Vol 18 No 1, January 2009
1674-1056/2009/18(01)/0051-05

Chinese Physics B

Linear optical realization of unambiguous quantum state comparison*

Lin Qing(林　青)†

College of Information Science and Engineering, Huaqiao University, Quanzhou 362021, *China*

(Received 25 March 2008; revised manuscript received 20 May 2008)

In this paper, we propose an experimental scheme for unambiguous quantum state comparison assisted by linear optical manipulations, twin-photons produced from parametric down-conversion, and postselection from the coincidence measurement. In this scheme the preparation of the general two mixed qubit states with arbitrary prior probabilities and the realization of the optimal POVMs for unambiguous quantum state comparison are presented. This proposal is feasible by current experimental technology, and may be used in single-qubit quantum fingerprinting.

Keywords: quantum state comparison, linear optics, quantum fingerprinting
PACC: 0367, 4250

In quantum communications and quantum computation, quantum states are used to transmit information, and how to discriminate the received quantum states is a basic problem. However, quantum no-cloning theorem makes a restriction that only a set of orthogonal states can be discriminated determinately.[1] In other words, a set of nonorthogonal quantum states can not be discriminated perfectly, whether the states are pure or mixed. Therefore, how to discriminate the quantum states more efficiently may be an important question. Recently, much effort has been devoted to this question, and then many schemes of discrimination have been proposed, for example, the minimum error discrimination (MED),[2] unambiguous discrimination (UD),[3,4] maximum confidence discrimination (MCD),[5] minimum disturbance discrimination (MDD),[6] and maximum mutual information discrimination associated with the capacity of the quantum channel,[7] etc.

In this paper, we limit our attention to MED and UD. The MED means that, for a set of input states $\{\rho_1, \ldots, \rho_n\}$ with the corresponding prior probabilities $\{p_1, \ldots, p_n\}$ which satisfy $\sum p_i = 1$, one wants to look for a set of measurements which are generally described by positive operator-valued measures (POVM)[8] $\{\Pi_1, \ldots, \Pi_n\}$ which satisfy $\sum \Pi_i = I$ to achieve the maximum average success probability $P^{\rm s}_{\rm MED} = \sum_{i=1}^n p_i {\rm Tr}(\Pi_i \rho_i)$ or the minimum average failure probability $P^{\rm f}_{\rm MED} = 1 - \sum_{i=1}^n p_i {\rm Tr}(\Pi_i \rho_i)$. It is clear that for any set of input states, POVMs always exist for MED, i.e. there is no constrains in the measurements of MED. Compared to MED, it requires that the measurements are error-free in UD, i.e. if the measurements are successful, they are always true, which are denoted by ${\rm Tr}(\Pi_i \rho_j) = 0$ for $i \neq j$. The cost of error-free is that we will have to accept an inconclusive result giving no information. Let $\Pi_?$ denote the POVM element corresponding to this inconclusive result, and then the problem of UD is to look for the optimal POVMs to achieve the minimum probability of inconclusive result denoted by $P^?_{\rm UD} = \sum_{i=1}^n p_i {\rm Tr}(\Pi_? \rho_i)$ under the constrains ${\rm Tr}(\Pi_i \rho_j) = 0$ for $i \neq j$. Different to MED, only the set of input states which satisfies certain conditions (for pure states, see Ref.[9]; for mixed states, see Ref.[10]) can be discriminated unambiguously under the requirement of error-free.

