量子暗号

鶴丸 豊広†

1. まえがき

量子暗号は、通信を盗聴しようとするどんな盗聴者に対しても盗聴を防止できる安全な暗号方式です。なおこの暗号方式は、これまでこのシリーズで対象としてきた暗号とは違って、まだ一般には普及していない、次世代の暗号方式です。

RSA方式をはじめとする、現在普及している暗号方式（これを以下、現代暗号と呼ぶことにします）は、既存の方式のコンピュータで、既知のアルゴリズムを使ったとしても、人間が想定しうるまともな時間内（例えば、100億年以内）では解読ができないという「予想」（計算量的な仮定）に基づいて安全性が保証されています。例えば、広くつかわれているRSA方式は、素因数分解が効率的に短い時間で実行できないという予想が正しい限りにおいて安全となっています。逆にいうとこれらの方式は、新アルゴリズムや、（量子コンピュータのような）新原理のコンピュータの出現により、ある日突然破られる可能性があります。

量子暗号の場合はこれより一歩進んでいて、安全性の根拠となっているのは予想ではなく物理法則です。そしてその物理法則は量子力学です。もしこの方式が破れたとすると、それは量子力学に反する現象が起こったことを意味します。量子力学がみつかったから100年近くたちますが、いまだにそれに反する現象は報告されていません。例えば、半導体の物性や素粒子の挙動といった具体的な物理現象でも、すべて量子力学と合致した測定結果が得られています。すなわち、仮に新原理のコンピュータが出現したとしても量子力学が変わることはありませんので、量子力学のもとで安全性が保証されている量子暗号は依然として盗聴不可能です。そのためそこで共有した乱数は未来永劫漏えいすることはないと考えられています。

本稿では、量子暗号の概要、現状の課題、および今後の方向性について紹介していきます。とくに既存の暗号方式

を比較対照にして、暗号装置として実際に使う場合のメリットとデメリットについて整理するとともに、その現状のデメリットの解消にむけた取組みについても紹介します。デメリットについて述べる箇所では、量子暗号を否定しているように感じられる内容も含んでいますが、著者の真意は決して量子暗号を否定することではありません。むしろ、このような課題を正面から分析して楽しむことによって、量子暗号研究のさらなる発展に寄与していきたいと考えています。なお量子暗号に関するこれまでの文献では、個々の課題については指摘されているものの、それらをまとめて分析したものは著者の知る限り存在しないようでした。それらをまとめて議論することも、本稿の目的の一つです。

2. 量子暗号の機能と安全性

比較として、現代暗号の機能について思い起こしてみましょう。RSA方式をはじめとする現代暗号方式では、メッセージから暗号文を作ることを目的としています。そして暗号文を自由に複製し、電子メールに添付したり、印刷して封書で送ったりすることができます。また、インターネットで送ることもできます。一方で量子暗号は、このような素朴な暗号方式と二つの意味で異なります。

一つ目の違いとして、量子暗号の役割はメッセージを直接送ることではなく、それを暗号化するために必要な鍵、つまり乱数を安全に送ることにあります。一旦そのような乱数が安全に共有できたら、あとはそれをメッセージと排他的論理和をとる（ワンタイムパッド）ための値や、ブロック暗号の秘密鍵として使えば秘密通信ができるので、「暗号」の名がついています。ただし量子暗号装置自身の機能は、あくまで秘密鍵を共有するところまでです。現代暗号の用語でいうなら、量子暗号の機能は鍵共有のみであり、メッセージの暗号化は別の方式に任せるといえます。ただし現代暗号でも、Diffie-Hellmann (DH) 方式のような鍵共有方式があり、この一つ目の意味だけですと量子暗号特有というほどの特徴ではありません。

二つ目の違いがむしろ量子暗号ならではの特徴です。上述のとおり、量子暗号の目的は乱数を安全に送る/共有す

† 三菱電機株式会社 情報技術総合研究所

"Security Technologies on Image Information (8): Quantum Cryptography" by Toyohiro Tsurumaru (Information Technology R&D Center, Mitsubishi Electric Corporation, Kanagawa)

ることですが、その際、乱数を運ぶための媒体は、インターネットや紙ではだめで、ある物理的性質を持つものでなければなりません。そしてその物理的性質を規定しているのが量子力学です。

またその性質をもつものを量子と呼ぶことがあります。この先の説明においては、量子とは要するに極端に弱めた光のことだと思っても支障はありません。量子暗号では、極端に弱めた光をランダムに変調して(スクランブルをかけて)光ファイバのような光が通る通信路を用いて送受信します。その光が途中で盗聴された場合、量子としての性質により、必ず何らかの変化が起こります。そしてその変化を見ることにより盗聴を検出する、というのが基本的な考え方です。

以下では、この点についてできるだけ詳しく述べていきます。本稿の理解する上で必要になると思い、量子力学についても一部触れています。この部分に興味のない方は3章まで飛んでいただいても、ひととおり意味はわかるようになっています。なお、以下はかなりデフォルメした説明になっていますので、意味不明な箇所もあると思いますが、そのような場所でも立ち止まらずに雰囲気を感じていただきたいと思います。より正確なところを知りたい方は、文献1)等を参照していただきたいと思います。

