招待論文

コヒーレント状態による量子鍵配送の通信路損失耐性

小 芦 雅 斗†

コヒーレント状態の位相を用いる量子鍵配送プロトコルについて，無条件安全性の証明を与え，通信路の透過率 $\eta \to 0$ の極限で，η に比例する秘密鍵の生成レートが達成可能であることを示す．この傾向は，送信者の用いるコヒーレント状態の振幅，規格化した raw key の生成レート，およびエラーレートのパラメータ領域のすべてにおいて成立する．この結果は，このプロトコルが本質的に通信路の損失に対して耐性を持つことを示している．

Robustness against Channel Loss of a Coherent-state Quantum Key Distribution Protocol

Masato Koashi†

We consider a quantum-key-distribution protocol based on the phase of coherent states, and give a proof of unconditional security showing that it is possible to achieve a key generation rate proportional to the channel transmission rate η in the limit of $\eta \to 0$. This holds for all the parameter region specified by the amplitude of the coherent state chosen by the sender, a normalized raw-key rate, and the bit error rate. This result shows that the protocol is essentially robust against the loss in the channel.

1. はじめに

量子鍵配送は，光の量子論的な性質を通信の中で活かすことにより，量子力学の原理によって安全性が保証される秘密鍵を送受信者間に分配する手法である．理想的な状況下でこの安全性を示すことは簡単であるが，雑音を含む現実的な状況下では，安全性の証明はかなり複雑なものになる．そのため，安全性の証明は，まず，次元の小さい Hilbert 空間で記述できる単一光子の偏光状態を用いる方式を中心に進められてきた[1)~4)]．

ところが，現在の技術レベルでは，単一光子光源はまだ実験室レベルであり，普及しているレーザ光源の光は光子数の揺らぎを持つコヒーレント状態である．レーザ光の強度を，平均光子数 ν が 1 より小さいレベルにまで落としたものを，単一光子の代替として用いた場合，$O(\nu^2)$ の確率で 2 光子が同じ偏光を持って送信されてしまう．したがって，$O(\nu^2)$ の割合のパルスについては，ビット値は盗聴者に完全に漏れていると考えなければならない[5)]．一方，光ファイバによる現実の通信路では，距離にともない大きくなる損失を考慮する必要がある．通信路の透過率を η とすれば，受信者が光子を検出できるパルスの割合は $O(\eta\nu)$ である．ここで，受信者のもとに光子が届くかどうかは，通信路を支配している盗聴者が自由に決められるため，$\eta\nu$ が ν^2 と同じオーダになると，受信者が検出できたビット値はすべて盗聴者に漏洩しているということになってしまう．したがって，レーザ光強度は $\nu < \eta$ となるように損失とともに小さくしなくてはならず，鍵の生成レートはたかだか $O(\eta^2)$ となる．単一光子を用いた場合のレート $O(\eta)$ と比較すると，η がすべてファイバの透過率からの寄与の場合には，同じレートが得られる距離が半分になってしまうことが分かる．また，検出器の効率のように，η の中に距離に依らない部分が含まれることを考慮すると，この距離の差はもっと大きくなる．

量子鍵配送の中には，B92 方式[6)] のように，コヒーレント光の位相を用いて通信を行う方式もある．送信者が複素振幅 α のコヒーレント状態を送信した場合，受信者の受け取る振幅は $\sqrt{\eta}\alpha$ であり，盗聴者は，ビームスプリッタなどを用いて振幅 $\sqrt{1-\eta}\alpha$ の光を

† 大阪大学大学院基礎工学研究科物性物理工学領域
Division of Materials Physics, Graduate School of Engineering Science, Osaka University

手にすることができる．したがって，この場合にも一部のビット情報はイブに漏れてしまう．しかし，光子偏光の場合と決定的に異なるのは，受信者がビット値を決定できるかどうかが，非直交状態への射影を含む受信者の測定の際にはじめて決まるという点である．そのため，どのパルスのビット値が採用されるのかを，外から盗聴者が制御することが難しくなっている．この違いのために，たとえ $\sqrt{\eta}|\alpha| < \sqrt{1-\eta}|\alpha|$ だったとしても，盗聴者は自分の知っているビット値だけを選択的に受信者に採用させることができないと予想される．そのため，この方式ならば，レーザ光を用いて $O(\eta)$ の鍵の生成レートが達成できるのではないかと期待されている．とはいえ，この方式は，BB84 方式[7] のような高い対称性を持たず，関与する Hilbert 空間の次元も大きいため，安全性の証明は簡単ではない．

本論文では，最近発展した安全性の証明法[8),9)] を用い，B92 方式に基づくあるプロトコルが，損失に対して耐性を持ち，高損失の極限 $\eta \to 0$ で η に比例する鍵の生成レートを達成できることを示す．より正確には，$\eta \to 0$ の極限で，

$$G/\eta \to g(|\alpha|^2, s_{\rm fil}, r_{\rm err})$$

となるような鍵生成レート G で秘密鍵を生成しても，通信パルス数を大きくした極限で，盗聴者への漏洩は指数的に小さくなることを証明する．ここで，$|\alpha|^2$ は送信するコヒーレント状態の平均光子数，$s_{\rm fil}$ は，raw key の生成レートを透過率 η の理想的な通信路の場合の値で規格化したもの，$r_{\rm err}$ は raw key のエラーレートであり，G の比例定数はこれら 3 つの量だけに依存して決まる．

以下，2 章ではプロトコルを定義し，その実施に必要な装置について述べる．3 章では，そのプロトコルで生成される秘密鍵の安全性の証明を与える．4 章では，高損失の極限で，鍵の生成レートが損失に比例することを示し，いくつかの具体的な数値を与える．

