Travel notes on bright future technology

雑学エンターテインメント

喜多が行く

明るい未来テクノロジー紀行

第4話

絶対破れない暗号通信システムは「消える魔球」だった!?

マツイのチームが量子暗号通信実験に成功

受け手と送り手がいて初めて通信は成立するが、受け手と送り手しかいない通信に暗号は必要ない。ピッチャーとキャッチャーのいるところにバッターが加わって初めて野球が成り立つのと同じように、盗聴者が存在する可能性のあることが、暗号のレーゾンデートル（存在理由）となっている。

1994年、それまで15年間破られなかった米国標準暗号「DES」を解読し、暗号業界の大リーグに鮮烈なデビューを果たした松井充氏は三菱電機情報技術総合研究所の主席研究員。世界の暗号学者を驚嘆させた「線形解読法」と呼ばれる技術を生かし、同社で「MISTY」という暗号アルゴリズムが作られる。強固にしてコンパクト、暗号化も復号も高速に行える「MISTY」は高く評価され、そこから派生した「KASUMI」はW-CDMA（第3世代携帯電話）の世界標準暗号としてに利用されるようになった。

私事だが実家の近所に「松井秀喜・野球の館」があり、またお名前も筆者の父と同名だったりとついつい親しみを感じてしまったが、松井充氏は世が世なら為政者がその頭脳に鍵をかけておきたいと思うような、暗号の世界を代表するホームランバッターなのである。

その松井氏のチームが昨年11月、「絶対に盗聴不可能な“量子暗号通信システム”で世界最長距離の実験に成功」というニュースを発表した。「量子暗号通信」とはいうが、実際には量子暗号通信は暗号鍵を生成するために利用され、生成された鍵を使って公開通信網で通常の暗号通信を行う仕組みで、現代暗号のアキレス腱である鍵配送の問題を解決する可能性を秘めた実験だ。

リリースには「絶対に解読されない究極の暗号」とあるが、これは何と魅力的な響きであろうか。1億分の1だろうが1兆分の1だろうが、ただ1つの反証さえ見つければ「絶対」は覆えせるというのに、それを「不可能」と言い切るのである。

一般に「暗号の強さ」は、「現在最速のスーパーコンピュータを使っても、○○万年かかる」などと、解読に必要とされる膨大な計算量に仮託して表現される。しかし、それでも「破れない」と断言しているのである。未来に登場する超高速コンピュータも含め、この世にあるすべてのコンピュータを、宇宙の寿命をすべて費やして計算したとしても「絶対に解読はできない」ことを保証できる暗号は、いったいどんなからくりで実現しているのだろうか。

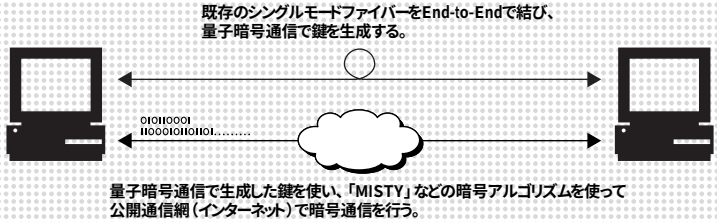
光の粒1つに情報を乗せるのがポイント

「暗号がやろうとしているのは、情報を隠すこと。意味のあるメッセージを、意味のなさそうな情報として送る技術です」

教科書の1行目に出てくるような真っ当

三菱電機株式会社 情報技術総合研究所 情報セキュリティ技術部 チームリーダー／主席研究員の 松井充氏は暗号業界では知る人ぞ知る存在。

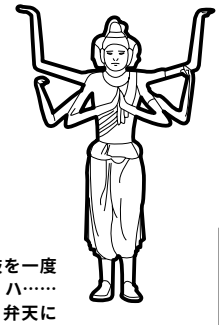
量子暗号通信は既存の通信／暗号システムと併用して実用化される



図説「量子暗号通信システム＝絶対安全な鍵を協調して生成するシステム」

量子暗号通信実験に利用された「BB84」プロトコルの原理

❶送信者・阿修羅は、二枚の皮と太鼓の胴を用意した。伝えたい情報（正か邪）を1枚に記し、もう1枚には適当に正邪を記した。そして、阿修羅は正邪が記された面を内側にしてこの2枚を貼り、太鼓を作った。天か地か、どちらに記された正邪を「伝えたかったか」を阿修羅は手元に控えておいた。



