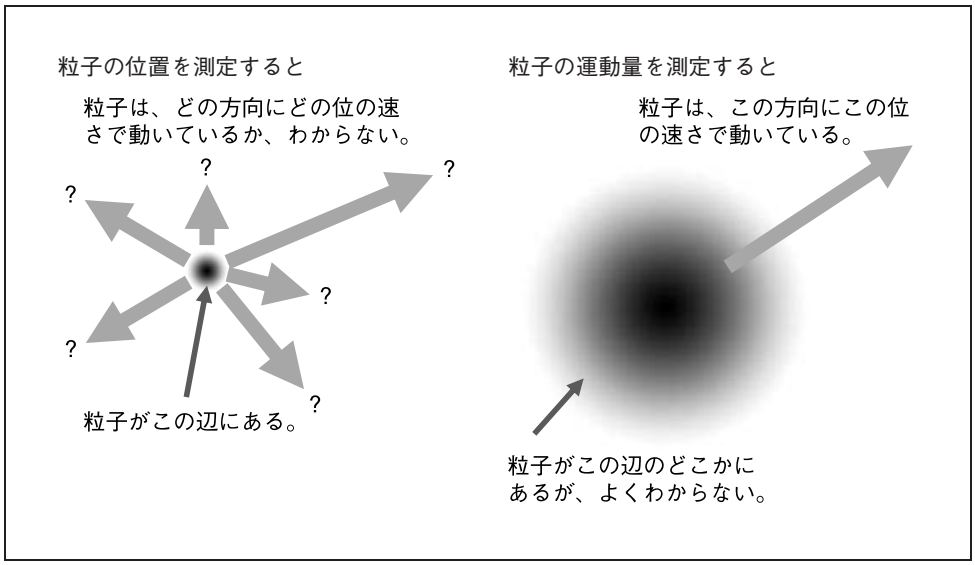
備考：ちなみに、サッカーボールは小さな粒子（水素の原子核とする）の 200,000,000,000,000 倍（200 兆倍）の大きさがある。水素の原子核はあまりに小さくてイメージが湧かないため、紙の上に直径 1 mm の点を描いて、それを水素の原子核の大きさだとしよう。するとサッカーボールの大きさは、太陽の大きさの 150 倍以上になる。これは、金星の軌道が全て含まれる大きさである。

「そんなことはない、光が粒子に与えた運動量（速さと質量を掛けたもの）から衝突後の運動量が計算できるので、速度もわかるはず」という反論があるかもしれないが、粒子の位置や運動量を測るために用いる光自体が同様の性質を持った粒子であり、位置や運動量を正確に測定することはできない。このため、どのような手段を用いても位置と運動量の両方を同時に正確に測定することは不可能である。

ここで古典力学[4]の考え方に慣れていると、「われわれが観測できないだけで、実際には位置も運動量も決まっているのであって、単に観測誤差の話をしているに過ぎないのではないか」と考えてしまう。しかし、さまざまな検証の結果、位置と運動量を同時に確定させることができないという性質は、こうした粒子が持っている本質的な性質であることがわかってきた。また、片方を正確に測るともう片方の不確定さが極めて大きくなるという性質もわかった。これが、不確定性原理と呼ばれるものである[5]（図 8 参照）。

4 量子力学以前の力学（ニュートン力学や相対性理論など）を古典力学と呼ぶ。
5 ここで示した「測定する粒子が光子により動いてしまう」という説明は不確定性原理の説明によく利用されるが、これは量子力学で導き出された数式の意味を現実に当てはめるために考えられた思考実験（実際に実験を行うことなく思考のみにより理論から導かれるはずの結果を得ること）である。

図 8　小さい粒子のイメージ（不確定性原理）



(3) 光の粒子性

西暦 1700 年頃、光を波と考える説（ホイヘンス[6]ら）と、光を粒子と考える説（ニュートン[7]）の両方が唱えられていた。その後、マクスウェルらによって光の正体が電磁波（テレビやラジオの電波と同じもの）であることが提唱されると、粒子説は姿を消す。しかし、光が波であると考えると説明できない現象が見つかった。金属の表面に波長の短い光を当てると電子が飛び出す光電効果[8]である。

その後、アインシュタイン[9]が光の粒子性を唱え、光が周波数に比例するエネルギーを持つ粒子であると考えることにより光電効果をうまく説明できることがわかった。もっとも、反射・屈折・回折・干渉といった波特有の性質も持つことから、光は波であり粒子であるという二面性を持つ「光量子」であるとしている。なお、光を波と捉えるとき「光波」といい、粒子と捉えるとき「光子」という。

6 Christiaan Huygens (1629–1695)、オランダの物理学者、天文学者。土星の環の発見や伝播する波に関するホイヘンスの原理が有名である。

7 Isaac Newton (1643–1727)、イギリスの科学者。万有引力の法則を発見したことで有名。

8 光電効果：金属の表面に波長の短い光を当てると、金属の表面から電子が飛び出す現象。強い光を当てると、出てくる電子の数が増えるが、個々の電子の持つエネルギーは増えない。より短い波長（高い周波数）の光を当てると、電子の持つエネルギーが増える。また、ある波長よりも長い波長（低い周波数）の光を当てた場合、いくら強い光を当てても電子は飛び出してこない。この現象は、光を波として考えると説明がつかず、光の持つエネルギーが $E = h\nu$（E: エネルギー、h: プランク定数、ν: 光の周波数）に従う粒子であるとすることで説明できる。強い光は、粒子を沢山含んでいるため、沢山の電子が飛び出す。高い周波数の光はエネルギーが大きく、エネルギーの大きい電子が出てくる。また、ある周波数以下の光は電子を飛び出させるだけのエネルギーを持っていない。

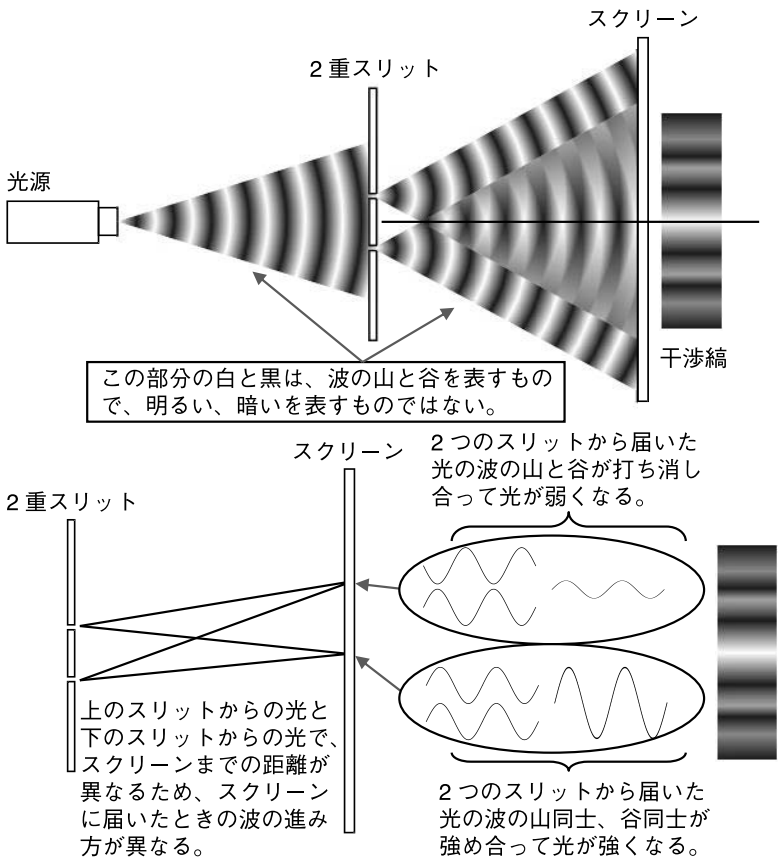
9 Albert Einstein (1879–1955)、ドイツ生まれの物理学者。特殊相対性理論（1905 年）、一般相対性理論（1915 年）が有名。

(4) 波と粒子の二面性

このような波であり粒子であるようなものを考えると、従来は波として簡単に説明できていた現象が、とても奇妙な現象にみえてくる。

光が波であることを示したヤング[10]の実験がよく知られている（図9参照）。これは、光を通さない板に開けた2つの細長い穴（スリット）を通った光が、その後ろに置いたスクリーンに当たる様子を観察するというもので、スクリーンには、縞模様が観察される。光が弱い所と、強い所ができる。これは、光が波の性質を持つために起こる現象で、2つのスリットを通った光の波の山同士、谷同士が重なるような

図9　ヤングの実験（2重スリット実験）



備考：ここで示した実験で観察される縞模様等は実際に観測されるものを模したイメージであり、実際に観測されたものではない。

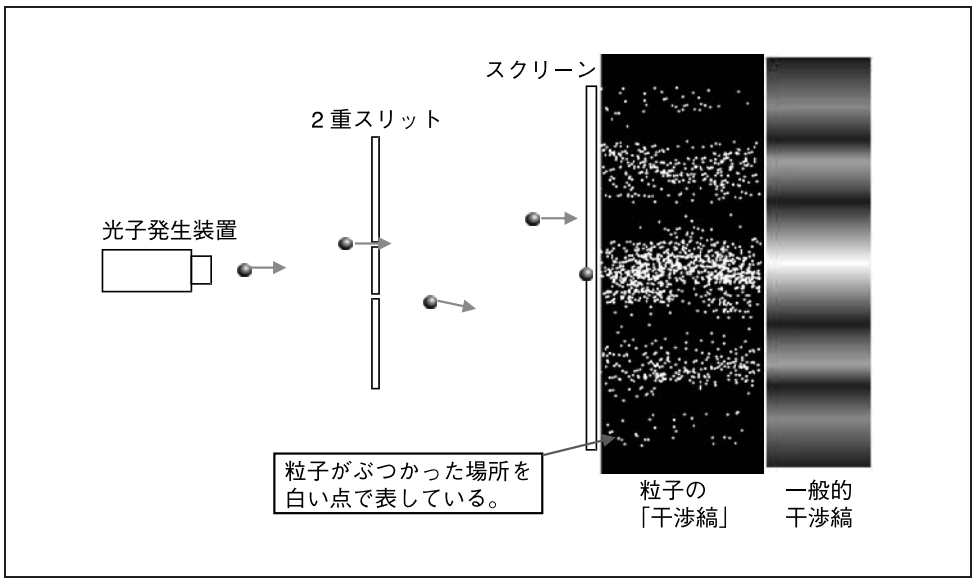
10 Thomas Young (1773–1829)、イギリスの物理学者。

所では光が強くなり、山と谷が重なるような所では波が打ち消し合って光が弱くなると考えられる。

しかし、同じ実験を光が粒子、すなわち光子であるとの立場からみると、とても不思議なことに思えてくる。

粒子は1個、2個と数えることができるものであり、1つの粒子が同時に2ヵ所で観測されることはないと考えられる（実際「1つの」粒子が同時に2ヵ所で見つかることはない[11]）。つまり、穴を通った1つ1つの光子は2つの穴のどちらかを通ると考えるのが自然だ。光には通常沢山の光子が含まれているため、2つの穴を通った光子がお互いに干渉して縞模様を作るというのは別に不思議ではない。そこで、光子を1個ずつ出すような装置を使って実験すると、どのような結果が出るのだろうか（現在ではそのような装置が手に入る）。1個の光子は穴のどちらかを通ってスクリーン上の1点に到着し、そこが明るくなる。スクリーンを写真のフィルムに置き換えると、1点だけ光が当たりフィルムが感光する。そこで、次々と1個の光子を発射して、沢山の光子がフィルムに到着した後に現像すると、元の実験と同じようにフィルムに縞模様ができる。1個1個の光子は、穴のどちらかしか通らず、また光子は一度に1個しか発射されないため、他の光子と干渉することができないと考えられるにもかかわらず、縞模様ができる[12]（図10参照）。

