量子暗号通信と光が果たす役割

松井　充・鶴丸　豊広

Quantum Cryptography and the Roles Played by Optics

Mitsuru MATSUI and Toyohiro TSURUMARU

Quantum cryptography is a type of cryptographic technology that achieves unconditional security by utilizing quantum theory. In this paper, we first illustrate its basic structure with the example of the well-known Bennett-Brassard 1984 (BB84) protocol, and then explain the development of the theory of security proofs.

Key words: optics, quantum cryptography, quantum key distribution, quantum information theory

量子暗号（quantum cryptography）は量子論を応用した暗号技術である[1,2]．しばしば量子計算機[1]（quantum computer）と混同されて，全くの未来技術だと思われることがあるが，実は現在でもすでに実用化できる段階にある．実際，通信距離 100 km 前後での実験報告が多くなされているのに加え[3]，いくつかのベンチャー企業からは量子暗号装置が発売されている[4]．本稿の目的はこの量子暗号の概要，およびその安全性証明の進展について解説することである．

量子暗号の最大の売りは無条件安全性（unconditional security）である．従来型の暗号はほぼすべて，何らかの計算量的仮定（computational assumption）をおいた上で初めて安全性が保証される[5]．たとえば現在広く用いられている RSA 暗号方式は，素因数分解問題を解く効率的アルゴリズムが現状では知られていない，ということを安全性の根拠としている．しかし一方で，素因数分解問題が困難であるという数学的な証明が得られているわけでもなく，将来そのようなアルゴリズムが見つかって RSA 暗号が破られる，という可能性は残っている．いいかえれば，RSA 暗号の安全性は数学的に無条件に保証されたものではなく，つきつめると経験則で保証されているにすぎない．

一方で量子暗号においては安全性の根拠として，量子力学のみを仮定して数学的に厳密に安全性証明を行う[1,2]．したがって量子暗号を破る方法を見つけた場合には，量子力学に反する現象を見つけたことを意味する．しかし量子力学はいわば物理における大原則であり，実際にその成立以降一世紀近くにわたって矛盾する現象は一切見つかっていない．この意味で，量子暗号は無条件安全性を達成している．

1.　量子暗号の概要

1.1　量子暗号の機能

本稿では，量子暗号の中でもとりわけ量子鍵配送（quantum key distribution, QKD）に特化して解説することとし，量子暗号といえば量子鍵配送をさすものとする．量子鍵配送の目的は，送信者 Alice と受信者 Bob が，秘密のビット列 $K=(k_1, ..., k_n)$，$k_i \in \{0, 1\}$ を共有することである．なおかつこの k が，いかなる盗聴者 Eve にも盗み見られていないことを，証明つきで保証できる．ただしここでいう「盗み見られない」の意味が，通常の暗号の場合とはやや異なっている．

まず，秘密のビット列 K は，送信者や受信者が自由に選ぶことはできない．もし K を自由に選べるならば，初めからメッセージ M を K として選べば，直接に暗号通信ができる．しかし量子暗号の場合，K の具体的な値はプロトコルが終わるまで判明しない．これはプロトコルの構造に起因する（第 2 章参照）．

次に，送ったビット列を途中で誰かに盗み見られたとし

三菱電機(株)情報技術総合研究所（〒 247-8501 鎌倉市大船 5-1-1）　E-mail: Matsui.Mitsuru@ab.MitsubishiElectric.co.jp

ても，事後の統計処理でそのことをほぼ確実に検出できる．しかしKが盗み見られた事実は覆すことができない．したがってこの場合は，その乱数列Kは捨て去って，同じプロトコルを再び実行する．そして，乱数列Kが盗聴されていないことが検証できるまで繰り返す．そもそも元々送っているのが乱数なので，盗聴された分は捨ててしまって，別の乱数を最初から送りなおせば問題はない．

乱数でなくメールや画像など，自分で選んだメッセージMを秘密に送りたいときは，まず量子暗号で乱数列KをMと同じ長さだけ共有する．そしてそれを秘密鍵として，ワンタイムパッド（one-time pad）で通信すればよい．つまりKとMの排他的論理和$C=M\oplus K$を暗号文として送ればよい．

それでは，乱数が途中で盗聴されたかどうかをどうやって判定するかというと，それは，手が加えられた場合には，高い確率で変化が起こるような特殊な媒体に乗せて送るのであり，それがすなわち量子である（量子力学の詳細については専門の教科書にゆずる[6,7]）．なおここでいう「変化」とは，通信の途中でその乱数に乗るビット誤りのことである．すなわち大まかにいうなら量子暗号とは，乱数ビットを送信者が量子に乗せて送り，それを受信者が読み取り，そこに乗ったビット誤り率を事後のランダムサンプリングによって検証する．そしてそのビット誤り率が想定していた値よりも多かったら，それは途中で盗聴された証拠だとして通信をやり直す，というものである．

