ホモダイン方式による量子暗号通信

平　野　琢　也

Quantum Key Distribution Using Homodyne Detection

Takuya HIRANO

We review the present status and future prospect of the quantum key distribution (QKD) using homodyne detection. Homodyne detection measures an optical quadrature-phase amplitude that is a continuous variable (CV). Unconditional security of the CV QKD has been proved recently. The CV QKD has high affinity with coherent optical communication systems, and is a promising technology for future QKD networks.

Key words: quantum key distribution, homodyne detection, coherent states, unconditional security

古典力学と量子力学の大きな違いのひとつに測定の果たす役割がある．古典力学では，物体の状態をどこまでも正確に，何度でも測定することが許されている．一方，量子力学では，測定を行うと測定対象の状態は一般に変化し，測定対象の状態を正確に知ることはできない．そこで，送信者から量子力学的な状態を送り，受信者が受け取った状態の変化を調べることで，途中の通信路でどのような測定が行われたのか，つまり，どのような盗聴が行われたのかを知ることができる．このような量子論の特徴を利用する安全な通信，量子暗号通信を実行するには，送信者はよく制御された量子状態を送信し，受信者は測定による量子状態の変化を検出できるような測定を行うことになる．実際に量子状態を遠方まで送信する最もよい手段は，光を利用することであり，送信者は，微弱な光，または，わずかに状態の異なる光をよく制御して送信し，そして，受信者は，わずかな状態の違いを精度よく見分ける光検出器が必要である．

微弱な光を検出するひとつの有力な方法は，単一光子検出である．単一光子検出は，光子の個数という離散的な物理量を測定するもので，多くの場合，光子が1個以上届いたかどうかを判別する．しかし，光ファイバー中の損失が小さい通信波長帯の光に対して単一光子検出を行うことは容易ではなく，検出効率の向上，ダークカウントの低減，高速動作の実現のための研究開発が活発に行われている．もうひとつの微弱光検出の有力な方法に，ホモダイン検出がある．ホモダイン検出は，電場の直交振幅（quadrature-phase amplitude, 量子光学分野では直交位相振幅とよぶことが多い）という連続的な物理量を測定するものである．

量子情報処理は，単一光子の偏光やスピンなどで実現される量子ビット（qubit）を基本単位として用いることが多いが，連続量を扱う量子情報処理も可能である[1]．ホモダイン検出を用いる量子暗号は，連続量量子情報処理のひとつであり，本稿では，ホモダイン検出を用いる量子鍵配布（quantum key distribution, QKD）について述べる[2]．単一光子を用いるQKDと比べると，研究の歴史が比較的新しいこともあり未開拓のことがらも多いが，この1, 2年で無条件安全性が理論的に示され[3, 4]，実装実験も進むなど研究が進展している．この量子鍵配布は，コヒーレント光通信と非常に親和性のよい技術であり，通常のフォトダイオードを室温で用いても量子雑音限界の測定が可能であること，パルスあたりの鍵生成率の向上が可能であるなどの特徴がある．

1.　ホモダイン検出QKDにおける変調と測定

ホモダイン検出を用いるQKDでは，受信者は光の直交振幅を測定する．直交振幅は，電場を複素表示したとき，

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

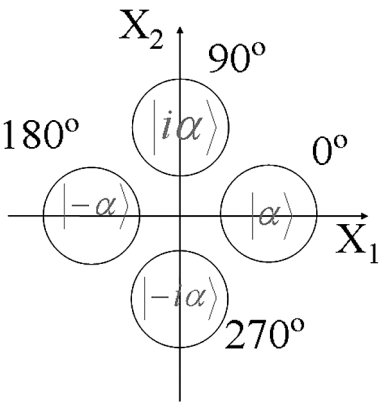

図1　90度ずつ位相回転した4つのコヒーレント状態.

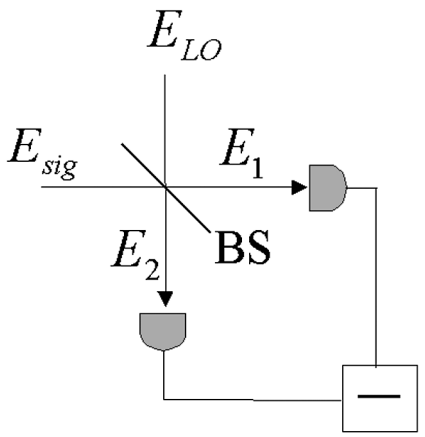

図2　ホモダイン検出の概念図.