図10　粒子によるヤングの実験



11 図10の実験において2重スリットの各スリットの直後に粒子の検出器を置き、粒子を1つずつ発射して実験をした場合、粒子はどちらかのスリットで1つだけ見つかる。

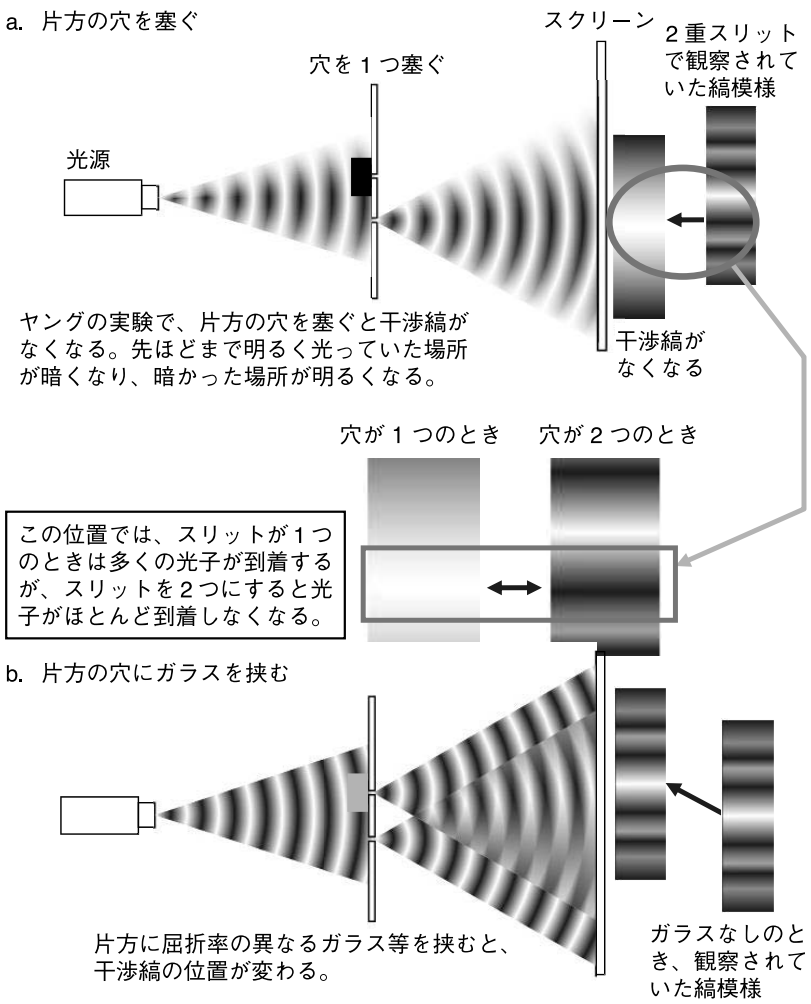
12 この実験も不確定性原理の1つの現れである。細いスリットを通った粒子は、位置の不確定性が小さくなったため運動量の不確定性が大きくなり、スクリーン上ではスリットの幅から常識的に予想される範囲よりも広い範囲に粒子が到着する。また、後述する、粒子がどちらの穴を通ったか観測すると干渉縞が観

(5) 粒子は自分が通らなかった穴の存在を知っている

次に、この実験の片方の穴に対して、穴を塞ぐ、空気と屈折率の異なるガラス等を挟む[13]といった実験を行うと、図 11 のようになる。

図 10 の実験と図 11 の a の実験において、塞がなかった片方の穴（図では下側の

図 11　縞模様の変化



測されなくなる現象も、粒子の位置を正確に測定したため、運動量の不確定性がより大きくなり、干渉縞を打ち消してしまうためと考えられる。

13 屈折率の異なる物質は、内部を光が通るときの速度が異なる（遅くなる）ため、これを挟むことにより光がスクリーンに届くまでの距離が長くなったのと同じ効果がある。

穴）を通った光子に注目してみよう。穴が1つのときには、光源と穴を結ぶ直線がスクリーンと交わる場所を中心として、そこから離れるに従って次第に到着する光子が少なくなるような模様が観測できる。穴を2つにすると、穴が1つのときには沢山の光子が到着していた場所なのに、もう1つの穴が空いた途端光子があまり到着しない場所ができてしまう。穴が1つのときに比べ、穴を2つにすると穴を通ってくる光子の数は2倍になり、全ての場所で穴が1つのときよりも到着する光子の数が増えると考えるのが自然である。しかし、実際に実験してみると、穴を増やした方が暗くなってしまう（到着する光子の数が減ってしまう）場所が出てくる。このことから、図の下側の穴を通った光子は、穴を2つにすると、これまで到着していた場所を避けて到着するようになることがわかる。つまり、この穴を通った光子は、もう1つの穴が存在していることを知っていて、それのあるなしによって到着位置を変えてしまっているようにみえるのである。両方の穴が空いた状態で、片方にだけ屈折率の違う物質を挟む実験でも、光子はもう1つの穴に屈折率が異なる物質があることを知っているような動きをする。

これらの実験の結果は、光を粒子と考えた場合、従来の常識では理解できない、とても不思議な現象である。同じような実験が、従来粒子だと思われていた電子を使って行われた。光に近い速度まで加速した電子を1個ずつ発射して穴を通したところ、光の場合と同じような縞模様が観測された。電子も波の性質を持っていたのである。こうした波の性質は物質波もしくは、ド・ブロイ波と呼ばれている。

(6) 粒子であり波である量子

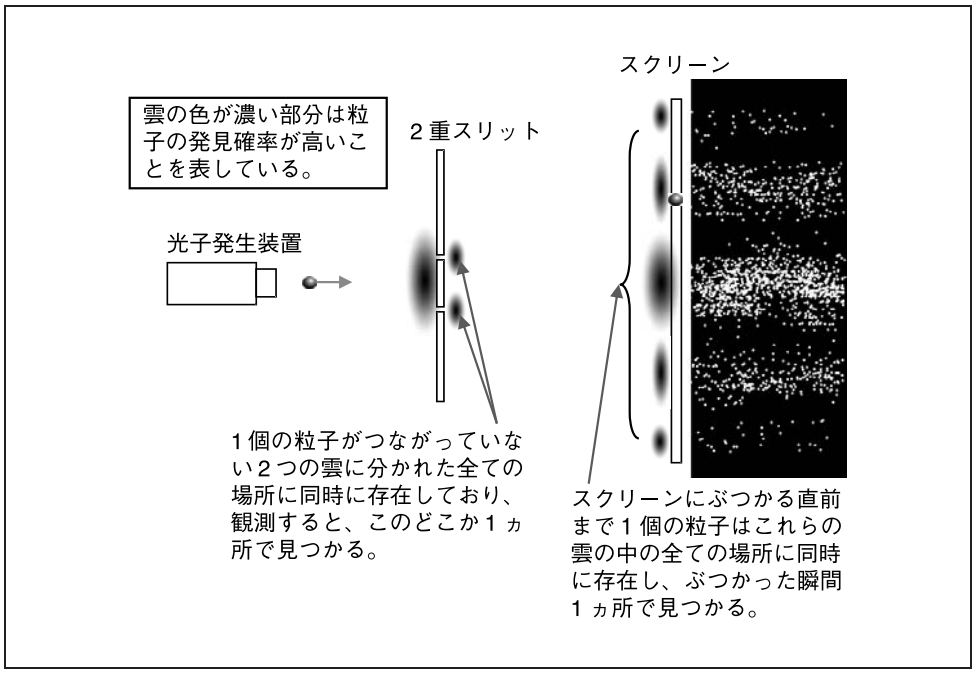
量子力学は、こうした不思議なものを扱う。量子力学の説明では、粒子は観測されるまでその位置は本質的に不明であり1個の粒子が2つの穴の両方に同時に存在する雲のような形で表される。穴を通った時点ではその1個の粒子の雲が両方の穴を「同時に」通る（ただし、どちらの穴を通ったかを観測するような装置を取り付けると、観測によってその状態[14]が変わり片方の穴だけで粒子が見つかって、スクリーンの縞模様はなくなる）。

図12では、スクリーンの直前の位置において雲は縞模様と同じような濃淡を持ち、粒子は雲の中のいたるところに同時に存在する。スクリーンに到着した時点でその雲の中の1点で粒子が見つかる。この雲は、粒子の発見確率を視覚的に表したもので、何度も観測を繰り返すと、色の濃い部分で粒子が発見される回数が多く、色の薄い部分ではほとんど粒子が見つからない。

このような不思議な性質を「量子」という概念で捉えている。本来「量子」は物理量（例えば波が持つエネルギーなど）の最小単位のことを指す。すなわち、物理

14 これ以降、「(量子の）状態」という表現を多く使うが、読みやすさを優先した結果、波動関数や確率で表されるような厳密な意味での「量子状態」と、観測の結果定まった量子の状態等を区別することなく記述している。このため、量子力学を学んだ読者にとっては読みにくい表現となっているがご容赦願いたい。

図 12　雲のような粒子



量にはそれ以上細かく分けることのできない最小単位があり、その整数倍の値しかとれない（最小値の 1.5 倍の値は存在しない）というもので、その最小単位が 1 個の粒子であり、整数倍になるのは粒子の個数だからという考え方である。