1.2 量子として光を用いる

そして量子暗号では，量子としてもっぱら光を用いている．よく知られている通り，世の中を構成する物質や相互作用は電子，陽子，電磁場などの微小な構成要素からなっているが，これらはすべて量子としての性質を示す．つまり物質でも光でもなんでも，微小に分割して精密測定を行うと量子性がみえてきて，上記でいう「手を加えると変化する」という性質が現れてくる．したがって原理的には，どんなものでも十分微小に分割すれば量子暗号に用いることができるのだが，現状では，雑音への耐性や制御の容易さから，もっぱら光のみを用いて実験が行われている．この光の粒子を特に光子（photon）とよび，その光子1つにつき1ビットずつ乱数列の情報を乗せて送り出す．そしてそれを光ファイバーで伝送し，最大で100 km程度の通信距離を実現している．

そして理想的には，送信者Aliceの光源として厳密な単一光子源を用いることが望ましい．これはすなわち，Aliceの光源が1パルスに厳密に光子を1つずつ出し，2つ以上を出すことは決してないという状況である．実際，初の量子暗号方式であるBB84方式が提案された当初はこのような状況が想定されていた．しかしこのような単一光子源を実装するのは困難なので，大多数の実験では，レーザー光を減衰器で極度に弱めた微弱コヒーレント光（weak coherent light）で代用している（詳しくは第3.3節「デコイ方式」参照）．

2. BB84方式

話をより具体的にするため，以下では代表的な量子暗号方式であるBennett-Brassard 1984（BB84）方式[8]について説明する．量子鍵配送方式としてはBB84方式以外にも，B92方式[9]，DPSQKD方式[10]ほか数多くの方式が提案されているが，これらの方式もすべて，多かれ少なかれBB84方式の改良版であるので，BB84方式に特定して説明することによって一般性は失われない．

2.1 符号化

BB84方式の基本となるのは，複素2成分のベクトルで記述される量子状態であり，これをしばしばキュービット（qubit）とよぶ．通信媒体として光を用いる場合は通常，キュービットとしては偏光や，パルス間の位相差を用いる．以下では話を単純にするために偏光の場合に特定して話を進める．詳細は量子光学の教科書等を参照していただくとして，単一光子のもつ偏光の量子状態は複素に成分のベクトルで表される．例えば乱数$b=0,1$をそれぞれ縦偏光（↕で表す），横偏光（↔）に乗せて送る場合には，それらが

$$|0\rangle_{+}=\begin{pmatrix}1\\0\end{pmatrix},\ |1\rangle_{+}=\begin{pmatrix}0\\1\end{pmatrix}$$

という状態ベクトルに対応する．この2状態は直交基底をなしているので「＋基底」とよぶことにする．しかしこれだけだと単なる通信であり，乱数bの値を敵Eveも自由に読み取れて暗号にならない．そこで装置を45度傾けて右斜め上偏光（↗），左斜め上偏光（↖）の状態も用いて，

$$|0\rangle_{\times}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix},\ |1\rangle_{\times}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$$

この2状態を「×基底」とよぶことにする．つまり乱数bを送るにあたって，符号化の方法（すなわち基底）をランダムに選び，それによってEveが盗聴しづらいようにするのである．

2.2 BB84方式の基本プロトコル

BB84方式の具体的な通信プロトコルは以下のとおりである．なおAlice-Bob間には，上記の光を送る通信路のほかに，通信の補助情報を送るための公開通信路もあるとする．この公開通信路はインターネット等の通常の通信路で

よく，暗号化されている必要はないが（したがって通信内容は敵 Eve に漏れていると想定する），通信の内容が改竄されることはないとする．

ステップ 1： 量子通信

1. Alice は，乱数列 $\hat{A}=(\hat{a}_1, ..., \hat{a}_m)$，$a_i \in \{0, 1\}$ と，ランダムな基底の列 $x=(x_1, ..., x_n)$，$x_i \in \{+, \times\}$ を選ぶ．
2. Bob はランダムな基底の列 $y=(y_1, ..., y_n)$，$y_i \in \{+, \times\}$ を選ぶ．
3. Alice は Bob に，n 個の光子をそれぞれ $|a_i\rangle_{x_i}$ の状態にして送る．
4. Bob は Alice から受け取った光子を，それぞれ基底 y_i で観測し，結果を $\hat{B}=(\hat{b}_1, ..., \hat{b}_m)$，$\hat{b}_i \in \{0, 1\}$ として記録する．
5. Alice と Bob は公開通信路を用いて双方の基底 x，y を教え合う．Alice は $\hat{a}_i$ のうち基底が一致したものだけを抽出して $A=(a_1, ..., a_n)$ とする．Bob も同様にして $B=(b_1, ..., b_n)$ をつくる．ここで一般に $n \leq m$ である．