2.1 量子力学について

どのような物質でも、分子のサイズ以下の微小な精密測定をすると、高校で習うようなニュートン力学や電磁気学とはつじつまが合わない性質を示すということに、100年ほど前のヨーロッパの物理学者が気付きました。そこで、そのつじつまを再度合わせるために登場したのが量子力学です。つまり量子力学は、ニュートン力学や電磁気学といった理論の後継バージョンです。そして、ニュートン力学や電磁気学では説明がつかないが、量子力学では説明のつくような性質のことを量子的な性質と呼びます。量子暗号ではこの量子的な性質を使って、絶対に破れない暗号を実現します。

とくに量子暗号に限っていえば、量子として使うのは原子核でも電子でもなく、もっぱら光だけです。以下に述べるとおり、光の強度を極端に弱めて、さらに2種類の変調方式を使い分けて送受信すると、量子的な性質が表れてきます。とくに量子暗号では、不確定性原理という性質が本質的になります。

2.2 光を弱める

物質を細かく測定する場合は分子レベルの精密測定をするを書きましたが、光の場合はそれが光を弱めることに相当します。これが量子暗号ですべきことのひとつ目です。具体的にどれくらい光を弱めればいいのかについても明確な基準があって、それがエネルギー量子(= $h\nu$ ジュール。ただし ν は光の振動数(毎秒)、 h はプランク定数 $h = 6.63 \times 10^{-34}$ ジュール秒)と呼ばれる量です。量子力学ではこのエネ

図1 量子暗号における光強度

ルギー量子を単位にして光を1個2個…と数えて、その1個ずつを光子と呼びます。量子暗号ではパルスレーザの光を減衰器で弱めて、1つのパルスあたり1個程度の光子しかない状況を作ります(図1)。これは通常的光通信の1/100万分くらいのエネルギーしかない弱い光です。

2.3 2つの変調方式をランダムに使う(スクランブル)

こうして弱めた光パルス1つずつに、乱数ビット値0,1をのせて送受信します。その際に、後で説明する2つの異なる変調方式、X基底とZ基底をランダムに切替えます。これは、盗聴行為を検出しやすくするために、スクランブルをかけることに相当します。量子暗号の用語では、変調方式のことを「基底」と呼びます。そして2種類ある変調方式をそれぞれX基底、Z基底と呼ぶことが多いです。

X基底、Z基底の実装法にはさまざまなやり方がありますが、イメージしやすいのは、光の偏光(振動方向のこと)を使うやり方です。この方法では、進行方向を軸として0°, 90°方向(45°, 135°方向)に振動する光パルスに、ビット値0,1をそれぞれあてはめるのがZ基底(X基底)です。要するに量子暗号では、光を弱めたうえで、1ビット分の情報(0,1)を、4つの状態(振動方向0°, 45°, 90°, 135°)に水増しして送っていることになります。

2.4 不確定性原理

もし通常の通信のように光が充分強ければ、測定によって、これら4つの振動方向を特定できてしまいます。すなわち、充分強い光を弱い光に分離して、4つの測定を行うことで、どの基底が使われ、どのビット値があてはめられているかがわかります。また1種類の変調方式(基底)しか使わなければ、光の強弱に関わらず、やはり乱数ビットを測定で特定できてしまいます。つまり例えば、X基底で0,1に符号化された光子を、同じくX基底で測定した場合を考

図2 盗聴者がいない場合の処理の流れ

えると、常に正しいビット値0,1が測定されます。これらにより盗聴が可能となります。しかし光を弱めて、なおかつスクランブルを行うとすると、乱数ビット0,1の値を確実に測定することは不可能になります。これが通常の電磁気学とは違う、量子論的な性質の一例であり、不確定性原理と呼ばれています。例えば、単一光子にX基底でビット値0,1に符号化したのち、それをZ基底で測定するとします。このときの測定結果は、もとの値0,1に関係ないランダム値0,1になります。なおかつ測定が終了した時点で光子の状態は変化しているので、基底を変えて再度測定し直したとしても、元の値は再現できません。

ここで重要なことは、このような現象が起こるのは、測定装置の性能が足りないからとか、測定の方法に不備があるからという理由によるのではないということです。そうではなく、単一光子を一度測定したら、同じ状態が保持されず、測定をやり直すことができないという状況が、物理法則（量子力学）のために生じています。したがってこの状況は、測定装置の性能がいくら向上しても改善しません。これがニュートン力学とは違う、量子的な性質の一例です。

2.5 BB84 プロトコル

量子暗号ではこの不確定性原理を使って盗聴を検出します。正規の送受信者は、X, Z基底をランダムに振って送受信します。一方で盗聴者は、どの基底が選択されているかを知らずに乱数値を測定せねばなりません。ここで光子を一旦測定してしまうとその状態が変化してしまいます。従いまして、誤った基底で測定をするとその状態を正確に知ることができず、測定しなおすこともできないため、元に戻すことができません。正しい基底で測定していれば、正しい状態がわかるので、同じ状態を持つ光を再送信するこ

とで、同じ状態を作ることが可能です。正規の送受信者は、少なくとも、誤った基底を用いて盗聴された場合の痕跡を検出すれば、盗聴を検出できます。

ここから先は具体的なプロトコルをみた方が速いので、Bennett-Brassard 1984 (BB84) 方式を例にとって話を進めます。この方式は1984年に提案された最古の量子暗号方式であり、これまで最も深く研究されてきた方式でもあり、安全性も厳密に証明されています。