❷阿修羅はこの太鼓を一度に1つずつ、イ、ロ、ハ……と通し番号を付けて弁天に送った。

公開通信網

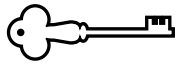
↑どちらを破ったか
意図した破られ方をしたのは↓

❸中身を読むには、皮を破らねばならぬが、この皮には破られた瞬間に霞と消えてしまう特別な性質がある。破られればその皮に記されていた正邪は読めなくなり、修復も、複製も不能である。

❹受信者・弁天（弁財天）は、受け取ったら天か地かどちらかを、そのときの気分次第で破る。天を破ると地に、地を破ると天に記された正邪が読める。何番目の太鼓で天地のどちらを破ったかを阿修羅に伝える。

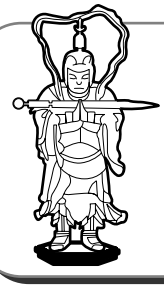
❺阿修羅は、弁天から送られてきた「破り方」と手元の控えを照合し、自分が意図したとおりに破られた太鼓が何番目と何番目の太鼓であったかだけを弁天に伝える。弁天は、阿修羅から伝えられた太鼓番号に従い、その太鼓から読みとられた正邪の情報だけを拾って並べ、これを合い言葉とする。

量子暗号通信実験のビットレート＝7.2bps
送受信者が協調して暗号鍵を生成する速度



❻第三者（韋駄天）からは完全に秘匿された鍵が生成され、阿修羅と弁天がその鍵を共有することになる。

量子暗号通信で生成した鍵を使い、「MISTY」などの暗号アルゴリズムを使って公開通信網（インターネット）で暗号通信を行う。

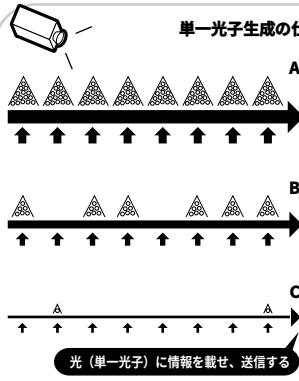


盗聴者・韋駄天

盗聴者は単一光子からは原理的に情報を得られない。盗聴したしても、盗聴者の存在を知らせることになるだけ（単一だから、盗聴するとなくなってしまい、バレる）なので、盗聴行為は完全に意味を失なう。

三菱電機が成功させた量子暗号通信システムの概要

単一光子生成の仕組み



A パルスを送り、レーザー光を発生させる。パルスのたびにたくさんの光子が発生するので、そのうち何個かを盗まれても、受信者はわからない

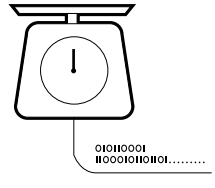
B パルスのエネルギーを小さくしていくと光も弱くなり、ときには発光しないケースも出てくる。当然、伝送スピードは低下する

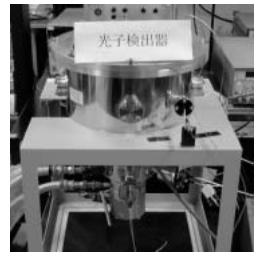
C 10回のパルスで発光が1回起きる程度までパルスを弱めると、1回の発光に2個以上の光子が含まれる確率はきわめて小さくなる。伝送スピードを犠牲にすることで、「単一光子」が生成された。