ステップ 2： 誤り率検証とふるい鍵抽出

1. （誤り率検証フェーズ）Alice と Bob は a_i，b_i のうち一部をランダムに選び出し，その値を公開通信路で教え合う．以下，これらのビットを「サンプルビット」とよぶ．Alice と Bob はサンプルビットの値を比較し，それらの値が食い違っている確率，すなわちビット誤り率 e を求める．
2. （ふるい鍵抽出フェーズ）誤り率検証に使わなかった残りのビット列を，Alice，Bob が鍵としてそれぞれ保存する．これを篩にかけられた鍵ということで「ふるい鍵」(sifted key）とよぶ．

ステップ 1 では，送信者 Alice はまず乱数を単一光子の偏光に乗せて送り，それを受信者 Bob が受信する．ただしその際，Alice と Bob が 2 種類ある基底をランダムに選ぶ．そうすると確率 1/2 で両者は同じ基底を選ぶことになるが，基底が一致した分だけを残して後は捨ててしまう．もともと送っているのが乱数なので，このように捨ててしまっても問題はない．この段階をもって光子を用いた量子通信はすべて終了し，これ以降はすべて通常のコンピューター上でのデータ処理である．

ステップ 2 で Alice と Bob は，盗聴者の有無を検証するために，通信で起こったビット誤り率 e を算出する．そして，ここで算出したビット誤り率 e が想定する値よりも高かったとしたら，それは盗聴者の攻撃のせいであるとして通信を打ち切り，最初からプロトコルをやり直すこととする（この「想定する値」については後述）．なお，このビット誤り率 e のことをしばしば，量子ビット誤り率（quantum bit error rate: QBER）とよぶ．また，ここで教え合ったサンプルビットはすべて Eve に漏れているので捨て去ることとし，以降の秘密鍵生成処理では，ふるい鍵のみを使用する．

2. 3　安全性のイメージ（intercept/resend 攻撃）

ここで「盗聴者がいるとビット誤り率が増える」ということのイメージをつかむために，最も簡単な攻撃法である intercept/resend 攻撃[11] について考えてみる．

この攻撃法は，Eve が＋，×のいずれかの基底を予測し，それを用いて Alice が送信した量子信号を測定する，という単純なものである．ここで盗聴が気づかれないためには，当然のことながら，Eve は測定を終えたあと，Alice に代わって何らかの光信号を Bob に届ける必要がある．しかしその際に，Alice が元々送り出したのと同じ信号を，Bob に常に届けるということはできない．というのも Eve は，Alice と Bob が基底を交換する前に攻撃を終えなければならないので，必ず 1/2 の確率で誤った基底を選んでしまうが，その場合 Eve が得るのは，Alice の送り出した状態と無関係なランダムビットである．それに加えて，「観測によって一度変化した状態は元に戻すことができない」という量子論の要請があるので，そのランダムな信号をそのまま Bob に送らなければならなくなる．この結果 Bob の側では，正しい基底を選んで測定しているにもかかわらず，サンプルビットの QBER が 1/4 になってしまい，盗聴が発覚する．

ただしここでは攻撃の一例を考えただけであり，これだけでは無条件安全性を示したことにはならない．無条件安全性を示すためには，以下で述べるように，Eve が量子論で許されるあらゆる攻撃を仕掛けてくると想定した上で，安全性証明を数学的に厳密に書き下す必要がある．

2. 4　通信路雑音のある場合の安全性

第 2.1 節で，Alice と Bob の測定する QBER が想定する値よりも高かった場合に，Eve の攻撃が発覚すると述べた．それではその「想定する値」はどうやって決まるのかといえば，それは現実の量子暗号装置の性能によって決まる．たとえば仮に，Alice と Bob が理想的な装置と通信路を使っていて，Eve がいなければ QBER が厳密にゼロになるとわかっているとする．このときは測定した QBER がゼロでなければすなわち盗聴されていることを意味し，逆に厳密にゼロであったら通信路が安全だとわかる．そして上記のステップ 2 で得られたふるい鍵 A，B を，そのまま秘密鍵 K として使うことができる（例えば文献 1, 第 12 章参照）．

