解説

応用 専般

量子暗号の実装の安全性向上に向けた試み
―理論と装置のギャップを埋める―

鶴丸豊広（三菱電機（株）情報技術総合研究所）
玉木　潔（日本電信電話（株）物性科学基礎研究所）

量子暗号の安全性に対する考え方の変化

■ 原理的に安全な暗号方式

量子暗号は，盗聴者に計算量や技術的な制限を課さなくても安全性が保証される，次世代の暗号方式である．量子暗号では，光子と呼ばれる光の粒子の1つずつにビット値0, 1をのせて通信する．一方で通常の光通信では，数万個以上の光子でできたパルスにビット値をのせて通信している．つまり同じビット値が多数の光子にコピーされて送られているため，通信の途中で光子を数個奪われても（盗聴されても）気づくことができない．しかし量子暗号においてそれを第三者が観測（盗聴）すると，状態が瞬時に変化し，盗聴が発覚する．

RSA方式をはじめとする現代暗号方式は，有効な解読アルゴリズムが現状で見つかっていないので安全だとされている．逆に言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る．また，仮に現在破られていないとしても，盗聴者は通信路上の暗号文を解読技術が発展するときまで保管しておけば，保管してきたすべての暗号文の内容を読み解くこともできてしまう．その一方で，もし仮に量子暗号が破れたとすると，それは物理の基本法則（量子力学）に反する現象が見つかったことを意味する．しかしこれまでの膨大な実験の蓄積のなかで，量子力学に反する現象は報告されていない．その意味で量子暗号は原理的に盗聴不可能であると考えられている．

なお以下本稿で量子暗号といった場合，もっぱら量子鍵配送（quantum key distribution, QKD）のことを指すこととする．

■ 量子暗号装置の実装の現状

世界初の量子暗号方式は，1984年にBennettとBrassardにより提案されたBB84プロトコルであり，現在もこれが事実上の標準になっている．1992年には提案者自らが実証実験に成功し，その後も世界中で実験報告が増え続けている．現在ではNECや東芝欧州研が，通信距離50km，通信速度1Mbps程度で安定動作する試作機を保有している．またスイスのid Quantique社からは，一般消費者向けの量子暗号装置が発売されている．

■ 理論と現実のギャップ

したがって量子暗号はすでに製品化された暗号装置であり，なおかつ絶対に安全であるということになる．であれば，その安全性をこれ以上改良する余地はないはずだが，実際には現在も研究は続けられている．そして「従来よりもさらに安全な方式」が新たに提案されることもある．これは一体どういうことであろうか．

その最大の理由は，安全性証明で使われる暗号装置の記述（数学モデル）と，実際の暗号装置との間に常にギャップがあるということである．

安全性証明の理論の進展

前述のとおり，量子暗号は絶対的な安全性を標榜しているので，盗聴者がいかなる盗聴方法を用いたとしても安全でなければならない．これを「コヒーレント攻撃に対する安全性」という．そしてこのコ

ヒーレント攻撃に対する厳密な安全性証明が初めて得られたのは2000年頃のことであった（Mayersのもの，Bihamらのもの，Shor-Preskillのものなど複数あるが，詳しくは文献3）参照．以下ではまとめて便宜的にShor-Preskill論文と呼ぶ）．それまでは盗聴者の能力を低く見積もった状況（個別攻撃や集合的攻撃（collective attack））のみが考慮されていた．

しかしこのShor-Preskill論文にも，前提条件が厳しすぎて非現実的であるという問題点があった．たとえば，送信者も受信者も光子1つ1つを厳密に制御できるという前提が置かれていた．言いかえるとこの証明は，厳密な単一光子源と，光子数を識別できる単一光子検出器との両方が使える場合にしか有効ではなかった．

当時すでに量子暗号の実験が盛んだったが，単一光子源や単一光子検出器を使ったとするものは少数派だった．実は現在でも，単一光子を，Shor-Preskill論文が要求するレベルで厳密に制御することはできていない．そして大多数の実験では代替手段として，光源にはレーザが，光検出器にはアバランシェ・フォトダイオード(APD)が使われている．そこにShor-Preskill流の安全性評価をあてはめることはもちろんできないのだが，2000年代中頃までの実験の論文では，Shor-Preskill流の証明をあてはめて安全性解析をするのが普通であった．つまり理論と実際の装置との間に明らかなギャップがあったわけである．