● 使用する通信路

このプロトコルでは、2つの通信路を使います。

- ・量子通信路：乱数を光子にのせて送るためのもので、通常は光ファイバが使われます。盗聴者は、ここを流れる光子を自由に盗聴できるものとします。
- ・認証つき公開通信路：乱数本体ではなく、補助的な情報（選択された基底、サンプルビットの値）を送るためのものです。これらはデジタル信号なので、例えば、インターネットや携帯電話が使えます。盗聴者は通信内容を自由に盗聴できますが、改変はできないとします。改変を防ぐために、通常はWegman-Carter方式と呼ばれる情報理論的なメッセージ認証方式を使います。

● プロトコルの手順

図2もあわせてご覧ください。またこの節では通信における送信者をアリス (Alice)、受信者をボブ (Bob)、盗聴者をイブ (Eve) と呼ぶことにします。

(1) 量子通信：

1-1 アリスは、 m ビットの乱数ビットを、それぞれ個別の光子パルスに、X, Z基底をパルスごとにランダムに選んで変調し、量子通信路を通じてボブに送信します。

1-2 ボブは、X、Z 基底をパルスごとにランダムに選び、受け取ったパルスを測定します。

1-3 アリスとボブはお互いに選択した基底を、公開通信路を使って公開します。お互いの基底が一致したパルスの乱数ビットのみを残し、それらをまとめて生鍵 (raw key) とします。それ以外のビット値は破棄し、以後の処理には使いません。

1-4 生鍵ビットのうち Z 基底のもの (長さ n ビットとする) をまとめて、ふるい鍵 (sifted key) と呼び、X 基底のもの (長さ l ビットとする) をまとめてサンプルビットと呼びます。

(2) サンプルビットの誤り率 p_{smp} の算出：アリスとボブはお互いが X 基底で測定した分 (つまりサンプルビット) を公開し、その誤り率を算出して p_{smp} とします。

(3) 誤り訂正：アリスは k ビットのシンドローム (パリティ情報) を公開します。ボブはそのシンドロームと誤り訂正符号を用いて、自分のふるい鍵の誤りを訂正します。なお訂正されたふるい鍵を、訂正鍵と呼びます。

(4) 秘匿性増強処理：

4-1 秘密鍵長算出：ステップ (2) で算出した p_{smp} をもとに、パラメタ $s = \max[n(1-h_2(\hat{p}_x)) - k - t, 0]$ の値を算出します。これが以下で最終的に生成される秘密鍵の長さです。なおここで $h_2(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ は 2 値エントロピー、 t はある定数です (4.1 節 (1) 参照)。また $\hat{p}_x$ は、ここではひとまず簡単のため、ステップ (2) で算出した p_{smp} と等しい、つまり $\hat{p}_x = p_{\text{smp}}$ だと思ってかまいません (正確にいうと $\hat{p}_x$ は p_{smp} を変数にもつ関数であり、ふるい鍵長が充分大きい ($n \rightarrow \infty$) とき、 $\hat{p}_x \rightarrow p_{\text{smp}}$ に漸近します)。

4-2 ランダム行列乗算：ランダムなビット値をもつ $s \times n$ 行列 M を生成し、それに (3) で出力した訂正鍵を乗算します。そして、その乗算の結果得られた長さ s のビット列を秘密鍵とします。

こうして得られた秘密鍵を、ワンタイムパッドの鍵として使えば、絶対安全な秘密通信ができます。またそれ以外にもメッセージ認証等の秘密鍵として使うこともできます。

● プロトコルの解説

上記の各ステップのここは以下の通りです。

まずステップ (1) の量子通信では、① イブからみると X、Z 基底がランダムに選ばれていて、なおかつ、② アリスとボブの基底選択は一致している、という状況が作りたいわけです。これを安直に実現するには、アリスとボブが予め乱数を共有しておいて、それで基底を選ぶという方法も考えられるのですが、それだと生成する乱数よりも消費する乱数が大きくなって意味がありません。そこで代わりにステップ (1) 1-1 で送りだす光パルス数に無駄を許して、余分

図3 盗聴検出のイメージ

に送りだすという戦略をとります。つまりアリス、ボブが基底を各自勝手にランダムに選び、たまたま基底が一致したパルスの測定結果だけを採用して生鍵とします。また基底が一致しなかったパルスは無視して捨てて (つまり忘れて) いますが、この行為は以下のとおり正当化できます。まず、そもそも送っているのがメッセージではなく乱数なので、捨ててそれ以降決して使わないという運用が可能です。決して使わない情報が盗聴者に漏れたところで実害はありませんので、暗号の安全性としても問題ないのです。

したがって安全性を考える分には、基底が一致しなかった部分は忘れて、生鍵だけを考慮すればよく、そこでは上記の状況①、② が実現できています。そしてその状況が、アリスとボブが Z 基底でふるい鍵を測定している最中に、たまたまランダムなタイミングで X 基底測定を繰り返しているとも解釈できます。イブにしてみれば、この X 基底測定はいわば抜き打ちチェックです。つまり、ふるい鍵の内容を探ろうと Z 基底で盗聴をしている最中に、アリスとボブが突如 X 基底に切替えるわけで、イブはある確率で誤った基底 (Z 基底) の測定を仕掛けることになり、それによりサンプルビット列の誤り率 p_{smp} が増えます (図3)。つまり p_{smp} はイブの盗聴行為の強さに相当しますが、これを検出するのがステップ (2) の役割です。