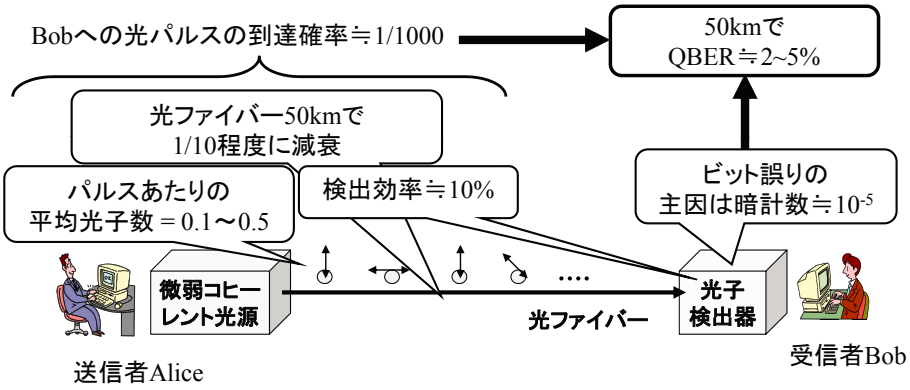

図 1　量子暗号装置はもともと減衰や雑音の巣窟で，敵がいないときでも通信路上でエラーが起こる．

しかし現実には光ファイバーや光子検出器での雑音や損失があるので，盗聴者がいない場合でも QBER はゼロとはならない．第 1.2 節でも述べたように，量子暗号では光源として微弱コヒーレント光を用いることが多く，その平均光子数は $\mu=0.1$ 程度に選ぶ．Alice はその光パルスを数十 km の光ファイバーで送り，Bob がそれを光検出器によって検出するのだが，その検出効率もせいぜい $\eta=0.1$ 程度である．したがって Alice が送ったパルスのうち Bob が検出できるのは 1/1000 程度である．ここに検出器の暗計数が加わった結果，QBER は典型的には 2〜5% となる（図 1）．

このような場合には QBER の扱い方に注意が必要になってくる．たとえば仮に，手元の量子暗号システムを実運用前に調整した結果，敵がいないときの QBER は 2% だとわかったとする．そして次に実運用を開始したところ QBER の測定値が 2% 以下だったとして，したがって通信路は安全であるといえるかというと，実はこれが全くいえないのである．これをみるために，例えば調整時の QBER＝2% がすべて通信路の偏波ゆらぎに起因していたと想定してみる．この場合，実運用時には実は Eve が通信路を乗っ取っていて，偏波ゆらぎが厳密にゼロの通信路に置き換えていたという可能性も否定できない．そうすると，実運用時の QBER＝2% は通信路雑音から来ていたのではなく，すべて Eve の攻撃に起因していたということになる．

もちろん，このような雑音が厳密にゼロの通信路を用意することは現実には困難である．しかし量子暗号が無条件安全性を標榜しているかぎり，攻撃者は物理法則（量子論）で許される限りあらゆる攻撃を行えるとみなさなければならず，上記のような最悪ケースも考慮する必要があるのである．また損失に関しても同様の考え方をする．Alice の出した光信号が Bob に到達しない場合，光ファイバーの損失で消滅したとみなすのが常識的であるが，安全性解析ではそのような常識には頼らない．あくまで可能な限り悲観的に考えて，それは Eve が盗聴のために信号を遮った結果であるとみなすのである．また通信路に限らず，一般に送信機や受信器でも同様に雑音や損失は起こるが，ここでもやはり最悪を想定して，それらもすべて Eve の攻撃の結果であるとみなす．ただし雑音に比べて，損失に関しては対処が簡単である．前にも述べたとおり，もともと Alice が送り出している信号は乱数なので，損失によって Bob に届かなかったとしても，それは最初からなかったものとして捨ててしまえばいいのである．

2. 5　鍵蒸留処理

以上をまとめると，一般に雑音（QBER）のある量子暗号の安全性を考えるときには，まず Alice と Bob は雑音も損失もない完全な送信機と受信器をもっていると仮定する．そして通信の際に起こる QBER や損失は，すべて Eve の盗聴の結果であるとみなす．こう考えながら，Alice が発して Bob に届いた光信号から，ふるい鍵を生成するのだが，QBER がゼロでないということは，Alice と Bob で共有したふるい鍵 A，B の値に食い違いがあるということである．そしてその食い違いはひとえに Eve が盗聴しているせいだとみなすわけだから，A, B の情報の一部（または全部）は Eve に漏洩していると考えなくてはならない．

ここでまず，A, B の値の食い違いは通常の誤り訂正符号によって除去できる．つまり，例えば A が B と等しくなるように誤り訂正できる．また Eve に漏洩した分の情報も，秘匿性増強（privacy amplification）とよばれる演算で除去できる．この誤り訂正符号と秘匿性増強処理とをあわせて鍵蒸留（key distillation）とよび，これによって最終的に秘密鍵 K が生成される．なお，両者ともふるい鍵に対する数値的な演算であり，既存のコンピューター上で実行できる（図 2）．