(7) 量子の不思議な性質

以上のように不思議な量子だが、このほかにも、いろいろと不思議な性質を持つことがわかっている。例えば、量子が取りうる 2 つの異なる状態があるときに、1 個の量子がその両方の状態を同時に持つことができ、測定されるまでどの状態であるかは決まらないこと（重ね合わせ）、互いに密接な係わり合いを持つ粒子のペアが存在し、その状態は粒子を遠く離した場合にも維持されること（エンタングルメント）などだ。重ね合わせは、例えばコンピューターの世界でいう 1 と 0 の 2 つの状態を 1 つの粒子が同時に持つことができることを意味し、これを利用してこれまでのコンピューターではできなかった特殊な計算を行うことができると考えられている。量子力学を応用したコンピューターは量子コンピューターと呼ばれ、実現すれば従来のコンピューターでは何万年もかかるような計算が一瞬でできるようになるといわれている。エンタングルメントも、量子コンピューターや量子暗号の中継の実現に不可欠な性質である。エンタングルメントを利用した量子暗号の方式も考案されている。

重ね合わせにおいて、量子は複数の状態を同時に持ち、測定されるまでその状態は決まらないが、エンタングルした2個の量子の場合、片方の量子を測定してその状態を知れば、その瞬間にもう片方の状態も決まる。両者の間がどんなに離れていてもこの現象が起こり、2個の粒子間で何らかの情報伝達が行われるように考えられ、その伝達速度が光の速度を超えるように思われる。本件はEPR（Einstein-Podolsky-Rosen）相関と呼ばれており、エンタングルした量子間の相関として理解され、実験によっても確認されている。このEPR相関を利用して量子を離れた場所に転送する量子テレポーテーション（瞬間移動）も実験により確認されている。これは、離れた2ヵ所（アリスとボブ）に送ったエンタングルした2個の量子（AとB）を使って、アリスが持っている別の量子Xの状態（アリスやボブにとって未知の状態でもかまわない）をボブに転送するというものである。アリスは送る量子Xと量子Aを同時に特別な方法で測定し、測定結果を通常の回線を使ってボブに送る。ボブはその測定結果の情報を使って、量子Bにある操作を加えると量子Xと同じ状態を再現できる。全く同じ状態にある2個の量子は区別できないため、量子Xがアリスからボブに転送されたようにみえる。ただし、アリスが行った測定によりXとAの量子は測定前の状態を再現できなくなり、量子をコピーできるわけではない。また、テレポーテーションにおいては通常回線による情報の伝達が必要であるため、光の速度を超えた情報（量子の状態）の伝達も不可能である。

こうした量子の性質をまとめると以下のとおり。

① 粒子と波の両方の性質を持っている
② 1個の量子を2つに分けることはできない
③ 1個の量子が、つながっていない離れた場所に同時に存在できる
④ 同時に複数の状態をあわせ持つことができる
⑤ 観測を行うまで量子の状態は決まらない
⑥ 観測を行うと状態が変化し[15]、元の状態を再現することはできない
⑦ 状態のわからない（観測していない）量子は同じ状態の量子をもう1つ作りだす（コピーする）ことができない
⑧ 遠く離れていても相互に関係を持っている量子の対がある（エンタングルメント）

15 粒子の性質が強く出るような測定（光子がどちらの穴を通ったか調べるなど）を行うと波としての性質が消え（縞模様がなくなる）、波の性質が強く出るような測定（縞模様の観測）を行うと、粒子としての性質（どちらの穴を通ったか）が消える（わからなくなる）。位置を測定すると運動量がわからなくなり、運動量を測定すると位置がわからなくなるなど。

〈コラム〉エンタングルメント

エンタングルメントとは、「もつれ」あるいは「絡み合い」という意味だが、量子に対して使われる場合は、2 つ以上の量子がお互いに深い係わり合いを持っており、遠く離れたとしてもそれが維持されるような状態をいう。話を簡単にするために古典的な（量子力学以前の古典力学的な）例を示す。

ある家があって、そこには夫婦が住んでいる。ある朝、夫婦が同時に家を出て、1 人は映画を見に行き、1 人はデパートにショッピングに出かけた。このとき、2 人は遠く離れてしまったが、夫婦であるということは変わらず、片方が妻でもう片方が夫である。こうした状態をエンタングルメントという。量子の世界にも結婚関係にあるような量子の対が存在する（もっとも、3 個以上の量子がエンタングルする場合もある）。

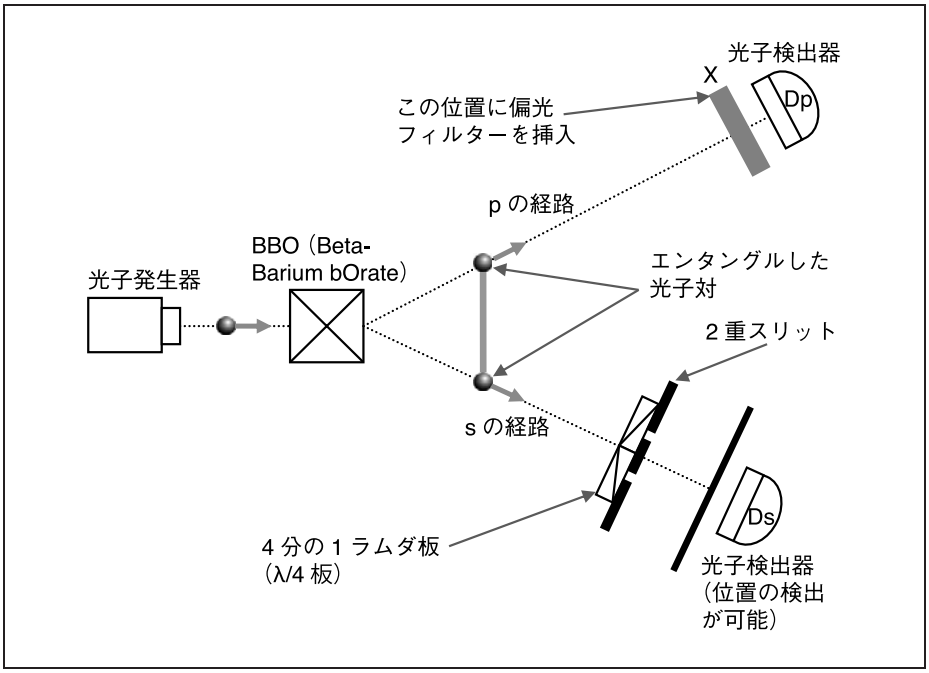
この例は古典力学的な例であるので、2 人が家を出た時点で夫がどちらに行ったのかが決まっている。例えば映画館に行ったのは夫でデパートに行ったのは妻であるという具合だ。しかし量子の場合、これに「量子の状態は観測されるまで決まらない」という量子の性質が加わることにより非常に奇妙なことが起こる。「わからない」ではなくて「決まらない」というところがポイントである。量子の場合はデパートに行ったのは夫と妻の重ね合わせの状態の人になる。誰かが観測するまでどちらであるかは決まらない。例えば、デパートに行った人がトイレに行ったとすると、その人は男子トイレと女子トイレの両方に同時に入ったという奇妙なことが起こる。これは、前述の「粒子であり波である量子」で述べた 1 個の粒子（量子）が 2 個の穴を同時に通るということと似たようなことだ。トイレの入り口で見張っていると、どちらか片方に入って行くが、これは観測したために状態が変わり、どちらか一方のトイレで見つかったということになる。

実際の量子ではどのよう現象がみられるのか。Walborn, Cunha, Pádua, and Monken [2002] が行った実験を紹介する。これは、エンタングルした 2 つの光子を別々の方向に飛ばし、そのうち 1 個の状態を観測することで、もう 1 個の光子が影響を受けることを示したものである。

レーザー光線を BBO（Beta-Barium bOrate）と呼ばれる結晶に当て、そこから出てくるエンタングルした 2 つの光子を観測する。2 つの光子のうち 1 個は右 45° に偏光しており、もう 1 個は左 45° に偏光している。光子は 2 つの方向に飛んで行くが、どちらの偏光を持った光子がどちらの方向に飛んで行くかは決まっておらず（量子力学的には両方の状態の重ね合わせ状態にある）、片側の光子を観測すると 2 分の 1 の確率で右、もしくは左が現れる（もう片方の光子は、その時点で、観測された偏光と反対の偏光に決まる）。図 13 をみてほしい。光子のうち 1 個が進む経路（p）上に光子検出器 Dp を設置し、もう一方の光子が進む経路（s）上には 2 重スリットと光子の位置を検出できる装置 Ds を置く。光子を 1 個ずつ発射して Ds における光子の検出位置を記録するが、このまま長時間観測を続けると、Ds では光子の到着位置が多数記録され、ヤングの実験と同様の縞模様が観測される。

次に、2 重スリットの手前（検出器 Ds と反対側）に 4 分の 1 ラムダ板と呼ばれる光学素子（直線方向の偏光を円偏光に変換する素子）を 2 枚、2 つのスリットそれぞれに貼り付ける。片側は右回りの円偏光に、もう片側は左回りの円偏光に変換するようにする。そうすると、先ほど観測された縞模様は観測されなくなる。正確な表現ではないが、量子がどちらのスリットを通ったか観測できるような装置を取り付けたために波としての性質が消え、干渉縞が消えたということができる。これで実験装置はセット完了だ。

図 13　Walborn, Cunha, Pádua, and Monken [2002] の実験



この状態で、Dp の検出器の前（図の X の位置）に偏光フィルターを入れる。そうすると、Ds において先ほどは観測されなかった縞模様が観測されるようになる。また、X の位置の偏光フィルターを回して偏光の角度を変えると、Ds では別の縞模様が観測される。2 つの光子のうち、Ds において縞模様が観測されたり観測されなかったりする方の光子（s の経路を通る光子）に対しては何も行わず、その光子と対になった方の光子（p の経路を通り Dp で検出される光子）に対してのみ観測方法を変えただけである。このように、エンタングルした光子対は、片方を観測するとその時点でもう片方の光子に影響を与えていることがわかる。

さらに奇妙なことに p 経路に設置した X の位置の偏光フィルターと検出器 Dp を BBO から遠く離し、Ds で光子が検出された後に p の経路を通る光子が偏光フィルターを通るようにしても縞模様が観測され、偏光フィルターを外すと縞模様が観測されなくなる。Ds で観測された光子は、自分が観測された時点より後に、p 経路側に飛んでいった光子が偏光板を通る、あるいは通らないことを知っているのであろうか。量子力学では、時間の前後関係についても曖昧になってしまうような不思議な現象が多く観察されているようだ。

4. 量子暗号

量子が不思議な性質を持つことはわかったが、それをどう使えば量子暗号が実現できるのだろう。ここでは、BB84（Bennett and Brassard [1984]）という方式を例にとって説明を進める。BB84 は、1984 年にベネット（Charles H. Bennett）とブラ