より定量的には、サンプルビットの誤り率が p_{smp} であれば、盗聴によってイブに $nh_2(p_{\text{smp}})$ ビット程度 (正確には $nh_2(\hat{p}_x)$ ビット) 分の情報が漏洩していると結論できます (安全性証明の理論による)。さらにステップ (3) の誤り訂正で k ビットのシンドロームを公開しているの、ステップ (3) で生成された訂正鍵 n ビットのうち、合計 $nh_2(p_{\text{smp}}) + k$ ビット程度 (正確には $nh_2(\hat{p}_x) + k$ ビット) 分がイブに漏洩していると結論できます。非常に大雑把ないい方をすると訂正鍵には、盗聴者の知っている $nh_2(p_{\text{smp}}) + k$ ビットと、知らない残りの $n - (nh_2(p_{\text{smp}}) + k)$ ビットが混在している状況にあります (図4)。

図4 秘匿性増強の大まかなイメージ

秘匿性増強とは、「大体安全」な暗号鍵を「完全に安全」にする統計処理です(*この図はあくまでイメージです)。

この訂正鍵を暗号通信用の秘密鍵として使うのは明らかに危険です。そこでステップ(4)の秘匿性増強処理では、訂正鍵にランダム行列をかけて搅拌、圧縮することにより、盗聴者が知らない $n-(n h_2(p_{\text{smp}}, \hat{p}_x) + k)$ ビット分だけを取り出しています(図4)。これによって最終的に、厳密な意味で安全な秘密鍵が生成されます。

秘匿性増強のイメージをつかむには、以下の例がわかりやすいと思います。訂正鍵が2ビットあり、どちらかわからないがそのうち1ビットの値が盗聴者に漏れていて、もう1ビットは漏れていないとします。このとき明らかに、その2ビットをXORして1ビットに圧縮してしまえば、その値は盗聴者にもまったくわからなくなります。より一般のビット数の場合には、XORではなくランダム行列を使えばいいことが知られていて、それがいわゆる秘匿性増強です。

なおここでは簡単のため、イブが常にX, Z基底のどちらかで盗聴を行うとして話を進めました。実際の量子暗号の理論ではこのような制約は存在せず、イブが物理法則で許される限りのあらゆる攻撃をしたとしても、安全性が成り立つということが証明できています。

3. 実装の現状

量子暗号の研究は1984年に提案されたBB84方式に始まりました。現在でも、この方式の改良版であるデコイBB84方式が事実上の標準方式になっています。1992年には提案者自らが実証実験に成功し、2000年代には世界中で実験報告が爆発的に増えました。2010年頃には通信距離50 km, 通信速度1 Mbpsといった性能を、NECや東芝欧州研など複数の研究機関が安定して叩き出すようになり今日に至ります。

またこのようなトップスピードとは乖離があるものの、量子暗号の製品を売る企業も複数存在しています。すでに2000年代前半にはベンチャー企業が複数存在していて、そのなかでもスイスのid Quantique社、および中国のQuantumCTek社は現在も活発に活動しています。とくにid Quantique社のある社員によれば、同社にはこれまで

100台程度の販売事例があるといえます(具体的な顧客名は公表されていません)。

2008年に欧州の複数の大学とベンチャー企業が、各々の量子暗号装置を持ちより、ウィーンでネットワーク通信実験を行いました(SECOQCプロジェクト)。つづいて類似のプロジェクトが2010年に東京(Tokyo QKD Network)、2012年に中国の合肥市、2013年に同じく中国の済南市でも実施されました。さらに2013年には米国Battelle社が、id Quantique社の量子暗号装置を複数つなぎ合わせて、全長400 kmの商用量子暗号通信ネットワークをオハイオ州に構築しました。さらに同社は2016年までに、オハイオ州・ワシントンDC間650 kmを結ぶ量子暗号線を構築するとしています。また中国も同じく2016年までに国家プロジェクトとして、上海・合肥・済南・北京の4都市を結ぶ全長2,000 kmの量子暗号ネットワークを構築するとしています。

4. 既存の暗号方式との比較

1990年代以降「量子コンピュータが実現すると公開鍵暗号が破れるのに対し、量子暗号は破れない。そこで量子暗号が必要になる」という宣伝文句が盛んに使われ、実際にそれが量子暗号の研究の推進に大きく役立ちました。そして2000年代には、量子暗号はすでに実験室の外に飛び出せており、2010年前後からは世界各国で、国家プロジェクトによる大規模ネットワーク実験も進んでいます。しかしながら現在でも、商用で運用された例は明らかになっておらず、普及しているとはいえない状況にあります。

量子暗号の研究者はそれに対して「まだ量子コンピュータが普及していないから」とか「量子暗号のコストが高いから」といった理由を挙げる人が多いですが、以下ではこの点を深く掘り下げてみます。とくに量子暗号を既存の暗号方式と比較することにより、暗号としてのメリットとデメリットを整理してみます。

