量子暗号

江崎　ひろみ[*1]

Quantum cryptography

Hiromi Ezaki[*1]

Quantum cryptography is a new method for secret communications using quantum mechanics principles, which is never broken by intruders even with a quantum computer.　In this paper, the aouthor briefly reviews history of cryptography and show core principles of the quantum cryptography by giving the example of Bennet-Brassard 1984 protocol.

はじめに

近年、インターネット等により様々なオンライン・サービスが提供されているが、そこで取り扱われるデータの安全性を確保するための技術が暗号である。当初、暗号は外交や軍事上の必要性から開発されたものであるが、インターネットの普及に伴い、オンラインバンキングやクレジットカードの認証等、日常生活に欠かせない技術となっている。現在広く利用されている暗号は、既存のスーパーコンピューターでは現実的な時間で解読できないことが安全性の根拠となっている。しかし、量子コンピュータを用いると、現行の暗号が破られる可能性があることが示された[1)]。そこで、量子コンピュータをもってしても破られない暗号が必要となってくる。そのような暗号の一つの候補が量子暗号である。本論文では、暗号の歴史を手短に概観した後に、量子暗号とはどのようなものかについて述べ、1984 年に提案された最古の量子暗号であり実用上の研究が最も進んでいるベネット-ブラッサード 1984 (BB84 プロトコル)[2)]を例にとって説明する。

暗号の仕組み

暗号とは、データを第三者に盗聴や改ざんされないように、一定の規則に基づいて変換する技術をいい、その変換の規則を「暗号鍵」という。送信者は暗号化鍵を用いてデータを暗号化して送信し、受信者は暗号化鍵に対応する復号合鍵を用いて受信したデータから復号する。暗号を利用した通信を行うためには、送信者と受信者で鍵を共有する必要がある。その仕組みによって、共通鍵暗号と公開鍵暗号の 2 種類がある。

共通鍵暗号は、暗号化と復号を同じ鍵で行うものである。暗号の歴史は古く、紀元前のギリシャの時代から使われていたが、1970 年代の前半まではすべて共通鍵暗号が用いられていた。たとえば、古代ローマの英雄、シーザーはアルファベットをずらして暗号文を作成していたそうである[3)]。何文字ずらすか、送信者と受信者であらかじめ決めておけば、秘密裏に通信を行うことができるわけである。しかし、アルファベットは 26 文字しかないので、暗号パターンは 25 通りしかなく、25 パターンを総当たりに調べればすぐに解読できてしまう。

その後、主に軍事上の必要性から解読不可能な暗号を目指して暗号技術は改良を重ねていった。その頂点ともいえるのが、第一次世界大戦後にドイツが開発した機械式暗号機「エニグマ」である。エニグマは「スクランブラー」と呼ばれる歯車の組み合わせでできた鍵によって、自動的に暗号化する機械である。送信者が「スクランブラー」を設定してキーボードをタイプすると自動的に暗号化された文章が出力される。受信者が暗号文を復号するときは、「スクランブラー」の設定を暗号化されたときと同じにして、暗号文をエニグマのキーボードで入力すれば、平文が出力されるという仕組みである。ドイツ軍が使用していたエニグマには「スクランブラー」は 3 個～5 個あり、他の工夫も施され、エニグマは解読不可能と思われた。

このエニグマを解読したのが、数学者のアラン・チューニングである。解読には「スクランブラー」の位置を割り出すことが文字通り鍵となる。チューリングはボンブと呼ばれる機械を開発して、この「鍵」を探り出すことに成功し、1940 年にエニグマの暗号解読に成功した。チューリングは「チューリングマシン」で知られるように、現代のコンピュータの基礎を築いた人物であり、この頃から暗号を解読することを主な目的として、コンピュータが競って開発されるようになった。