サール（Gilles Brassard）が提案した量子暗号の方式で、初代量子暗号といえるものである。

BB84 以外にも、B92（Bennett [1992]）やエンタングルメントを利用する E91（Ekert [1991]）等が提案されているが、ここでは、原理を理解するうえで最もわかりやすい BB84 を例にとることにする。

（1）偏光

光は波の性質を持っているが、波には振れる方向がある。縄跳びの縄を揺らすことを考えてみよう。地面と平行に縄を揺らすと、縄は蛇が進むように動き、垂直に揺らすと海の波のようになる。それぞれ横方向、縦方向に振れる波ができた。このほか、垂直から 45 度傾いた波などいろいろな方向に振れる波を作ることができる。これと同様に、光にも振れる方向がある。懐中電灯を照らしたとき、その光には縦方向に振れる光、横方向に振れる光、斜め方向に振れる光と、180 度（光の振れる方向に上下の区別はないため、180 度反転すると同じ方向になる）あらゆる方向に振れる光が含まれているが、この光を偏光フィルターと呼ばれるフィルターに通すと、1 つの方向に振れる光だけになる。こうした、波が振れる方向が一方向に偏っていることを偏光という（図 14 参照）。

偏光サングラスは、水面の反射を抑える効果があるため、釣り人などによく利用されている。これは 1 方向に振れる光のみを通し、それと直角の方向に振れる光を通さない偏光フィルターを使ったものである。太陽光が水面などで反射すると、反射光は一定の方向に偏光した光になる。その振れる方向の光を通さないように偏光フィルターを使うと、反射光がフィルターで遮られて目に届かなくなり水面の反射がなくなって水の中がよく見えるようになる（図 15 参照）。

図 14　偏光

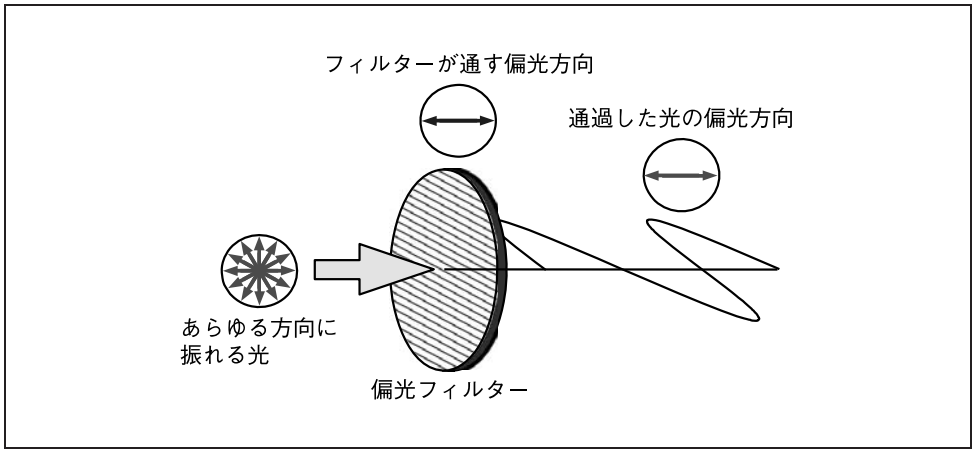


図 15　偏光フィルターの効果

下の写真のうち偏光フィルターなしの方は、普通に池の写真を撮ったもので、水面に空や木の影が写り込んで水面下の鯉の姿が見えづらくなっている。偏光フィルターありの方は、偏光フィルターの効果を最大にして撮影したもので、写真の下半分では水面の反射がなくなり、水面下の鯉がよく見える。

偏光フィルターなし

偏光フィルターあり

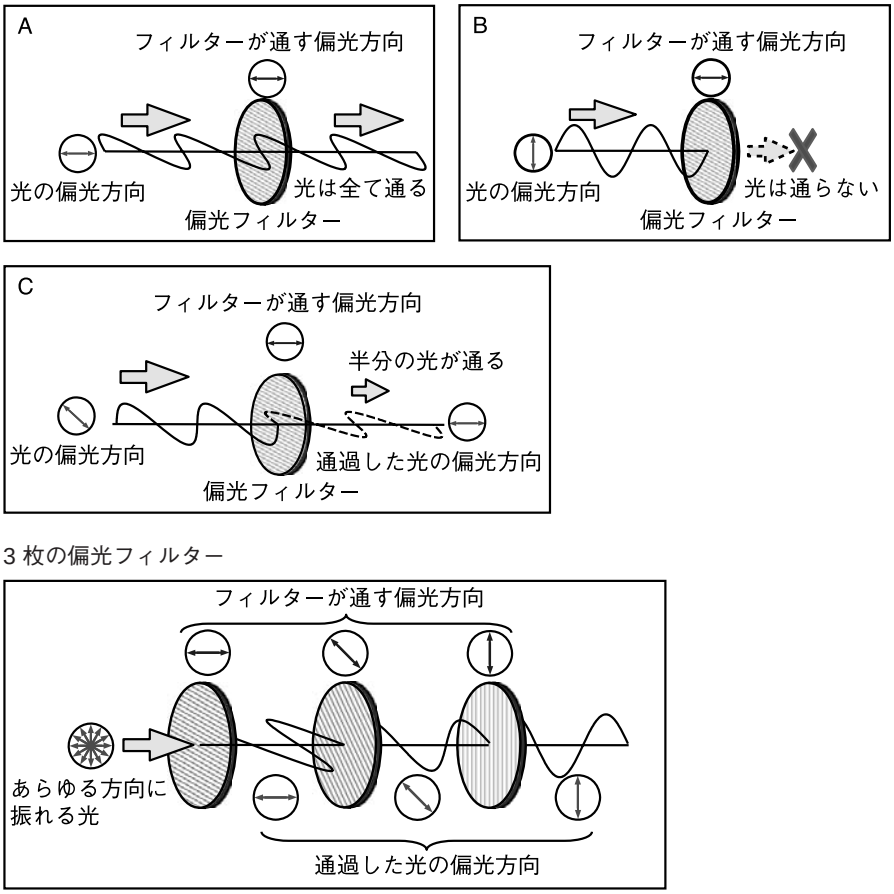
(2) 偏光に関する性質

偏光フィルターを 2 枚用意して、通す偏光の方向が直角になるように重ねると、真っ黒になり向こうが見えなくなる。1 枚目のフィルターが横方向に偏光した光のみ通し、2 枚目のフィルターは縦方向に偏光した光のみ通すとき、両方を重ねると光を全く通さなくなるからだ。ここで、2 枚の偏光フィルターの間にもう 1 枚の偏光フィルターを挟み、2 枚のフィルターの偏光方向と 45 度傾いた状態にする。手前から 3 枚のフィルターの偏光方向は 0°、45°、90° となる。こうすると、先ほど 2 枚のときは真っ暗だったのが、光が通るようになる。

1 枚目の偏光フィルターを通った光は横方向（0° の方向）に振れている。2 枚目の偏光フィルターは、45° 傾いた偏光を持つ光（以下「○° の光」という、○は偏光の角度）を通すが、ここでは、先ほどの直角に傾いていた場合とは異なり、一部の光が 2 枚目のフィルターを通る。そして、3 枚目の偏光フィルターのところでは、2 枚だけのときには全く光が通らなかった（3 枚目は 1 枚目と直角方向に傾いており、完全に光を通さない）にもかかわらず、今度は光が通るようになる。

少し整理する。まず、横方向に偏光した光を横方向の偏光フィルターに通すと、完全に光が通る（図 16 A）。また、縦方向に偏光した光を横方向の偏光フィルターに通すと、全く光が通らない（図 16 B）。そこで、45° の光を通すと、半分の光が通過する（図 16 C）。なお、半分とは光子の半分がフィルターを通過でき（フィルターと同じ偏光方向だと観測される）、残り半分は通過できない（フィルターと異なる偏光方向だと観測される）ということを意味しており、光子を 1 個だけ通すと、2 分

図 16　偏光フィルターの特性



の 1 の確率で通る。通った後の光は偏光フィルターと同じ偏光方向だと観測されたので、偏光の方向が変わっている。正確な表現ではないが、前節の量子の考え方でみると、横方向に偏光した光は、45° の偏光と –45°（135°）の偏光の重ね合わせ状態にあり、観測すると 2 分の 1 の確率でどちらかが観測されるということになる。3 枚目のフィルターのところを見ると、45° の光は 0° の光と 90° の光の重ね合わせになるので、90° の光を通すフィルターでは、2 分の 1 の確率で 90° の光が観測される[16]。

16　この現象は、前節のヤングの実験において、2 つのスリットを同時に通った光子と同様に考えることができる。スクリーン上で縞模様として観測される光子は上のスリットを通った光子と下のスリットを通った光子の両方の重ね合わせ状態にあると考えられる。どちらのスリットを通ったかを観測すると縞模様は観測されなくなり、片方のスリットを通った光子としての性質のみが現れる。少々イメージは異なるが、偏光においても 45° の光は、0° の光と 90° の光の重ね合わせ状態にある。観測を行い、例えば 90° の偏光であったとすると、0° の偏光の性質は観測されなくなる（横方向の偏光フィルターを置くと光は一切通らない）。

BB84 では、こうした偏光の性質を利用する。

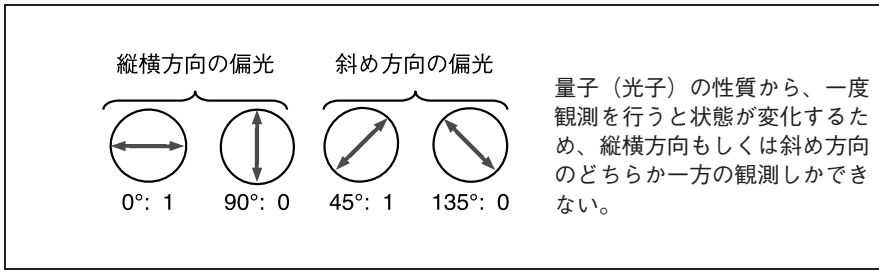
(3) BB84

BB84 の原理を使ってアリスとボブが暗号通信を行う場合の状況をみてみよう。この方式では、送るデータの「1」と「0」を光子の偏光方向で表す。図 17 のように、0° の光を「1」、90° の光を「0」と決め、アリスは光子を偏光させて送る。ボブは受け取った光子の偏光を測定して「1」か「0」の情報を受け取る。もっとも、これだけでは盗聴者イブが途中で光子を測定して同じ偏光の光子をアリスに向けて送り出すと盗聴が可能になってしまう。そこで、前述の偏光の性質を利用する。アリスは 0° と 90° のほかに、45° と 135° の光も利用し、45° を「1」、135° を「0」と決める。そして 0° と 90°（以降これを「縦横方向」という）を利用したデータと、45° と 135°（以降これを「斜め方向」という）を利用したデータをランダムに切り替えて送信する。