Quantum state comparison is a special case of quantum state discrimination, and it was first considered by Barnett *et al.*[11] Recently it was widely applied in quantum communications, for example, quantum cryptography,[11,12] quantum fingerprinting[13] and quantum digital signatures,[14] etc. Therefore it is worth discussing the realization of quantum state comparison, and in Ref.[12], the realization of quantum comparison of coherent states has been reported. Moreover, Horn *et al* used the minimum-error quantum state comparison to realize the single-qubit optical quantum fingerprinting in experiment.[15] Compared to their experiment, in this paper we consider

*Project supported by the Research Projects of Huaqiao University of China (Grant No 07BS406).
†E-mail: qlin@mail.ustc.edu.cn

the realization of unambiguous quantum state comparison in linear optics. The paper is organized as follows. Firstly, we review the problem of quantum state comparison briefly. Secondly, we present a scheme to prepare the two mixed qubit states with arbitrary prior probabilities. Thirdly, the realization of unambiguous quantum state comparison, i.e., the realization of the optimal POVMs with only linear optical elements is discussed. Fourthly, we show our scheme can be used in quantum fingerprinting and compare our scheme with the experimental one.[15] We end with concluding remarks.

Suppose that there are two identical quantum particles which are each prepared either in the state $|\psi_1\rangle$, or in the state $|\psi_2\rangle$, with prior probabilities q_1 and q_2, respectively, and then we wish to determine whether the two states are equal or different. This problem is called quantum state comparison and it is related to the discrimination of the following two density matrices:

$$\begin{aligned}\boldsymbol{\rho}_1 &= \frac{1}{\eta_1}\left(q_1^2|\psi_1,\psi_1\rangle\langle\psi_1,\psi_1| + q_2^2|\psi_2,\psi_2\rangle\langle\psi_2,\psi_2|\right),\\ \boldsymbol{\rho}_2 &= \frac{1}{2}\left(|\psi_1,\psi_2\rangle\langle\psi_1,\psi_2| + |\psi_2,\psi_1\rangle\langle\psi_2,\psi_1|\right),\end{aligned} \tag{1}$$

with prior probabilities $\eta_1 = q_1^2 + q_2^2$ and $\eta_2 = 2q_1q_2$. In Ref.[11], Barnett *et al* considered the following special case:

$$\begin{aligned}|\psi_1\rangle &= \cos\theta|0\rangle + \sin\theta|1\rangle,\\ |\psi_2\rangle &= \cos\theta|0\rangle - \sin\theta|1\rangle,\end{aligned} \tag{2}$$

with equal prior probabilities $q_1 = q_2 = 1/2$, where $\theta \in [0, \pi/4]$, and they obtained the optimal solutions of MED and UD of quantum state comparison. For MED the optimal measurements are the separate measurements of the single qubit, with the minimum error probability $P_{\mathrm{MED}}^{\mathrm{f}} = \frac{1}{2}\cos^2(2\theta)$, while for UD, the minimum probability of inconclusive result is $P_{\mathrm{UD}}^{?} = \cos(2\theta)$. Then the case that the two states $\{|\psi_1\rangle, |\psi_2\rangle\}$ are arbitrary qubit-states with equal prior probabilities 1/2 was considered by Rudolph *et al* in Ref.[16], and they provided a way to construct the optimal POVMs with the minimum probability of inconclusive result $P_{\mathrm{UD}}^{?} = 1 - F(\rho_1, \rho_2)$, where $F(\rho_1, \rho_2) = \mathrm{Tr}\left[\left(\sqrt{\rho_1}\rho_2\sqrt{\rho_1}\right)^{1/2}\right]$ is the fidelity.[8] This case was also considered in Ref.[17], and the analytical expression of optimal POVMs with minimum probability of inconclusive result was given. The general case of Eq.(1) has been solved by Kleinmann *et al* in Ref.[18], and they also discussed the more general case that the two states may be N-dimensional chosen from a set of linearly independent pure states $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_N\rangle\}$ associated with the prior probabilities $\{q_1, q_2, \ldots, q_N\}$, i.e., the discrimination of the following two density matrices,

$$\begin{aligned}\boldsymbol{\rho}_1^N &= \frac{1}{\eta_1}\sum_i^N q_i^2|\psi_i,\psi_i\rangle\langle\psi_i,\psi_i|,\\ \boldsymbol{\rho}_2^N &= \frac{1}{\eta_2}\sum_{i\neq j}^N q_iq_j|\psi_i,\psi_j\rangle\langle\psi_i,\psi_j|,\end{aligned} \tag{3}$$

with prior probabilities $\eta_1^N = \sum\limits_i q_i^2$ and $\eta_2^N = \sum\limits_{i\neq j} q_iq_j$. Unfortunately, they did not provide the optimal POVMs and the minimum probability of inconclusive result. In this paper, we only consider the realization of the comparison of the two qubit states ρ_1 and ρ_2.