その実部と虚部に相当する物理量である．送信者は光の電場を複素平面上で変調して送信し，受信者は，測定の結果，ある実数値を得ることになる．この実数値は，送信者の行う変調と関係があるので，送信者と受信者は情報を共有することが可能である．このとき，盗聴者が得ることができる情報量よりも，正規の送受信者が共有する情報量のほうが多いとき，安全な通信を行うことが可能となる．安全性についてのより詳しい議論は，次章で述べる．

ホモダイン検出 QKD では，送信者は電場の振幅と位相に変調を与えるが，このとき，原理的に2つの変調方式がありうる．有限種類の変調か，無限に多くの種類の変調を行うかという2つの方式である．これまでに最もよく研究されているのは，後者の変調方式であり，送信する光の複素電場の確率密度が，複素平面上でガウス分布するように変調を行う方式である[5-8]．前者の有限通りの位相変調を与える方式では，例えば，4通りの位相変調を与える QKD を考えることができる[4,9]．ガウス変調方式では，送信者の行う直交振幅変調は実数値で指定されるので，送信者と受信者は相関をもった実数値のペアをもつことになる．有限通りの変調の場合には，送信者の行う変調は離散量で指定されるので，連続量と離散量の雑種的な方式であるといえる[1]．

図1は，4通りの位相変調を複素平面上に表したものである．これは，無線などのディジタル変調で用いられる四位相偏移変調（QPSK, quaternary phase-shift keying）と基本的には同じである．ホモダイン検出 QKD に対する量子力学的な効果は，不確定性関係に起因する量子ゆらぎに現れる．量子ゆらぎの存在のために，質点の位置と運動量の両方を同時に正確に定めることが原理的にできないのと同じように，位相が90度ずれた（複素平面上で直交する）2つの直交振幅を同時に正確に定めることはできない．量子論では，レーザー光の状態は，コヒーレント状態として扱うことができる．コヒーレント状態は，2つの直交振幅の不確定さが等しい最小不確定状態であり，位相に依存しない一定の量子ゆらぎをもっている（そのゆらぎの大きさは常に真空状態と等しい）．図1は，微弱なレーザー光に，0度，90度，180度，270度の4つの位相変調のいずれかを与えたものである．これら4つの状態の中心は複素平面上の4つの点で表される．しかし，コヒーレント状態のもつ量子ゆらぎのために，直交振幅の測定値は不確定となる．4つのコヒーレント状態は互いに非直交な状態であるため，これら4つの状態の直交振幅の測定値の分布は重なり合い，4つの状態を，すべての測定について，誤りなく区別することは原理的にできない．そして，レーザー光が微弱になればなるほど状態の重なり合いが大きくなり，状態を区別することは難しくなる．そのため，盗聴者は送信者が送った状態を判別しようとしても，確実に読み出すことは原理的に不可能である．

送信者が送る光の量子状態については，いま述べたコヒーレント状態が，実験的には実現が容易である．しかし，量子ゆらぎを制御したスクイーズ状態を送る方式もあり，量子ゆらぎが増加することにより，通信路の雑音に対する耐性が高まる場合があることが指摘されている[10]．

次に，受信者の行うホモダイン検出について説明する．ホモダイン検出で行う操作は，図2に示すように，測定したい光の電場 E_{sig} を局部発振光（LO 光）と，反射率と透過率が50：50のビームスプリッターで重ね合わせ，その2つの出力光の強度の差を測定するものである．この強度の差信号は，LO 光強度が信号光に比べて十分強いとき，信号光の直交振幅を与える．微弱光を直接測定するのではなく，比較的強度の強い LO 光と重ね合わせて測定するので，室温で動作させるフォトダイオードで光の強度を測定し，量子雑音限界の測定を行うことが可能である．また，LO 光

のモードと重なり合う信号光が測定されるので，LO 光が空間的，時間的，そして周波数のフィルターとして働き，単一光子検出に比べて迷光の影響を受けにくいという特徴もある．しかし，LO 光は信号光に対して位相がロックされていなければならず，その LO 光をどのようにして受信者が用意するかという点が実験上の課題となる．