やがてその後，安全性証明の理論が進展し，このギャップを埋める方法が提案された：

- レーザ光源を用いた場合の安全性証明
  (Gottesman-Lo-Lütkenhaus-Preskill)
- デコイ法(Hwangほか)
- Squash演算子を用いた方法
  (鶴丸―玉木, Beaudry et al.ほか)

この結果，レーザやAPDといったかつての「代替手段」を用いたとしても安全性が示せるようになり，現在に至っている．

現在進行中の変化

このように量子暗号の分野では，すでにある暗号装置を，安全性証明があとから追認するということがよくある．そしてこの「現実へのキャッチアップ」はいまだに続いている．その1つは有限長解析であり，もう1つは安全性ループホールの解析である．本稿では，これらの新たな要素を考慮した安全性の考え方について概観する．

量子暗号方式の概要

安全性の説明に入る前段階として，まず，量子暗号の代表的な方式であるBB84プロトコルについて説明する．このプロトコルの目的は，送信者Aliceと受信者Bobが通信を行い，第三者に秘密の乱数列（以下，秘密鍵）を共有することである．

■BB84プロトコル

AliceとBobは，光子を送るための「量子通信路」(例：光ファイバ）と，通常のディジタル通信路である「古典通信路」の2種類の通信路を使う．そして盗聴者Eveは，量子通信路に対していかなる盗聴行為もできるとする．一方で古典通信路については，盗聴は自由にできるが通信内容の改変はできないとする（この条件は，量子暗号を用いずとも，従来型のメッセージ認証方式（Wegman-Carter方式など）を用いれば満足できる）．また説明を簡単にするためにこの節では，Aliceが単一光子源を，Bobが単一光子検出器を持っていると仮定する．

AliceとBobは，盗聴行為を検出するために一種のスクランブルを行う．つまり乱数ビットを送受信する際に，X基底とZ基底という2種類の変調方式を，毎回ランダムに切り替える（X, Z基底の詳細については後述）．このときもちろん，Aliceがどちらの基底を選んだかを，Eveが常に正しく当てることはできない．

後にもう少し詳しく説明するが，量子力学の不確定性原理によれば，光子にのせられた情報を誤り確率ゼロで読みとるには，変調時と同じ基底を選択し

なければならないことが知られている．つまり光子を，正しい基底，すなわち送信時に用いたのと同じ基底で測定すれば，正しいビット値を得ることができる．しかし誤った基底で測定すると，ランダムなビット値が得られる．なおかつ，後から正しい基底で測定をやり直したとしても，元の値は確実には再現できない．

したがって，基底選択を知らずに盗聴をしなければならない Eve は，ある確率で盗聴の痕跡であるエラーを残すことになる．以下に BB84 プロトコルを具体的に記述する [3]．