First of all, we consider the preparation of the two mixed states ρ_1 and ρ_2. Our scheme is shown in Fig.1. In this scheme we use the polarization of photons as qubit and denote the horizontally linear polarization $|H\rangle$ as qubit $|0\rangle$ and the vertical linear polarization $|V\rangle$ qubit $|1\rangle$. Using a Type-I BBO ($\beta{-}\mathrm{BaB_2O_4}$) crystal and two polarizers, a photon pair in the product state $|H\rangle|H\rangle$ can be generated through the process of parametric down-conversion, and then the two photons are injected into two unbalanced Mach–Zehnder interferometers consisting of two variable beam splitters (VBS) and two symmetric beam splitters (BS). Denote $L_{1(2)}\ (S_{1(2)})$ as the optical length of the long (short) paths 1 (2) (from the crystal to the output), and the following two conditions are required for the preparation of the two mixed states:

$$\varDelta_{1(2)} = |L_{1(2)} - S_{1(2)}| \gg c\tau, \tag{4}$$

$$L_1 = L_2;\ S_1 = S_2;\ \varDelta_{1(2)} > cT_{\mathrm{D}}, \tag{5}$$

where c is the velocity of light, τ is the coherent time of the photon, and T_{D} is the time resolution of the detectors. The condition (4) guarantees that there is no interference at the BS1 (BS2), i.e. the location modes will be traced out and then a mixed state will be obtained. The condition (5) guarantees that only pairs of photons transmitted through paths of the same length contribute to the following coincidence detection.

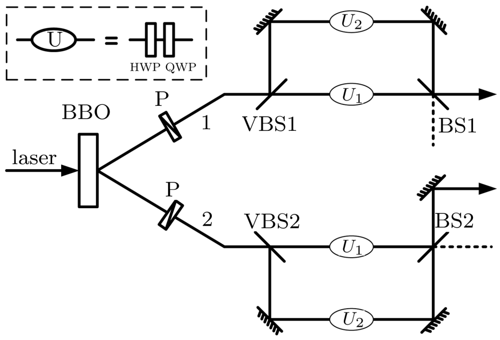

Fig.1. Schematic diagram of the preparation of two mixed qubit states with arbitrary prior probabilities. A photon pair is prepared through the process of parametric down-conversion at a Type-I BBO crystal, and then two mixed states are prepared by introducing time delay using two unbalanced Mach–Zehnder interferometers.

Denote the transmittivity of the two VBS as T_1 and T_2, respectively, and let U_1 (U_2) denote the single-photon unitary transformation $U_{1(2)}|H\rangle = |\psi_{1(2)}\rangle$. Suppose the experimental setups are arranged as Fig.1, then if the two photons are transmitted through the two short paths $S_{1(2)}$, one gets the state $|\psi_1,\psi_1\rangle$ with the probability $\frac{1}{4}T_1T_2$; while if the two photons are transmitted through the two long paths $L_{1(2)}$, one get the state $|\psi_2,\psi_2\rangle$ with the probability $\frac{1}{4}(1-T_1)(1-T_2)$. Through the following coincidence detection to which only the two photons transmitted through the paths of the same length contribute, we can obtain the following mixed state (unnormalized) in the output port:

$$\rho_1' = \frac{1}{4}[T_1T_2|\psi_1,\psi_1\rangle\langle\psi_1,\psi_1| \\ + (1-T_1)(1-T_2)|\psi_2,\psi_2\rangle\langle\psi_2,\psi_2|]. \quad (6)$$