信号光をビームスプリッターで 2 つに分け，2 つの直交する位相振幅を同時に測定することも可能であり，このような測定を，量子情報の分野では，ヘテロダイン検出とよぶことが多い．ただし，共役な 2 つの物理量を測定する代償として，それぞれの直交振幅測定の信号対雑音比は悪化する．

2. ホモダイン検出 QKD の安全性

現実的な状況下で連続量 QKD の安全性を議論するためには，通信路の損失と過剰雑音（excess noise）について考慮する必要がある[9]．過剰雑音は，受信者の測定するゆらぎが，量子雑音限界に比べてどの程度大きくなっているかを表すものである．盗聴者の能力に技術的な制約をつけず，物理法則に反しない限りどのような盗聴も行える場合においても安全であるとき無条件に安全であるという．冒頭で述べたように，連続量 QKD の無条件安全性が最近理論的に示された[3,4]．

通信路の損失と過剰雑音が安全性にどのような影響を与えるかについては，いくつかの具体的な盗聴者の攻撃方法を検討することにより，理解を深めることができる．

ひとつめの盗聴方法は，分岐攻撃（beam splitting attack）とよばれる攻撃であり，これは，通信路の損失分をビームスプリッターで分岐して盗聴者が測定し，残りを損失のない通信路で正規の受信者に送るという攻撃である．この分岐攻撃は，受信者の受け取る状態を変化させないので，盗聴者は気付かれることなく，情報を盗み見ることが可能である．特に，透過率が 50％以下の場合には，盗聴者が受け取る光の強度は，正規の受信者よりも強くなるので，送信者が送った状態についての情報を，正規の受信者よりも盗聴者のほうがより多くもつことになり，安全な通信はできないという議論が行われたこともあった[11]．しかし，実際には，このような場合においても安全な鍵を得ることが可能であり，その方法として，事後選択（post selection）[12] と逆調整（reverse reconciliation）[6] という手法が研究されている．この 2 つの手法は組み合わせることも可能であり，組み合わせることでよい結果が得られることも示されている[13]．

事後選択は，受信者が自分に都合のよい測定値を得たときのみ選択して鍵を作る手続きである[9]．量子ゆらぎにより受信者の得る測定値はランダムに変動するが，一般に，振幅の大きな測定値を得たときは，送信者の行った直交変調を推測する際の誤り率が小さくなる（正規の送受信者の相互情報量が多くなる）．ここでポイントとなるのは，正規の送受信者は，自分たちに都合のよいパルスを選ぶことができるが，盗聴者が都合のよいパルスを選ぶことはできないという量子鍵配布における立場の違いであり，このことを事後選択は利用している．過剰雑音がない場合には，どんなに損失が大きくても，事後選択により安全な鍵を配布することが可能である[14]．

逆調整では，送受信者がもつ相関をもったデータから，第三者の知らない正しいビット列を送受信者がどのようにして共有するかという手続きに注目する．通常は，送信者のデータに一致するように，受信者が自分のデータを修正していくのに対し，逆調整では，受信者のデータに一致するように，送信者側のデータを修正する．通常の手続きでは，送信者と盗聴者の相互情報量が，送信者と受信者の相互情報量よりも多い場合は，安全な鍵を配送できないが，逆調整では，受信者と盗聴者の相互情報量が，送信者と受信者の相互情報量よりも少ないことを利用して安全な鍵を作ることができる[5]．例えば，送信者の送った光の強度が 1 で，そのうちの 0.7 を盗聴者が受け取り，残りの 0.3 を受信者が受け取った場合を考えると，送信者のデータについては，受信者よりも盗聴者がよく知っていることになる．しかし，受信者のもつデータについては，送信者のほうが盗聴者よりもよりよく知っているはずであり，このことを逆調整では利用する．

単一光子を用いる QKD において，第三者による盗聴により誤り率の増大が起こるのと同じように，ホモダイン検出を用いる QKD では，盗聴は過剰雑音の増加をもたらす．そして，実験装置の不完全性等により，受信者のデータに過剰雑音が存在しているときは，その過剰雑音が盗聴者によって引き起こされたという可能性を原理的には排除できない．そのため，過剰雑音が存在している場合は，盗聴者に情報が漏れている可能性があることになる．過剰雑音の大きさは，定量的には，受信者が測定する直交振幅の分散が，量子雑音限界よりも（$1+\delta$）倍であるとき，δ として表されることが多い．

