特集論文

鶴丸豊広*
Toyohiro Tsurumaru

量子暗号

Quantum Cryptography

*情報技術総合研究所(博士(理学))

要　旨

量子暗号(Quantum Cryptography)は，量子技術を利用した暗号方式であり，絶対に破れない暗号方式として知られる。

三菱電機は2000年前後から量子暗号の研究を開始し，装置実装と理論の両面で様々な成果を上げており，現在は理論研究に注力している。理論研究というと，実験結果を後追いで述べるだけと思われがちだが，量子暗号の場合は必ずしもそれにとどまらず，現実の量子暗号装置の性能向上やコスト削減に直接役に立つものである。

1. ま え が き

本稿ではまず，量子暗号とは何かを，既存の暗号方式と比較したのち，この分野での当社の研究成果を述べる。日常生活で最も馴染(なじ)みのある暗号は，無線LANでのパスワード暗号化だと思われるため，それと比較する。三菱電機は2000年前後から量子暗号の研究を開始し，装置実装と理論の両面で様々な成果を上げてきたが，現在は理論研究だけに注力している。そのため，理論研究を中心に成果を述べる。

なお本稿での量子暗号とは，専門的には量子鍵配送(Quantum Key Distribution：QKD)のことだが，一般には量子暗号という呼び方が定着しているので，ここでもそれを採用した。また，詳細を知りたい場合は参考文献(1)を参照されたい。

1.1　既存の暗号方式(現代暗号)との比較

量子暗号の目的は，無線LAN暗号化をはじめとする既存の暗号方式(以下“現代暗号”という。)と全く同じで，ユーザーが選んだメッセージを，誰にも盗聴されずに(以下“安全に”という。)誰かに送ることである。

1.1.1　暗号通信での役割が異なる

無線LAN暗号化の場合は，ユーザーが一旦手動でパスワードを設定すれば，それ以降はルーターが通信内容を暗号化し続ける。暗号の使い方は基本的に全てこれと同じであり，抽象的には，次の２ステップに分かれる。

ステップ１“秘密鍵配付”　：秘密の基になる，ランダムな文字列を何らかの方法で配付する。その文字列が覚えられるほど短ければパスワード，長くて完全にランダムであれば秘密鍵と呼んで区別することが多い(以下“秘密鍵”という。)。

ステップ２“暗号アルゴリズム”：ユーザーが自由に選んだメッセージを，ステップ１で配付した秘密鍵とともに，“暗号アルゴリズム”というソフトウエアに入力して暗号文を作って，相手に送る。相手も同じ秘密鍵を知っている(かつ復号アルゴリズムは公開されている)ので，メッセージを復号できる。結果として通信が成立する。

この二つのステップの中で，現代暗号と量子暗号は，それぞれ異なる役割を果たす。

まず現代暗号とは，ステップ２の暗号アルゴリズムのことである。それを実際に使うためには，あらかじめステップ１で秘密鍵を配付しておく必要がある。通常は，秘密鍵を人がその場に赴いて設定したり，媒体に記録して運んだりして配付する。このやり方をここでは“秘密鍵を手で配付する”と呼ぶことにする(なお公開鍵暗号でも，この状況は緩和されるが解消されず，証明書は手で配付する必要がある)。手で配付するので，秘密鍵を大量に又は頻繁に送ることはできない。例えば無線LANの場合，短め(数百～数千ビット)の秘密鍵を一旦設定したら数年は使い回すことになる。

一方，量子暗号は，ステップ１の秘密鍵配付を，光通信によって桁違いに高速化するものである(**図１**左)。典型的には数Mbpsで配付できる。このため秘密鍵を頻繁に更新できるようになり，安全性(暗号の強度)が向上する。

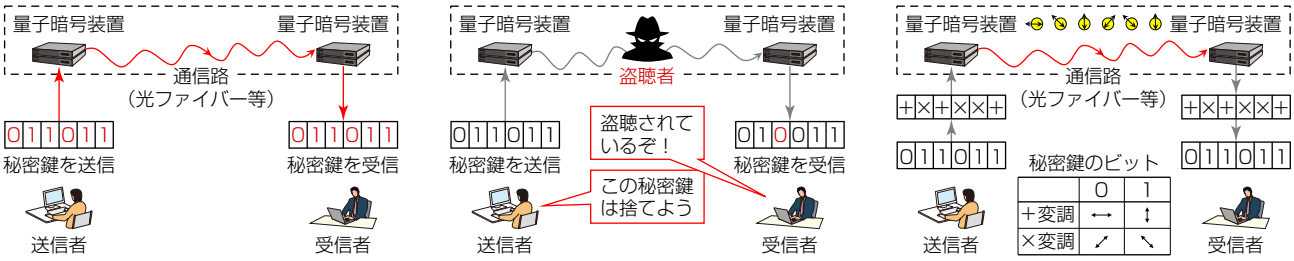

図１−量子暗号のイメージ

特に，秘密鍵の更新頻度を究極まで高めて，メッセージと同じ長さの秘密鍵を毎回使い捨てする場合，“ワンタイムパッド”という究極の暗号方式になる。

ワンタイムパッドは，従来の“手で配付する”やり方では実用的でないが（メッセージを手で運ぶのと同じことになってしまうので），量子暗号があれば実用的になる。量子暗号は，ワンタイムパッドを実用化するための方式とも言える。

1.1.2　安全性の実現方法が根本から異なる

端的に言えば，現代暗号は“見られても漏れない”ようにするが，量子暗号は“見られたことが分かる”ようにする。

現代暗号は，ステップ２のメッセージを漏らさないようにする。そのために暗号アルゴリズムが，メッセージを複雑に攪拌（かくはん）して，見た目のかけ離れた暗号文を作る。万が一暗号文を見られても，元のメッセージを推測できないようにする。

一方，量子暗号は，ステップ１の秘密鍵を漏らさないようにする。そのために，まず“秘密鍵が通信途中で盗聴されたら，痕跡が必ず残る”仕組みを埋め込んでおく（**図１**中央）。そして盗聴の痕跡が見つかった場合，その秘密鍵は誰かに漏洩（ろうえい）したと結論付けて捨てて（秘密鍵はランダムな文字列であり，メッセージではないので捨てて構わない），別の秘密鍵を送り直す。もし痕跡が見つからなければ，盗聴されていない，つまり安全だと結論付けてステップ２で使う。

量子暗号ではこの“痕跡が必ず残る”仕組みを実現するために，秘密鍵をわざと壊れやすい媒体に載せて送る。それが“量子”である。ここで量子技術が必要になる。

量子暗号の場合，量子とは，強度を極限まで弱めた光のことである（**図１**右）。光の強度を極限まで弱めたものを，極めて高感度で測定する場合，高校や大学で習った電磁気学からのずれが目立つようになり，代わりに量子力学の性質が見えるようになる。その性質には“光は波であるにもかかわらず，一つ二つと個数を数えられる”や“測定すると状態が変化することがある”などがある。量子暗号では，この二つ目の性質で起こる変化を盗聴の痕跡として使う。

1.1.3　実装難易度は量子暗号の方が高い

実装の難易度は，現代暗号より量子暗号の方が高い。暗号アルゴリズムはソフトウエアなので，スマートフォンやパソコン上で容易に実装できる。量子暗号は，極限に弱めた光で通信する必要があるので，専用の光通信装置が必要になる。

1.1.4　暗号強度（安全性）は，量子暗号が比較にならないほど強い

現代暗号であっても量子暗号であっても，今の暗号は強度（安全性）が非常に強くなっており，現実的な時間（年単位）で実際に解いてみせるのは難しい。したがって，各暗号方式を実際に解いてみて，各々の強度を比べるのは現実的でない。

そこで今の暗号業界では，各暗号方式の安全性を“証明する”ことによって比較する。“証明する”ことの具体的な作業は，安全性を数学的に証明して，それを文書として書き下すことである。良い文書が付属した暗号方式ほど強い方式とされ，ユーザーに安心して使ってもらえる。いわば暗号方式の“血統書”のように機能する。

この観点では，量子暗号が現代暗号とは比較にならないほど強い。予想に頼らず厳密な証明が書けるからである（**図２**）。

現代暗号は，**1.1.1項**で述べたとおり，短い秘密鍵を長い間使い回す前提になっている。このため最初から明確な弱点（秘密鍵を全数探索すれば必ず解ける）があり，そのままでは証明を完結できない。そこで通例は，何らかの予想（最も有名なのは“素因数分解を解くのは難しい”というもの）を持ち込んで，“もしその予想が正しかったら”という前提で証明を書

く。しかしその予想は証明できていないので，証明があるとはいえ，結局は“現代暗号は“恐らく”破れない”としか言えない。ある日突然，新しい解読法によって破られる可能性は否定できない(なお，この状況は耐量子計算機暗号でも同じで，“耐量子計算機暗号は，量子コンピューターを使っても“恐らく”破れない”としか言えない)。

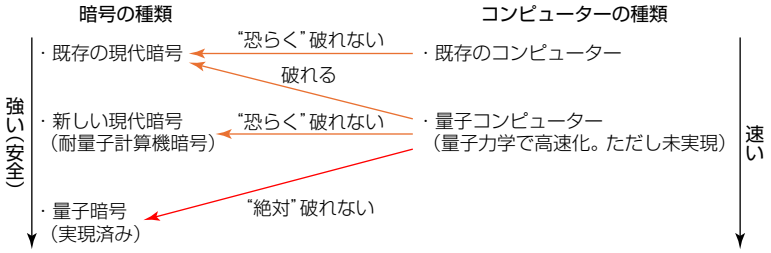

図２-各種の暗号と各種コンピューターの関係

一方，量子暗号方式の場合は，予想を一切導入せずに，最後まで厳密に証明できる。量子力学は，万有引力や電磁気の法則と同じく厳密に検証された物理法則である。その物理法則を前提にして，安全性が数学的に厳密に証明されている。したがって，将来いかなる解読法や新型コンピューターが出現しようとも解読されない。つまり“絶対に破れない”。

1.2　量子コンピューターとの比較

量子コンピューターも量子暗号も，どちらも，量子力学を使った情報技術(狭義には量子情報技術)である。

1.2.1　機能が全く異なる

その一方，差異も複数あり，まず機能が全く異なる(**図２**)。量子コンピューターはコンピューターであり，高速に計算することが目的である。一方，量子暗号の目的は，この章の冒頭で述べたとおり暗号であり，計算ではない。

1.2.2　実装難易度は量子暗号の方がはるかに低い

差異のもう一つは実装難易度である。有用な量子コンピューターは未実現だが，量子暗号は30年前に実現済みである。

量子コンピューターの理論は30年以上前からあり，その理論どおりに動く装置がもしあれば，計算が高速化できることも分かっている。しかしそのような装置の実装は困難であり，いまだに誰も成功していない。結果として，何らかの役に立つ計算を，既存のコンピューターよりも高速にやってみせたという報告はいまだにない。

それに比べると量子暗号の実装ははるかに容易である。誤解を恐れず単純化するなら，既存の光通信システムを微修正(送信側に減衰器を挿入し，受信側の検出器を高感度化)すれば量子暗号になる。そのため，1990年代には既に実装の報告が複数あり，暗号通信ができていた。続いて2000年代に複数のベンチャー企業が量子暗号装置を販売し始め，2020年前後には日本電気㈱や㈱東芝が事業化を開始した。

2．当社の量子暗号への取組みと研究成果

当社は2000年前後から継続して量子暗号の研究に取り組んで，様々な成果を上げてきた。当初は装置実装と理論の両面で研究を行い，装置実装での大きな成果として“東京QKDネットワーク”への参画[2]があった。しかし2012年に実験研究から撤退し，それ以降は理論研究だけに注力して今日に至る。そこでこの章では，理論研究の成果だけを幾つか選んで述べる。なお当社の研究紹介ページ[3]で，更に詳しい情報を随時更新しているので，そちらも参照されたい。

2.1　理論研究をする意義

理論研究というと，実験結果を後追いで述べるだけと思われがちだが，量子暗号の場合は必ずしもそれにとどまらず，現実の量子暗号装置の性能向上やコスト削減に直接役立つ。そのことを一つの例で述べる。

2. 1. 1　成果例その１：スカッシュ演算子

2000年代前半までは量子暗号の理論が未発達であったため，量子暗号を作るには，単一光子を厳密に制御できる装置が必要と考えられていた（**図３**(a)）。つまり，光源は光子を１回当たり厳密に１個発して，誤って０個，又は２個以上発してはならないとされていた。同様に検出器も，光子一つ一つを別々に検出できるとされていた。その前提の下，**1. 1. 4項**の前半で述べた意味で，安全性を証明していた。

(a)　当初の量子暗号のアイデア

(b)　現実の量子暗号装置

図３−当初の量子暗号のアイデアと現実の量子暗号装置

だが実は，当時も今も，そのような光源も検出器も存在しない。あっても近似的なものであり，かつ高価である。そこで実験家はそれらを安価な部品で代用することを考えて，光源にはレーザーを弱めたもの，検出器にはフォトダイオードを使用した（**図３**(b)）。そうして作成した量子暗号装置はその場しのぎの廉価版と考えられて，実際に盗聴法も知られていた。

だがその後理論研究が進展した結果，実はその廉価版の装置を用いても，厳密な安全性を達成できることが分かった。具体的には，まず盗聴法に対しては，“デコイ法”という新たなプロトコル（装置の操作手順）を採用すれば対処できると分かった。また検出器の問題は，“スカッシュ演算子”という数学的手法[4]を用いれば，厳密な安全性証明を書けるようになって解決すると判明した。なお後者のスカッシュ演算子は，当社とNTT㈱による共同研究成果である[4]。

2. 1. 2　理論研究でもたらされる装置の性能向上とコスト削減

2. 1. 1項の例では，かつてその場しのぎの廉価版とされていた量子暗号装置を，理論研究の成果によって，正規の装置に昇格できた。結果，理論研究によって，装置のコストを大幅に削減できたことになる。同様に，理論研究によって装置の性能を向上できる事例も多くある（**2. 2. 1項**，**2. 2. 2項**参照）。これが理論研究をする意義である。

2. 2　その他の成果例

2. 2. 1　双対ユニバーサルハッシュ関数の提案

これは理論研究によって装置の性能が向上できた事例であり，名古屋大学との共同研究である。量子暗号の安全性を保証するには，秘匿性増強と呼ばれるデータ処理が不可欠である。そのデータ処理用の新たなアルゴリズムとして，当社は“双対ユニバーサルハッシュ関数”を提案した[5][6]。このアルゴリズムのメリットは多々あるが，一例として，誤り率が小さい状況で最大の鍵生成速度を達成できることが挙げられる。

2. 2. 2　有限長解析による鍵生成速度の改良

これも**2. 1. 2項**と同様に，理論研究によって装置の性能が向上できた事例であり，名古屋大学との共同研究でもある。

Bennett−Brassard 1984（BB84）方式は最初に提案された量子暗号方式であり，現在でもデファクト標準になっている。当社はこのBB84方式に対する有限長解析（秘密鍵の長さが現実には有限であることを考慮に入れた安全性証明）を厳密に実施し，既存成果をしのぐ鍵生成速度の算出に成功した[7]。特に秘密鍵長が短い領域で，鍵生成速度が倍増される。

2.2.3　DPSQKD方式に対する最強攻撃と厳密スケーリングの導出

BB84方式以外にも様々な量子暗号方式が提案されている。とりわけ国産で有名なのが，2002年に日本電信電話㈱(現NTT㈱)が提案したDPSQKD(Differential Phase Shift Quantum Key Distribution)方式である。当社は2007年にこの方式に対する攻撃手法を提案し，現在もこれが同方式に対する最強の攻撃手法だとされている[8]。

また2024年の富山大学との共同研究では，先に述べた攻撃手法を援用することによって，この方式の性能指標の一つである“スケーリング”の厳密な導出に成功し，それがBB84方式と同等であると示すことができた[9]。

2.2.4　異なる安全性証明手法を数学的に統合

この項では安全性証明の手法に関する研究成果について述べる。安全性証明では“Leftover Hashing Lemma(LHL)の手法”，及び“位相誤り訂正(PEC)による手法”という２種類の異なる数学的手法が広く用いられている。しかし2020年頃までは，これら両手法の関係は不明であり，両者は独立した手法とみなされていた。実際に，同一の量子暗号方式を，異なる手法で解析した論文が，それぞれ新たな成果として発表されることが常であった。これに対して当社は，両手法が実は，数学的には同一である，と厳密に示すことに成功した[10][11]。

2.2.5　放射線乱数の安全性を初めて厳密に証明

当社は，量子暗号の理論研究で培った知見を，以前からあった放射線を使った乱数生成器(以下“放射線乱数”という。)に適用し，東京大学工学部，大学共同利用機関法人 高エネルギー加速器研究機構(KEK)との共同研究として，放射線乱数のランダム性と秘匿性を，世界で初めて(注1)理論的に厳密に証明することに成功した[12][13]。なお証明に当たっては，原子核の持つパリティ対称性という性質と量子力学を活用した。詳細は参考文献[12][13]及び東京大学工学部，KEKのプレスリリースを参照されたい。

(注１)　2022年７月７日，当社調べ

3. む　す　び

量子暗号とは何かを述べたのち，当社の理論研究の成果を述べた。量子暗号の場合は，理論研究の成果によって，現実の装置の性能向上やコスト削減が可能になるということを，幾つかの成果例とともに述べた。なお当社の研究紹介ページ[3]で最新の研究成果を随時更新しているので，興味のある方はそちらも参照されたい。

参 考 文 献

(1)　鶴丸豊広：量子暗号，映像情報メディア学会誌，**69**，No.11，889～897 (2015)
(2)　Sasaki, M., et al.：Field test of quantum key distribution in the Tokyo QKD Network，Optics Express，**19**，No.11，10387～10409 (2011)
(3)　三菱電機：三菱電機の量子技術
https://www.mitsubishielectric.co.jp/corporate/randd/quantum/
(4)　Tsurumaru, T., et al.：Security proof for quantum-key-distribution systems with threshold detectors，Physical Review A，**78**，No.3，032302 (2008)
(5)　Tsurumaru, T., et al.：Dual Universality of Hash Functions and Its Applications to Quantum Cryptography，IEEE Transactions on Information Theory，**59**，No.7，4700～4717 (2013)
(6)　Hayashi, M., et al.：More Efficient Privacy Amplification With Less Random Seeds via Dual Universal Hash Function，IEEE Transactions on Information Theory，**62**，No.4，2213～2232 (2016)
(7)　Hayashi, M., et al.：Concise and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths，New Journal of Physics，**14**，093014 (2012)
(8)　Tsurumaru, T.：Sequential attack with intensity modulation on the differential-phase-shift quantum-key-distribution protocol，Physical Review A，**75**，No.6，062319 (2007)
(9)　Mizutani, A., et al.：Tight scaling of key rate for differential-phase-shift quantum key distribution，Phys. Rev. Research，**6**，No.4，043300 (2024)
(10)　Tsurumaru, T.：Equivalence of Three Classical Algorithms With Quantum Side Information: Privacy Amplification, Error Correction, and Data Compression，IEEE Transactions on Information Theory，**68**，No.2，1016～1031 (2022)
(11)　Tsurumaru, T.：Leftover Hashing From Quantum Error Correction: Unifying the Two Approaches to the Security Proof of Quantum Key Distribution，IEEE Transactions on Information Theory，**66**，No.6，3465～3484 (2020)
(12)　Tsurumaru, T., et al.：Secure random number generation from parity symmetric radiations，Communications Physics，**5**，No.147 (2022)
(13)　暗号システム向けの理想的な乱数実現へ ―“パリティ対称性”利用が有効―，三菱電機技報，**98**，No.1，1-3-01 (2024)