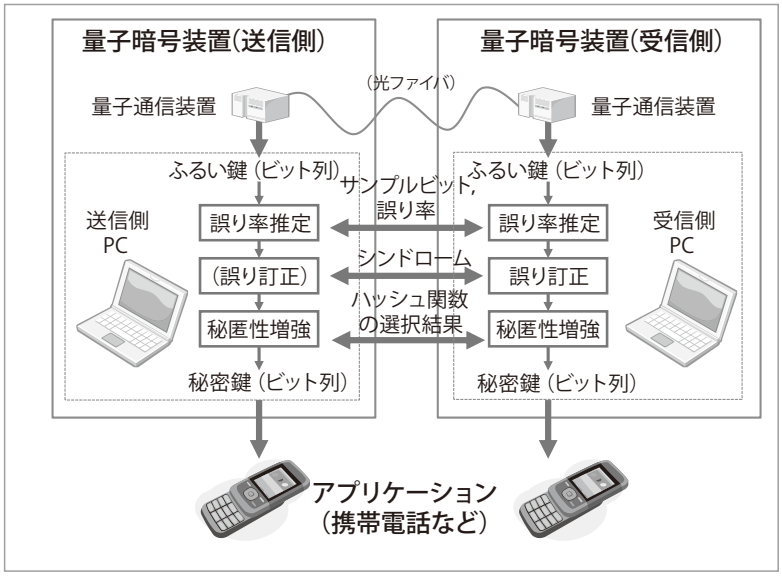

図 -1　量子暗号プロトコルの処理の流れ：量子暗号装置の役割は秘密鍵を配送するところまでである．水平方向の矢印は古典通信路での通信を表している．また最下段は，秘密鍵を携帯電話に移して，秘密通信に使う状況を表している．ふるい鍵の情報の一部は盗聴者に漏れている可能性があるので，秘匿性増強でそれをキャンセルする（→図 -2）．

(1) 量子通信：

1.1　送信者 Alice 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 Bob に送信する．

1.2　受信者 Bob は，受け取ったパルスを，X, Z 基底をパルスごとにランダムに選び測定する．

1.3　Alice と Bob はお互いの基底選択を，公開通信路を使って公開する．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) と呼ぶ．それ以外のビット値は破棄し，以後の処理には使わない．

(2) 位相誤り率推定：生鍵ビットのうち，X 基底のもの（l ビットとする）をまとめてサンプルビットと呼ぶ．Alice と Bob はお互いのサンプルビットを公開し，ビット値が異なっている比率を算出して p_{smp} とおく．そして p_{smp} をもとに，受信側の位相誤り率 p_{ph}（後述）の推定値 $\hat{p}_{\mathrm{ph}}(p_{\mathrm{smp}})$ を算出する．

(3) 誤り訂正：生鍵ビットのうち Z 基底のもの（n ビットとする）をまとめて，ふるい鍵（sifted key）と呼ぶ．Alice（または Bob）は k ビットのシンドローム（パリティ情報）を公開し，誤り訂正符号を用いて，お互いのふるい鍵の食い違いを訂正する．

(4) 秘匿性増強処理：(3) の出力を，ランダムに選んだハッシュ関数に入力して

$$s = \max\left[n\left(1 - h_2\left(\hat{p}_{\mathrm{ph}}\right)\right) - k, 0\right]$$

ビットの秘密鍵を得る．ここで $h_2(x)$ は 2 値エントロピーである．

この処理により，盗聴や (3) の誤り訂正で漏れた情報と，秘密鍵の相関をほぼゼロにすることができる（図 -2）．

なおハッシュ関数は，Alice または Bob が，ステップ (1) の終了後に，（双対）ユニバーサルハッシュ関数族から関数を 1 つランダム選択し，それを相手方に公開する．

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ることになる（**図 -1**）．またそれ以外の目的の使用も可能であり，たとえばメッセージ認証用の秘密鍵に使うこともできる．

■ 不確定性原理と盗聴検出

ここで盗聴検出についてやや詳しく説明する．盗聴検出で重要なのは光子の送受信を行う際に 2 つの基底を用いることであるが，現実の量子暗号装置で，

X 基底や Z 基底として使われる変調方式の例としては，光の偏光（振動方向）を使うものがある．この場合，進行方向を軸として 0 度，90 度方向（45 度，135 度方向）に振動する単一光子に，ビット値 0, 1 をそれぞれあてはめるのが Z 基底（X 基底）である．

これ以外の X, Z 基底の設定方法の一般論はここでは触れないが，この先の議論ではさしあたって以下の事実が必要となる．つまり，X, Z 基底が適切に設定されている場合，Eve が盗聴で得た情報量に応じて，ステップ (2) における誤り率 p_{smp} が増えるということである．詳細については文献 2)，3) を参照願いたいが，概要は以下のとおりである．

まず量子力学では不確定性原理が成り立ち，粒子の位置と速度を同時に，誤差ゼロで決定することはできない．光子も量子力学に従うので，量子暗号で使う X, Z 基底も，同様に不確定性原理が成り立つように設定できる．その場合，一方の基底でのビット値が確定すると，もう一方の基底におけるビット値は不定になる．

したがって光子を，正しい基底，つまり送信時に用いたのと同じ基底で測定すれば，正しいビット値を得ることができる．しかし誤った基底で測定すると，ランダムなビット値が得られる．なおかつ，後から正しい基底で測定をやり直したとしても，元の値は確実には再現できない．

ステップ (2) にあるとおり，Alice と Bob は，2 人とも同じ基底を用いたときの乱数ビット列だけを事後選択し，サンプルビット列を生成している．一方で盗聴者 Eve は，光子が通信路上にあるときに盗聴をしなければならないが，この段階では Alice と Bob の基底は公開されていない．このため Eve は，確率的に誤った基底で測定を仕掛けることになる．したがって盗聴を行うと，サンプルビット列に必ず誤りが生じ，誤り率 p_{smp} が増える．

つまり p_{smp} は Eve の盗聴行為の強さに相当する．また，p_{smp} が増加すれば $\hat{p}_{\mathrm{ph}}$ も基本的には増加する関係にあることが知られているので，ステップ (4) で最終的に生成される秘密鍵の長さ s は，p_{smp} の単調減数関数になる．したがって p_{smp} が大きくなり，Alice と Bob の生成する秘密鍵は短くなる．そして p_{smp} がある閾値を超えていたら，Alice と Bob は秘密鍵をまったく生成しない．これが盗聴検出の原理である．

■秘匿性増強と位相誤り率

続いてステップ (2) で言及した位相誤り率 p_{ph} と，ステップ (4) の秘匿性増強について概要を説明する．理論的な詳細については，たとえば文献 2)，3) を参照願いたい．

まずステップ (2) の p_{ph} とは，Alice と Bob の両者が，ふるい鍵に対して仮に X 基底を用いて測定した場合に表れる誤り率のことである．もし p_{ph} を直接測定することができれば，Eve が盗聴で得た（量子論的な）情報量は $nh_2(p_{\mathrm{ph}})$ ビット以下だと正確に結論できる．しかし BB84 プロトコルではステップ (1) の 1.1 ですでに Z 基底の測定を行っており，そこに後から X 基底の測定を行うことはできない（行ったとしてもランダムな値が出るだけで，p_{ph} の正しい値は得られない）．そこでかわりに，サンプルビットに対して X 基底の誤り率 p_{smp} を測定し，そこから p_{ph} の上界の推定値 $\hat{p}_{\mathrm{ph}}(p_{\mathrm{smp}})$ を求めるという作戦をとっている．そうすれば，Eve が盗聴で得た情報量はたかだか $nh_2(\hat{p}_{\mathrm{ph}})$ ビットであると結論付けられる（ちなみにこの段落は，前節の盗聴検出に別の説明を与えたことにもなっている）．

結果としてステップ (3) の終了時に，Eve に漏洩している（量子論的な）情報量はたかだか，公開した k ビットのシンドロームと，盗聴による $nh_2(\hat{p}_{\mathrm{ph}})$ ビットである．そこで続くステップ (4) の秘匿性増強では，訂正鍵をハッシュ関数で撹拌することにより，これらの漏洩情報をキャンセルしている（**図 -2**）．そして残った s ビットが秘密鍵として得られている．

上記のような，盗聴者の情報を秘匿性増強で打ち消すという枠組みは，いわゆるワイヤタップ通信路（たとえば文献 1）17 章）や抽出器 (extractor) の設

定と非常に似ている．ただし量子暗号では大きな違いが2つある．1つは，Eveへの漏洩情報量は未知なので，p_{smp}の値から毎回推測する必要があることである．もう1つは，Eveが量子力学的な盗聴操作を行うことを想定しているので，安全性証明に量子力学を用いる必要があることである．

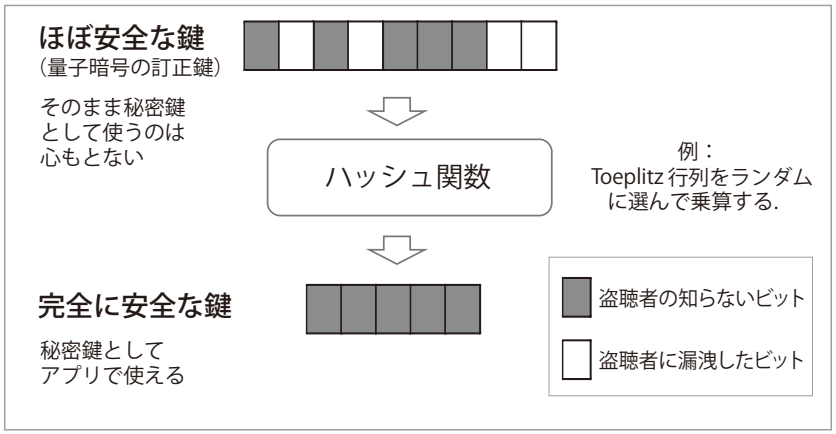

図-2　秘匿性増強のイメージ：非常に大まかにいうと「大体安全」な暗号鍵を「完全に安全」にする確率的アルゴリズムである．ハッシュ関数としては，ユニバーサルハッシュ関数，または双対ユニバーサルハッシュ関数が広く用いられている（※ただしこの図はあくまでイメージである．実際には各ビットが白黒はっきり分けて漏洩するわけではないし，漏洩するのは量子状態である）

有限長解析

前章で述べたとおり，量子暗号の安全性を正しく評価するには，位相誤り率p_{ph}が重要である．しかしp_{ph}は直接測定できないので，かわりにサンプルビットの誤り率p_{smp}から推定値$\hat{p}_{\mathrm{ph}}(p_{\mathrm{smp}})$を求めて代用している．ここでもしサンプル数$l\to\infty$の漸近的な振舞いを見たいだけなら，単純に$\hat{p}_{\mathrm{ph}}(p_{\mathrm{smp}})=p_{\mathrm{smp}}$とおいてもよい．実際2010年以前のほとんどの実験の論文ではそうやって秘密鍵長sを算出していた．しかし現実の装置ではサンプル数lが有限であり，$\hat{p}_{\mathrm{ph}}(p_{\mathrm{smp}})$と$p_{\mathrm{smp}}$の値が統計的にずれるので，これは正しくない．

■有限長解析

厳密にやるなら，統計学の教科書にあるような区間推定を行って$\hat{p}_{\mathrm{ph}}(p_{\mathrm{smp}})$を求める必要があるが，それを実行するのが有限長解析である．その場合もちろん，漸近的な場合（つまり$\hat{p}_{\mathrm{ph}}(p_{\mathrm{smp}})=p_{\mathrm{smp}}$とした場合）と比較して，鍵生成率（$=s/m$）は低下するが，これを有限長効果という．

本章では，有限長解析を厳密に行いつつ，鍵生成率s/mを最大化するための最新の試みについて紹介する．鍵生成率s/mは，量子暗号装置の通信速度（鍵生成速度）そのものであり，応用上も重要な意味を持っている．

まず最初に，一度のプロトコルで扱う光子パルス数mを一定にしたまま，鍵生成率s/mを最大化させる方法を考えてみる．そのためにはステップ(2)で$\hat{p}_{\mathrm{ph}}$をタイトに区間推定し，(4)で削られるビット数$nh_2(\hat{p}_{\mathrm{ph}})$を小さくすることが望ましい．そのためには，区間推定の方法を改良することと，サンプル数lを増やすことが考えられる．

サンプル数lを増やす安直な方法として，ステップ1.1と1.2において，X基底を選ぶ確率をZ基底より高く設定し，サンプルビット長lを増やすということが考えられる．しかしこの場合，ふるい鍵長nも同時に減ってしまうので，最終的な鍵生成率s/mが改善するとは限らない．つまり有限長解析では，X, Z基底の選択確率にはトレードオフが存在する．

■秘匿性増強処理のボトルネック

サンプル数lを増やすもう1つの方法として，光子パルス数mを増やすというものもある．しかしこの場合，秘匿性増強の処理速度がボトルネックになるという新たな問題が生じる．以下でこの問題を，具体的な数字をあてはめて考察してみよう．

まず安全というからには，推定の失敗率（危険率）は大きくても10^{-10}以下にしたい．またサンプルが多すぎると，それだけで鍵生成率が低下するので$m\gg l$としたい．そこでたとえば$l/m=1/1000$という条件のもと，危険率10^{-10}，推定誤差1%で，p_{ph}の上界を片側区間推定することにすると，パルス数mを10^6以上にする必要があることが分かる．

次に装置のパラメタについて考えてみる．まずス

テップ(1)量子通信の典型的スループットは1Mbps程度である．一方で，従来型の秘匿性増強アルゴリズム（計算量 $O(m^2)$）を用いてソフトウェア実装を行うと，$m \geq 10^6$ のときのスループットは100kbpsに満たない．つまり秘匿性増強が，量子暗号システム全体のボトルネックになってしまう．専用FPGAボードを用いることにより若干状況は改善するものの，$O(m^2)$ のアルゴリズムを用いている限り $m \cong 10^6$ 程度が限界である．

以上をまとめると，サンプル数 l に対して $10^6 \geq m \gg l$ という関係が得られる．つまり秘匿性増強の処理速度の限界のために，サンプル数 l にも上限があるということが分かる．

■鍵生成率低下の解決策

これらの鍵生成率の低下の問題を解決するには，以下の2つのアプローチがある．

1つめは量子暗号の安全性証明の理論を改良することである．この方面の最近の成果として，林―鶴丸は，安全性証明の理論を改良することによって，量子暗号の鍵生成率 s/m を（m の各値に対し）向上させることに成功した[2]．つまりこの方法により，同じ光子パルス数 m から，より多くの秘密鍵を抽出することが可能になった．従来研究では，p_{smp} によらず秘密鍵長 s を一定にしていた．これに対し林―鶴丸論文では，p_{smp} に応じて秘密鍵長 s を変化させ（前章のプロトコル参照），平均として高い秘密鍵長を実現している．さらに，従来使われていた二項分布の代わりに超幾何分布を用いることによって，解析を精密化させている．

2つめの解決策は，秘匿性増強の方式（ハッシュ関数）を最適化して，処理速度を向上させることである（たとえば文献7）参照）．実際，Toeplitz行列によるユニバーサルハッシュ関数を用いることにより，秘匿性増強が計算量 $O(m \log m)$ で実装可能であることが知られている．実はこの方法は既存技術の組合せであり真新しさはないのだが，量子暗号研究者に広く知られるようになったのは比較的最近（2010年頃）のことだった．この方法により，ソフトウェア実装でも $m \geq 10^9$ の秘匿性増強処理が可能になった．

上記2種類の改良を組み合わせることにより，高い鍵生成率 s/m を保ちつつ，ソフトウェア実装でも十分な速度が達成可能となった．

ちなみに秘匿性増強方式の性能の尺度としては，処理速度以外に，シード乱数の消費量やエントロピーがある．この方面の改良方式としてはたとえば，鶴丸―林によって提案された「双対」ユニバーサルハッシュ関数を用いるものがある[7]．

安全性ループホール

最初の章で見たとおり，今日では，レーザとAPDを用いた安価なQKD装置についても，安全性が厳密に証明できている．しかしここで新たな疑問が生じる．安全性証明で仮定されているような，レーザやAPDを記述する数学的モデルは，現実の装置を正しく記述できているのであろうか？

理論的にはレーザはコヒーレント光源，APDは閾値検出器であり，それぞれ量子力学の演算子として数式で記述されている．もし目の前にある暗号装置が，それらの数式通りの振舞いをするなら安全性は厳密に保証できる．しかし実際の装置を厳密に記述することは非常に困難であるし，想定していない動作領域では何が起こるか分からない．

このような，現実の装置と数学モデルとの差を「安全性ループホール」と呼ぶが，これを突いた盗聴実験が実際に報告されている．またそれに対するさまざまな対策も提案されているが，光源と検出器とで，その難易度が若干異なっている．

まず光源においては，正規の送信者が，自ら用意した光パルスに対してデータを変調しているので，盗聴者の自由度は低い．したがって安全性ループホールのいくつかは比較的容易に閉じることができる[4]．

その一方で光子検出器に対しては，盗聴者が任意の光パルスを自由に入射できるので，強力な盗聴方法が存在する．たとえばTime Shift AttackやDetector Blinding Attackと呼ばれるものがそれで

ある．2010 年までの段階で，この種の盗聴方法に対する対策はいくつか知られていたものの，安全性ループホールすべてを完全に塞がれているとは言いがたかった．

■ 検出器に対する解決策：Measurement Device Independent QKD

しかし 2011 年になって，光子検出器の安全性ループホールすべてを完全に塞ぐ Measurement Device Independent QKD (mdiQKD) と呼ばれるアイディアが，Lo, Curty, Bing らによって提案された[5]．この方式の基本的な考えは，Alice と Bob はともにパルスの送信だけを行うことである．つまりビット値の生成に光子検出器を一切用いないので，光子検出器の任意の安全性ループホールを塞ぐことができるのである．しかし，光子を送っているだけだと鍵を生成することができないので，鍵を生成するためには Alice と Bob から送られてくる 2 つの光子に対し相関を持たせるような測定を行う必要がある．その測定装置は Alice と Bob 間に置かれており，さらに測定結果を Alice と Bob に公開チャネルを通じて伝える機能も備わっている．この測定結果に応じたデータ処理を行うことにより，暗号鍵が生成される．重要なことは，この測定装置が Eve の支配下に置かれており，どのような測定が行われているかを Alice と Bob は知らなくても，暗号鍵が生成できることである．言い換えると，Eve は盗聴者であるが，プロトコルを実行する際にはプロトコルの参加者にもなっており，このような状況でも安全な鍵が生成できるのである．以下では，mdiQKD がなぜ鍵を生成できるかについてもう少し詳しく説明する．

■ mdiQKD の詳細

まず説明を簡単にするために，雑音や盗聴を考えない理想的な場合を考えてみる（**図 -3** も参照されたい）．まず，送信される状態が実際のプロトコルと同じである盗聴者の視点からはまったく同じプロトコルに見える次のような仮想的なプロトコルを考える．この仮想プロトコルでは Alice は以下のような最大エンタングル状態を準備するとする．

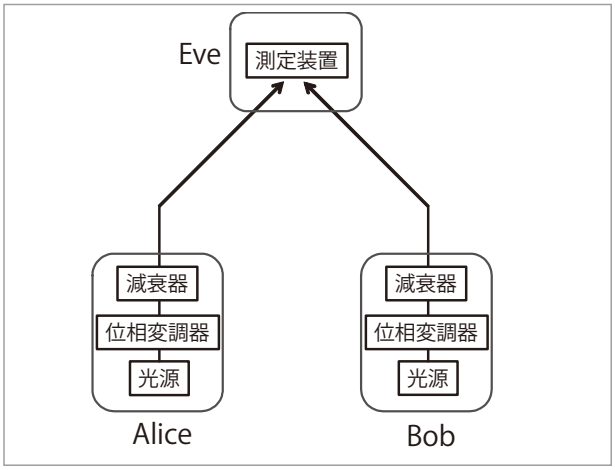

図 -3　mdiQKD の概念図．Alice と Bob はレーザ光源からの光に位相変調器で位相変調を施し，減衰器で単一光子レベルの平均光子数の強度に落としかつ囮状態も生成し Eve へ送信する．Eve は測定装置を用いて測定し，その測定結果を Alice と Bob へ伝える

$$\left|\Phi^{+}\right\rangle_{VACA} := \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_{VA}\left|0\right\rangle_{CA} + \left|1\right\rangle_{VA}\left|1\right\rangle_{CA}\right)$$

ここで，系 VA は Alice が状態準備の後に手元に残しておく物理系であり，系 CA は量子通信路を介して Alice が送信する単一光子を表す．ここで，$|0\rangle_{CA}$ と $|1\rangle_{CA}$ は互いに直交しているキュビット状態であり，Bob についても Alice とまったく同様な状態を準備し，光子を送信することを考える．

ここで，もし，何らかの方法で系 VA と系 VB を最大エンタングル状態に変換できれば，系 VA と系 VB を測定することによって，鍵が生成できることが知られている．この状態変換に必要な操作を行っているのが測定装置とその測定結果に応じたデータ処理なのである．

もし測定装置がベル測定と呼ばれる 2 つの光子に相関を持たせるような測定を行えば，系 VA と系 VB は最大エンタングル状態に変換される．しかし，Eve は必ずしもベル測定を行うとは限らず，ベル測定以外の測定を行ったり，嘘の測定結果を伝えることも考えられる．これらの場合，系 VA と系 VB は最大エンタングル状態以外のなんらかの雑音がのった状態になっているが，Alice と Bob はテストビットを用いることにより，雑音の割合を推定するこ

とができる．もしこの雑音の割合が大きすぎなければ公開チャネルを介した状態操作により雑音がのった状態から最大エンタングル状態を取り出せ，鍵を生成できることが知られている．

上記の仮想プロトコルでは最大エンタングル状態を生成し，系 VA と系 VB に対して状態操作を行い，鍵生成することを考えたが，これら一連の操作で得られる鍵の安全性と実際のプロトコルで生成される鍵の安全性はまったく同じであることが数学的に示されるので，実際のプロトコルで生成される鍵の安全性も保障されることになる．

■光源ループホールも含めた解決策

mdiQKD の出現で，安全性ループホールについては送信機のみ考えれば良いことになるが，送信機の安全性ループホールを塞ぐ研究も進んできている．たとえば，文献 5）で初めて提案された mdiQKD 方式ではレーザ光源が BB84 で規定された状態を厳密に準備できることを仮定しているが，文献 4）で提案された方法を mdiQKD に適用すると，状態の準備は正確である必要もないことが分かる．さらに，光源がキュビットを放出していなくても mdiQKD が可能なことも示されている[6]．これらの方法を発展させ実装することにより，安全性ループホールがほとんど存在しないきわめて安全な QKD が完成する日も近いと思われる．

今後の展望

量子暗号は物理法則を安全性の根拠にした暗号方式である．そしてその安全性を保証するためには，現実の暗号装置の振舞いを正確に記述したうえで，数学的に厳密な安全性証明を与える必要がある．これは現代暗号において，数学的な安全性証明だけではなく，安全性ループホールへの対策も同様に重要であるという状況によく似ている．

ただし量子暗号の場合は，サイドチャネルを塞ぐという目的のためにも，量子力学特有の対策方法が使えるという利点がある．本稿で解説した mdiQKD がその例であり，これを用いると受信機のいかなるサイドチャネルをも防ぐことができる．

とはいえこの方向を推し進めて，まったく信用できない暗号装置から安全な鍵を生成することはもちろん不可能である．したがって一部のコンポーネントについては，何らかの検証を行ったうえで信用する必要がある．そしてその検証手法においては，現代暗号における，20 年にわたるサイドチャネル研究の蓄積が活用できると考えられる．このために今後，現代暗号と量子暗号の研究者の，サイドチャネル研究における協力を促進していきたい．

参考文献

1) Csiszàr, I. and Körner, J. : Information Theory : Coding Theorems for Discrete Memoryless Systems, Second Edition (Cambridge University Press, Cambridge, UK, 2011).
2) Hayashi, M. and Tsurumaru, T. : Concise and Tight Security Analysis of the Bennett-Brassard 1984 Protocol with Finite Key Lengths, New J. Phys. 14 (2012) 093014.
3) Nielsen, M. A. and Chuang, I. L. : Quantum Computation and Quantum Information (Cambridge Univ. Press., Cambridge, 2000).
4) Tamaki, K., Curty, M., Kato, G., Lo, H-K. and Azuma, K. : Preprint : to appear in Phys. Rev. A
5) Lo, H-K., Curty, M. and Qi, B. : Phys. Rev. Lett. 108, 130503 (2012).
6) Tamaki, K., Lo, H-K., Fung, C-H. F. and Qi, B. : Phys. Rev. A 85, 042307 (2012).
7) Tsurumaru, T. and Hayashi, M. : IEEE Trans. IT 59, pp.4700-4717 (2013).

（2014 年 8 月 7 日受付）

鶴丸豊広　Tsurumaru.Toyohiro@da.MitsubishiElectric.co.jp

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．博士（理学）．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．

玉木　潔　tamaki.kiyoshi@lab.ntt.co.jp

2004 年総合研究大学院大学にて博士過程修了．その後，ペリメータ理論物理学研究所，トロント大を経て 2006 年 NTT 物性科学基礎研究所入社．専門は量子情報理論．