本章で考える 2 つ目の具体的な盗聴方法は，ヘテロダイン検出を行う“なりすまし攻撃”（intercept/resend attack）である[14]．これは，過剰雑音がある一定以上あるときに可能となる重要な盗聴方法である．ヘテロダイン検出は，前に述べたように，複素平面上で 90 度位相のずれた 2 つの直交振幅を同時に測定する検出方法のことで，具体的には，

盗聴者は信号光をビームスプリッターで半分ずつに分割し，片方で直交振幅の実数成分，もう片方は90度位相をずらした虚数成分を，それぞれホモダイン検出する．そして，送信者に“なりすます”ために，盗聴者は測定で得た直交振幅をそれぞれ$\sqrt{2}$倍した複素振幅をもつ光を，正規の受信者へ送る．このなりすまし攻撃が行われた場合，受信者の受け取る信号光は盗聴者が送信したものであり，盗聴者に対する正規の送受信者の優位性は失われ，安全な鍵を配送することは不可能となる．また，この攻撃は特に高度な未来の技術（量子メモリーや損失ゼロの光ファイバーなど）を必要とせず，現在の技術でも実行可能であることにも留意しておくべきであろう．

次に，なりすまし攻撃が成立する条件について述べる．なりすまし攻撃の過程で盗聴者が再送する信号光の分散は，もとのコヒーレント状態の3倍まで増加するが，透過率ηの通信路を通った後は，分散は$2\eta+1$倍まで小さくなる．そのため，過剰雑音の大きさδが2η以上であるときは，なりすまし攻撃を受けている可能性がある．結局，ホモダイン検出を行うQKDで安全な鍵を配送するためには，$\delta<2\eta$である必要がある．これは，コヒーレント状態を送受信し，ホモダイン検出を行うQKDであれば，プロトコルの詳細によらず満たさなければならない条件である[14]．例えば，通信路の透過率が1%である場合は（長さ100 kmの低損失光ファイバーに相当），過剰雑音は2%以下でなければならない．

ホモダイン検出を用いる量子暗号の無条件安全性は，量子de Finetti表現定理を用いることで示されている[3]．この定理が成り立つとき，collective攻撃に対して安全であれば，量子論の枠内で可能なあらゆる攻撃に対して安全であることになる．ガウス変調方式の連続量QKDのcollective攻撃に対する安全は，2007年に示されているので[15,16]，量子de Finetti表現定理により，無条件安全性も示されたことになる．有限個の変調を行う場合も同様であり，二値変調のcollective攻撃に対する漸近的な安全が示されているので[17]，無条件に安全であることも示されていることになる．では，ガウス変調と有限個の変調のどちらがすぐれているのかということが興味をひく質問となるが，LeverrierとGrangierは，4状態の変調方式と逆調整を組み合わせることで，長距離の無条件安全なQKDが可能であることを示している[4]．彼らは，ガウス変調では信号対雑音比が低下することが問題となるのに対し，4状態の場合では高効率の誤り訂正が可能であり，過剰雑音が0.2%以下であれば，伝送距離200 kmで10^{-6}の秘密鍵生成率を達成でき，4状態のほうがガウス変調よりもはるかにすぐれていると述べている．