さて、先に述べたように、「エニグマ」も含め、1970 年代の前半までは共通鍵暗号が用いられていた。共通鍵暗号は、通信に先立って共通鍵を共有する必要があり、これは 1 対 1 の通信には向いているが、多数間の通信には不便である。第二次世界大戦までは、暗号は国家や軍などの限られた人間の間で使用するものであったため、共通鍵暗号で何ら問題はなかったが、1959 年に IC(集積回路)が発明され、コンピュータが民間にも普及するようになると、大勢の人々が暗号を介した通信を必要とするようになった。そ

[*1] 東京工芸大学工学部工学科電気電子コース 教授
2022 年 9 月 16 日 受理

こで登場したのが、公開鍵暗号である。

公開鍵暗号は、暗号化鍵と復号鍵とが異なる方式であり、暗号化鍵を公開することで、多数間の通信でいかに秘密裡に共通鍵を共有するかという難問に逆転の発想で解決した方式といえる。公開鍵暗号の仕組みは以下の通りである。まず、送信者が受信者に秘密に文書を送りたいときには、送信者は受信者が公開している鍵（公開鍵）を使って文書を暗号化する。受信者は公開鍵に対する秘密鍵を使って文書を復号化するというわけである。公開鍵と秘密鍵は対になっており、逆に秘密鍵で暗号化した文書は公開鍵でしか復号できなくなっている。公開鍵暗号の安全性は、公開鍵から秘密鍵を現実的な時間では求められないことで保障されている。たとえば、代表的な公開鍵暗号である RSA 暗号は、素因数分解問題を利用している。素因数分解は桁数の大きな 2 つの素数の積から元の素数を求めるものである。たとえば、187=11×17 のように分解できる。これは単純な例だが、桁数が大きくなると飛躍的に計算量が増加し、現在用いられている 600 桁程度の数に対しては、最速のスーパーコンピュータをもってしても現実的な時間で求められないことが知られている。この安全性を担保として、現在 RSA 暗号は広くオンライン・サービスなどに利用されている。

しかし、1994 年に大きな衝撃が走った。ショアが、素因数分解が圧倒的な速さで実行できる量子計算のアルゴリズムを発表し、量子コンピュータが実現すると、RSA 暗号が破られる可能性が出てきたのである [1]。まだ現時点では RSA 暗号を解読できる量子コンピュータは作成されていないが、通信の安全性を保つためには、そのような量子コンピュータが完成する前に、量子コンピュータをもってしても現実的な時間で解けない暗号（耐量子計算機暗号）へ移行する必要がある。そのような耐量子計算機暗号の一つが量子暗号である。次に、BB84 プロトコルを例にとり、量子暗号について説明しよう。

BB84 プロトコル

ベネットとブラッサードは、量子力学固有の性質を利用して、安全に共通鍵を共有する方式を 1984 年に提案した。これが BB84 プロトコルである。BB84 プロトコルは、光子にビット 0,1 の情報を載せて、安全に乱数列（共通鍵）を共有する方式である。一般に、量子暗号とは、この量子共通鍵の共有を呼ぶ。量子鍵を共有することから、量子鍵配送などとも呼ばれる。光は強度を弱めていくと、粒子のような性質を表すようになる。これが光子である。通常の光通信では、ビット 0, 1 を載せるレーザパルスには 1 パルス当たり 10^6 個程度の光子が含まれている（図 1(a)）。これに対して、量子暗号では、光を弱めて 1 パルス当たり 1 個程度の光子しかない状態を作る（図 1(b)）。1 個の光子というところが安全に通信する要である。1 個の光子ごとにビット値 0, 1 をのせて送受信を行うには、光子の偏向状態を利用する。図 2 のように、