秘匿性増強に関してはここでは詳細を述べないが，直感

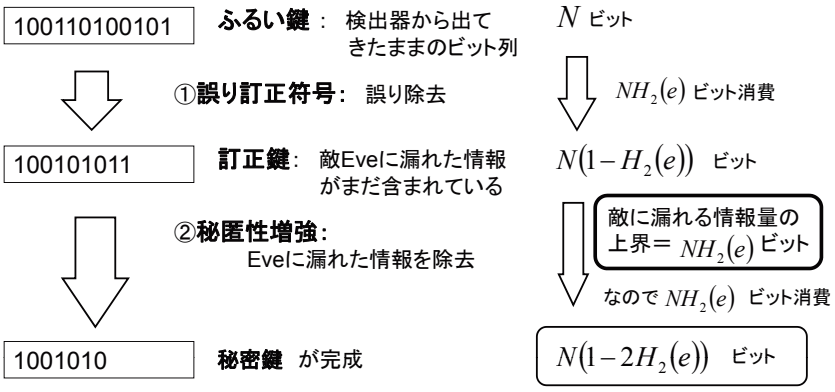

図2　鍵蒸留処理の流れ．ここでeはビット誤り率（QBER）である．

的には暗号学でいうハッシュ関数（hash function）とよく似ている．Eveからみてランダム性の弱いビット列（＝ふるい鍵B）を，ランダム行列Mをかけることによって攪拌・短縮し，よりランダム性は高いが短いビット列（＝秘密鍵$K^T=MA^T$）に変換する．

ただしここでもちろん，秘密鍵が生成できるためにはQBERが十分小さいこと，すなわちEveの攻撃が十分弱くて漏洩情報量が小さいことが必要となる．一般にどの程度のQBERのときに，どのような鍵蒸留処理を行えばいいのかを厳密に解析することが，以下で述べる安全性解析の目的である．

3.　安全性証明の変遷

3.1　無条件安全性の証明

量子暗号の目的は秘密鍵の無条件安全性を保証することである．第2.3節ではintercept/resend攻撃について簡単に触れたが，これはあくまで攻撃の一例にすぎない．無条件安全性をいうためには，Eveは量子力学的に許される限りあらゆる攻撃手法をしかけてくると想定する必要がある．そして第2.4節で述べたとおり，通信路で起こったビット誤りは，すべてEveの攻撃によるものだと想定する．つまりビット誤りが大きければ大きいほど，Eveにより多くの情報が漏れているとみなす．そしてその漏洩情報が，第2.5節の秘匿性増強によって正しく除去されることが保証できれば，秘密鍵Kは安全だということになる．これを理論的に保証するためには，量子論をベースに，数学的に厳密な安全性証明を書き下す必要がある．

これは非常に難しい問題で，初めて厳密な証明が与えられたのはBB84方式が提案されてから12年後の1996年で，Mayers[12]による．ただしその証明は複雑であったため，2000年になってShor-Preskillによってより簡略化された証明方法[13]が提案され，その後数年はこれが主流となった．なお現在では，これら以外にもさまざまな安全性証明の手法が提案されており，おもなものだけをあげても，量子論の相補性を用いるもの[14]，一般化されたPauli通信路の性質に帰着するもの[15]，各信号パルスの置換対称性を用いるもの[16]などがある．そしてそれぞれ適用範囲が微妙に異なっているが，基本的な問題に関してはすべて同じ結論を与える．

これらの安全性証明の結果，ふるい鍵の長さをnビット，QBERをeとしたとき，誤り訂正および秘匿性増強でそれぞれ$nH_2(e)$ビットずつが消費され，最終的な秘密鍵の長さは$n(1-2H_2(e))$ビットとなることがわかった．ただしここで$H_2(e)$は，二値エントロピー$H_2(e)=-e\log_2 e-(1-e)\log_2(1-e)$である（図2）．したがって秘密鍵が少しでも残るためには$1-2H_2(e)>0$となる必要があり，ここから，量子暗号が安全であるためにはQBERが11%未満（$e<0.11$）でないとならないという条件が導かれる．

3.2　Photon Number Splitting（PNS）攻撃

このように，MayersやShor-Preskillの成果によって，安全性証明の土台は2000年ごろまでに完成した．しかし実はこれらの証明にはまだ，量子暗号装置の現実を完全には反映していないという問題点があり，そのうちのひとつが以下で述べる光源の問題であった（もう一方の光検出器の問題については3.4節参照）．これは具体的にいうと，証明の前提として，送信者Aliceは厳密な単一光子源を用いると仮定しているにもかかわらず，現実のほとんどのQKD装置では微弱コヒーレント光が用いられていたというものである（第1.2節）．そして深刻なことに，この代用光源の弱点につけこむ形で，Photon Number Splitting攻撃（PNS攻撃）という強力な盗聴法がLütkenhausによって1999年に発見され[17]，微弱コヒーレント光によるQKDは安全でないということになってしまった．