3. ホモダイン検出を用いるQKD実験

3.1 ガウス変調方式

2003年にGrosshansらは，ガウス変調方式と逆調整を用いたホモダイン検出QKDの実験を報告し，通信路の透過率が2分の1以下でも個別攻撃（individual attack）に対して安全な鍵を配送できることを示した[5]．この実験は短距離の自由空間を通信路とするテーブルトップの原理検証実験であり，通信路に光損失がないときの鍵生成率は1.7 Mbps, 3.1 dBの損失があるときは75 kbpsであった．同グループは2007年に通信波長帯のレーザー光源を用い，長さ25 kmの光ファイバーを通信路（透過率は0.302）とする実験を報告した[7]．これは一方向の伝送実験であり，送信者から受信者へ向けて，LO光も同じファイバーで伝送する．時間幅100 nsのパルス光を500 kHzの繰り返しで送信し，collective攻撃に対して安全な鍵を2 kbpsで配送している．光学系は二重マッハ・ツェンダー干渉計を用いたもので，信号光とLO光は送信者の装置の中のディレイファイバーで時間差をつけて通信路となるファイバーを伝わり，受信者のディレイファイバーで再度時間差を一致させることで干渉するようになっている．信号光とLO光間の位相差の同期は，全体のパルスのうち5分の1をレファレンスに用いて実現している．また，SECOQCの実験のひとつとして，長さ8 kmの光ファイバーを通信路とするフィールドテストも行っている[18]．

Bing Qiらは同じくガウス変調と逆調整を用い，長さ5 kmのシングルモードファイバーを通信路とする連続量QKD実験を報告している[8]．この実験も二重マッハ・ツェンダー干渉計を用いたものであるが，信号光とLO光を偏光と周波数によっても分離することで，両者を70 dB以上分離できたことを報告している．また，信号光とLO光の位相差については，事後に送信者のデータを回転させて解釈することを提案している．この実験では，盗聴者は通信路のみにアクセスでき，送受信者の装置にはアクセスできないという現実的なモデル（realistic model）において，1パルスあたり0.3ビットの秘密鍵が配送できるとしており，これは離散量QKDよりも2桁すぐれた性能であると報告した．

Symulらは，ガウス変調と事後選択を用いるQKD実験について報告している[6]．これは自由空間を通信路とするテーブルトップの実験であるが，通信路の透過率が0.2で過剰雑音が0.1であってもcollective攻撃に対して安全な鍵を配送できることを示した．この実験では，送信者はサイ

ドバンドの直交振幅に変調を行い，受信者はヘテロダイン検出する方法を用いている．サイドバンドを用いる方法は，周波数領域に多重化することが原理的に可能であるので，高い鍵配送レートを実現できる可能性がある．

3.2 有限通りの変調

送信者がコヒーレント状態に4通りの位相変調を与える4状態のプロトコルは，学習院大学において，2000年前後から研究を進めている方式である．受信者は，2つの共役な直交振幅をランダムに切り替えてホモダイン検出を行う．この方式は，送信者は位相変調を行うだけでよいので実装が容易であり，2つの直交振幅の測定データから量子通信路の特性を評価できる，事後選択による鍵の生成が簡便であるという特徴がある．通信波長帯のパルスレーザーを使用し，長さ1 kmの光ファイバーを通信路とした実験では[9]，受信者の測定する直交振幅はガウス分布でよく表されるが過剰雑音があること，事後選択を行うことで誤り率の低減が可能であることなどを示した．光学系は，二重マッハ・ツェンダー干渉計を用いるものであったが，バルクの光学部品を用いていたこともあり，信号光とLO光の位相を長時間安定に保つのは困難であるという問題があった．

位相を安定に保つひとつの方法に，通信路を往復させる，いわゆるプラグ・アンド・プレイ方式がある[2]．この方式では，受信者の側に光源があり，光ファイバーを往復させることで，ファイバー中で生じる偏光の乱れを自動補正できるほか，信号光とLO光の相対的な位相差も安定に保たれる．離散量QKDの場合でも，光学系の安定性を容易に実現できるというメリットから，よく用いられてきた方式であるが，受信者から送信者へ送る光の後方散乱光が受信者へ戻ってくるので，通信距離を延長する際には問題となっている．同様に，連続量QKDの場合も，後方散乱光による過剰雑音の増加が問題となることが明らかになった．単一光子検出と比較すると，ホモダイン検出は迷光に強いという利点があるが，強度の強いLO光を送らなければならないことは不利な面である．過剰雑音の増加を抑える方法として，音響光学素子を用いて，光の周波数をシフトさせる方法があり，10 kmの伝送距離で，なりすまし攻撃に対して安全な鍵配送を実現できることが示されている[2]．もうひとつの位相を安定に保つ方法として研究を進めているのは，媒質中の屈折率の異方性を利用して，同軸の光学系で二重マッハ・ツェンダー干渉計を構成する方法である[2]．従来の方法に比べて高い安定性をもつこと，外部からの擾乱に対してロバストであることが確認され，自由空間および光ファイバーを用いた長距離の伝送に向けて研究を進めている．