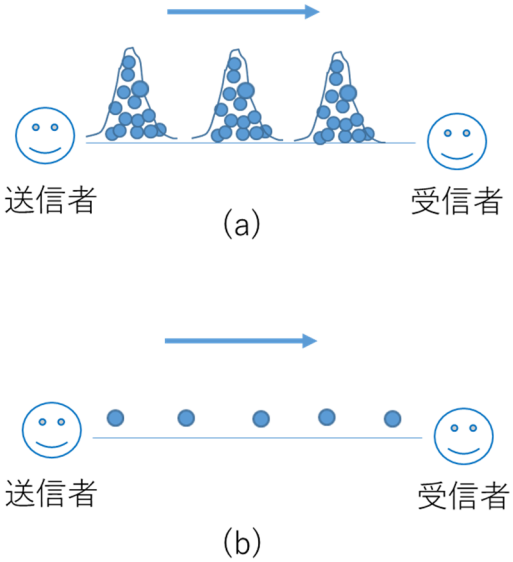

図 1. 通常の光通信(a)と量子暗号(b)。通常では、1 つのパルスに非常に多数の光子が含まれているが、量子暗号では、単一の光子にビットの情報を載せて送信する。

光の進行方向に対して 0°、90°方向に振動（Z 基底と呼ぶ）する光パルスと、45°、135°方向に振動（X 基底と呼ぶ）する光パルスにそれぞれビット値 0, 1 をあてはめる。

ビット値	0	1
Z基底	↕	↔
X基底	↗	↘

図 2. 2 つの基底とビット値の対応。

このように、2 つの基底を使用し、かつ、単一光子を使うことによって、盗聴不可能な通信が実現される。もし、1 つのパルス中の光子数が多ければ、測定によって 4 つの振動方向を特定することが可能である。しかし、単一光子であれば、測定によって光子の状態が変化してしまうため、4 つの振動方向を特定することは不可能である。例えば、0°方向に振動する光パルスを X 基底で測定すると、50%の確率でビット値は 0 または 1 となって特定できない。さらに、測定によって、ビット値 0 の場合は 45°方向に、ビット値 1 の場合は 135°方向に振動する状態に、光子の状態は変化してしまうため、元の光子の状態は失われてしまう。後で示すように、これが安全に量子鍵を共有するため

の要となっている。
ただし、1つの基底しか用いないと、単一光子であってもビット値を測定で特定できてしまうため、2つの基底を用いることが重要である。例えば、Z基底で0,1に符号化した光子を、同じZ基底で測定すれば、確実に正しいビット値 0,1 が得られ、かつ光子の状態は変わらない。そこで、測定後の光子を送信すれば、盗聴が可能となる。

それでは、具体的にBB84プロトコルをみていこう。
まず、盗聴者がいない場合を考えよう。送信者アリスは受信者ボブに、光子にビット値を符号化して送る。その際、ランダムに基底を選んで送信する（図3）。