一方、受け取るボブは、偏光を測定する方向を縦横方向と斜め方向にランダムに切り替えて測定する。アリスは送信の際に使った偏光の方向をボブに教えないため、ボブは 2 分の 1 の確率で誤った方向を使って光子を測定することになる。上記（2）のとおり、誤った方向で測定した場合（例えばアリスが 90° の偏光で 0 を送ったときにボブが斜めの偏光で測定したような場合）光子の偏光の方向を正確に測定することができず、2 分の 1 の確率で「1」と「0」がランダムに観測され、正しいデータを受信できないことになる。

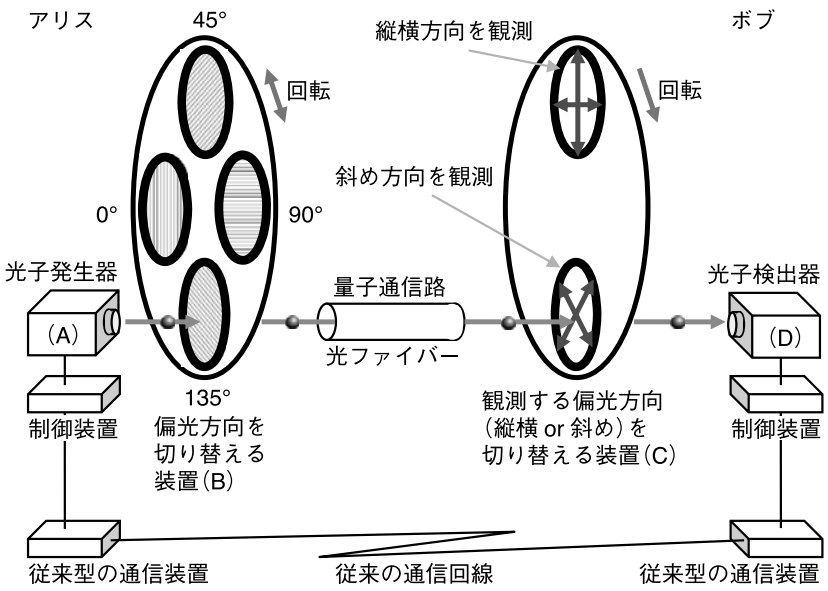
偏光によるデータの送受信が終わった後、ボブは自分が測定する際に使った偏光の方向を通常の回線（盗聴される危険性がある回線[17]）でアリスに教える。アリスは、自分が送信の際に利用した偏光の方向と同じ方向でボブが測定したデータがどれであったかを、同じく通常の回線によりボブに伝える。ただし、データの内容自体は教えないので、盗聴されても情報が漏れることはない。アリスとボブは、同じ偏

図 17　光の偏光方向により 1 と 0 を表す



17 後述するが、量子暗号を利用した回線ではアリスが持っている情報をボブに送ることはできない。アリスとボブが同じ情報を共有することができるだけである。このため、情報のやりとりが必要な通信は通常の回線を利用して行われる。

図 18　BB84 による通信



備考：装置（B）・（C）の図は機能のイメージであり、実際の装置とは異なる。

光の方向で送り合ったデータのみを残し、そこで送受信したデータを共有する。このようにして、アリスとボブは同じデータを共有することができる。

図 18 に示すように、アリスは光子を発生させる装置（A）と、偏光の方向を 4 通り（0°、45°、90°、135°）に切り替える装置（B）を用意する。一方ボブは、観測する偏光方向を切り替える装置（C）と、偏光の方向を検知する光子検出器（D）を用意する。この装置は検出した光の偏光方向に応じて 1 もしくは 0 を出力する。さらに、量子暗号通信をコントロールする制御装置と従来の通信回線も用意する。

アリスは光子を 1 個ずつ発射し、（B）を操作して偏光の方向を変える。例えば斜め方向の偏光で「1」を送る場合は 45°、「0」を送る場合は 135° に制御する。受け取るボブは（C）を操作して縦横方向で受信するのか斜め方向で受信するのかをランダムに決定する。光子は（D）により測定され、「1」もしくは「0」としてデータを記録する。あとは制御装置が従来型の通信装置および通信回線を利用して偏光方向に関する情報を交換すればアリスとボブは同じデータを共有することができる。具体的なデータ共有の様子を表 3 に示す。

そこにイブがいた場合はどうなるのか。情報は 1 個の量子に載せられているため、量子力学の原理からその量子を 2 個に分けることはできない。また、観測していない（状態が未知の）量子を複製して同じ状態の量子をもう 1 個作り出すこともできない。そこで、イブは量子をいったん観測した後で別の光子をボブに対して送る必

表 3　BB84 によるアリスとボブの通信

送信するデータ[1]		1	1	0	1	0	1	0	0
アリス	送る光子の偏光	↔ 0°	⤢ 45°	⤡ 135°	↔ 0°	⤡ 135°	↔ 0°	↕ 90°	⤡ 135°
	偏光方向（基底）[2]	＋ 縦横	× 斜め	× 斜め	＋ 縦横	× 斜め	＋ 縦横	＋ 縦横	× 斜め
ボブ	偏光方向（基底）[2]	＋ 縦横	＋ 縦横	× 斜め	× 斜め	× 斜め	＋ 縦横	× 斜め	＋ 縦横
	観測した偏光	↔ 0°	↕ 90°	⤡ 135°	⤢ 45°	⤡ 135°	↔ 0°	⤢ 45°	↕ 90°
	受信したデータ	1	0	0	1	0	1	1	0
偏光方向が一致？		○	×	○	×	○	○	×	×
共有データ[3]		1	なし	0	なし	0	1	なし	なし

備考：シャドーを付けた部分は、アリスが送った際の偏光方向と、ボブが受信した際の偏光方向が一致しており（両者が通常の回線で確認）、アリスが送ったとおりにボブがデータを受信できるが、それ以外の部分では、ボブが受信したデータは信頼できない。
1）乱数発生器等で発生させたランダムなデータ。
2）アリスとボブが自由に選んだ偏光の方向（基底）。
3）偏光方向が一致したデータのみを残し、一致しなかったものは破棄する。

要がある。イブは通信回線を途中で切り、自分が用意した受信機（ボブが保有するものと同等）と測定後に偽データを送る送信機（アリスが保有するものと同等）を接続する。

アリスが送信したデータをイブが受信するが、この際イブもボブと同様に測定する偏光の方向を縦横方向か斜め方向かに決める必要がある。これは、量子の世界では縦横方向と斜め方向の偏光を同時に測定することが原理的に不可能なためである。また、いったん測定を行うと量子の状態が変わってしまい、同じ量子を再度測定しても元の情報を知ることはできないため、アリスと異なる方向で測定した光子の偏光は正しく知ることができず、イブは 2 分の 1 の確率で誤ったデータを得ることになる。ボブに送る際には、誤った偏光を再現して送ることになるため、最終的にアリスとボブが共有したデータの中に間違ったデータが混じってしまう。そこで、アリスとボブは送受信したデータの一部を比べ合い（そのデータは検証用としてのみ利用し、共有するデータとして利用しない）、高い確率で誤りが見つかったときは、途中でイブに盗聴されていることがわかる（表 4 参照）。これが、盗聴が不可能といわれる所以である。

(4) 無条件安全性

BB84 に関しては、原理的に無条件安全性が証明されている。これは、無限大の計算能力を持ち、さらに量子力学において理論上可能な全ての操作を行えると仮定

表４　イブがいる場合のアリスとボブの通信

送信するデータ[1]		1	1	0	1	0	1	0	0
アリス	送る光子の偏光	↔ 0°	⤢ 45°	⤡ 135°	↔ 0°	⤡ 135°	↔ 0°	↕ 90°	⤡ 135°
	偏光方向（基底）[2]	＋ 縦横	× 斜め	× 斜め	＋ 縦横	× 斜め	＋ 縦横	＋ 縦横	× 斜め
イブ	偏光方向（基底）[2]	＋ 縦横	× 斜め	＋ 縦横	× 斜め	＋ 縦横	× 斜め	＋ 縦横	× 斜め
	観測した偏光（ボブに送る偏光）	↔ 0°	⤢ 45°	↔ 0°	⤡ 135°	↔ 0°	⤢ 45°	↕ 90°	⤡ 135°
	受信したデータ	1	1	1	0	1	1	0	0
ボブ	偏光方向（基底）[2]	＋ 縦横	＋ 縦横	× 斜め	× 斜め	× 斜め	＋ 縦横	× 斜め	＋ 縦横
	観測した偏光	↔ 0°	↕ 90°	⤢ 45°	⤡ 135°	⤡ 135°	↕ 90°	⤢ 45°	↕ 90°
	受信したデータ	1	0	1	0	0	0	1	0
偏光方向が一致？		○	×	○	×	○	○	×	×
共有データ[3]		1	なし	1	なし	0	0	なし	なし

備考：薄いシャドーの部分はアリスとボブの偏光方向が一致している部分。斜線部分はイブが間違った基底で観測したため、誤りを含んでいる部分。この結果、濃いシャドーの部分ではイブがいなければアリスとボブが同じデータを共有するはずだが、イブの存在により誤りを含んでおり、上の例では、共有データ４つのうち半分が誤った値となっているのがわかる。

1）乱数発生器等で発生させたランダムなデータ。

2）アリス、イブ、ボブが自由に選んだ偏光の方向（基底）。

3）偏光方向が一致したデータのみを残し、一致しなかったものは破棄する。

したイブによっても盗聴が不可能という意味であり、原理通りに通信装置を作れば、決して盗聴されることはない。

もっとも、実際の量子暗号通信では必ずしも原理通りにいかない点もあり、それが盗聴の危険性となって残ってしまうことになる。例えば、光子を１個ずつ発生させることは難しく、多くの場合非常に弱いレーザーのパルス光（極短時間だけ光らせたレーザー光）を使う。具体的には10個のパルスを発生させたときに、その中に平均１個の光子が見つかるような光を使う。10回に１回しか光っていないように思えるが、量子力学的にみると、光子がある状態とない状態の重ね合わせにあるパルスを発生させ、それを観測すると、10回に１個の割合で光子が観測される。あくまで確率に従うため、一定の確率で１つのパルスの中に２個以上の光子が含まれる。この場合は、同じ情報を運ぶ２個の光子のうち１個をイブが分離して横取りすることができてしまう。イブはこの光子を何らかの方法で保存し、アリスとボブが通常の回線で情報をやりとりするのを盗聴して偏光方向を知った後で、保存しておいた光子をアリスとボブが使ったのと同じ方向の偏光で観測すれば正確な情報を得ることができる。そこでイブは１個の光子だけが含まれていたパルスについては捨て去