2. プロトコル

本論文では，コヒーレント状態の光パルスの送信によって，盗聴者イブの介入のもとでアリスとボブとの間に秘密鍵を生成する次のようなプロトコルを考える．以下，$\mathcal{H}_A$ および $\mathcal{H}_B$ は，単一モードの光パルスの Hilbert 空間とする．$\mathcal{H}_A$ の基底として光子数状態 $|n\rangle_A (n = 0, 1, 2, \ldots)$ をとると，振幅 α のコヒーレント状態は $|\alpha\rangle_A := e^{-|\alpha|^2/2} \sum_n (\alpha^n/\sqrt{n!})|n\rangle_A$ で定義される．以下のプロトコルにおいて，整数 N，実数 α および η（$\alpha > 0$，$0 < \eta \leq 1$）は，自由に選べるパラメータである．また，公開通信路で交わされる通信内容は，イブにも知られるが，イブによって改ざんはされないと仮定する．

(1) アリスは，ランダムにビット値 a を選び，その値に応じて，光パルス（$\mathcal{H}_A$）の状態を $a = 0$ なら振幅 α のコヒーレント状態 $|\alpha\rangle_A$ に，$a = 1$ ならコヒーレント状態 $|-\alpha\rangle_A$ に準備する．

(2) 量子通信路に光パルス（$\mathcal{H}_A$）が入力され，ボブのもとに光パルス（$\mathcal{H}_B$）が出力される．

(3) ボブは受け取った光パルスに対して，次の正値演算子で定義される一般化測定を行う．

$$\begin{aligned} F_0 &= \frac{1}{2}(\mathbf{1}_B - |-\beta\rangle_B\langle -\beta|) \\ F_1 &= \frac{1}{2}(\mathbf{1}_B - |\beta\rangle_B\langle \beta|) \\ F_2 &= \mathbf{1}_B - F_0 - F_1 \end{aligned} \quad (1)$$

ここで，$\beta = \sqrt{\eta}\alpha$ であり，測定される光パルスの状態が密度演算子 ρ だった場合，測定結果 μ が得られる確率は $\mathrm{Tr}(F_\mu \rho)$ になる．

(4) 以上の操作を $2N$ 回繰り返す．なお，イブは本来の通信路に代わって，すべての光パルス（$\mathcal{H}_A^{\otimes 2N}$）を入力として受け取り，好きな状態の $2N$ 個の光パルス（$\mathcal{H}_B^{\otimes 2N}$）をボブに渡すことができる．

(5) 以上のようにして行った $2N$ 回の通信結果に，ランダムに順番を付ける．ただし，公開通信路での通信により，アリスとボブの順番の付け方が同じになるようにする．

(6) この順番に従い，最初の N 回の通信結果については，ボブは測定結果をすべて公開する．アリスは，自分のビット値が $a = 0$ でボブの測定結果が $\mu = 1$，または $a = 1$ で $\mu = 0$ となる場合が N 回のうち何回起きたかを数え（この数を $n_{\rm err}$ とする），公開する．

(7) 残りの N 回の通信については，$\mu = 2$ か否かという情報のみをボブが公開する．$\mu \neq 2$ だったイベントの数を $n_{\rm fil}$ とする．

(8) $\mu \neq 2$ だった $n_{\rm fil}$ 回について，ビット値 a を順に並べたものをアリスの raw key，μ をビット値として順に並べたものをボブの raw key とする．

(9) $n_{\rm err}$ と $n_{\rm fil}$ の値から，次節で述べるように raw key の誤り率とイブへの情報漏洩量の上限を見積もり，公開通信路において誤り訂正と秘匿性増幅を行い，$n_{\rm key}$ ビットの秘密鍵を生成する．

安全性の証明のためには，通信路はイブの支配下にあると考えなければならないため，その性質については上記のプロトコルでは言及されていない．仮に通信

路が透過率 η で無雑音なら，その出力は $|\pm\beta\rangle$ となるので，$n_{\rm err}=0$ となる．すなわち，プロトコルにおけるパラメータ η は，実際に用いる通信路の透過率に等しくなるように選ぶべきである．

上記のプロトコルは，次に述べるような装置を用いて実行することができる．まず，ステップ (3) におけるボブの測定を行うには，パルスレーザ光源からのコヒーレント状態の光と，通信路の出力の光を重ね合わせて光子検出器に入力する．なお，この検出器は，真空とそれ以外の状態を見分けられればよく，光子 1 個と 2 個以上を見分ける必要はない．したがって，現在市販されている光子検出器がそのまま使用できるので都合がよい．通信路の出力を切った（真空にした）ときに，光子検出器に入る光の状態が $|\beta\rangle$ となるよう，パルスレーザからの光の強度を調整する．通信路の出力と光子検出器の結合効率は 100%にはできないが，これは検出器の量子効率と合わせて通信路の損失に繰り込んで考えることができる．また，検出器のダークカウントも通信路の雑音として考えてよい．こうした繰り込みを行ったうえでの通信路の出力が被測定光であると考える．もし，被測定光の状態が $|-\beta\rangle$ であれば，検出器の入力光の状態は真空となり，光子検出は起こらない．したがって，光子検出が起きた場合は，被測定光が $|-\beta\rangle$ と直交する成分を持つことを示している．この場合の測定結果を $\mu=0$ とする．検出が起きない場合は $\mu=2$ とする．さらに，確率 1/2 で非測定光の位相を π シフトさせ，検出が起きた場合を $\mu=1$，起きない場合を $\mu=2$ とすれば，式 (1) の測定が実行できる．なお，実際の検出器は光の単一モードにだけ反応するのではないが，このプロトコルではとくにフィルタを工夫する必要はない．$\mathcal{H}_B$ を検出器に反応するすべてのモードを含む大きな空間だと考え，$|\beta\rangle$ はパルスレーザによって指定される単一のモードが振幅 β のコヒーレント状態で，他のモードは真空という状態を表すと解釈しなおせば，次章の安全性の議論はそのまま成り立つ．これは，局部発振光を用いるホモダイン測定の持つ利点の 1 つである．

アリスの光源は，パルスレーザの出力を振幅 $\pm\alpha$ にするだけでよい．なお，モードがボブのレーザのモードと完全に一致していなくてもよいし，雑音を含んで混合状態になっていてもよい．これらの状態は，適当な α の正しい純粋状態から仮想的な通信路を通して生成できるため，いつでも通信路に繰り込んで考えることができる．