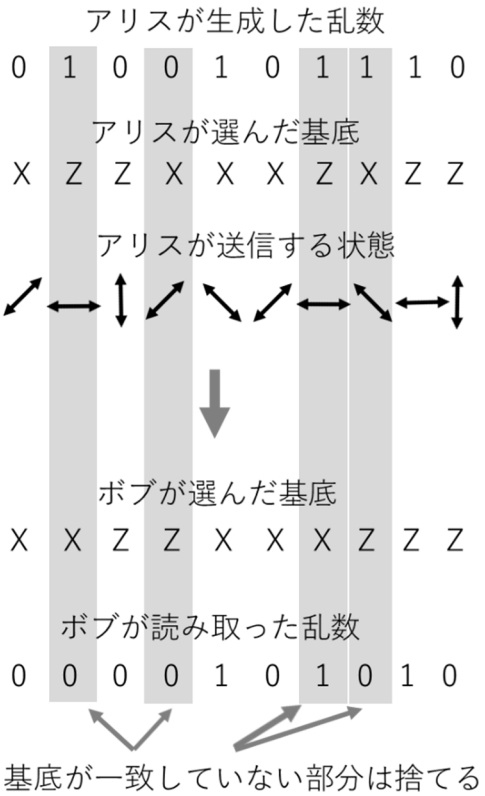

図3. 盗聴者がいない場合の量子鍵配送。

この図では、アリスは 0100101110 という乱数を選び、それぞれに基底 XZZXXXZXZZ を選んで送信する。アリスが送信する光子の状態は図3の3行目の状態である。光子を受け取ったボブは XXZZXXXZZZ という基底を選んで測定する。その結果、得られたビット値が 0000101010 である。ボブは光子を測定した後に、電話などの古典回線を使って、お互いがどのような基底を選んだかを伝え合う。基底が違った場合には、図の影の部分のように違ったビット値になったり、50%の確率で同じになったりするが、同じ基底を使った場合には100%の確率で二人のビット値は一致することになる。この一致した乱数列 001010 を暗号の共通鍵とするわけである。このようにすれば、たとえ基底のやり取りの部分を盗聴されても、それだけではビット値はわからないので、安全に鍵を共有することができる。

次に、盗聴者イブが存在する場合を考えよう。先ほどの図にイブを加えると見づらくなるので、盗聴を検出できる部分だけをわかりやすく取り出したものが図4である。イブは何らかの方法でアリスが送った光子を送信途中で読み取り、その結果をボブに送信する。その際、アリスはX基底を用いてビット値 1 を送ったとする。イブはアリスの用いた基底はわからないので、それとは異なるZ基底を用いて光子を測定すると、光子の状態は変わってしまい、それを受け取ったボブはアリスと同じ X 基底を用いて測定してもアリスとは異なったビット値 0 を得てしまう。

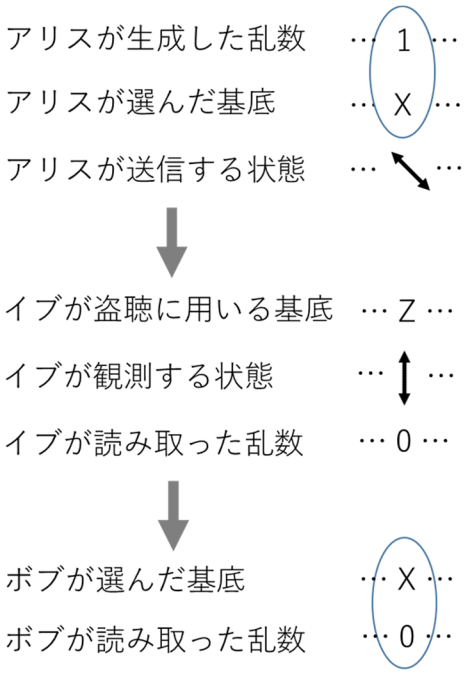

図4. 盗聴者イブがいる場合の量子鍵配送。

送信が終わった後で、選んだ基底を照らし合わせてみると、同じ基底を選んだにも関わらず、ビット値が異なるという状況になる。これにより盗聴者の存在が明らかになるわけである。もちろん、得られたビット値すべてをお互いに古典回線で問い合わせたりしたら、量子暗号を用いる意味がなくなってしまう。そこで、実際には、得られたビット値の一部を照合して盗聴者がいないかチェックし、いない場合は残りのビット値を秘密鍵として使用するというやり方をしている。また、ここでは触れなかったが、実際の通信では盗聴者がいなくても通信路の雑音によりエラーが生ずるため、誤り率の変化をチェックすることにより盗聴の検出を行っている[4]。

量子暗号の現状

BB84 プロトコルの実証実験は、提案者自らによって1989 年に IBM の研究室において行われた。当初、送信者と受信者の距離はわずか30cm ほどであったそうである[5]。先に述べたように、BB84 プロトコルでは、１つの光子にビット情報をのせることが安全性を保証する要であった。そのため、光源には厳密な単一光子源が必要であり、検出には単一光子検出装置が必須と考えられてきた。単一光子源や単一光子検出装置は今でも難しい課題であり、これが量子暗号実現のネックとなっていた。しかし、その代替装置として使用されていたレーザと減衰器、アバランシェフォトダイオードによって検出しても安全性が保証されることが証明され、2000 年代には世界中で実証実験が行われるようになった。