Alternatively, if we exchange the VBS1 (VBS2) with the BS1 (BS2) and exchange U_1 with U_2 in path 2 simultaneously, we can obtain the following mixed state (unnormalized):

$$\rho_2' = \frac{1}{4}[T_1(1-T_2)|\psi_1,\psi_2\rangle\langle\psi_1,\psi_2| \\ + (1-T_1)T_2|\psi_2,\psi_1\rangle\langle\psi_2,\psi_1|]. \quad (7)$$

Select $T_1 = T_2 = q_1$, then $(1-T_1) = (1-T_2) = q_2$. After normalization, the above two mixed states are the desired mixed states ρ_1 and ρ_2 with the success probability $\frac{1}{4}\left(q_1^2+q_2^2\right)$ and $\frac{1}{2}q_1q_2$, respectively. In this scheme, the prior probabilities q_1 and q_2 can be adjusted by the transmittivity of the two VBS.

In addition, the method of introducing the time delay to generate mixed state has been usually used in linear optics, for example, in the Refs.[19–21]. In Ref.[20], Kwiat group presented two schemes to prepare arbitrary two-photon polarization mixed states. They used the method of Schmidt decomposition and then prepared the desired mixed states by mixing its eigenstates with probabilities proportional to their eigenvalues. It looks like that their schemes are more efficient, however, the mixed states prepared through their schemes are the same as the mixed states of Eq.(1) just only in density matrices, but the preparations can not show the original problem of quantum state comparison, i.e. two photons are each prepared either in the same state or in different states.

Next we consider the realization of the comparison, i.e., the realization of the optimal POVM for unambiguous discrimination. The optimal POVM was given in Ref.[17, 18], and a scheme of the realization of all possible bipartite POVMs of two-photon polarization states was proposed in Ref.[22]. However, for the reason that the generation of the ancilla three-photon entangled state and the realization of five-photon teleportation are too complicated to be realized in lab with current experimental technology, their scheme may not be applicable in a real experiment. In this letter, we first propose a feasible scheme of the realization of quantum state comparison of the special case of Eq.(2), and then show that this proposal is also available for the general case of Eq.(1). Through some calculation based on the Ref.[17], the optimal POVMs for the states given in Eq.(2) can be described as follows,

$$\begin{aligned} \Pi_1 &= |r^+\rangle\langle r^+| + |\psi^+\rangle\langle\psi^+|, \\ \Pi_2 &= |r^-\rangle\langle r^-| + |\psi^-\rangle\langle\psi^-|, \\ \Pi_? &= I - \Pi_1 - \Pi_2, \end{aligned} \quad (8)$$

where $|r^\pm\rangle = \frac{\sqrt{2}}{2}\left(\tan^2\theta|00\rangle \pm |11\rangle\right)$, and $|\psi^\pm\rangle = \frac{\sqrt{2}}{2}(|01\rangle \pm |10\rangle)$, with I as the identity matrix. It is clear that the optimal operators Π_1 and Π_2 can be regarded as projection onto the subspaces spanned by the basis states $\{|00\rangle,|11\rangle\}$ and $\{|01\rangle,|10\rangle\}$, respectively, associated with UD of two linearly independent pure states in each subspace. In the first subspace, the projector is $P_1 = |00\rangle\langle 00| + |11\rangle\langle 11|$ and the corresponding optimal POVMs of two pure states are,

$$\boldsymbol{A}_1^1 = \frac{1}{2}\begin{pmatrix} \tan^4\theta & \tan^2\theta \\ \tan^2\theta & 1 \end{pmatrix},$$

$$\boldsymbol{A}_2^1 = \frac{1}{2}\begin{pmatrix} \tan^4\theta & -\tan^2\theta \\ -\tan^2\theta & 1 \end{pmatrix},$$
$$\boldsymbol{A}_?^1 = \begin{pmatrix} 1-\tan^4\theta \\ 0 \end{pmatrix}. \tag{9}$$

While in the second subspace, the projector is $P_2 = |01\rangle\langle 01| + |10\rangle\langle 10|$, and then the remaining two pure states are orthogonal to each other which can be discriminated determinately by Von Neumann measurement with two elements $A_\pm^2 = \frac{\sqrt{2}}{2}(|01\rangle \pm |10\rangle)$.