光（単一光子）に情報を載せ、送信する

光ファイバー長「87km」が世界最長記録。減衰は避けられないが、それでも送られた光子1000個の内18個が届く。

単一光子検出器





単一光子（きわめて微弱な光信号）を検出するために検出器の制御やチューニングに独特のノウハウが。15パーセント（100個に15個）という検出効率を実現。

「BB84」プロトコル処理により「鍵」の元となるデータを生成

パリティーチェック／プライバシー増幅処理

パリティーチェックを行って通信エラーを検出し、さらにエラー検出に用いたビット数分の情報を削って、「鍵」データを完成させる。

な解説も、松井氏から聞かされるとなにやら神秘的な香りが漂う。

「今回の量子暗号通信システムは、光の粒1つに情報を乗せるという、通信の常識からすればまったくナンセンスなことをやっている。確実を旨とする通信の考え方とは、発想がそもそも違うんです」

量子暗号通信の最大の特徴は「1個の量子（この場合は光子）を使うこと」である。波であると同時に粒子の性質も備える光をかすかなものにしていくと、なくなる直前にそれは1粒の光子となる。この1粒に情報を託すから、途中で盗聴されてもその時点で「消え」てしまう……、ここがまず第一のポイントだ。同じ情報が乗せられた光子が2つ以上流れれば、途中で1つ盗まれてもわからないわけである。

さらに、きわめて小さい粒は「複数の状態が同時に存在する」という禅問答のような性質を帯びてくる。有であり無、空であり全であり、0と1の両方の状態を同時に兼ね備えているのだ。この粒をつかまえて白黒はっきりさせることはできるが、それが正解かどうかはさっぱりわからぬ……。まったく言語化しにくい性質が宿命づけられている、とハイゼンベルグ（の不確定性原理）は言うのである。それが1か0かは不確定だから、当然ながら複製もできない。これが第二のポイントとなる。途中で量子を中継する形で盗聴しようとしても、その不確定性のために最終的なパリティーチェックでエラーレートが極端に跳ね上がり、盗聴者の存在が判明するのである。

夫婦仲の良いことで知られる将棋の羽生夫妻には余計なお世話だが、まことにやっかいで扱いづらく言語化の難しい「量子」を使った暗号通信システムをエイヤッと、モデル化してみた。それが「阿修羅の量子太鼓」（p.185図）である。

盗聴者の存在を見破れる通信システム

このモデルで特徴的なのは「破られた瞬間に雲散霧消する皮」という約束だ。受信者（弁財天）は太鼓が伝える情報が0なのか1なのかを、皮を破って観測する。

「阿修羅太鼓版ＢＢ８４プロトコルの通信例」

①阿修羅は量子太鼓を作った

太鼓番号	イ	ロ	ハ	ニ	ホ	ヘ	ト	チ	リ	……
意図は	天	地	天	天	天	地	天	天	天	……
	正	邪	邪	邪	正	正	正	正	正	……
天の皮に	正	正	邪	邪	正	正	正	正	正	……
地の皮に	邪	邪	邪	邪	正	正	邪	正	正	……

④弁天はどちらかを破って中身を読んだ

太鼓番号	イ	ロ	ハ	ニ	ホ	ヘ	ト	チ	リ	……
破ったのは	天	天	地	天	天	地	天	地	地	……
読んだのは	地	地	天	地	地	天	地	天	天	……
弁天が読みとれた情報										
天の皮に			邪			正		正	正	……
地の皮に	邪	邪		邪	正		邪			……

⑤上 弁天は阿修羅に伝えた

読んだのは	地	地	天	地	地	天	地	天	天	……

⑤下 阿修羅は手元の控えと照合した

太鼓番号	イ	ロ	ハ	ニ	ホ	ヘ	ト	チ	リ	……
弁天が読んだのは	地	地	天	地	地	天	地	天	天	……
阿修羅の意図は	天	地	天	天	天	地	天	天	天	……
意図したとおりか	偽	真	真	偽	偽	偽	偽	真	真	……