4.1 現代暗号との強度比較

まずは量子暗号の安全性、つまり暗号強度について整理します。

(1) 情報理論的安全性

量子暗号のメリットは、何といたってもその安全性です。冒頭でも述べたとおり、現代暗号は結局のところ、ある種の予想(仮定)にもとづいて安全とされているだけです。何らかの都合のよい予想(例:素因数分解が効率的に解けない)を設定し、さらに盗聴者の計算能力を制限(チューリングマシン上で多項式時間)したうえで、盗聴成功確率を評価しています。そしてその確率が無視できるほど小さい場合のみ、その暗号方式は安全だとされます。逆にいうと現代暗号は、設定した予想や制限の根拠が失われた場合には破れる可能性があります。例えば、量子コンピュータが実現したら、RSA方式やDH方式といったメジャーな公開鍵暗号方式は破れてしまうことが知られています。

これに対し量子暗号には、そのような予想や制限は一切ありません。盗聴者が通信路上の光子をどう盗聴しても、その盗聴成功確率はある確率以下であると厳密に証明できます。なおかつ送受信者は、その確率を(秘匿性増強におけるパラメータ t (現代暗号における鍵の長さに類似するパラメータ)を大きくすることにより)いくらでも小さく抑えることができます。このように、盗聴者の計算量の制約なしに、盗聴成功確率を抑えることのできる暗号方式を、情報理論的に安全な暗号方式と呼ぶことがあり、量子暗号もその一種です。もちろん量子コンピュータが実現しても、量子暗号は安全なままです。

このように量子暗号には、現代暗号とは次元の違う高いレベルの安全性(情報理論的な安全性)が実現できるというメリットがあります。もし現代暗号の安全性を、量子暗号と同じ設定で考えるなら、つまり予想や制限を一切撤廃したら、現代暗号はたちどころに破れてしまいます。すなわち量子暗号の基準でいうと、現代暗号は暗号ですらないということになります。現代暗号と量子暗号の安全性を直接比較することは、そもそも不可能なのです。

(2) 量子コンピュータへの耐性

繰り返しになりますが、量子コンピュータが実現した場合、RSA方式やDH方式といった主な公開鍵暗号方式は破れてしまいますが、量子暗号は安全なままです。ただし現代暗号側にも公平を期していうなら、これは決して、現代暗号がすべて破れるという意味ではありません。

そもそもRSA方式やDH方式が公開鍵暗号のすべてというわけではなく、それ以外にも昔からさまざまな方式が知られています。とりわけ多変数多項式暗号や格子暗号といった方式については、量子コンピュータによる解読法は見つかっていませんし、恐らく解けないだろうと予想されています。むしろこれらの方式は最近、その性質から「ポスト量子暗号」(Post-quantum Cryptography)と呼ばれ、盛んに研究されるようになっていきます(例えば文献2))。またAESやMISTYといった共通鍵暗号も同様に、量子コンピュータによる解読法は見つかっていません(Groverのアルゴリズムと言われる演算方法を使っても、解読時間が従来の $1/2$ 乗に削減されるだけです。したがって指数関数時間の指数部分が半分になるだけで、依然として指数関数時間であることには変わりありません)。

したがって量子コンピュータが実現したとしても、解けないという予想で満足できるならば、ひきつづき現代暗号を使い続けることができます。量子暗号が必要なのはそのような予想では満足できず、情報理論的な安全性が欲しいというユーザーに限られます。

4.2 公開鍵暗号との機能比較

つぎは公開鍵暗号との機能比較をします。

そもそも公開鍵暗号が広く利用されている最大の理由は、暗号通信を始めるまでに必要な鍵のセットアップが簡便に

なることにあります。もし公開鍵暗号が使えなくなったとして、そのとき量子暗号が、公開鍵暗号と同様のメリットをもたらすことはできるのでしょうか(これは要するに現代暗号でいうところの鍵配送の問題ですが、量子鍵配送やDH鍵共有といった用語との混乱を避けるため、ここでは「鍵のセットアップ」という言葉を用いることにします)。

太古の昔から1970年代前半に至るまで、すべての暗号は共通鍵暗号でした。これはユーザAとBがそれぞれ同じ秘密鍵 k_{AB} を共有しておいて、メッセージの暗号化に使うものです。AがBだけと秘密通信を行いたい場合にはこれで終わりですが、そこにさらにCさん、Dさん、…が加わっていくと、それに応じて秘密鍵 k_{AC} 、 k_{AD} 、…を共有する必要があります。一般に N 人のユーザがお互いに自由に秘密通信をしたい場合、各ユーザは自分以外の $N-1$ 人と異なる鍵を共有したうえで、安全に保管しなければなりません。したがって N 人全体では、合計 $\binom{N}{2} = N(N-1)/2$ 種類の異なる鍵を共有、保管する必要があります。

しかし1990年代以降インターネットが普及して、世界中と自由に通信できるようになると、すべての相手と秘密鍵をいちいち共有しておくのは不便だということになり、RSA方式に代表される公開鍵暗号、およびデジタル署名が使われるようになりました。具体的にはまず、各ユーザが自らの公開鍵を一つ公開します。つぎに、公開鍵のすり替えを防ぐために、信用できる認証局を最低1ヵ所設置し、公開鍵をデジタル署名してもらいます。つまり公開鍵基盤(PKI)を構築します。結果として、各ユーザは公開鍵を生成したのち、認証局と一度だけ安全なやりとりをすればよいだけであり、セットアップの手間は大幅に削減されます。全体としては最初に $O(N)$ 個の公開鍵を、認証局に安全に送ればよいだけです。