プロトコルでは，アリスとボブのパルスレーザの位相が同期していることが前提されている．これは，実際にはアリスからボブへ強い参照光パルスを送ることで，ボブが 2 つのパルスレーザの位相差を検出し，補正することを想定している．この場合，厳密に正確な同期をとることは不可能であるが，パルスレーザの位相のずれと，通信路を通る信号に加わる位相のずれは，ステップ (3) の測定に対してまったく同じ効果をもたらすため，この不完全性も通信路に繰り込んで考えることができる．

3. 安全性の証明

3.1 測定の分解

前章のプロトコルの安全性を証明するうえでのキーポイントは，パルス $\mathcal{H}_B$ に対するボブの測定 $\{F_0,F_1,F_2\}$ を，パルスを入力して仮想的な 2 準位系（qubit）の状態を出力として取り出すフィルタと，qubit に対する標準的な測定の 2 段階に分解することである．これによって，BB84 方式のように qubit を仮定する量子鍵配送プロトコルの安全性の証明に用いられた技法が使えるようになる．

$\mathcal{H}_B$ の部分空間 $\mathcal{K}_B$ を，$|\beta\rangle_B$ と $|-\beta\rangle_B$ で張られる 2 次元の空間とし，$\mathcal{H}_B=\mathcal{K}_B\oplus\mathcal{H}_{\rm ex}$ と分解する．c_β と s_β を，

$$2c_\beta^2-1=1-2s_\beta^2=\langle-\beta|\beta\rangle=e^{-2|\beta|^2}$$

によって定まる正数とし，qubit $\mathcal{K}_B$ の正規直交基底（X 基底）を

$$\begin{aligned}|0_x\rangle_B&:=(|\beta\rangle_B+|-\beta\rangle_B)/(2c_\beta)\\ |1_x\rangle_B&:=(|\beta\rangle_B-|-\beta\rangle_B)/(2s_\beta)\end{aligned}\qquad(2)$$

とする．また，Z 基底を，

$$\begin{aligned}|0_z\rangle_B&:=(|0_x\rangle_B+|1_x\rangle_B)/\sqrt{2}\\ |1_z\rangle_B&:=(|0_x\rangle_B-|1_x\rangle_B)/\sqrt{2}\end{aligned}\qquad(3)$$

とする．$\mathcal{H}_{\rm ex}$ のある正規直交基底を $\{|c_l\rangle_B\}_{l=1,2,\ldots}$ とし，演算子 $A_j:\mathcal{H}_B\to\mathcal{K}_B(j=0,1,\ldots)$ を次のように定義する．

$$\begin{aligned}A_0&:=s_\beta|0_x\rangle_B\langle 0_x|+c_\beta|1_x\rangle_B\langle 1_x|\\ A_l&:=|0_x\rangle_B\langle c_l|\ \ (l=1,2,\ldots)\end{aligned}\qquad(4)$$

この演算子 $\{A_j\}$ により，次のようなフィルタ（「通過」,「非通過」の 2 値の測定および通過時の状態出力）が定義される．すなわち，入力となる光パルス（$\mathcal{H}_B$）の状態が密度演算子 ρ で与えられるとき，このパルスは確率 $p:=\sum_j{\rm Tr}(A_j\rho A_j^\dagger)$ でフィルタを通過し，そのとき出力される qubit $\mathcal{K}_B$ の状態は $\sum_j A_j\rho A_j^\dagger/p$ となる．

このような仮想的なフィルタを用いて，通過した場合には出力 qubit をただちに Z 基底で射影測定する

という操作を考える．この測定結果が $|k_z\rangle_B (k=0,1)$ だった場合の測定値を $\mu=k$ とし，フィルタを非通過だった場合の測定値を $\mu=2$ とすると，全体として 3 値の測定となる．ここで，

$$F_k = \sum_j A_j^\dagger |k_z\rangle_B\langle k_z| A_j \qquad (5)$$

が成立することは容易に確かめられるので，フィルタを用いた 3 値の測定は，前章のプロトコルにおけるボブの測定とまったく同じであることが分かる．

3.2 等価プロトコル

2 章のプロトコルにおけるボブの測定がフィルタを用いて行う測定と等価であるという事実を用いると，イブの立場から見てまったく等価な別のプロトコルを構築することができる．

ステップ (1) において，アリスはビット値 a をランダムに選んでから状態を準備したが，この操作は，補助的な qubit の系（Hilbert 空間を $\mathcal{K}_A$ とする）を利用して，まず $\mathcal{K}_A\otimes\mathcal{H}_A$ を状態 $(|0_z\rangle_A|\alpha\rangle_A+|1_z\rangle_A|-\alpha\rangle_A)/\sqrt{2}$ に準備し，続いて $\mathcal{K}_A$ を Z 基底で測定して a を決めても同じことになる．また，この Z 基底での測定は，a の値に関係する情報を公開する必要に迫られるまでは遅らせることができる．そこで，ステップ (1) を次の操作に替える．

(1′) アリスは，補助 qubit と光パルスの系（$\mathcal{K}_A\otimes\mathcal{H}_A$）を状態 $(|0_z\rangle_A|\alpha\rangle_A+|1_z\rangle_A|-\alpha\rangle_A)/\sqrt{2}$ に準備する．

ステップ (2) は前と同じとする．ステップ (3) の時点では，まだボブは何も測定を行わないとする：

(3′) ボブは光パルスを保存しておく．

ステップ (4)，(5) は前と同じである．(6) 以降は，次のように替える．

(6′) 最初の N 個の光パルスについては，ボブは測定 $\{F_0,F_1,F_2\}$ を行い，結果 μ を公開する．アリスは対応する補助 qubit $\mathcal{K}_A$ を Z 基底で測定し，a を決める．アリス側が $a=0$ でボブの測定結果が $\mu=1$，または $a=1$ で $\mu=0$ となる場合が N 回のうち何回起きたかを数え（この数を $n_{\rm err}$ とする），公開する．

(7′) 残りの N 個の光パルスについては，ボブはフィルタの操作を行い，通過か非通過の結果を公開する．通過したパルスの数を $n_{\rm fil}$ とする．この時点で，アリスとボブには $n_{\rm fil}$ 対の qubit が分配されている．

(8′) アリスとボブはそれぞれ $n_{\rm fil}$ 個の qubit を Z 基底で測定し，測定結果をビットとして並べたものを raw key とする．

このように，qubit 対に対する測定に帰着する等価プロトコルに置き換えると，Shor と Preskill によって与えられた安全性の証明の技法をあてはめることができる．その準備として，ある qubit 対のそれぞれを Z 基底で測定した結果得られる 2 つのビット値が異なるケースをビットエラー，また，X 基底で測定した結果得られる 2 つのビット値が異なるケースを位相エラーと呼ぶことにする．ステップ (7′) で得られる $n_{\rm fil}$ 対の qubit について，2 つの観測量，$n_{\rm bit}$ と $n_{\rm ph}$ を，それぞれビットエラーを示す対の数，位相エラーを示す対の数として定義する．ちなみに，この 2 つの量の演算子はベル基底で対角化されており，可換である．実際のプロトコルでは，(7′) の時点で，これらの量の測定結果は手に入らない．ここで，仮定として，これらの量の上限の推定値 $n_{\rm bitmax}$，$n_{\rm phmax}$ が与えられ，ステップ (7′) で得られた $n_{\rm fil}$ 対の qubit の状態に対し，$n_{\rm bit}$ と $n_{\rm ph}$ を測定したら，ある微小な確率を除いて，$n_{\rm bitmax}\geq n_{\rm bit}$，$n_{\rm phmax}\geq n_{\rm ph}$ となることが約束されているとしよう．このとき，$n_{\rm key}$ 個の論理 qubit を $n_{\rm fil}$ 個の物理 qubit に符号化し，$n_{\rm bitmax}$ 個のビットエラーと $n_{\rm phmax}$ 個の位相エラーを（ある微小な確率を除いて）訂正できる CSS 量子誤り訂正符号を見つけられれば，ステップ (9) における古典誤り訂正および秘匿性増幅の方法が与えられ，それによって得られる $n_{\rm key}$ ビットの秘密鍵は微小な確率を除いて安全であるということが Shor らによって示されている[3]．ちなみに，その議論は，上記の量子誤り訂正符号を用いて entanglement distillation[10] を行い，ほぼ純粋状態になった qubit 対への測定から秘密鍵を生成する（したがって明らかに漏洩はない）というプロトコルとの等価性に基づいている．

2 章のプロトコルの安全性を証明するには，プロトコル内で手に入る $n_{\rm fil}$，$n_{\rm err}$ の値から，上記の仮定が満たされるように $n_{\rm bitmax}$，$n_{\rm phmax}$ を計算する方法を与えればよい．

3.3 ビットエラーと位相エラーの推定

ビットエラーの推定は比較的簡単である．$2N$ 個のサンプルを N 個ずつの 2 グループにランダムに分けて，それぞれのビットエラーを数えた結果が $n_{\rm err}$ と $n_{\rm bit}$ であると考えられるので，$n_{\rm err}/N$ と $n_{\rm bit}/N$ の差はほとんどないと考えられる．実際，$2N$ 個のサンプルがどのように準備されたかによらず，任意の $\epsilon>0$ に対して $|n_{\rm err}-n_{\rm bit}|>N\epsilon$ となる確率は，N が大きいときたかだか $e^{-N\epsilon^2}$ のオーダであることが簡単に示せる．したがって，

$$n_{\rm bitmax} = n_{\rm err} + N\epsilon \quad (6)$$

とおけば，N に対して指数的に小さくなる確率を除いて，$n_{\rm bitmax} \geq n_{\rm bit}$ が成立することが分かる．

一方，位相エラーの推定はかなり複雑である．ステップ ($7'$) の直後に，$n_{\rm fil}$ 対の qubit を X 基底で測定して $n_{\rm ph}$ を決めるという手続きを考えると，全体としては，Hilbert 空間 $\mathcal{K}_A \otimes \mathcal{H}_B$ を持つ系が $2N$ 個与えられ，それを N 個ずつ 2 グループにランダムに分けて，一方については $n_{\rm err}$ を測定し，もう一方については $n_{\rm fil}$ および $n_{\rm ph}$ を測定したと見なせる．そこで，このような測定において得られる測定結果の組合せ $(n_{\rm fil}, n_{\rm ph}, n_{\rm err})$ のうち，サンプルの初期状態によらず微小な確率でしか起こらないものを除いていくことで，$(n_{\rm fil}, n_{\rm ph}, n_{\rm err})$ の領域を定めれば，与えられた $n_{\rm err}$，$n_{\rm fil}$ の値のもとで，$n_{\rm ph}$ の領域内での上限値を与える関数 $n_{\rm phmax}(n_{\rm fil}, n_{\rm err})$ を以下に述べるように陰に決定することができる．

まず，$n_{\rm fil}$，$n_{\rm ph}$，$n_{\rm err}$ のそれぞれが，$\mathcal{K}_A \otimes \mathcal{H}_B$ に対するどのような測定の結果を数えたものかを考える．状態 $|\cdot\rangle$ への射影演算子を $P(|\cdot\rangle) := |\cdot\rangle\langle\cdot|$ と書くことにすれば，$n_{\rm fil}$ は，$\mathcal{K}_A \otimes \mathcal{H}_B$ に対する正値演算子

$$\begin{aligned} M_{\rm fil} :&= \mathbf{1}_A \otimes \sum_j A_j^\dagger A_j \\ &= \mathbf{1}_A \otimes [c_\beta^2 P(|1_x\rangle_B) + s_\beta^2 P(|0_x\rangle_B) + \mathbf{1}_{\rm ex}] \end{aligned} \quad (7)$$

を含む POVM 測定を N 個の系に行い，対応する結果が出た数を数えたものになる．同様に，$n_{\rm ph}$ には

$$\begin{aligned} M_{\rm ph} :&= \sum_j P(|0_x\rangle_A) \otimes A_j^\dagger |1_x\rangle_B\langle 1_x| A_j \\ &\quad + \sum_j P(|1_x\rangle_A) \otimes A_j^\dagger |0_x\rangle_B\langle 0_x| A_j \\ &= s_\beta^2 P(|1_x\rangle_A|0_x\rangle_B) + c_\beta^2 P(|0_x\rangle_A|1_x\rangle_B) \\ &\quad + P(|1_x\rangle_A) \otimes \mathbf{1}_{\rm ex} \end{aligned} \quad (8)$$

が対応し，$n_{\rm err}$ には

$$\begin{aligned} M_{\rm err} &:= P(|0_z\rangle_A) \otimes F_1 + P(|1_z\rangle_A) \otimes F_0 \\ &= (1/2)[P(|\Gamma_{11}\rangle) + P(|\Gamma_{01}\rangle) \\ &\quad + \mathbf{1}_A \otimes \mathbf{1}_{\rm ex}] \end{aligned} \quad (9)$$

が対応する．ここで，$\mathcal{K}_A \otimes \mathcal{K}_B$ の基底 $\{|\Gamma_{ij}\rangle\}_{i,j=0,1}$ を，

$$\begin{aligned} |\Gamma_{ij}\rangle &:= c_\beta |i_x\rangle_A |j_x\rangle_B \\ &\quad -(-1)^j s_\beta |(1-i)_x\rangle_A |(1-j)_x\rangle_B \end{aligned} \quad (10)$$

により定義した．

ここで，$P_{ij} := P(|i_x\rangle_A|j_x\rangle_B)$ と書いて，

$$\{P_{00}, P_{11}, P_{10}, P_{01}, P(|0_x\rangle_A) \otimes \mathbf{1}_{\rm ex}, P(|1_x\rangle_A) \otimes \mathbf{1}_{\rm ex}\}$$

という射影演算子の組で表される射影測定を考える．$M_{\rm ph}$ と $M_{\rm fil}$ の形から，$n_{\rm ph}$ と $n_{\rm fil}$ の測定法として，まず上記の射影測定を N 個の系に対して行い，さらに確率 c_β^2 あるいは s_β^2 のベルヌーイ試行を行うという方法が可能であることが分かる．このような測定法を行うとき，N 回の射影測定の結果の分布を，同じ順番で

$$\{n_+(1-\delta_+), n_+\delta_+, n_-(1-\delta_-), n_-\delta_-, m_0, m_1\}$$

と表せば，ベルヌーイ試行の性質から，

$$\begin{aligned} &|n_{\rm ph} - m_1 \\ &-n_-[s_\beta^2(1-\delta_-) + c_\beta^2\delta_-]| \leq N\epsilon \end{aligned} \quad (11)$$

$$\begin{aligned} &|n_{\rm fil} - m_0 - m_1 - c_\beta^2(n_+\delta_+ + n_-\delta_-) \\ &-s_\beta^2[n_+(1-\delta_+) + n_-(1-\delta_-)]| \leq N\epsilon \end{aligned} \quad (12)$$

が指数的に小さい確率を除いて成立する．

同様に，もう一方のグループの系に対する $n_{\rm err}$ の測定は，$Q_{ij} := P(|\Gamma_{ij}\rangle)$ として，射影測定

$$\{Q_{00}, Q_{11}, Q_{10}, Q_{01}, \mathbf{1}_A \otimes \mathbf{1}_{\rm ex}\}$$

とベルヌーイ試行によっても行える．この場合，射影測定の結果の分布を

$$\{n'_+(1-\delta'_+), n'_+\delta'_+, n'_-(1-\delta'_-), n'_-\delta'_-, m\}$$

とすれば，

$$|n_{\rm err} - (n'_+\delta'_+ + n'_-\delta'_- + m)/2| \leq N\epsilon \quad (13)$$

を得る．

ここで，アリスのもとにある qubit は，送信されることがないため，イブによって状態を変化させられることはないという点に着目する．ステップ (1) で準備された状態では，$\mathcal{H}_A$ の系を除いたときの qubit($\mathcal{K}_A$) の状態は $\rho_A := c_\alpha^2 P(|0_x\rangle_A) + s_\alpha^2 P(|1_x\rangle_A)$ と書けるが，これはイブによる介入の後も不変である．一方，$m_1 + n_+\delta_+ + n_-(1-\delta_-)$ という量は，アリスの qubit のうち $|1_x\rangle_A$ に射影されたものの数にほかならないので，これは確率 s_α^2 のベルヌーイ試行の結果と見なすことができて，

$$|m_1 + n_+\delta_+ + n_-(1-\delta_-) - s_\alpha^2 N| \leq N\epsilon \quad (14)$$

を得る．

次に，$P_{00} + P_{11} = Q_{00} + Q_{11}$ という関係に着目する．この関係式によれば，異なるグループに対してなされる n_+ と n'_+ の測定は，どちらも $\{|0_x\rangle_A|0_x\rangle_B, |1_x\rangle_A|1_x\rangle_B\}$ で張られる 2 次元の空間 $\mathcal{H}_+$ へ射影された対の数を数えていることが分かる．n_- と n'_- についても同様である．グループ分けがランダムであるから，ビットエラーの推定のときと同様に

$$|n_\pm - n'_\pm| \leq N\epsilon \quad (15)$$

を得る．

一方，δ_+ と δ'_+ は，ともに $\mathcal{H}_+$ の状態に対して行

われる射影測定の結果を数えたものと考えられるが，その射影測定は同じものではなく，δ_+ は $\{P_{00}, P_{11}\}$，δ'_+ は $\{Q_{00}, Q_{11}\}$ である．仮に，すべてのサンプルが $\mathcal{H}_+$ のある 1 つの状態 ρ に独立に準備されたもの（つまり $\rho^{\otimes(n_++n'_+)}$）であれば，$\mathrm{Tr}[\rho P_{11}] \cong \delta_+$，$\mathrm{Tr}[\rho Q_{11}] \cong \delta'_+$ が成り立つはずである．すなわち，パラメータ空間 (δ_+, δ'_+) 上で，点 $(\mathrm{Tr}[\rho P_{11}], \mathrm{Tr}[\rho Q_{11}])$ をすべての ρ に対してとった領域 A を考えると，A からある微小距離以上離れた点に対応する測定結果 (δ_+, δ'_+) を得る確率は，指数的に小さい．実際には，イブの介入が個々のパルスに対し独立であるという保証はないので，$\rho^{\otimes(n_++n'_+)}$ という形を仮定することはできない．では，相関を持たせることで，ある点 (δ_+, δ'_+) を得る確率をどのくらい増強させることができるだろうか．実は，ステップ (5) のようなランダムな置換のもとでは，この増強はせいぜいサンプル数の多項式のオーダであることが示されている[8]．したがって，任意の相関を許しても，指数的に確率が小さいという事実は変わらない．領域 A についての条件を具体的に書き下すと，次の不等式が得られる．

$$\delta'_\pm \geq c_\beta^2\delta_\pm + s_\beta^2(1-\delta_\pm) - 2c_\beta s_\beta\sqrt{\delta_\pm(1-\delta_\pm)} - \epsilon \quad (16)$$

以上のように求めた不等式 (11)–(16) と，自明な式

$$n_+ + n_- + m_0 + m_1 = N \quad (17)$$

$$n'_+ + n'_- + m = N \quad (18)$$

を組み合わせることで，与えられた n_{fil}，n_{err} のもとでの n_{ph} の上限 $n_{\mathrm{phmax}}(n_{\mathrm{fil}}, n_{\mathrm{err}})$ を決定することができる．

3.4 秘密鍵の生成レート

とくに興味があるのは，$N \to \infty$ において得られる鍵の生成レート $G := n_{\mathrm{key}}/N$ である．これまでに出てきた n_{ph} や n_{err} などを N で規格化して，$\hat{n}_{\mathrm{ph}} := n_{\mathrm{ph}}/N$，$\hat{n}_{\mathrm{err}} := n_{\mathrm{err}}/N$ などと書くことにする．

この極限での CSS 量子誤り訂正符号の存在の条件より，生成レートは，$h(x) := -x\log_2 x - (1-x)\log_2(1-x)$ として，

$$G = \hat{n}_{\mathrm{fil}}\left[1 - h\left(\frac{\hat{n}_{\mathrm{bitmax}}}{\hat{n}_{\mathrm{fil}}}\right) - h\left(\frac{\hat{n}_{\mathrm{phmax}}}{\hat{n}_{\mathrm{fil}}}\right)\right] \quad (19)$$

で与えられる[11),12)]（右辺が負になるときは，$G = 0$ と見なす）．この式に現れている $\hat{n}_{\mathrm{bitmax}}$，$\hat{n}_{\mathrm{phmax}}$ を，$\hat{n}_{\mathrm{fil}}$，$\hat{n}_{\mathrm{err}}$ から決定するには，以下の処方箋に従えばよい．

$N \to \infty$ の極限では，これまで導いた等式，不等式における ϵ もゼロとしてよい．したがって，式 (6) は，

$$\hat{n}_{\mathrm{bitmax}} = \hat{n}_{\mathrm{err}} \quad (20)$$

となる．また，不等式 (11)–(15) はすべて等式になる．不等式 (16) に $\hat{n}'_\pm$ を乗じて足し合わせると，左辺は式 (13) より $2\hat{n}_{\mathrm{err}} - \hat{m}$ に等しくなるが，式 (12)，(15)，(17)，(18) より，

$$\hat{n}'_+[c_\beta^2\delta_+ + s_\beta^2(1-\delta_+)] + \hat{n}'_-[c_\beta^2\delta_- + s_\beta^2(1-\delta_-)] = \hat{n}_{\mathrm{fil}} - \hat{m}_0 - \hat{m}_1 = \hat{n}_{\mathrm{fil}} - \hat{m}$$

となることを使うと，

$$2\hat{n}_{\mathrm{err}} \geq \hat{n}_{\mathrm{fil}} - 2c_\beta s_\beta\left[\hat{n}_+\sqrt{\delta_+(1-\delta_+)} + \hat{n}_-\sqrt{\delta_-(1-\delta_-)}\right] \quad (21)$$

を得る．式 (11)，(12)，(14)，(17) を書き直した 4 つの等式

$$\hat{n}_{\mathrm{ph}} = \hat{m}_1 + \hat{n}_-[s_\beta^2(1-\delta_-) + c_\beta^2\delta_-] \quad (22)$$

$$\hat{n}_{\mathrm{fil}} = \hat{m}_0 + \hat{m}_1 + c_\beta^2(\hat{n}_+\delta_+ + \hat{n}_-\delta_-) + s_\beta^2[\hat{n}_+(1-\delta_+) + \hat{n}_-(1-\delta_-)] \quad (23)$$

$$\hat{m}_1 + \hat{n}_+\delta_+ + \hat{n}_-(1-\delta_-) = s_\alpha^2 \quad (24)$$

$$\hat{n}_+ + \hat{n}_- + \hat{m}_0 + \hat{m}_1 = 1 \quad (25)$$

を用いると，不等式 (21) の右辺から $\hat{n}_\pm$，$\delta_\pm$ を消去できて，$\hat{n}_{\mathrm{err}} \geq f(\hat{n}_{\mathrm{fil}}, \hat{n}_{\mathrm{ph}}, \hat{m}_0, \hat{m}_1)$ の形になる．したがって，$\hat{n}_{\mathrm{fil}}$，$\hat{n}_{\mathrm{ph}}$ の関数としての $\hat{n}_{\mathrm{err}}$ の最小値 $\hat{n}_{\mathrm{errmin}}$ が

$$\hat{n}_{\mathrm{errmin}}(\hat{n}_{\mathrm{fil}}, \hat{n}_{\mathrm{ph}}) = \min_{\hat{m}_0, \hat{m}_1} f(\hat{n}_{\mathrm{fil}}, \hat{n}_{\mathrm{ph}}, \hat{m}_0, \hat{m}_1)$$

により定まる．一般に，$\hat{n}_{\mathrm{err}}$ と $\hat{n}_{\mathrm{ph}}$ は単調の関係にあるので，$\hat{n}_{\mathrm{phmax}}$ は $\hat{n}_{\mathrm{err}} = \hat{n}_{\mathrm{errmin}}(\hat{n}_{\mathrm{fil}}, \hat{n}_{\mathrm{phmax}})$ を解くことによって決定できる．

4. 高損失極限

この章では，通信路の損失が大きい極限での秘密鍵生成レートについて述べる．2 章で述べたように，送信するコヒーレント光の 2 乗振幅が $|\alpha|^2$ のとき，受信側の検出器のパラメーターを $|\beta|^2 = \eta|\alpha|^2$ に設定するのは，通信路の透過率が η であることを想定してのことである．透過率 η の理想的な通信路を仮定した場合，入力 $|\alpha\rangle_A, |-\alpha\rangle_A$ に対する出力は $|\beta\rangle_B, |-\beta\rangle_B$ となる．このとき raw key の生成レート $\hat{n}_{\mathrm{fil}}$ の値は，

$$\hat{n}_{\mathrm{fil}} = \hat{n}_{\mathrm{fil0}} := (1 - e^{-4\eta|\alpha|^2})/2 \quad (26)$$

であり，$\hat{n}_{\mathrm{err}} = 0$ となる．実際には，通信路の雑音などのために，$\hat{n}_{\mathrm{fil}}$ と $\hat{n}_{\mathrm{err}}$ の値は上記の値からずれる．$\eta \to 0$ の極限では，$\hat{n}_{\mathrm{fil}}$ と $\hat{n}_{\mathrm{err}}$ の値そのものはゼロになるので，raw key の生成レート $\hat{n}_{\mathrm{fil}}$ の相対変化を表すパラメータ $s_{\mathrm{fil}} := \hat{n}_{\mathrm{fil}}/\hat{n}_{\mathrm{fil0}}$ と，raw key のエラーレート $r_{\mathrm{err}} := \hat{n}_{\mathrm{err}}/\hat{n}_{\mathrm{fil}}$ を定義し，これらの 2 つの値を一定にして $\eta \to 0$ の極限をとることにする．

まず，位相エラーレート $r_{\rm ph} := \hat{n}_{\rm ph}/\hat{n}_{\rm fil}$，および $s_0 := m_0/\hat{n}_{\rm fil0}$，$s_1 := m_1/\hat{n}_{\rm fil0}$ を定義しておく．上記の極限で式 (22)–(25) を $\hat{n}_{\pm}$，$\delta_{\pm}$ について解くと，$\delta_{\pm} \to 0$ となることが分かるので，$s_{\pm} := \delta_{\pm}/\hat{n}_{\rm fil0}$ とおいて，

$$n_+ = c_\alpha^2 \tag{27}$$

$$n_- = s_\alpha^2 \tag{28}$$

$$s_+ = \frac{s_{\rm fil}(1-r_{\rm ph}) - s_0}{c_\alpha^2} - \frac{1}{2} \tag{29}$$

$$s_- = \frac{s_{\rm fil} r_{\rm ph} - s_1}{s_\alpha^2} - \frac{1}{2} \tag{30}$$

を得る．不等式 (21) は，

$$r_{\rm err} \geq \frac{1}{2} - \frac{c_\alpha^2\sqrt{s_+} + s_\alpha^2\sqrt{s_-}}{\sqrt{2}s_{\rm fil}} \tag{31}$$

となる．3.4 節で述べたように，右辺を最小化するように s_0，s_1 をとって，等号にしたものが $r_{\rm phmax} := \hat{n}_{\rm phmax}/\hat{n}_{\rm fil}$ を決める方程式となる．$s_0 = s_1 = 0$ が右辺の最小値を与えるのは明らかなので，

$$r_{\rm err} = \frac{1}{2} - \frac{1}{2s_{\rm fil}} \left(c_\alpha \sqrt{2s_{\rm fil}(1-r_{\rm phmax}) - c_\alpha^2} + s_\alpha \sqrt{2s_{\rm fil} r_{\rm phmax} - s_\alpha^2} \right) \tag{32}$$

が $r_{\rm phmax}$ を与える方程式となる．秘密鍵の生成レートは，同じ極限で，

$$G/\eta \to 2|\alpha|^2 s_{\rm fil} \left[1 - h\left(r_{\rm err}\right) - h\left(r_{\rm phmax}\right)\right] \tag{33}$$

となる．

式 (32)，(33) の結果は，高損失極限 $\eta \to 0$ における秘密鍵の生成レートが，送信したコヒーレント光の 2 乗振幅 $|\alpha|^2$，エラーレート $r_{\rm err}$，およびパラメータ $s_{\rm fil}$ のみで決まる比例定数に従い，η に比例して減少することを示している．この意味で，コヒーレント状態の位相を用いた量子鍵配送は，通信路の損失に対して（透過率に比例して生成レートが低下するという自明な影響を除いて）耐性があると考えられる．

次に，通信路が理想的な透過率 η の通信路に近い極限 $r_{\rm err} = 0$，$s_{\rm fil} = 1$ での鍵の生成レートを具体的に求める．このとき，式 (32) の解は $r_{\rm phmax} = s_\alpha^2$ であるから，

$$G/\eta \to 2|\alpha|^2 \left[1 - h\left(\frac{1-e^{-2|\alpha|^2}}{2}\right)\right] \tag{34}$$

となる．この右辺は，送信するコヒーレント状態の 2 乗振幅を大きくすると raw key の生成レート $\sim 2|\alpha|^2\eta$ は大きくなるが，イブへの漏洩量も大きくなるため，

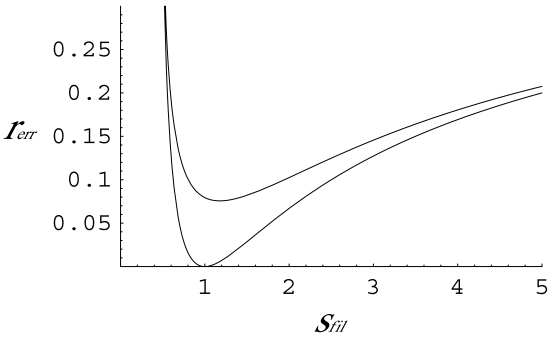

図 1 鍵生成の限界を与えるエラーレート（上の曲線）．下の曲線より下の領域は物理的にありえない

Fig. 1 Threshold error rate for key generation (upper curve). The region below the lower curve is not physically allowed.

秘匿性増強によって鍵をより短くしなければならないというトレードオフ関係を示している．最大になるのは，$|\alpha|^2 = 0.23$ の時で，このとき $G \sim 0.14\eta$ となる．理想的な単一光子光源を用いて BB84 方式を行った場合の生成レート $G = 0.5\eta$ と比較すると，より簡単に発生できるコヒーレント光源を用いても，1/3 弱のレートで秘密鍵の生成が可能であることが分かる．

最後に，どの程度のエラーレートまで秘密鍵の生成が原理的に可能であるかを調べる．鍵生成が不可能になるエラーレートは，式 (33) の因子について，

$$1 - h(r_{\rm err}) - h(r_{\rm phmax}) = 0 \tag{35}$$

という条件で決まる．式 (32) の形から，$|\alpha|^2$ が小さいほど $r_{\rm phmax}$ も小さくなるので，$|\alpha|^2 \to 0$ の極限をとると，

$$r_{\rm phmax} = 2s_{\rm fil} r_{\rm err}(1 - r_{\rm err}) - \frac{(1-s_{\rm fil})^2}{2s_{\rm fil}} \tag{36}$$

を得る．この式を式 (35) に代入したものが，鍵生成の限界となるエラーレートとパラメータ $s_{\rm fil}$ との関係を表す方程式であり，その様子を**図 1** に示した．$r_{\rm err} \sim 7.6\%$ 以下であれば，鍵生成が原理的に可能であることが分かる．なお，この図からは，$s_{\rm fil}$ の値が 1 から大きく隔たると，より高いエラーレートでも鍵生成が可能であることが分かるが，通常の雑音の場合にはこのような領域の観測結果は得られない．

5. おわりに

光子の偏光に基づく BB84 方式でも，送信する状態を追加することでコヒーレント状態を用いて原理的に $O(\eta)$ の鍵生成レートが達成できることが最近指摘されている[13),14)]．どちらの方法が優れているのかを現時点で決めることはできないが，本論文で取り上げたプロトコルの利点はその簡潔さにある．もともとの

B92 方式の提案における測定に何も追加しなくても，$O(\eta)$ の鍵生成レートが達成可能であり，エラーが小さいときの比例定数は単一光子を用いたプロトコルの場合と 1 桁も変わらない．また，光源や測定器に仮定している条件も，非常に緩いものになっている．

一方，安全性の証明において残された課題は，ボブ側にパルスレーザをおく仮定である．現実には，アリスの送信する強い位相の参照光を，そのまま減光して局部発振光として使用することが望ましい．参照光が強い極限では，今回の結果とまったく同じになると考えられるが，参照光を弱くしていった場合にどのくらい鍵を余計に短縮しなければならないかという問題は，応用上も理論的にも大変興味深い問題である．

参 考 文 献

1) Mayers, D.: Quantum Key Distribution and String Oblivious Transfer in Noisy Channels, *Lect. Notes Comput. Sci.*, Vol.1109, p.343 (1996).
2) Lo, H.K. and Chau, H.F.: Unconditional Security Of Quantum Key Distribution Over Arbitrarily Long Distances, *Science*, Vol.283, p.2050 (1999).
3) Shor, P.W. and Preskill, J.: Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, *Phys. Rev. Lett.*, Vol.85, p.441 (2000).
4) Koashi, M. and Preskill, J.: Secure quantum key distribution with an uncharacterized source, *Phys. Rev. Lett.*, Vol.90, p.057902 (2003).
5) Brassard, G., Lütkenhaus, N., Mor, T. and Sanders, B.C.: Limitations on Practical Quantum Cryptography, *Phys. Rev. Lett.*, Vol.85, p.1330 (2000).
6) Bennett, C.H.: Quantum cryptography using any two nonorthogonal states, *Phys. Rev. Lett*, Vol.68, p.3121 (1992).
7) Bennett, C.H. and Brassard, G.: Quantum cryptography: public key distribution and coin tossing, *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, pp.175–179, IEEE, New York (1984).
8) Tamaki, K., Koashi, M. and Imoto, N.: Unconditionally secure key distribution based on two nonorthogonal states, *Phys. Rev. Lett.*, Vol.90, p.167904 (2003).
9) Koashi, M.: Unconditional Security of Coherent-State Quantum Key Distribution with a Strong Phase-Reference Pulse, *Phys. Rev. Lett.*, Vol.93, p.120501 (2004).
10) Bennett, C.H., DiVincenzo, D.P., Smolin, J.A. and Wootters, W.K.: Mixed-state entanglement and quantum error correction, *Phys. Rev. A*, Vol.54, p.3824 (1996).
11) Hamada, M.: Reliability of Calderbank-Shor-Steane Codes and Security of Quantum Key Distribution, quant-ph/0308039.
12) Koashi, M.: Simple security proof of quantum key distribution via uncertainty principle, quant-ph/0505108.
13) Hwang, W.Y.: Quantum Key Distribution with High Loss: Toward Global Secure Communication, *Phys. Rev. Lett.*, Vol.91, p.057901 (2003).
14) Lo, H.K., Ma, X. and Chen, K.: Decoy State Quantum Key Distribution, quant-ph/0411004.

(平成 17 年 2 月 3 日受付)
(平成 17 年 7 月 4 日採録)

小芦 雅斗

NTT 基礎研究所，総合研究大学院大学を経て 2004 年 4 月より大阪大学大学院基礎工学研究科助教授．量子情報，量子光学に関して広く興味を持って研究を進めている．