なぜこのような状況に陥ったかを振り返ってみると，ま

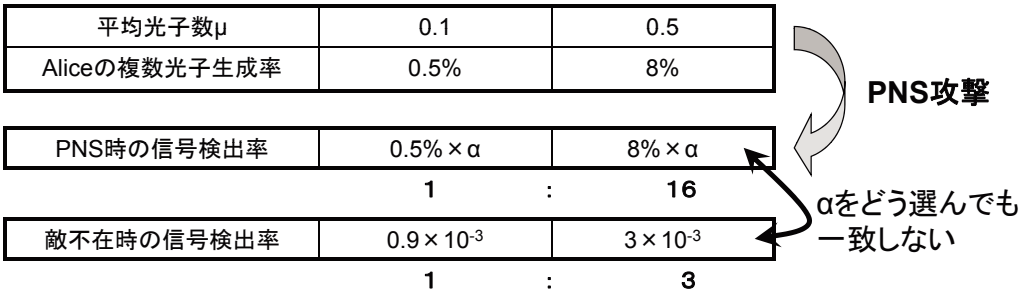

図3　デコイ方式の数値例．ここで平均光子数をデコイ光では μ_d=0.1，信号光では μ_s = 0.5 とし，通信路損失を $\eta=10^{-2}$ とする．また Eve は 1 光子パルスをブロックし，複数光子パルスの一部（その比率を α とおく）を Bob に送り込むとする．

ず BB84 方式が理論的に提案された段階では，Alice の光源は厳密な単一光子源とすべしとされていた．これは光源が各パルスに光子を厳密に 1 つずつ出し，2 つ以上を出すことは決してないという状況である．しかしこのような光源を実装するのは，決して不可能ではないが困難なので，90 年代以降に量子暗号の実験が始まったときには，もっぱら微弱コヒーレント光で代用されていた．この背景にあったのは以下のような考えである．例えば 1 パルスあたりの平均光子数を μ =0.1 とした場合，9 割以上のパルスは光が出ていない真空状態（ゼロ光子状態）であり，また 1 割程度は単一光子であり，2 光子以上を含むパルスは全体の 0.5% 程度である．ここでこれまで何度か用いた「もともと送っているのは乱数なので」というロジックを再び用いると，光が出なかったパルスは最初からなかったことにして捨てることができる．一方で，光子を含んでいるパルスのほうは大多数が単一光子パルスであり，これを近似的に単一光子源とみなせるのではないかという予測が立つ．実際，PNS 攻撃が提案されるまでは（実はその後数年間も），量子暗号実験の安全性解析をする際にはこのような仮定をおくのが普通であった．そして微弱コヒーレント光を用いつつ，通信距離数十 km を達成した量子暗号実験の論文発表や報告が多数なされていた．

この状況に大きな打撃を与えたのが PNS 攻撃であり，これを考慮に入れて安全性評価を正しくやりなおした結果，微弱コヒーレント光を用いた BB84 方式の通信距離は，30 km 未満にしかならないという結論が得られた [17]．この攻撃法のアイディアは，上記でのべた複数光子パルスを利用するというものである．Eve はまず，Alice の発した単一光子パルスをすべて遮断する．そして複数光子パルスにのみ着目し，その中に含まれている光子のうち，1 つはそのまま Bob に送り，残りはすべて自分の手元に残す．そして量子通信が終了して Alice と Bob が公開通信路で基底を公開した後に，その基底で手元の光子を測定する．このとき Eve は 100% 正しい基底でふるい鍵 A を測定できるので，A の値を完全に正しく知ることができる．

ここで，なぜ発生率の極度に低い複数光子パルスだけを送り込んでも攻撃が発覚しないかというと，以下のような事情による．まず，Eve がいなくても Bob への信号到達率はそもそも低い（典型的には 1/1000 程度, 第 2.4 節参照）．また一般に，Eve は損失ゼロの通信路を用いることができると仮定する（第 2.4 節）．したがって到達率が 1/1000 といっても，それが通信路損失によるものなのか，Eve の攻撃によるものなのか，Bob には区別がつかないのである．

3. 3　デコイ方式

この光源の問題に対する自明な解決策はもちろん，厳密な単一光子源やもつれ合い光源を用いることである．しかし一方でより巧妙な解決策も存在し，それが 2002 年に Hwang によって提案されたデコイ（decoy＝おとり）方式である [18]．このデコイ方式によって，コヒーレント光の QKD でも再び長距離で無条件安全性が達成できることが示せることとなった．現在では光ファイバーを用いて通信距離 100 km 程度を実現した実験も報告されている [3]．

この方式は BB84 方式と組み合わせて使うもので，量子信号の強度変調を行うことを特徴とする．Alice は本来の信号（signal）パルスの中に，強度の異なるおとり（decoy）パルスを，ある確率でランダムに混ぜ込んで送る．一方で，攻撃者 Eve はどれがおとりパルスでどれが信号かがわからない状況で攻撃を行うので，光子数分割攻撃を行うと光子数分布を乱してしまい攻撃が発覚する．

なぜこの方法で PNS 攻撃を防げるかを直感的にみるために，数値例を考えてみることとし，信号パルスの平均光子数を μ_s=0.5，デコイ状態について μ_d=0.1 とし，通信路損失を $\eta=10^{-2}$ とする（図3）．このときもし Eve がいなければ，Bob の受け取る信号の検出確率の比は，デコイパルスと信号パルスとで 1：3 となる（ポアソン分布から信号検出率は $e^{-\mu}\mu$ に比例）．一方で Eve が PNS 攻撃を考えて，Al-

ice の送った信号のうち複数光子パルスのみを Bob に送り込んでいたとすると，検出確率の比は 1：16 となって PNS 攻撃の痕跡が現れることになる（複数光子生成率 $\propto e^{-\mu}\mu^2$）．