それでは量子暗号の場合はどうかというと、少なくとも現状の方法そのままでは、共通鍵暗号の場合と同様に、セットアップに際して $O(N^2)$ 個の秘密鍵共有が必要になります。量子暗号は、DH方式と同様に、鍵共有の機能を実現できる方式なのになぜ?と思われるかもしれませんが、問題は古典通信路のメッセージ認証にあります。

量子暗号の存在意義は、情報理論的な安全性にあるので、メッセージ認証にも情報理論的な方式を使わなければなりません。このため公開鍵的なメッセージ認証方式、つまりデジタル署名は使えません。実際の量子暗号装置ではそのかわりに、Wegman-Carter方式と呼ばれる情報理論的な方式を使っています。この方式では、共通鍵暗号の場合と同様に、 N 人のユーザがいたら、各ユーザは $N-1$ 種類の異なる秘密鍵を事前に共有しなければなりません。そして全体としてはやはり、合計 $N(N-1)/2$ 種類の異なる鍵を共有して保管する必要となります。

以上をまとめると、 N 人のユーザがいたとして、公開鍵暗号では鍵のセットアップの手間は $O(N)$ で済みます。こ

れに対し量子暗号は1対1の秘密通信に適した方式であり、セットアップに $O(N^2)$ の手間がかかってしまいます。つまりこの比較においては、公開鍵暗号と同様のメリットを果たせないようにみえます。

4.3 秘密鍵を手で運ぶ場合とのコスト比較

最後にコストを比較します。4.1節(1)でみたとおり、量子暗号と現代暗号の安全性はそもそも直接比較できないので、コストの直接比較も意味をなしません。そもそも量子暗号の目的は、秘密鍵を安全に配布することでありましたが、そのためのもっとも簡単な方法は他ならぬ、人間が手で運ぶことです。実際に戦前から、軍事用の暗号の乱数表は手で運ばれていたという記録がありますし、現在でも簡単に実行できる方法です。そこでこの方法と量子暗号を、コスト面から比較してみます。

現状の量子暗号装置の例を図5に示します。このような装置は、材料費だけでも1セットあたり数百万円はかかります。そして性能としては、通信距離50 km、通信速度1 Mbpsが敷設ファイバ上で達成できています³⁾。そこでかなり楽観的な見積りではありますが、以下では通信距離50 km、通信速度1 Mbpsの量子暗号装置が1,000万円で実装できて、1年間継続して使えるという仮定をおいてみます。そうすると1,000万円で、4 TB程度(= 1 Mbps × 60秒 × 60分 × 24時間 × 365日/8bit)の乱数が運べるという計算になります。これはいまどきのハードディスクドライブ(HDD)1, 2台程度に収まる量ですし、そのようなHDDは1台あたり1万円程度で買えます。であれば、自組織内の信用できる人に毎年1回、HDDを50 km先まで運んでもらえばよいことになります。これだと1日程度の人件費が余計にかかるだけで10万円程度ですみます。一方で量子暗号は1,000万円ですから、現状ではコストとして100倍程度の開きがあることになります。

ただしこの100倍という数字の精度は高くなく、上下10倍くらいの誤差は平気でありえるので、あくまで一つの目安として考えていただきます。誤差の原因としてまず、量子暗号装置のコストを押し下げる要素があります。いまのところ量子暗号装置の材料には特注品が多いうえに、それを研究者が1台ずつ手作りで組み上げているような状況なので、量産効果はまったく効いていません。したがって、例えば、3節でふれた中国や米国の国家プロジェクトにおいて装置が大量生産されれば価格が下がる可能性はあります。さらに上の比較では距離を50 kmに固定しましたが、これが例えば、10 kmでよければ通信速度は10倍の10 Mbps程度に増やせます。量子暗号では、距離を縮めると、通信速度が指数関数的に増えるという性質があるためです。その一方でもちろん、コスト差を逆に拡げる要素もあります。そもそも上の比較では量子暗号装置の開発費、製造コスト、維持費等は含まれていませんし、その一方で比較対象であるHDDの価格は今後も下落していくと予想されます。

図5 量子暗号装置の例 (NEC提供)

5. デメリットの解消にむけた方向性

5.1 運用方法の改良

4章でも述べましたが「量子コンピュータが実現すると公開鍵暗号が破れるのに対し、量子暗号は破れない。そこで量子暗号が必要になる」という宣伝文句がよく使われてきました。しかし4.2節でみた通り、量子暗号は実は1対1の秘密通信に適した方式です。したがって、仮に公開鍵暗号がすべて破れてしまったとしても、量子暗号にその代役は務まらないようにみえます。公開鍵暗号では鍵のセットアップの手間は $O(N)$ ですむのに対し、現状のままの量子暗号方式では、セットアップに $O(N^2)$ の手間がかかってしまうからです。このデメリットの解消が今後もひき続き重要です。