⑥弁天と阿修羅の手元に秘密鍵が生成された

意図したとおりか	偽	真	真	偽	偽	偽	偽	真	真	……
天の皮に			邪			正		正	正	……
地の皮に	邪	邪		邪	正		邪			……
鍵生成		邪	邪					正	正	……

ここで生成された鍵「邪邪正正」は第三者（韋駄天）からは完全に秘匿されている。

※BB84とは、BennettとBrassardが1984年に発表したプロトコル

盗聴者（韋駄天）は太鼓を盗んでも、どちらかの皮を破らないと中を見ることができないが、見ることで太鼓（に記された情報）を毀損することになる。当然ながら完全な形での複製も不可能となる……。

おまけに、一度に一鼓ずつしか送られてこないから、盗んだこともすぐバレる。従来の通信方式では可能性にすぎなかった盗聴者の存在が、「1個ずつ送る」ことで察知可能となる。プロトコルやら暗号強度やらといったこと以上に、この点が従来の暗号通信システムと最も違う点だ。もし存在が明らかになれば、送信を止めるか、別のルートで送る、という対策も取れるわけだ。

さて、太鼓を破って正邪が読めた（上の表の4）。受け取った弁天にとっても送った阿修羅にとっても、自分が持っているデータはまだ意味のあるものにはなっていない。

どっちの皮の情報を伝えたかったのか、どっちを破って読んだのかという情報をやりとりし（これは量子通信が終わった後に行う。盗聴可能な公開通信網を使ってもかまわない）、それを総合することでようやく2人の間に共通の鍵が生成される（p.185の図と上の表の6）。

鍵を配送するというよりは、共同で暗号鍵をつくるシステムといったほうが、正しくその機能を体現していることになるだろう。

とにかく光の粒を１つずつにする必要があった

「このシステムは、通常の光通信と同様、光を発生する装置、光ファイバー、光検出器のセットでで成り立っています。光ファイバーは普通に使われているものですが、光子発生装置は1個の光子だけを生成する特殊なもの。検出器も1個の光子を効率良く捕らえられるよう、特殊な制御をしています。三菱電機には、これらのそれぞれの部門の専門家がいて、その助けを借りることができた。我々情報セキュリティ

ーチームはハード屋さんではないのですが、そういう助けがあって今回の実験が成功したということになります」

今回の実験での鍵の生成速度は7.2bps。8ビットが1バイトだから、1秒間に1文字に満たない情報量なのである。遅い？　そう、遅いのには理由がある。

光子発生装置は、1個ずつの光子を発生させるために入力するエネルギーを非常に弱くしているため、実は10回に9回は光っていない。「光子が2個出ないことが盗聴不可能であることを保証している」ため、スピードを犠牲に、それを実現したわけだ。絶対打てない消える魔球は、そもそも投げられている数が10球に1球と、少ないのである。

ファイバーは通常の光通信に使われるシングルモードファイバーで、十分に透明なものだ。それでもだいたい15kmで光のエネルギーは半減する。通常の光通信なら、光子数でカウントすれば億のオーダーとなる強度の光を送り出しているため、これが半分になっても信号は十分伝わる。しかし1個の光子がここを通る場合、1個が半分になることはできない。ある時間の間に15kmを通過しようとした光子のうち、確率的に半分は伝わり、半分はファイバーの中で消失して熱となって失われてしまう、ということを意味する。今回の実験で使われた長さ87kmのファイバーだと、ざっと1000分の18ぐらいに信号が弱まる（確率的に1000個の光子を送ったら、届くのが18個）わけだ。届かなかったのはもともとなかったのと同じことになる。