In our previous work, the projector and the corresponding UD of two linearly independent pure states can be realized by current experimental technology.[23] The scheme is shown in Fig.2. Unfortunately, determinate Bell state analysis is impossible with linear optical elements, while two of them can be distinguished perfectly.[24,25] Also we can not realize the optimal POVMs $\{\Pi_1, \Pi_2, \Pi_?\}$ determinately, but with some probability. The detailed process of the realization is the following. Firstly, by interference at a polarizing beam splitters (PBS1) and the following coincidence detection, the mixed states can be projected onto the subspace spanned by the basis states $\{|00\rangle, |11\rangle\}$ with the success probability $1-\frac{1}{2}\sin^2(2\theta)$. Secondly, the following M–Z interferometer is the realization of UD of two linearly independent pure states, and we set a half wave plate (HWP) at $\cos(2\delta) = \tan^2\theta$. The click on detector D3 corresponds to the inconclusive result with the probability $\cos(2\theta)/\left(1-\frac{1}{2}\sin^2(2\theta)\right)$, and the coincidence between detectors D1 and D5 (or D2 and D4) corresponds to the POVM element A_1, which means that the mixed state is ρ_1, i.e. the two states are the same. Otherwise the coincidence between detectors D1 and D4 (or D2 and D5) corresponds to the comparison result that the two states are different. Alternatively, if a σ_x operation is made on one of the photons before PBS1, the first process is the realization of the projector P_2 with the success probability $\frac{1}{2}\sin^2(2\theta)$. Now the following von Neumann measurement $A_\pm^2$ can be realized by the M–Z interferometer too, or simplified to a Hadamard operation followed by a PBS with two detectors. The sum of the success probabilities of two projectors associated with UD of two pure states is equal to the optimal one, but it is evident that the two projectors can not be realized simultaneously, so we can only demonstrate the scheme of optimal unambiguous quantum state comparison in principle.

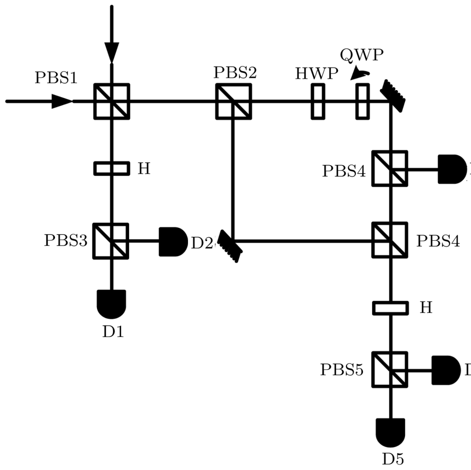

Fig.2. Schematic diagram of the realization of the optimal POVMs for the unambiguous quantum state comparison. A projection is realized by the interference in PBS1 and the following coincidence detection. The Mach–Zehnder interferometer is used for the realization of unambiguous discrimination of two linearly independent pure states.