方向性の一つは、量子暗号の運用方法を工夫して、セットアップの手間を $O(N)$ に削減することです。例えば、非常に単純なやり方として、信用できるセンターを1ヵ所設置するものがあります(公開鍵暗号の場合でも、信用できる認証局を最低1ヵ所設置する必要があったことを思い出してください)。そしてセットアップ時に N 人のユーザすべてが、センターとの間に、メッセージ認証用の秘密鍵を共有しておきます。あとはすべての暗号通信をセンター経由で行うことにすれば、 N 人のユーザが自由に暗号通信できます。もちろんこのような単純な方式では、センター1ヵ所に負荷が集中するので必ずしも効率的ではありません。また仮にセンターが悪意を持った場合の被害パターンが、公開鍵暗号のそれと同じとは限りません。これらの問題の解消にむけて、今後さらなる研究が必要と思われます。

5.2 量子鍵配送としての性能向上

4.3節でみたとおり、量子暗号と現代暗号のコストを直接比較することは意味がなく、むしろ、秘密鍵を人間が自ら手で運ぶ状況とのコストを比較すべきです。そしてその差

は現状で100倍程度です。この100倍という数字の精度はあまり高くないし、これを大きいと考えるか小さいと考えるかは個人の感覚や信条の問題です。しかし仮にこのギャップを埋めることができて、秘密鍵を手で運ぶよりも、量子暗号を使った方が安いとか簡単だということになれば、ユーザのメリットははっきりしますし、普及する可能性がでてきます。例えば、コストが1,000倍下がって、毎年1,000台のHDDを自分で運ぶ手間を、100万円の量子暗号装置が代行できるということになれば、その方が便利だと思える人はいるかもしれません。

なおこの種の話では性能指標として、距離、速度、コストの3種類がありますが、どれが改善しても本質的には同じだと思ってかまいません。量子暗号では、距離を縮めると通信速度が指数関数的に増えるという性質がありますので(光ファイバにして50 km縮まるごとに10倍以上)。したがって限界距離が改善したということは、同時に短距離での速度が向上したことも意味します。そして速度が向上すればもちろん、秘密鍵を共有するのにかかるコストも削減できるのです。

いずれにせよ、今ある方式を変えずに、実装技術の工夫だけでコストを1/1,000まで下げるのは難しいことです。したがって今後さらに何段階かのブレイクスルーが必要なわけですが、以下ではそれを狙った取組みについて紹介します。

(1) これまでのブレイクスルー

まず過去を振り返っても、理論の進展やプロトコルの改良によって、量子暗号の性能が向上してきた経緯があります。2000年代前半までは、プロトコルや安全性証明に対する理解が未熟だったために、量子暗号装置には単一光子源、単一光子検出器が必須だと考えられていました。つまり光子1つ1つを厳密に制御する技術が必要だと考えられていました。しかしながら(当時も今も)単一光子源や単一光子検出器の実装は困難なので、量子暗号の実験では安価な代替手段として、光源にはレーザと減衰器が、光検出器にはアパランシェフォトダイオード(APD)が広く使われていました。これらは代替手段であるから、それらを用いた量子暗号装置は、厳密には安全ではないと考えられていました。

しかし2004年になって新たなプロトコルとして、デコイBB84方式が提案され、それにより、レーザを用いたとしても厳密な安全性が保証できるようになりました。また2000年代後半には安全性証明の理論が改良されたことにより、APDを用いても安全性が保証できることが新たに判明しました。この結果、現在ではレーザやAPDはもはや代替手段ではなく、量子暗号の正当な部品とみなされています。そして量子暗号装置の実装コストは劇的に下がり、上述の50 km、1 Mbpsが達成されるに至りました。

(2) プロトコルの改良の方向性

現在でもそのようなブレイクスルー狙いは続いていま

す。1つ目の方向性はプロトコルの改良です。最近の主流は、デコイBB84方式を一旦忘れて、プロトコルを根本から設計し直すものです。有名なものとして、連続変数量子暗号(CVQKD)やRR-DPSQKD方式がありますが、ここでは日本発の技術としてRR-DPSQKD方式について述べます。時系列で説明すると以下のとおりです。

まず発端となったのは、2002年に提案されたDPSQKD(Differential Phase Shift Quantum Key Distribution)方式です⁴⁾。この方式は実は、すでに光通信の世界で知られていたDPSK(Differential Phase Shift Keying)という方式の光強度を落としただけのものでした。DPSKの送信側に減衰器を挿入して出力を単一光子レベルまで落とし、受信側の検出器を高感度なものにおき換えれば、それがDPSQKD方式の量子暗号装置となります。このように既存の光通信用の部品を流用して、比較的簡単に実装できるので安定性が高く、(盗聴者由来ではない)装置由来のノイズが少ないという長所があります。そしてこの長所により、200 kmを超える長距離通信が可能になることが最大の売りです。またヨーロッパではその変形版であるCOW(Coherent One Way)プロトコルが研究されていまして、最近では300 kmを超える通信が可能になったという報告もあります。

ただしこれらのプロトコルでは、デコイBB84方式よりも装置を単純化した反動として、安全性証明は格段に難しくなっていました。このため現在でも、盗聴者の能力にある制約を課した場合(コレクティブ攻撃)の安全性しか証明できておらず、制約なし(コヒーレント攻撃という)での安全性は証明できていません。

この状況を打開するため、2014年にRR-DPSQKD(Round Robin DPSQKD)方式が提案されました⁵⁾。これはDPSQKD方式に、ある種のスクランブル処理を付加したものです。それによって安全性証明で扱う数式が単純化され、コヒーレント攻撃に対する安全性が証明できるようになりました。なおかつこの方式が、通信路の擾乱に対して非常に優れた耐性を持つということが判明しました。この性質を利用すれば、量子暗号の性能を飛躍的に向上できる可能性があるため、現在研究が盛んになりつつあります。