さらに検知器のほうも、かすかな光を検知できるように感度を上げて運用されるが、いかんせん対象が微弱な光なので来ていないのに来たとか、来たのに来ていないと結果を出力してしまうこともどうしても出てしまう。なるべくそういうことのないように制御に工夫を凝らしても、検出効率は15パーセント、つまり100個に85個は取り落としてしまっている。「確実に1個だけを出せる、読める機器ができたとしたら、それだけで業界では大きなニュースになると思います」と言うほど難しいものなのだ。

公開網の暗号通信と併用される量子暗号通信

しかし、鍵の生成速度が遅いと言っても、7.2bpsであれば18秒ごとに128bitの新しい鍵が手に入る計算だ。たとえばMISTYで128bitの長さの鍵を使うなら、それこそ最速のスパコンで何万年という強度の、十分に堅牢な暗号通信が可能となる。

我々も実は「複数の暗号方式の組み合わせ」のお世話になっている。我々が普段インターネットで利用する「SSL」は、公開鍵と秘密鍵を使うRSA暗号で共通鍵のやりとりを行い、その共通鍵で暗号化されたデータをやりとりしている。いわばハイブリッド暗号方式だ。

いっぽう将来、量子コンピュータが登場すれば、素因数分解の難しさに依拠する公開鍵暗号方式なども破られる可能性が出てくる。量子コンピュータは、現在のコンピュータが数万年かかる計算を、マイクロ秒で終えてしまう可能性を秘めているというのだ。

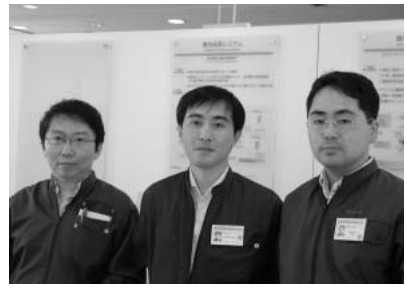
「だからこそ絶対に盗聴不可能な量子暗号通信が必要になる、と言われています」

目には目を、量子コンピュータには量子暗号でということになろうか。

だが、今の暗号がすぐに使われなくなってしまうかと言うと、そうではない。

暗号そのものの強さと、それが正しく運用されているかどうかはまったく別問題である（パスワードを書き留めておいたりする）のと同様、要は使い方。暗号のアルゴリズムもいってみればネジやクギなどと同じ道具なわけで、場所によって使い分けていくことになる。

◇　◇　◇



松井氏とともに解説して頂いた情報セキュリティ技術部の石塚裕一氏、西岡毅氏、長谷川俊夫氏。鎌倉は大船の研究所にて。

「純粋な数学屋さんからすれば暗号というのは世俗にまみれたものかもしれないですがね」と松井氏は謙遜するが、世間一般の「暗号」の認知はやはり「ムズカシク、何やらオソロシイもの」ではないだろうか

まるで武器などと同等に暗号システムも輸出規制の対象となるのだからムリもない。しかし、モノモノしい響きの裏には、世の中の他の多くの開発や製造や研究と同じような人間の営みがあったと知って、少しホッとした気分になった。

本稿の入稿直前に、東芝欧州研究所（英ケンブリッジ）が101kmの量子暗号通信実験に成功したというニュースが入った。詳細は明らかになっていないが、低ノイズの光子検出器が鍵らしい。三菱電機がこの挑戦を受けて立つかどうかは明らかではないが、こうした競争が実用化の時期を早めるのは間違いない。

喜多充成（きた みつなり）

1964年石川県生まれ。
産業技術・モノ作りを10年来のテーマとする技術系ライターで、本誌草創期からの執筆陣の1人。連載「インターネットビジネス利用の現場から」（1995～）、「2005年へ光る道」（1998～）、「超未来ラボ」（2001～）、特集「電子メール革命」（1995）、「いまそこにある定額制」（1999）などを担当。ウェブ上ではキヤノン広報記事『開発者が語る「これがキヤノン！」』などがある。
URL http://web.canon.jp/technology/interview/

次回は「小さいのにたっぷり入るお皿」に行く！（予定）

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp