光学からみた量子通信・鍵配布

並木　亮・平野　琢也

Quantum Communication and Key Distribution from a View Point of Optical Technology

Ryo NAMIKI and Takuya HIRANO

Recently, there has been an increasing interest in quantum information technology. Quantum communication is an application of quantum mechanics to communication, and poses innumerable possibilities of extending communication capabilities. The most promising technology is quantum key distribution in which the security of communication is protected by the laws of physics; its technological level is now almost suitable for practical use. Here we review the current status of quantum key distribution with a comparison between various protocols.

Key words: quantum key distribution, quantum communication, quantum cryptography, secure key gain, quantum entanglement

量子情報技術は，量子力学の特異な性質を直接利用することにより，従来は不可能であった，あるいは従来よりもすぐれた情報処理を実現することを目的としている．例えば，量子計算機は，重ね合わせの原理が成り立つような量子力学的な計算素子を用いて，これまでの計算機よりも桁違いに高速な計算を行うものである．量子力学的な効果が顕著に現れるためには，デコヒーレンスが小さいこと，つまり環境との相互作用による損失や位相の乱れが少ないことが必要である．このような観点から，レーザー光のもつすぐれた可干渉性，低損失な光ファイバーの存在は，他の手段では得られないものであり，量子情報技術の中で光が重要な位置を占めている理由のひとつとなっている．特に，量子力学的な状態を遠く離れた場所に送る手段としては，光を用いるほかなく，量子通信の研究では光学からの視点が重要といえる．

1.　量子通信と量子鍵配布

1.1　量子通信とは

量子通信とは，ひとことでいうと，量子力学の原理を利用した通信である[1]．従来の通信との違いを考えるうえで最もわかりやすいのは，通信に用いる手段の違いを考えることである．従来の通信は，複数の参加者間で，古典的な情報をやり取りするものであった．量子通信では，新たに，量子的な状態の送受信と，量子エンタングルメントの共有という2つの新しいリソースが提供されている．

量子的な状態の例として，単一光子の偏光状態を考えてみる．もしも，この光子が水平または垂直方向の直線偏光である場合には，偏光ビームスプリッターを通した後に単一光子検出器をおけば，水平であったか垂直であったかを知ることができる．しかし，水平偏光か，右回り円偏光のどちらかである場合には，そのどちらであるかを100%の確率で誤りなく測定することはできない．もっと一般にいうと，たった1つだけの光子に対して，それが未知の偏光状態にあるとき，その偏光状態を知ることはできない[2]．また，未知の偏光状態にある光子の複製をつくり出すことは不可能である．このように，量子状態は，正確に読み出すことや複製をつくることができないという特徴がある．それに対して，古典的な情報は，自由にコピーしたり読み出

学習院大学理学部（〒171-8588 東京都豊島区目白 1-5-1）　E-mail: takuya.hirano@gakushuin.ac.jp

したりすることが可能である．

2つ目の新しいリソースである量子エンタングルメントは，複数の粒子間に成立する量子力学特有の相関である．量子エンタングルメントの代表的な例は，次式のような重ね合わせ状態にある2つの光子の偏光状態である：$|\psi^{(-)}\rangle=\{|\leftrightarrow\rangle_1|\updownarrow\rangle_2-|\updownarrow\rangle_1|\leftrightarrow\rangle_2\}/\sqrt{2}$．ここで，右辺第1項の $|\leftrightarrow\rangle_1$ は1つ目の光子が水平偏光状態にあること，$|\updownarrow\rangle_1$ は2つ目の光子が垂直偏光状態にあることを表す．第2項は，1つ目が垂直，2つ目が水平偏光にある状態を表すので，2つの光子の偏光状態を測定すると，片方が水平であれば，もう片方は垂直であるというように，測定結果には相関が生じる．この相関は2つの光子がどんなに離れた場所にあっても生じるので，量子エンタングルメントというリソースは，時空の任意の2地点間である種の関係をもつことを可能にするとみることができる．

1.2 量子鍵配布

量子暗号は，量子状態を正確に読み出せないといった量子力学の特徴を積極的に利用して，安全な通信を行うことを目的としている[3-6]．量子鍵配布というときには，正規の送信者と受信者しか知らない秘密鍵を共有することが目的で，第三者に秘密鍵が漏れないことを物理法則により保障する．一般に量子力学では，測定を行って測定対象についての情報を読み出すと，測定後の測定対象の状態は，測定前とは異なる状態に変化してしまう．そこで，送信者から受信者へ量子力学的な状態を送り，伝送後の状態が伝送前の状態から変化していなければ，伝送中に測定が行われなかったこと，すなわち第三者による盗聴が行われなかったことを確認できる．ただし，量子力学的な状態を使って意味のある情報を忠実に送ることは難しいので，ランダムなビット列(秘密鍵)を伝送して共有するのが量子鍵配布のアイデアである．ランダムなビット列であれば，そのうちの一部しか伝送できなかったとしても，送ることができた部分を使うことにすればよいからである．

量子鍵配布の最初の具体的な実現方法は，1984年にBennettとBrassardにより提案された[7]．これは，単一光子の4つの偏光状態，水平偏光と垂直偏光，それらの偏光面を45度回転した右45度および左45度の直線偏光を用いる手続きで，BB84プロトコルと呼ばれている．送信者と受信者が行う手続きを順番に表に書いていけば，その手続き自身や簡単な盗聴に対する安全性は容易に理解することができる[8]．しかし，実用化という観点からは，送信者と受信者が現在の技術で実行できることの範囲内で安全性を保証しなければならない．例えば単一光子の発生装置や雑音のない検出装置は存在しないといったことを考慮する必要がある．これは難しい問題であると同時に，物理学，光学，情報科学等の学際領域に広がる魅力的な研究テーマとなっている．

1984年以降，多くのプロトコルが提案されているが，これまでに実験が行われている代表的なプロトコルをあげると，量子エンタングルメントを用いるE91プロトコル[9]，2つの状態を用いるB92プロトコル[10]がある．このほか，単一光子検出を用いない量子暗号も最近注目を集めている(3章参照)．

1.3 量子鍵配布の安全性

上で述べたように，量子鍵配布はランダムなビット列を共有することを目的としており，送受信の際に量子状態が変化しなければ，送信者と受信者が共有するビット列は一致するようにプロトコルはつくられている．そして，第三者による盗聴があった場合には，ビット列にくい違い（ビットエラー）が生じる．そこで，送信者と受信者でビット列の一部を照合し，もしもビットエラーがなければ，照合に使用しなかった残りの部分についても盗聴が行われなかったと推定でき，盗聴がなかったことが保障される安全な秘密鍵を共有できる．これが，量子暗号により盗聴が絶対に不可能な安全な通信を実現するというひとつの意味である．この場合，盗聴という行為を積極的に禁止しているのではなく，気づかれずに盗聴することができないという意味で，盗聴が不可能になっている．

しかし，現実の通信では，検出器の不完全性や通信路に存在する雑音等により，ビットエラーが発生する．そのため，エラーが発見されたら盗聴者が関与したとして信号を破棄するという立場をとるとしたら，量子鍵配布の実用化は不可能になってしまう．また，現実の通信路には必ず損失が伴うので，損失による状態の変化の影響も考慮する必要がある．現実的な状況下，すなわち送信者と受信者が現時点で利用できる技術により量子鍵配布を行うためには，ビットエラーや損失等があっても安全性を保障する仕組みが必要である．

そのような仕組みのひとつが，送信者と受信者が量子鍵配布により得たビット列に対して，従来の情報処理技術を利用して，誤り訂正と秘匿性の増強（privacy amplification）という手続きを行うことである[11-16]．秘匿性増強は，ビット列をうまく圧縮することで，圧縮後のビット列に関する盗聴者の知識を小さくする手続きである．例えば，3つのビットのうち，盗聴者が2つのビットまでを知っている場合に，3つのビットのパリティーを新しい鍵として用いることにすれば，鍵の長さはもとのビット列の長さの3分の1になってしまうが，圧縮後の鍵に関する盗聴者の知識

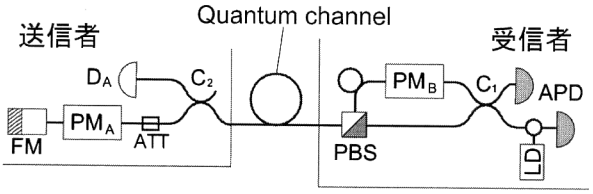

図1　プラグアンドプレイ量子鍵配布システム[26]．

をゼロにすることができる．一般に，もとのビット列についての盗聴者の（Rényi）情報量が正規の受信者の（相互）情報量より小さければ，圧縮後のビット列についての盗聴者の（相互）情報量を漸近的にゼロにできることが証明されている[17]．ここで重要なのが，鍵生成率（secure key gain）という量である．鍵生成率は，量子鍵配布で得たビット列のうち，誤り訂正と秘匿性増強を行った後に安全な鍵となる割合である．鍵生成率の値が正であれば，たとえ量子鍵配布の段階で盗聴者に多少の情報が漏れていたとしても，最終的な鍵についての盗聴者の情報はゼロになる．この意味で，現実的な状況下で安全な鍵配布が実現可能である．いくつかのプロトコルに対しては，実験装置の性能が決定した場合に，鍵生成率を示す表式が導かれている[16,18,19]．

2.　単一光子検出を用いる量子鍵配布

世界ではじめて行われた量子鍵配布の実験は，前章で述べた4つの偏光状態を用いるBB84プロトコルの実証実験で，プロトコルの提唱者であるBennettらによって1990年ころに行われた[20]．光源は波長550 nmの発光ダイオードで，空中を32 cm飛ばした後，光電子増倍管を使って単一光子検出を行うというテーブルトップの実験であった．この実験以降，長距離化，安定性や安全性の向上を目指して，数多くの研究が行われてきた．この章では，量子鍵配布の実験に用いられる装置の現状について簡単に述べた後，BB84プロトコルの実験を紹介する．

2.1　光源，通信路，検出器

BB84とB92プロトコルの実験では，レーザー光を減衰させて微弱にした光源を通常用いる．微弱なレーザー光の平均光子数をμとすると，n個の光子が含まれる確率は，平均と分散がμのポアソン分布に従う．平均光子数を小さくすると，2個以上の光子が含まれる確率が十分小さくなるので，これを擬似的な単一光子光源とみなすことができる．ただし，1光子が含まれる確率が小さくなるうえ，2個以上の光子が含まれる確率もゼロではないので，理想的な1光子状態とは異なる．1光子が含まれる確率が小さいことは伝送レートの低下に，2個以上の光子が含まれる確率がゼロでないことは盗聴者に漏れる情報の増加につながる．E91プロトコルではパラメトリック光子対を用いるが，この場合も，光子対が2つ以上含まれる確率を考慮しなければならない．これらの問題を解決するために，量子ドットなどを用いた1光子光源が研究されている[21,22]．

量子通信路としては，光ファイバーまたは自由空間中の伝播を用いた実験が行われている．光ファイバーの場合には，損失を小さくするためには，波長1.55 μmのレーザー光の使用が有利である．このとき，1 kmあたりの損失は0.2 dB程度であるので，50 km伝播した後の透過率は10%，100 kmでは1%しか透過しない．また，光ファイバーを通して任意の偏光状態を保存したまま長距離を安定して送ることは困難なので，偏光状態ではなく，2つのパルス間の位相に情報をのせる方法が用いられる[6]．自由空間を伝播させる実験は，地上と人工衛星の間での量子鍵配布に道を開くものである[23]．空中を飛ばす場合には，光の偏光状態は基本的に変化しないが，大気による光ビームの乱れと周囲の迷光の影響が問題となる．

検出器としては，量子効率が高いことが求められるので，光電子増倍管ではなく，アバランシェフォトダイオード（APD）をガイガーモードと呼ばれる特別な動作法で用いるのが普通である．ガイガーモードは，ブレークダウン電圧よりも高い電圧を印加しておき，1個の光子によって引き起こされるなだれ電流により単一光子検出を行う方法である．このため，光子が1個以上きたということがわかるだけで，例えば1光子状態と2光子状態を区別することはできない．

以上，ごく大まかに実験装置の現状について述べた．単一光子検出を用いる量子鍵配布の研究では，実験的な面では種々の装置の性能を向上させること，そして理論面では，現実的な状況下での安全性を調べることが主要なテーマとなっている．

2.2　BB84プロトコルの実験

BB84プロトコルは実験の容易さと安全性の高さのバランスがよい面があり，実験的にも理論的にも最もよく研究されているプロトコルとなっている．ここでは，光学の観点からも興味深いと思われるファラデーミラーを用いたプラグアンドプレイ・システムと呼ばれる光学系について紹介する（図1参照）[24,25]．

図1をみるとわかるように，プラグアンドプレイ・システムでは受信者となる側にレーザー光源（LD）があり，光は量子通信路を往復して，受信者の側に戻ってくる．基本的には，受信者側のビームスプリッター（C_1）で分かれた2つのパルスが，ファラデーミラー（FM）で反射して戻っ

てきて干渉を起こす干渉計である．マッハ・ツェンダー干渉計と原理的には同じなので，2つの光路間の位相差が0度の場合には，2つの出力の片方にのみ光パルスは出力され，180度の場合にはもう片方の出力のみに光子が現れる．これは，光子の偏光状態を用いる量子鍵配布で，水平か垂直の直線偏光を送り，偏光ビームスプリッターのどちら側に光子が現れるかということと等価であるので，2つのパルス間の位相差を用いて量子鍵配布が実行できる．この光学系では，ファラデーミラーを用いているために，光ファイバー中の偏光の乱れや，2つのパルス間の光路長の変動などが自動的に補正される．量子通信路となる光ファイバーを送信者と受信者のボックスに接続するだけで，無調整で量子鍵配布を実行できるので，プラグアンドプレイと呼ばれており，実用化を考える際には大変有効な仕組みである．ただし，コヒーレント光を反射して送り返すので，量子ドットのような単一光子光源があっても利用できない．実際の実験では，ジュネーブ湖底に敷設された光ファイバーを使って，ジュネーブ-ローザンヌ間67 kmで量子鍵配布の実験が行われている[26]．国内では，三菱電機のグループが長さ87 kmの光ファイバーを使った実験を行った．

プラグアンドプレイ・システムでない実験では，NECが平面光回路を用いることにより高い安定性をもつ光干渉計を実現し，150 kmの単一光子伝送を行っている*1．また，自由空間中を伝播させる実験では，23.4 km離れた2500メートル級の山の頂上間で偏光状態を用いた鍵配布が報告されている[27]．この実験では，4つの偏光状態をつくるのに4つのレーザーを用い，受信側では無偏光ビームスプリッターの後ろに2つの偏光ビームスプリッター，さらにその後ろに計4つの光子検出器を用いることで，能動的に制御する部品が不要な光学系を使用している．地上実験では，B92プロトコルによる1.6 kmの距離の実験が行われている[28]．

3. ホモダイン検出を用いた量子鍵配布

この章では，連続変数の量子暗号と呼ばれる，単一光子検出を用いない量子暗号方式を，筆者らの研究を中心にして紹介する．

3.1 連続変数の量子情報処理

量子情報処理はおもにスピンや偏光等，量子ビット（qubit）を基本単位として発展しているが[1,2]，位置や運動量のような連続スペクトルをもつ物理量（連続変数）を基本単位として扱った量子情報処理も可能である．光に関する連続変数の代表例は，電磁場の直交位相振幅である．光の直交位相振幅を扱った量子通信に関する実験では，量子テレポーテーションの実験が有名である[29]．一方，連続変数の量子暗号も，EPR相関をもった状態を用いる方法[30]，スクイーズド状態を用いる方法[31-33]，コヒーレント光を用いた方法[34-37]等が提案されている．

光の直交位相振幅は交換関係 $[\hat{x}_1, \hat{x}_2]=i/2$ を満たすので，直交位相振幅の同時測定は制約があり[38]，$\hat{x}_1$，$\hat{x}_2$ のいずれかを測定した場合のみ信号を読み取ることができるという状況をつくり出すことができる．これが連続変数を用いる量子暗号の原理となっている．

平衡型ホモダイン検出は，光の直交位相振幅の検出法であり，量子雑音を測定する方法として発展してきた．特に，時間領域の平衡型ホモダイン検出では，単一測定（single shot measurement）を実現できる．そのため，パルスごとに量子状態を選んで送信して測定する量子鍵配布に直接利用できる．実際，量子鍵配布の実験は，能動的に変調をほどこした信号をホモダイン検出する作業になっている．

3.2 連続変数の量子暗号実験

連続変数の量子鍵配布の実験装置は，マッハ・ツェンダー干渉計となっている（図2参照）．信号を送信するには，干渉計の片方の腕の光強度，また光学距離を適当なタイミングで変調してやればよい．つまり，パルスごとに位相変調や振幅変調を加えればよい．

光強度は固定して，位相変調のみを加えるほうが実験装

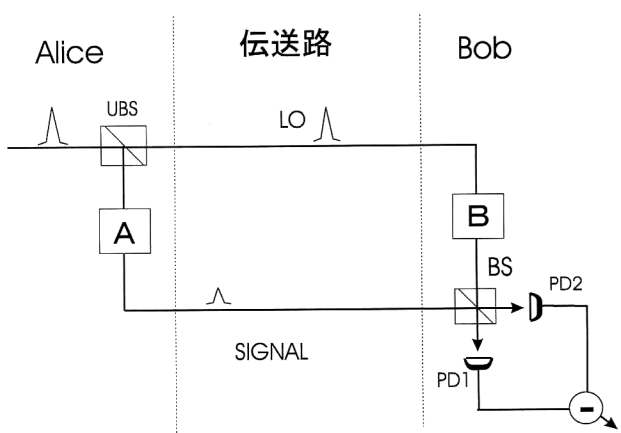

図2 平衡型ホモダイン検出を用いた量子鍵配布装置の概略図．レーザーパルスは，非対称ビームスプリッター（UBS）で強い強度の参照光（LO）と弱い強度の信号光（signal）に分岐される．送信者アリスは信号光に変調を加える（A）．受信者ボブは参照光に位相変調を加え（B），平衡型ホモダイン検出を行う．ホモダイン検出器は50：50のビームスプリッター（BS）と2つのフォトダイオード（PD1，2）からなっており，2つのPDの差信号を出力する．

*1 T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka and K. Nakamura: arXiv quant-ph/0403104.

置はシンプルになる．4状態の方式[37]では，送信者は $\phi_A=\{0,\pi/2,\pi,3\pi/2\}$，受信者は $\phi_B=\{0,\pi\}$ のランダムな位相変調を加える．測定後，$|\phi_A-\phi_B|=\{0,\pi\}$ となったデータからビット列を生成する．これは干渉計を用いた量子暗号[3,10]と同じ手続きであり，実際の実験装置[37]は時間領域干渉計[3]を利用している．ただし，観測される値は，位相差 ϕ として $\sqrt{n}\cos\phi$ を中心としたガウス分布に従う実数の列となる．実数の列からビット列をつくり出すために，閾値 $x_0\geq 0$ を導入する．測定値が $+x_0$ 以上をビット1，$-x_0$ 以下をビット0として，実数値の列からビット列をつくり出す．$|x|<x_0$ の信号はビット列として利用しないことにする．x_0 を大きく設定すると，利用されないデータが増えるため効率が低下するが，ビットエラーは小さくなる．このように測定結果に従って選択的にデータを利用することをpostselectionと呼ぶ．伝送路の光損失のみを考慮した状況では，postselectionが有効に機能することがわかっている[36,39,40]．

以上の方法では，変調そのものは離散的（4種類の変調）である．一方，連続値の変調を行い連続量を直接信号として扱うことも可能である．このような例として，位相振幅がガウス分布となるように振幅と位相を変調させる方式が提案されている[34,35]．実験装置はやはり干渉計であるが，この方法では，位相変調だけでなく振幅変調を行う必要がある[35]．

3.3 検出器の性能と安全性

連続変数の値がどこまで正確に読み取れるかが，ホモダイン検出器の性能を反映する．デバイス等の雑音で決まる分散を $(\Delta x_d)^2$ とすると，実際に観測される分布は，理想的な分布を $(\Delta x_d)^2$ のガウス関数で畳み込んだ分布となる．つまり，現実環境の雑音の影響は，検出器の測定値が有限の幅をもつことと考えることもできる．盗聴者が直交位相振幅の同時測定[38]を行うと分散が大きくなるが，測定された分散の増加が同時測定によって引き起こされるものよりも大きい場合，同時測定の可能性を排除することができず，秘密鍵をつくることが不可能となる[40]．

最後に，検出器の技術的な面に関して少し述べる．APDを冷却してガイガーモードで動作させ単一光子検出を行う場合，伝送レート（単位時間に測定できるパルスの数）をある程度高くすると，アフターパルスのためエラーが増加してしまう[6]．このため，伝送レートは数MHz以上には上げられないといわれている．また，通信波長帯に対して高い量子効率は得られていない[5,6]．一方，ホモダイン検出は，常温で通信波長帯でも高い量子効率が達成できる通常のフォトダイオードを利用する．伝送レートに関しては，800 kHzで行われたという報告がある[35,41]．また，強い参照光で微弱な信号光をサンプルするという形になっているため，迷光の影響を受けにくいという特徴がある．このように，室温で動作し環境の影響を受けにくいことから，連続変数を用いる方法は，既存の光ネットワークへの組み込みでは有利と予測される．ただし，まだ研究の歴史が浅いことから，安全性についての理論的な研究も発展途上であり，高い伝送レートが実現できるという予測もあるが[35]，その結論は今後の研究を待たなければならない．

量子通信や量子鍵配布は光の量子的な性質を利用しようとする試みであるが，実際の実験は，種々の光学技術に基礎をおいたものである．量子鍵配布は非常に実用に近い段階にあるとはいえ，伝送距離や伝送レート等の点で改善すべき余地がある．第3章では，新しい可能性として研究が進んでいる，連続変数の量子鍵配布について紹介した．また，紙数の関係で紹介できなかったが，初期に共有している秘密鍵を使って，送受信する量子状態を暗号化し，高い伝送レートを得ようという試みも行われている[*2]．今後も，理論・実験の両面でブレークスルーが続くことを期待したい．

総務省の戦略的情報通信研究開発推進制度，および科学技術振興機構の戦略的創造研究推進事業による支援に感謝する．

文　献

1) C. H. Bennett and D. P. DiVincenzo: Nature, **404** (2000) 247.
2) M. A. Nielsen and I. L. Chuang: *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).
3) 清水　薫：“量子暗号と光通信”，光学，**29** (2000) 412.
4) 井元信之：Computer Today, No. 113 (2003) 34.
5) 西岡　毅，長谷川俊夫：数理科学，**38**，No. 9 (2000) 34.
6) N. Gisin, G. Ribordy, W. Tittel and H. Zbinden: Rev. Mod. Phys., **74** (2002) 145.
7) C. H. Bennett and G. Brassard: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India, December 1984) pp. 175-179.
8) C. H. Bennett, G. Brassard and A. K. Ekert: Sci. Am., October (1992) 26-33; 日経サイエンス，12月号 (1992) 50-60.
9) A. Ekert: Phys. Rev. Lett., **67** (1991) 661.
10) C. H. Bennett: Phys. Rev. Lett., **68** (1992) 3121.
11) N. Lütkenhaus: Phys. Rev. A, **54** (1996) 97.
12) H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin and G. Ribordy: Appl. Phys. B, **67** (1998) 743-748.

[*2] H. P. Yuen: arXiv quant-ph/0311061.

13) B. A. Slutsky, R. Rao, P. Sun and Y. Fainman: Phys. Rev. A, **57** (1998) 2383.
14) B. Slutsky, P. C. Sun, Y. Mazurenko, R. Rao and Y. Fainman: J. Mod. Opt., **44** (1997) 953.
15) H. E. Brandt: J. Math. Phys., **43** (2002) 4526.
16) N. Lütkenhaus: Phys. Rev. A, **61** (2000) 052304.
17) C. H. Bennett, G. Brassard, C. Crépeau and U. M. Maurer: IEEE Trans. Inf. Theory, **41** (1995) 1915.
18) E. Waks, A. Zeevi and Y. Yamamoto: Phys. Rev. A, **65** (2002) 052310.
19) K. Tamaki, M. Koashi and N. Imoto: Phys. Rev. A, **67** (2003) 032310.
20) C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin: J. Cryptography, **5** (1992) 3.
21) E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon and Y. Yamamoto: Nature, **420** (2002) 762.
22) 山本喜久：応用物理，**72** (2003) 146.
23) J. G. Rarity, P. R. Tapster, P. M. Gorman and P. Knight: N. J. Phys, **4** (2002) 82.
24) A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden and N. Gisin: Appl. Phys. Lett., **70** (1997) 793.
25) D. S. Bethune and W. P. Risk: IEEE J. Quantum Electron., **36** (2000) 340.
26) D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden: N. J. Phys., **4** (2002) 41.1-41.8.
27) C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster and J. G. Rarity: Nature, **419** (2002) 450.
28) W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt and C. G. Peterson: Phys. Rev. Lett., **84** (2000) 5652-5655.
29) A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble and E. S. Polzik: Science, **282** (1998) 706-709.
30) M. D. Reid: Phys. Rev. A, **62** (2000) 062308.
31) M. Hillery: Phys. Rev. A, **61** (2000) 022309.
32) T. C. Ralph: Phys. Rev. A, **62** (2000) 062306.
33) N. J. Cerf, M. Lévy and G. Van Assche: Phys. Rev. A, **63** (2001) 052311.
34) F. Grosshans and P. Grangier: Phys. Rev. Lett., **88** (2002) 057902.
35) F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf and P. Grangier: Nature (London), **421** (2003) 238.
36) Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus and G. Leuchs: Phys. Rev. Lett., **89** (2002) 167901.
37) T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi and R. Namiki: Phys. Rev. A, **68** (2003) 042331.
38) U. Leonhardt: *Measuring the Quantum State of Light* (Cambridge, 1997).
39) R. Namiki and T. Hirano: Phys. Rev. A, **67** (2003) 022308.
40) R. Namiki and T. Hirano: Phys. Rev. Lett., **92** (2004) 117901.
41) H. Hansen, C. Lodahl, A. I. Lvovsky, J. Mlynek and S. Schiller: Opt. Lett., **26** (2001) 1714.

(2004年4月12日受理)