り、2 個以上の光子が含まれていたパルスのみ残してボブ宛に送り出す。こうすると、イブはボブに届いた全てのデータを盗聴することができてしまう。また、これは従来の暗号方式も含め全ての暗号に共通のことであるが、暗号化と復号を行う装置の動作に伴って発生する電磁波や、消費電力の増減を詳細に解析することで、共有した鍵が漏れる可能性があり、暗号方式の実装の面での対策も重要になる。

(5) 量子暗号は本当に暗号通信か？

ここで疑問が生じる。理想的な量子暗号通信を考えた場合でも、ボブはアリスが送信したデータのうち、2 分の 1 のデータを受信できるだけであり、アリスが用意したデータをそのまま受信できるわけではない。例えばアリスが数字の 9 を送りたいとき、二進数では「1001」を送るわけだが、ボブはこのうちの半分、例えば 1 番目と 4 番目のデータの受信に成功したとすると「11」を受信する。1 番目と 3 番目であれば「10」になる。つまり、アリスは 4 桁の数を送りたかったにもかかわらず、ボブが受信するのは 2 桁になってしまう。ボブが受信したデータはアリスが送信したデータと一致するが、それは、送ったデータのうちランダムに選ばれた約 2 分の 1 のデータでしかない。

さらに、光子 1 個を送受信するということは非常な困難を伴う。まず、上記のとおり光子を発生させる装置では、10 個のパルスに平均 1 個の光子を含むような光を使うため、パルスを 100 個観測しても、平均 10 個しか光子を観測できない。また、アリスとボブの距離が離れると光ケーブルの減衰によって観測できる光子が少なくなり、長距離の送信を行った場合、アリスが送信した光子のうちボブが正しく受信できる光子の数は極端に少なくなってしまう。さらに、ノイズによりデータが変わってしまうこともあり、エラー訂正も必要になる。これらの事情により、アリスが送るために用意したデータのうちボブが受け取れるのは 1,000 分の 1 以下になってしまい、通信速度が数 kbps というような値になる。

これでは、アリスが秘密のデータをそのままボブに送ろうとしても、その役には立たない。量子暗号は本当に「暗号」といえるのだろうか。

(6) 本当の暗号通信を行うために

ここで、前述のバーナム暗号の登場となる。アリスとボブが量子通信路によって共有したデータを鍵として利用し、バーナム暗号によって送りたいデータを暗号化する。例えばアリスが数字の 9（二進数で「1001」）を送りたいとき、共有したデータ（例えば「0110」）を用いて暗号化する（両者の排他的論理和により「1111」）。これを通常の回線を利用してボブに送る。受け取ったボブは共有した鍵（「0110」）を使って復号し（「1111」と「0110」の排他的論理和により「1001」）数字の 9 を受け取ることができる。こうして、量子通信路によって鍵を共有し、その鍵を使って通

常の回線上でバーナム暗号による通信を行うことで本当の暗号通信を行える。このことから、量子暗号は、量子鍵共有方式（QKD: Quantum Key Distribution）とも呼ばれている。

もっとも、前述のとおり量子通信路によるデータの送受信では、アリスが送り出したデータのうちボブに届くデータは極端に少なくなる。このため通信速度は数 kbps（ビーピーエス：1 秒間に送ることができるデータのビット数）程度と昔のパソコン通信程度の速度にしかならず、大量のデータを送信したい場合には、事前に長時間かけて鍵を共有しておく必要がある。例えば 100 Mbps（メガビーピーエス：1 秒間に百万ビットのデータを送る速度）の速度で 1 分間分のデータ（総容量 750 メガバイト、CD 1 枚強分のデータ）を送る場合、そのための鍵 750 メガバイト分を共有するには、量子通信路の速度が 10 kbps だとすると 166 時間 40 分（約 7 日間）かかってしまう。これでは、よほど特殊な用途でない限り大量のデータを送る役には立たない。したがって、現時点では応用範囲がかなり限定されてしまう。もっとも、情報理論的に安全なバーナム暗号をあきらめて、AES や Triple-DES の鍵を送り合う程度であれば十分実用になる。1 秒の間に何度も鍵を変えることもでき、現在の技術水準では解読はほぼ不可能といえる。

ブロードバンドの普及により、通信するデータの容量が爆発的に増大している今日の通信事情において、量子鍵共有方式の課題は通信速度の高速化にある。現在さまざまな改良が加えられ高速化が図られているが、ブロードバンドに対応できるようになるまでには、まだまだ時間がかかるとみられている。もっとも、最近 BB84 とは全く異なるやり方で量子の性質を利用しながら高速な通信を行う、Y-00 と呼ばれる方式も開発されている。

（7）もう 1 つの量子暗号

Y-00 は、ノースウェスタン大学の Yuen 教授のグループが 2000 年に提案した方式で、Yuen 教授のイニシャル Y と、2000 年の下 2 桁をとって Y-00 方式もしくは、Y-00 プロトコルと呼ばれている。2007 年 4 月 6 日には、商用の光ファイバーを利用して、192 km の距離で 2.5 Gbps の通信に成功したとの報道があった。BB84 における 100 km で 10.1 kbps と比べると、格段に速いスピードでの通信が可能となっている。

この方式は、従来研究されてきた BB84 等の方式とは大きく性格を異にしている。BB84 等では 1 個の光子に 1 ビット分の情報を載せて送り、ランダムなビット列をアリスとボブが共有する仕組みであるのに対し、Y-00 は 1 ビットの情報を送るのに多数の光子を使い、送りたい情報そのものを伝送する仕組みになっている。光子 1 個は分割やコピーができないため BB84 では盗聴のリスクはないが、この方式では多数の光子が同じ情報を運んでいるため途中で一部の光子を抜き取ることが可能となってしまう。それでは、どのような仕組みで盗聴を防止するのだろうか。

(8) Y-00 の仕組み

この方式では、量子雑音を使って情報を隠す。量子雑音とは、量子が本質的に持っている正確に情報を測定できない性質のことである。前述のとおり量子には運動量と位置の両方を正確に測定することができないという性質があるが、では片方のみであれば完全に正確な値を測定できるかというと、それもできず、ある程度の誤差が必ず付きまとう。そこで、送る情報が 1 であるのか、0 であるのかを量子雑音の中に隠してしまい、測定してもどちらだかわからなくしてしまおうというのがこの方式の原理である。もっとも、これだと正規の受信者ボブも情報を得ることができなくなるため、予めアリスと取り決めた情報（鍵）を使えば、送られた情報を正しく判別することができるようにする必要がある。以下では歯車を使って情報を送る方式にたとえて、Y-00 の仕組みを説明する。

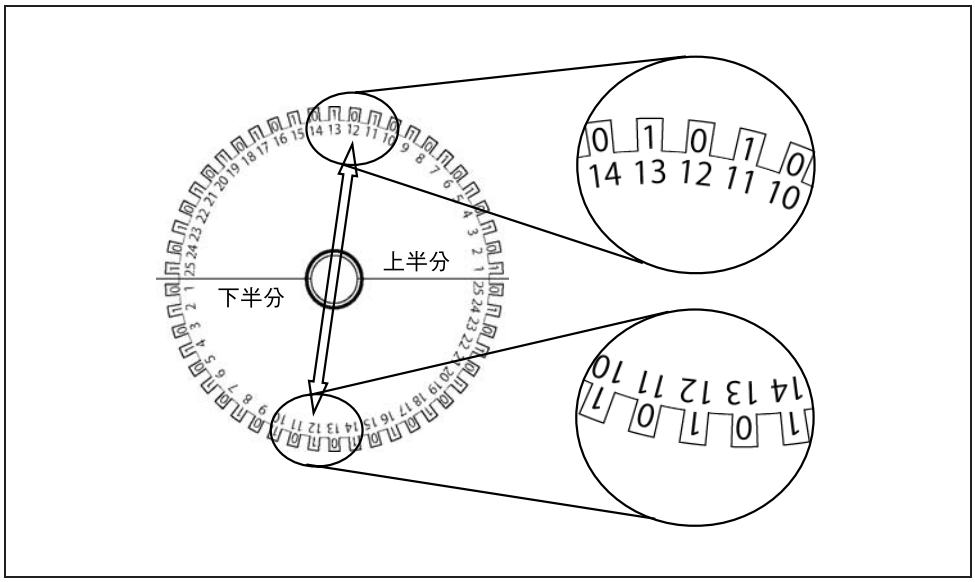
歯が 50 枚ある歯車を考えてもらいたい。歯の 1 枚 1 枚に 1 または 0 の数字が書かれており、その数字は次のような決まりに従っているとする。

① 隣り合った歯に書かれている数字は必ず異なる
② 180 度反対側にある歯には異なる数字が書かれている

次に歯車の歯に通し番号を付ける。歯車を上半分と下半分に分け、上半分に 1 番から 25 番までの番号を付け、下半分にも同じように番号を付ける。この際、上半分の 1 の 180 度反対側に同じく 1 を付け、そこから順番に上半分の番号の 180 度反対側には同じ番号が書かれるようにする。このとき、例えば上半分の 12 番の番号がついた歯に 0 の数字が書かれていたとすると、11 番は 1、13 番も 1 になっており、180 度反対側の下半分の 12 番の歯にも 1 が書かれていることになる（図 19 参照）。こうした歯車を何枚も連ねたものを考える。

この歯車を多数使ってアリスはボブに情報を送ることにする。歯車は中央に穴が空いており、その穴に 1 本の棒を通して多数の歯車を連ね、それを物理的に輸送するのである。1 枚の歯車が 1 ビット分の情報に相当するため、日本語で 10 文字分の情報を送る場合は 160 枚の歯車を使う必要がある。アリスは、送る情報が 1 か 0 かに従って、1 または 0 が書かれている歯の部分を真上に向けて歯車を次々と棒に通し、必要な枚数を全て通してボブに送る。ここで、歯車と棒はしっかり固定されておらず、輸送の最中に少しずつ動いてしまうと仮定する。しかも、おのおのの歯車がばらばらに動き、受け取ったときには最初にどの歯が上向きにセットされていたのかがわからなってしまう（ただし、動くのは歯が数枚分程度とし、歯車の上下が逆になってしまうようなことは、ないものとする）。しかし、これでは受け取ったボブも情報を読み取ることができない。このため、予めボブとアリスの間で、どの番号の歯で情報を送るのかを取り決めておく。例えば、16—5—23—19—……の順番というような具合になる。アリスは情報を送る際、上半分と下半分に 1 つずつある通し番号 16 番の歯のうち、送りたい情報（1 もしくは 0）に一致する方の歯を選ん