最後にやや技術的な話になるが，Hwang の 2002 年の論文はデコイ方式の有効性をはっきり示したものではあったが，実はこの段階では無条件安全性はまだ示されていなかった．無条件安全性をはっきりと示したのは 2004 年ごろの Lo *et al.* [19] および Wang[20] の仕事であり，またその中で重要な役割を果たしたのが Gottesman *et al.* の安全性証明の手法（いわゆる GLLP 論文 [21]）である．GLLP の手法についてはここでは詳しくは触れないが，これは Shor-Preskill の安全性証明を改良したものである．そして複数光子の発生率が厳密にゼロでなくても，それが十分小さい場合には安全性が保てることを保証したものである．

3. 4　検出器の問題点と解決策

これまでは Shor-Preskill の証明における前提と，現実の量子暗号装置で用いられている光源との間のギャップ，およびその解消法について説明した．しかし実は Bob の検出器に関しても同様に，以下のようなギャップが存在する．まず Shor-Preskill の安全性証明では仮定として，受信者 Bob は光子数識別検出器を持っていて，複数光子を受け取ったとしても，それを識別して拒否できるとされていた．一方で，現実の QKD 装置で用いられている検出器はほぼすべて「閾値検出器」とよばれる種類のものであり，光子があるかないか（光子数がゼロか否か）は識別できるが，光子数が具体的にいくつかは判別できない．したがって証明の前提を満たしていない．これはキーワード的には上記の光源の問題と似ているが，あくまで別個の問題である．

なぜこれが問題になるかというと，仮に（デコイ方式等によって）Alice が常に単一光子を発しているとみなせる状況でも，Eve の攻撃によってそれらが複数光子に変えられている可能性が否定できないからである．そして閾値検出器を用いている場合には，Bob はそれを知らずに単一光子として検出してしまう．

直感的に考えるなら，Eve がそのように光子数を増やしたとしても，量子論的な制約から劣化コピーしか作ることができないので（非クローン化定理 [1]），有用な攻撃にならないと予想されるが，はたしてそれは正しいだろうか．結果としてはこの予想は正しくて，閾値検出器を用いたとしても安全性上は問題ないことがわかっている．しかしそれが厳密に証明されたのは 2006 年以降と意外に最近のことである．まず一方向古典通信を用いる BB84 方式の場合については，小芦 [22] およびそれに引き続いて林 [15] の安全性証明が得られた．ただしこれらの証明は適用範囲が若干狭く，エンタングル状態による BB84 方式（すなわち BBM92 方式 [23]）や，双方向古典通信を用いている場合には適用できなかった．この点も解決した安全性証明方法としては，2008 年の鶴丸・玉木 [24] および Beaudry *et al.* [25] によるもの（squash 演算子の手法），および小芦らによるもの [26] がある．

本稿では BB84 方式を中心として，量子暗号方式の概要，およびその安全性証明の変遷について解説した．量子暗号はすでに現実の技術であり，通信距離 100 km 程度での実験例がいくつも報告されているほか，いくつかのベンチャー企業からは製品が発売されている．

その一方で，量子暗号はあくまで暗号であるので，安全性証明が正しく与えられて初めて意味をもつという事情がある．また，すでに広く普及している RSA 暗号や AES 暗号といった現代暗号とは異なり，量子暗号は無条件安全を標榜しているため（第 1 章参照），より厳しい前提に基づいて安全性解析を進めなければならない（第 2 章参照）．したがって量子暗号の実現や普及を進めるという立場からすれば，安全性解析は足を引っ張るものと考えられがちである．実際にある時期までは，単一光子源や光子数識別検出器の実装の難しさが，量子暗号実装の大きな足かせと考えられていた．

しかし逆に，安全性解析の理論が進展した結果，実装が容易になった事例も多く存在し，これが本稿で強調したかった点である．いわば「ある条件が満たされていなければ安全でない」という制約を加えるのが安全性解析であるのと同時に，「安全性を損なわないかぎりは何をやってもよい」ということをいうのも安全性解析なのである．たとえば第 3 章で述べた，デコイ方式によって PNS 攻撃が回避できたという事例がそれにあたる．

現在のところさまざまな研究成果（第 3 章の内容を含む）によって，通信距離 100 km 程度の量子暗号に関しては，実装と理論とのギャップはひととおり埋められたと考えられている．その一方でもちろん，数百 km 以上の量子暗号をどう実現するかという根本的な問題が残っていて，その解決のためには量子リピーターなどの新たな技術が必要と考えられている．またそれ以外にも，深刻度はずっと低いが，鍵蒸留処理における有限ブロック長の問題 [15,27] などさまざまな研究課題が残っている．われわれはこれらの問題の解決においても，安全性解析の手法が引き続き大きな貢献をできると期待している．