Elserらは，2つの状態を用い，事後選択を行う方式で，100 mの自由空間のQKD実験を報告し[19]，迷光に強いというホモダイン検出の特徴により，日中でもQKDが可能であると述べている．

ホモダイン検出を用いるQKDの概略，安全性，および実験の現状を紹介した．室温で動作可能で小型化に有利である，迷光に強いなどの実装上のメリットがあるうえ，この2，3年で無条件安全性が示され，プロトコルについての理解が深まってきている．しかし，長距離化，高速化，多重化などの実装研究や，最適なプロトコルの模索など多くの課題が残されており，現在はさらなる研究の進展が期待される状況であると思われる．また，コヒーレント光通信技術と類似の方式であることから，長期的には，2つの技術が融合する新しい光通信の可能性が拓かれることが期待される．

原稿を読んでいただいたソニー株式会社の川元洋平さん，学習院大学平野研究室の量子暗号チームの皆さんに感謝します．

文　献

1) S. L. Braunstein and P. van Loock: “Quantum information with continuous variables,” Rev. Mod. Phys., **77** (2005) 513 (arXiv quant-ph/0410100).
2) 平野琢也，川元洋平，並木　亮：“コヒーレント光とホモダイン検波による量子鍵配送”，量子情報通信（オプトロニクス社，2006）pp. 179–204.
3) R. Renner and J. I. Cirac: “de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography,” Phys. Rev. Lett., **102** (2009) 110504.
4) A. Leverrier and P. Grangier: “Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation,” Phys. Rev. Lett., **102** (2009) 180504.
5) F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf and P. Grangier: “Quantum key distribution using Gaussian-modulated coherent states,” Nature (London), **421** (2003) 238.
6) T. Symul, D. J. Alton, S. M. Assad, A. M. Lance, C. Weedbrook, T. C. Ralph and P. K. Lam: “Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise,” Phys. Rev. A, **76** (2007) 030303(R).
7) J. Lodewyck, M. Bloch, R. Garcia-Patron, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin and P. Grangier: “Quantum key distribution over 25 km with an all-fiber continuous-variable system,” Phys. Rev. A, **76** (2007) 042305.
8) B. Qi, L.-L. Huang, L. Qian and H.-K. Lo: “Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers,” Phys. Rev. A, **76** (2007) 052323.
9) T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi and R. Namiki: “Quantum cryptography using pulsed homodyne de-

tection," Phys. Rev. A, **68** (2003) 042331-1–7.
10) R. García-Patrón and N. J. Cerf: "Continuous-variable quantum key distribution protocols over noisy channels," Phys. Rev. Lett., **102** (2009) 130501.
11) F. Grosshans and P. Grangier: "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett., **88** (2002) 057902.
12) Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus and G. Leuchs: "Continuous variable quantum cryptography: Beating the 3 dB loss limit," Phys. Rev. Lett., **89** (2002) 167901.
13) M. Heid and N. Lütkenhaus: "Security of coherent-state quantum cryptography in the presence of Gaussian noise," Phys. Rev. A, **76** (2007) 022313.
14) R. Namiki and T. Hirano: "Practical limitation for continuous-variable quantum cryptography using coherent states," Phys. Rev. Lett., **92** (2004) 117901.
15) M. Navascues, F. Grosshans and A. Acin: "Optimality of Gaussian attacks in continuous-variable quantum cryptography," Phys. Rev. Lett., **97** (2007) 190502.
16) R. Garcia-Patron and N. J. Cerf: "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution," Phys. Rev. Lett., **97** (2007) 190503.
17) Y.-B. Zhao, M. Heid, J. Rigas and N. Lütkenhaus: "Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks," Phys. Rev. A, **79** (2009) 012307.
18) S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri and P. Grangier: "Field test of a continuous-variable quantum key distribution prototype," New J. Phys., **11** (2009) 045023.
19) D. Elser, T. Bartley, B. Heim, Ch. Wittmann, D. Sych and G. Leuchs: "Feasibility of free space quantum key distribution with coherent polarization states," New J. Phys., **11** (2009) 045014.

(2009 年 9 月 10 日受理)