図 19　通し番号と「1」「0」が書かれた歯車

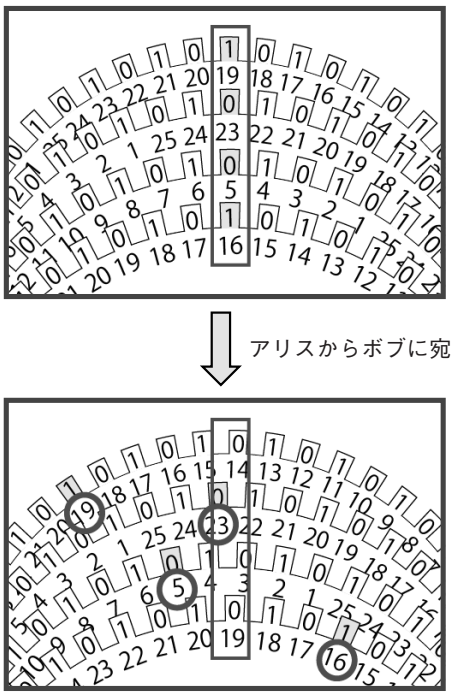


で真上に向けてセットし、次は 5 番の歯を使ってセットする。このようにセットする番号を決めておくと、届いたとき少々歯の位置がずれていたとしても、ボブは本来セットされている位置の近くにある予め決めておいた番号の歯を見て情報を正確に読み取ることができる。途中で盗聴したイブは、どの番号の歯を使うか知らないため、全く情報を入手することができない（図 20 参照）。

歯車が運ぶ途中で動いてしまい、正確に読み取ることができないというのが前述の量子雑音に相当し、歯車の歯をアリスがボブに送る光子の位相あるいは光の強度に置き換えたのが Y-00 である。もっとも、実際には歯車つまり光子の位相や強度が通信の途中で変化してしまうわけではなく、量子雑音により正確に測定することができず、変化したようにみえるのである。量子雑音は量子自体の性質により発生するものであり、規則性がなく打ち消すこともできないため、元の情報に乱数を加えたような効果が出る。

BB84 は「量子は観測すると状態が変わってしまい、元の状態を再現することができない」という性質を使い、盗聴されたら必ずわかる仕組みを実現しようとするものである。これに対して、Y-00 は「量子雑音により量子の状態を正確に測定することができない」という性質を使い、盗聴されているかどうかはわからないものの、鍵を知らない盗聴者は暗号文を正しく入手できない仕組みを実現しようとするものである。

図 20　歯車を使って情報を伝える



（9）BB84 と Y-00

BB84 では、送りたい情報をそのまま送ることはできない。あくまで、バーナム暗号やその他の暗号で使う鍵を共有することができる方式だ。このため、データを送信するには量子通信路のほかに通常の暗号化を行う通信路が必要になる。また、通信速度（鍵の共有速度）が極端に小さく、大容量の通信を行う用途には向いていない。

一方 Y-00 は、送りたい情報をそのまま相手に送ることができる。さらに、現在一般的に利用されている光通信の中継機器が利用でき、通信速度も非常に高速である。

このように比べると、Y-00 が優れているようにみえるが、安全性の面についてはどうだろうか。BB84 は前述のとおり無条件安全性が証明されているが、Y-00 方式は今のところ無条件安全性は証明されていない。本件に関しては日本の学者による「Y-00 方式の安全性は従来の暗号と同程度の計算量的安全性に過ぎない」との主張（Nishioka *et al.* [2004, 2005]）もあり、安全性をめぐる議論は結論をみていないのが実情だ。したがって、本来量子暗号に求めていた「絶対に盗聴できないことが理論的に証明されている通信（暗号）」という意味では、現時点では BB84 に軍配が上がる。また、Y-00 はアリスとボブが鍵を共有する必要があり、鍵が第三者に漏れたと

きには盗聴が可能になってしまう。この意味では鍵の管理をしっかりと行うことの重要性は現在の暗号と変わらない。

もっとも、通信の一連の流れを考えた場合、BB84 であれば鍵の管理が不要であり、理想の暗号通信が実現できるかというと、そうでもないようだ。後述するように、事前に何らかの情報を交換しておき、相手の認証を行う必要がある。

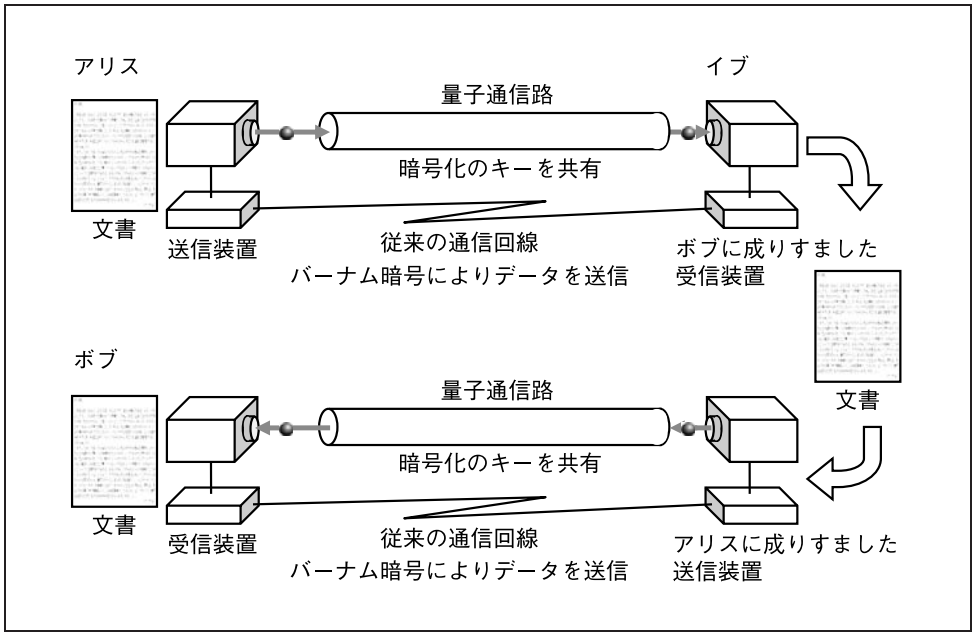
5. 秘密を守るためには

通信の秘密を守るに当たって、通信系路上での盗聴や解読を防ぐことは最も重要な点であるが、このほかにもう 1 つ重要なことがある。

アリスとボブが通信を行う場合、通常 2 人は遠く離れた所におり、直接顔を見て確認することができない。このため、相手がボブだと思って送ったところ、実は相手がイブであるかもしれない。相手を確認しないと、図 21 のようにイブが光ケーブルを途中で切断して受信機と送信機を付け、ボブおよびアリスに成りすまして、盗聴ができてしまう。このため、アリスとボブは通信している相手が正しい相手であることを確認することが必要になる。

相手の認証を行うには、通常、当事者しか知らない秘密の情報を使う。BB84 においても、予め共有した数百ビットの鍵によってメッセージ認証を行う。Y-00 であれば、予め共通鍵を交換しているため、それを用いて通信が行えることで相手を認証できる。しかし、ネットワークの規模が大きく通信相手が多い場合には鍵の管理が

図 21　相手の確認を行わないケース



煩雑になる。インターネットではRSA暗号等の公開鍵暗号方式が使われるが、極めて高い計算能力を持つ量子コンピューターの登場を考えると、より強固な別の方式、すなわち量子の性質を利用した全く新しい認証の方式や、量子コンピューターを利用しても破れないような新しい公開鍵暗号方式等が必要である。前述のとおりRSA暗号では、2つの素数を掛け合わせて公開鍵を作成する計算は比較的簡単だが、公開鍵を2つの数の積に分解（素因数分解）して秘密鍵を導き出す計算は極めて難しいという性質を用いて鍵の安全性を守っているが、量子コンピューターを相手にする場合には、公開鍵を作成する計算にも量子コンピューターを用いなければならないようなものを考える必要があろう。公開鍵から秘密鍵を導き出す計算はそれよりも遥かに多くの計算量を要し、量子コンピューターを用いても計算に何万年もかかるようなものでなければならない。現状では、こうした公開鍵暗号のアイディアが議論されている段階ではあるが（Okamoto, Tanaka, and Uchiyama [2000]）、将来的に量子暗号がインターネットのような大規模ネットワークで活用されるようになるためには、現在インターネットにおいて利用されている認証基盤であるPKI（Public Key Infrastructure）の代わりに、量子コンピューターや量子暗号の時代においても通用する新たなインフラの整備が必要となると考えられる。

6. 量子暗号を実装した製品

量子暗号を実現する製品は既に何種類か入手が可能だ。海外の主な製品をみると、米MagiQ Technologies, Inc.[18]のQPN Security Gateway 8505、スイスid Quantique SA[19]のCerberis、仏SmartQuantum[20]のSQBox Defenderなどが挙げられる。日本勢では、三菱電機、NEC、NTT、東芝欧州研究所、日立情報通信エンジニアリング等のメーカーのほか、政府系研究機関、大学において研究が進められており、一部には製品として入手可能なものもある。

日立情報通信エンジニアリングはY-00プロトコルにより通信データそのものを暗号化して伝送する方式を採用している。それ以外は、BB84など単一光子を利用する量子鍵共有方式を採用している。なお、BB84等を採用している製品では、データ暗号化用としてAESやTriple-DES等、現在広く使われている共通鍵暗号方式と組み合わせて利用できるようになっており、情報理論的安全性は実現できなくなるものの、高速な通信にも対応可能な仕様となっている。

現状では①量子通信経路の中継が難しいこと、②量子コンピューターの実用化にはまだ時間がかかり、従来の暗号により安全性確保が可能と考えられており、投資に見合う効果を期待できそうもないこと、③通信可能距離がファイバー長にして50〜100 km程度と短いことなどから量子暗号は本格的な実用化には至っておらず、軍や

18 http://www.magiqtech.com/
19 http://www.idquantique.com/
20 http://www.smartquantum.com/SmartQuantum.html

政府など可能な限り高いセキュリティを求める先や一部先進的なユーザーが、小規模なネットワークへ適用したり将来のネットワークのテストベッドとして導入したりしているに過ぎない。近い将来では、比較的近距離に設置されているコンピューターセンターと、バックアップセンターもしくはストレージセンターとの間の接続や、機密事項を扱う研究室間をつなぐネットワーク、センター内における SAN（Storage Area Network）、雑居ビルの異なるフロア間を接続するネットワークなどの用途が想定される。