2010 年頃には通信距離 50km、通信速度 1Mbps が NEC や東芝欧州研など複数の研究機関によって実現されるようになった。このような実証実験だけでなく、すでに 2000 年代前半には、スイスの ID Quantique 社、中国の QuantumCTek 社などベンチャー企業も複数存在しており、量子暗号装置は市販されるようになっている。最近では中国の躍進が目覚ましく、2017 年に北京、済南、合肥、上海をつなぐ長さ 2000km の量子通信ネットワークを完成させると、2020 年には、そのネットワークと衛星をつないで 4600km の量子通信ネットワーク実験に成功している。

量子コンピュータによって現行の暗号が破られることは、個人の情報保護レベルにとどまらず、国家の安全上の危機でもある。そのため、アメリカ、欧州、中国では、国策として量子暗号研究が進められてきている。例えば、米連邦政府は、RSA 暗号を数時間で解読できる量子コンピュータが 2030 年頃までに実現する可能性があるとの見解を示している。その上で、2026 年頃までに耐量子計算機暗号へ移行する計画だそうである[6]。日本でも、独立行政法人情報通信研究機構(NICT)が NEC、三菱電機株式会社、NTT と共に、2010 年に量子暗号ネットワークの試験運用を開始している。さらに、東芝が通信距離 45km、通信速度 3Mbps の通信装置を完成させるなど、盛んに研究が行われている。

おわりに

ここで紹介した量子暗号は、その安全性を量子力学の物理法則に因っているため、量子力学が正しい限り、量子コンピュータをもってしても破られない方法である。BB84 プロトコルは最初に提案された量子暗号であるが、現在でも BB84 の改良版が標準方式となっている。このように最強の暗号といえる量子暗号だが、実用面では課題も多い。量子暗号はその仕組みから、1 対 1 の秘密通信に適した方式となっている。多数間の通信において、鍵配送をどのように効率よく行うか、そのコストの問題など、解決すべき問題は多い。したがって、当面は、軍事、外交、金融などの限られた当事者間の秘密通信に量子暗号は限定されると考えられる。

しかし、一方で量子コンピュータが実用化されれば、既存の暗号の安全性が脅かされるため、耐量子計算機暗号は一般市民レベルでも重要である。このため、量子暗号以外に耐量子計算機暗号を探求する研究も盛んに行われている。それは“ポスト量子暗号”と呼ばれており、多変数多項式暗号など、量子コンピュータによっても解読不可能と期待できる方式がいくつか提案されている[7]。

最後に、量子暗号は、これまで原子・分子などのミクロな世界にのみ適用される“特異な力学”と考えられてきた量子力学を日常の技術に応用した最初の例といえる。量子暗号を先陣として、量子コンピュータ、量子テレポーテーション、量子計測など、いわゆる量子情報と呼ばれる分野が確立されてきている。20 世紀は量子力学が生れ、発展した世紀だったが、21 世紀は量子暗号や量子コンピュータなどの量子力学を基礎とする技術が、日常生活において当たり前の時代となるだろう。

参考文献

1) P. W. Shor, in Proceeding of the 35th Annual Symposium on Foundation of Computer Science, IEEE Computer Society Press, pp.124-134 (1994).
2) C. H. Bennet and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), p.175.
3) 中西　啓, 暗号と暗号史, https://www.hummingheads.co.jp/reports/series/ser01/110322.html　2011 年
4) 鶴丸豊広, 映像情報メディア学会誌 **69** (2015) pp.889-897.
5) C. H. Bennet, G. Brassard and A. K. Ekert, Sci. Amer. **257** (1992) 50. 日本語訳が日経サイエンス 12 月号 (1992) 50 にある
6) 四方順司, 金融研究所ディスカッション・ペーパー2019-J-4, 日本銀行金融研究所, 2019 年
7) 高木剛,　IEICE Fundamentals Review, 11, (2017) p.17-27.