(3) 安全性証明理論の改良の方向性

ブレイクスルー狙いのもう1つの方向性は、安全性証明理論の改良です。中でも最近では、装置無依存量子暗号(Device Independent QKD、以下DIQKD)に関する研究が活発になっています(文献6)およびその参考文献参照)。これは一言でいうと、光の送受信機(装置)をどう実装したかには関係なく(無依存)、ある手順(プロトコル)にしたがって通信している限りは、必ず盗聴が検出できるというアイデアです。そしてその手続き(プロトコル)のことを、装置無依存量子暗号方式と呼びます。

DIQKDの目的は、サイドチャネル攻撃の問題を一気にすべて解決することにあります。現代暗号と同様に、量子

暗号でもサイドチャネル攻撃の問題があります。つまり暗号装置が壊れたり、調整を間違えたりした場合、それによって盗聴が容易になり、乱数が漏えいするという問題があるわけです。例えば、BB84方式のレーザの強度の調整を誤って、単一光子レベルよりずっと強い光が出ていれば、盗聴者は4種類の状態(振動方向 0° , 45° , 90° , 135°)を測定によって識別でき、乱数の値を確実に読取れてしまいます。ただしこれも一例にすぎず、これ以外にもサイドチャネル攻撃は無数にありえます。そしてそれを人がすべて1つずつチェックして塞ぐことは事実上不可能です。

DIQKDとは、安全性証明理論の改良により、そのようなサイドチャネル攻撃を一網打尽にする考え方です。まずBB84方式では誤り率をチェックすることによって、盗聴を検出していました。その一方で1991年に提案されたEkert 1991 (E91) 方式では、誤り率に加えて、ベル(J.S. Bell, 人名)不等式と呼ばれる関係式をチェックしています。そして2000年以降の理論研究の進展により、実はこのベル不等式チェックが、あらゆるサイドチャネル攻撃を検出する能力を秘めていた、ということが判明しました。例えば、前段落のレーザ強度の例でいえば、光強度が強ければそれは必ずベル不等式チェックで検出されます。なおかつそれ以外のあらゆるサイドチャネルについても、同様にベル不等式チェックで検出されるということです。したがってE91プロトコルでは、ベル不等式チェックさえ通過できている限り、サイドチャネル攻撃の心配をする必要がないのです。

このようにDIQKDはもともと、量子暗号の安全性向上のために導入された証明テクニックです。しかし著者はこれが量子暗号のコスト削減にも役立つと期待しています。まず量子暗号全般にいえることとして、コストダウンを狙って部品を安価なものに置き換えると、安全性証明は難しくなります。部品が安価であればあるほど、その挙動を記述するための数式は複雑になる傾向があって、その結果、安全性証明で扱う数式も難しくなるからです。DPSQKD方式やCOW方式の安全性証明が困難を極めているのも、このような事情によります。しかし「装置無依存」の名が示す通り、DIQKDの理論では、部品に対応する数式の複雑さに関

係なく、安全性証明をつけることができます。これによりDPSQKD方式やCOW方式の安全性証明が成功すれば、量子暗号の通信距離は飛躍的に向上すると期待されます。

6. むすび

本稿では、既存の暗号方式を比較対象にして、量子暗号の暗号装置としてのメリットとデメリットを整理するとともに、デメリットの解消にむけた取組みについて議論しました。これをきっかけにして、現代暗号の研究者が量子暗号について興味を持っていただき、ざっくばらんな議論ができるようになれば幸いです。

なお本文中では量子暗号をつかった秘密通信のみについて紹介しましたが、決してこれが量子暗号研究のすべてというわけではありません。これ以外にも量子的な性質を使った電子現金、デジタル署名、暗号プロトコル等に関する研究も引き続き続けられています。これらの分野の今後の発展についても期待したいと思います。

(2015年8月7日受付)

〔文 献〕

- 1) M.A. Nielsen and I.L. Chuang: "Quantum Computation and Quantum Information", Cambridge University Press (2000), 日本語版: 木村達也訳: "量子コンピュータと量子通信", オーム社 (2005)
- 2) 高木剛: "ポスト量子暗号", 数学セミナー, 7, 日本評論社 (2015)
- 3) A.R. Dixon, Z.L. Yuan, J.F. Dynes, A.W. Sharpe and A.J. Shields: "Continuous operation of high bit rate quantum key distribution", Appl. Phys. Lett. **96**, 161102 (2010)
- 4) K. Inoue, E. Waks and Y. Yamamoto: "Differential Phase Shift Quantum Key Distribution", Phys.Rev.Lett., **89**, 037902 (2002)
- 5) T. Sasaki, Y. Yamamoto and M. Koashi: "Practical quantumkey distribution protocol without monitoring signal disturbance", Nature **509**, 475-478 (2014)
- 6) U. Vazirani and T. Vidick: "Fully device independent quantum key distribution", Phys. Rev. Lett. **113**, 140501 (2014)

鶴丸 豊広 2001年、東京大学大学院理学系研究科物理学専攻博士後期課程修了。同年、三菱電機(株)入社。情報技術総合研究所勤務。以来、現代暗号と量子暗号に関する研究開発を続けている。博士(理学)。