ここで紹介した研究の一部は，情報通信研究機構（NICT）の支援のもとで行われました．

文　献

1) M. A. Nielsen and I. L. Chuang: *Quantum Computation and Quantum Information* (Cambridge University Press, 2000)；邦訳は木村達也訳, 量子コンピュータと量子計算Ⅰ, Ⅱ, Ⅲ(オーム社，2005)．
2) 小芦雅斗，小柴健史：量子暗号理論の展開(サイエンス社，2009)．
3) QKD 実験は膨大に報告されているが，最近のものでは例えば：A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe and A. J. Shields: "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate," Opt. Express, **16** (2008) 18790–18979; A. Tanaka, M. Fujiwara, S. W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K. Yoshino, S. Miki, B. Baek, Z. Wang, A. Tajima, M. Sasaki and A. Tomita: "Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength-division multiplexing clock synchronization," Opt. Express, **16** (2008) 11354–11360.
4) id Quantique社, www.idquantique.com; Magiq Technologies 社, www.magiqtech.com.
5) 現代暗号については例えば，黒澤　馨，尾形わかは：現代暗号の基礎数理(電子情報通信学会，2004)；岡本龍明，山本博資：現代暗号(産業図書，1997)．
6) P. A. M. Dirac: *Principles of Quantum Mechanics*, 4th Ed. (Claredon Press, 1981)；邦訳は朝永振一郎ほか訳，量子力學(岩波書店，1968)．
7) J. J. Sakurai: *Modern Quantum Mechanics* (Addison-Wesley, 1994)；邦訳は桜井　純訳：現代の量子力学(上，下)（吉岡書店，1989)．
8) C. H. Bennett and G. Brassard: "Quantum cryptography: Public key distribution and coin tossing," *Proc. of International Conference on Computers, Systems & Signal Processing* (Bangalore, India, 1984) pp. 175–179.
9) C. H. Bennett: "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett., **68** (1992) 3121–3124.
10) K. Inoue, E. Waks and Y. Yamamoto: "Differential phase shift quantum key distribution," Phys. Rev. Lett., **89** (2002) 037902.
11) C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin: "Experimental quantum key distribution," J. Cryptol., **5** (1992) 3–28.
12) D. Mayers: "Unconditional security in quantum cryptography," J. ACM, **48** (2001) 351–406.
13) P. W. Shor and J. Preskill: "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett., **85** (2000) 441–444.
14) M. Koashi: "Simple security proof of quantum key distribution via uncertainty principle," arXiv:quant-ph/0505108v1; "Complementarity, distillable secret key, and distillable entanglement," arXiv:0704.3661v1 [quant-ph].
15) M. Hayashi: "Practical evaluation of security for quantum key distribution," Phys. Rev. A, **74** (2006) 022307; "Upper bounds of eavesdropper's performances in finite-length code with the decoy method," Phys. Rev. A, **76** (2007) 012329.
16) R. Renner: "Security of quantum key distribution," arXiv:quant-ph/0512258.
17) N. Lütkenhaus: "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A, **61** (2000) 052304; G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders: "Limitations on practical quantum cryptography," Phys. Rev. Lett., **85** (2000) 1330–1333.
18) W.-Y. Hwang: "Quantum key distribution with high loss: Toward global secure communication," Phys. Rev. Lett., **91** (2003) 057901.
19) H.-K. Lo, X.-F. Ma and K. Chen: "Decoy state quantum key distribution," Phys. Rev. Lett., **94** (2005) 230504.
20) X.-B. Wang: "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett., **94** (2005) 230503.
21) D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill: "Security of quantum key distribution with imperfect devices," Quant. Inf. Comput., **4** (2004) 325–360.
22) M. Koashi: "Efficient quantum key distribution with practical sources and detectors," arXiv:quant-ph/0609180v1.
23) C. H. Bennett, G. Brassard and N. D. Mermin: "Quantum cryptography without Bell's theorem," Phys. Rev. Lett., **68** (1992) 557–560.
24) T. Tsurumaru and K. Tamaki: "Security proof for quantum-key-distribution systems with threshold detectors," Phys. Rev. A, **78** (2008) 032302.
25) N. J. Beaudry, T. Moroder and N. Lütkenhaus: "Squashing models for optical measurements in quantum communication," Phys. Rev. Lett., **101** (2008) 093601.
26) M. Koashi, Y. Adachi, T. Yamamoto and N. Imoto: "Security of entanglement-based quantum key distribution with practical detectors," arXiv:0804.0891v1 [quant-ph].
27) V. Scarani and R. Renner: "Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing," Phys. Rev. Lett., **100** (2008) 200501.

(2009 年 10 月 7 日受理)