7. 量子暗号普及への取組み

現在手に入る製品は量子暗号鍵共有の速度が低く、情報理論的に安全なバーナム暗号との併用では用途が限定される。通信距離の長距離化と通信速度の高速化については各国の研究機関や大学で実験や研究が進められており、日本においてもこれまで、産業技術総合研究所（AIST）[21]や、三菱電機、NTT などがフィールドでの試験を行い、次第に長距離、高速での鍵交換が可能になってきた。また、量子の中継技術についても研究が進んでいる。

こうした中、2008 年 10 月 8 日から 10 日にかけ、オーストリアのウィーンにおいて SECOQC（development of a global network for SEcure COmmunication based on Quantum Cryptography）[22]が主催する Network Demonstration Scientific Conference が開催され、オーストリアのウィーン市内 4 ヵ所とザンクトペルテン（St. Pölten）の計 5 ヵ所を商用の光ファイバーケーブルで結んだ、最長 85 km の量子暗号鍵配送バックボーン・ネットワークのデモンストレーションが行われた。こうした大規模なフィールド実験は初めての試みである。このバックボーン・ネットワークを通じて共有された鍵を利用して音声通信やビデオ会議が行われ、その模様を録画したビデオがインターネットで公開されている。このほか、光ファイバー等を使わずに量子暗号通信を行おうという試みもみられる。空気中を伝送しようというもので、夜間ばかりでなく日中においても通信に成功したとの報告がある（Kurtsiefer [2008]）。天候状況に左右されるものの、仮設の拠点との通信への応用や、人工衛星を活用した量子暗号通信への応用が考えられる。NICT[23]では「Space Quest」[24]と題して人工衛星を活用した量子暗号通信の実証実験を計画中（豊嶋ほか［2006］）。今後とも目

21 http://www.aist.go.jp/

22 EU（ヨーロッパ連合）における量子暗号通信の推進プロジェクト。元々は ECHELON（米国が中心になって作られた軍事目的の通信傍受システムで、世界中のあらゆる通信を盗聴しているといわれているが、詳細は不明）等の諜報活動からヨーロッパの通信を守ろうということで絶対に盗聴できない暗号を求めて始まったとされる。プロジェクトは 2004 年にスタートした。http://www.secoqc.net/

23 National Institute of Information and Communications Technology: 独立行政法人情報通信研究機構。http://www.nict.go.jp/

24 人工衛星を利用して長距離での単一光子量子暗号通信実験やエンタングルメントの確認試験を行うプロジェクト。衛星―地上間における長距離量子暗号鍵配送の実証を行い、将来のグローバルな量子ネットワーク構築を目指す。

が離せない状況が続くと思われる。

現在のインターネットは、通信量が急速に増加する中で、プロトコルそのものが限界を迎えつつある。具体的には、①回線遅延の影響により一定以上スループットが上がらない、②用途ごとに通信の優先制御を行うことができない、③参加者の認証が十分ではなくフィッシング詐欺等への抵抗力が小さい、④ネットワークの管理が個々のプロバイダに任せられており設定ミスがネットワーク全体に波及するリスクがあるなどの問題が挙げられる。これらは、プロトコルの設計が古くネットワークの拡大や攻撃手法の高度化に対応できなくなった結果、深刻化した問題である。また AS 番号および IP アドレスが枯渇しネットワーク拡張に制約が出ているなど、ネットワークの構造自体も早晩限界を迎えるといわれており、Future Internet 実現に向けた検討が各国で開始されている。米国における GENI（Global Environment for Network Innovations）プロジェクト、欧州における GÉANT2 プロジェクトでは、国家的プロジェクトとして巨費を投じて研究が進められている。わが国でも NICT および関連分野の企業、有識者、総務省が 2007 年 11 月に「新世代ネットワーク推進フォーラム」[25]を設立して本格的な検討を開始した。これらプロジェクトにおける検討では、TCP/IP プロトコルをベースに構成されている現在のインターネットの発想から離れ、白紙から（Clean Slate）考え直すことを基本方針としている。今は構想を固めている段階であり、個別技術に関する検討は今後活発化が予想される。こうした構想では 2020 年以降の技術水準を見通して検討することが求められるため、現在利用している、あるいは近々利用が開始される暗号技術に関しては既に陳腐化していることも想定して技術に関する検討を行う必要がある。こうした中で、量子暗号は盗聴防止の要素技術の候補となると考えられている。

8. おわりに

従来の暗号による通信では、暗号化および復号のプロセスと通信経路とは無関係であり、暗号化したデータを高速な回線を利用して地球の裏側まで送ることもできる。1 ビットの情報を運ぶために何千万個の光子でも使うことができ、仮に途中で大多数の光子が失われたとしても問題なく通信が可能である。一方 BB84 等単一光子を利用する量子暗号（量子鍵共有方式）は、鍵生成のプロセスが通信経路と密接に関係しており、1 ビットの情報を送るのに 1 個の光子のみを使う。これは途中で半分の光子が失われるとボブに届く情報が半分になることを意味し、長距離になるに連れてボブに届く情報が少なくなることから、通信速度が大幅に制限されてしまう。また、一定の距離を超えると全く情報が届かなくなる。このため通信距離や通信速度に限界が存在し、距離や速度を成果として強調する報道となっていたのである。こうした制約の見返りとしてのメリットは、途中での盗聴が不可能であること

25 http://forum.nwgn.jp/

が理論的に証明されているという情報理論的安全性である。同じく情報理論的に安全なバーナム暗号と組み合わせることにより、鍵配送から文書の送信まで情報理論的に安全な通信が行えることになる。

BB84 等の量子鍵共有方式は接続相手を確認（認証）済みの通信経路において情報理論的な安全性を確保できる。今後どれだけコンピューターの計算能力が増大しても盗聴リスクや解読リスクが増大することがない暗号方式という面では非常に有用であり、何にもまして高い安全性が求められる場面で活用されていくと思われる。しかし、その守備範囲は暗号鍵の生成と配送（共有）に限られ、それ以外の、通信データの暗号化、相手の認証、機器の中における情報の秘匿等は従来の方式を使うことになる。またセキュリティの確保においては、機器や暗号方式以上に運用等人的な面の対応が重要になる。したがって、現在のシステムに量子暗号を組み込み、「最強の暗号を利用することで最強のセキュリティを手にすることができる」と考えるのは早計である。暗号により機密を保持するシステムにおいては、どこか１ヵ所でも脆弱な部分が存在すると、システム全体のセキュリティがその部分に引きずられて低下し、十分な機密を確保できなくなってしまう。このことは、逆にどこか１ヵ所のみ完璧なセキュリティを実現したとしてもシステム全体のセキュリティが飛躍的に向上するわけではないことを意味する。場合によっては逆にリスクが増大してしまうこともありうる。また、量子暗号を使用することが最良の選択になるとも限らない。鍵共有にかかる時間や通信効率、インフラ整備にかかるコスト、運用の妥当性等も加味して総合的に判断する必要があろう。

量子暗号は「夢の暗号方式」として取り上げられることもあり、高い期待が寄せられているが、その機能を最大限活かすためには、認証機能や鍵の保管方法・運用方法等も含めたシステム全体にバランスよく対策を講じていくことが必要であり、そうしてこそ「夢の暗号システム」の完成となる。今後通信距離の長距離化や通信速度の高速化に加えて、量子状態を長期間保存する技術や量子を応用した認証方法の開発等により量子暗号の応用範囲が広がっていくと予想されるが、それらがどういった用途に向いており、どういった用途には使えないのかといった点を冷静に評価することが必要である。「最新の科学理論を応用した」とか、「究極の暗号方式を採用した」といった宣伝文句に惑わされることなく、新しい暗号技術をシステムに組み込むことにより、どういったリスクが軽減されるのか、それ以外のリスクに関してはどうなのかといった分析を十分に行い、トータルのセキュリティレベルを虚心坦懐に評価し把握するよう心がけていくことが大切であろう。

参考文献

独立行政法人情報通信研究機構・独立行政法人情報処理推進機構、「CRYPTREC Report 2006」、独立行政法人情報通信研究機構・独立行政法人情報処理推進機構、2007 年 3 月

豊嶋守生・ヴェルナ、クラウス・國森裕生・藤原幹生・佐々木雅英、「日本における宇宙量子暗号通信の研究開発について」、第 22 回宇宙利用シンポジウムプロシーディング、宇宙航空研究開発機構宇宙科学研究本部、2006 年、110～113 頁

内閣官房情報セキュリティセンター、「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 および RSA1024 に係る移行指針」、内閣官房情報セキュリティセンター、2008 年 4 月

Bennett, Charles H., "Quantum Cryptography Using Any Two Nonorthogonal States," *Physical Review Letters,* 68 (21), American Physical Society, 1992.

———, and Gilles Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of the IEEE International Conference on Computers, Systems & Signal Processing,* Bangalore, India, 1984.

Ekert, Artur K., "Quantum Cryptography Based on Bell's Theorem," *Physical Review Letters,* 67 (6), American Physical Society, 1991.

Kurtsiefer, Christian, "Status of R&D on Quantum Communication and Related Research in Singapore," *Proceedings of the Updating Quantum Cryptography 2008,* AIST, IPA, NICT, December 2008.

Nishioka, Tsuyoshi, Toshio Hasegawa, Hirokazu Ishizuka, Kentaro Imafuku, and Hideki Imai, "How Much Security Does Y-00 Protocol Provide Us?" *Physics Letters A,* 327 (1), June 2004, pp. 28–32.

———, ———, ———, ———, and ———, 'Reply to: "Comment on: 'How Much Security Does Y-00 Protocol Provide Us?'" [Phys. Lett. A 346 (2005) 1],' *Physics Letters A,* 346 (1-3), 10 October 2005, pp. 7–16.

Okamoto, Tatsuaki, Keisuke Tanaka, and Shigenori Uchiyama, "Quantum Public-Key Cryptosystems," *Proceedings of the CRYPTO2000,* Lecture Notes in Computer Science, 1880, Springer-Verlag, 2000, pp. 147–165.

Walborn, Stephen P., Marcelo O. Terra Cunha, Sebastião Pádua, and Carlos H. Monken, "Double-Slit Quantum Eraser," *Physical Review A,* 65, 033818, American Physical Society, 2002.

Wang, Xiaoyun, Yiqun Lisa Yin, and Hongbo Yu, "Finding Collisions in the Full SHA-1," *Proceedings of the CRYPTO2005,* Lecture Notes in Computer Science, 3621, Springer, 2005 (available at http://people.csail.mit.edu/yiqun/SHA1AttackProceedingVersion.pdf).