Next, we show that if the two mixed states are in the forms of Eq.(1), our scheme is also available. Let $\mathcal{H}$ denotes the Hilbert space spanned by the two mixed states ρ_1 and ρ_2, i.e., $\mathcal{H} = S_{\rho_1} \bigoplus S_{\rho_2}$, where S_{ρ_1} (S_{ρ_2}) is the support of ρ_1 (ρ_2). Then, an orthonormal basis of $\mathcal{H}$ is given by

$$\begin{aligned} |e_{1,2}\rangle &= \frac{1}{\sqrt{2}n_\pm}\left(|\psi_1\psi_1\rangle \pm |\psi_2\psi_2\rangle\right), \\ |e_{3,4}\rangle &= \frac{1}{\sqrt{2}n_\pm}\left(|\bar{\psi}_1\bar{\psi}_2\rangle \pm |\bar{\psi}_2\bar{\psi}_1\rangle\right), \end{aligned} \tag{10}$$

with $n_\pm = \sqrt{1 \pm |\langle\psi_1|\psi_2\rangle|^2}$, where $|\bar{\psi}_1\rangle$, $|\bar{\psi}_2\rangle \in \mathrm{span}(|\psi_1\rangle, |\psi_2\rangle)$ and $|\bar{\psi}_1\rangle \perp |\psi_1\rangle$, $|\bar{\psi}_2\rangle \perp |\psi_2\rangle$. The optimal POVMs for the general case are given as follows:[18]

$$\Pi_1 = \Pi_1' + |e_2\rangle\langle e_2| \text{ and } \Pi_2 = \Pi_2' + |e_4\rangle\langle e_4|, \tag{11}$$

where Π_1' and Π_2' are constructed from $|e_1\rangle$ and $|e_3\rangle$. From Eq.(11), one will find that the two POVM elements can also be firstly regarded as projection onto two subspaces associated with the projectors $P_1 = |e_1\rangle\langle e_1| + |e_3\rangle\langle e_3|$ and $P_2 = |e_2\rangle\langle e_2| + |e_4\rangle\langle e_4|$, respectively, and then in the first subspace, the remaining problem is the UD of two linearly independent pure states for $\mathrm{Tr}(\Pi_1' \cdot \Pi_2') \neq 0$, while in the second subspace, that is the UD of two orthogonal pure states for $\langle e_2|e_4\rangle = 0$. Therefore, the unambiguous comparison of the general two qubit states can be realized in principle using our scheme also.

Quantum state comparison can be used in quantum fingerprinting. The basis of quantum fingerprinting is the comparison of two states chosen from a set S according to two long messages. The comparison result that the two states are identical or not infers the original two long messages being identical or not. Single-qubit optical quantum fingerprinting with $|S| = 4$ has been demonstrated by Horn *et al* in experiment in 2005.[15] In their experiment they compared the two states with minimum-error, for which the measurement is simplified to a projection onto symmetric or antisymmetric subspace, and this projection can be realized just by a BS. Because their comparison has minimum-error, the error is inevitable, i.e., the one-side error is larger than zero,[26] and then one has to repeat the comparison several times to guarantee the error rate to be less than a small value $\varepsilon > 0$. If one uses the above unambiguous comparison scheme in quantum fingerprinting, sometimes one can not get any information because of the existence of inconclusive result, but if one gets a result, the result is error-free, i.e. there is no one-side error, which is the main advantage with respect to the minimum-error one. Unfortunately, since only linearly independent pure states can be discriminated unambiguously[9] and the number of linearly independent pure states of qubit is only two, our scheme can only be applied to the trivial case $|S| = 2$. However, if the unambiguous quantum state comparison with the more general case of Eq.(3), i.e., the two states are N-dimensional, can be realized, then the unambiguous quantum state comparison may be applied to quantum fingerprinting with no one-side error more efficiently, which may be considered in the future.

In conclusion, we first propose a scheme to prepare two mixed qubit states with arbitrary prior probabilities and then propose a scheme to realize the optimal POVMs for unambiguous quantum state comparison in principle. Our scheme is available even for the general case that the two states have arbitrary prior probabilities. Recently, ultrabright resource of photon pairs generated through the process of parametric down-conversion of a BBO crystal has been widely used in linear optics quantum computation, for example, the Ref.[27], and if we carefully arrange the optical elements for the conditions (4) and (5), we think our preparation scheme is feasible by current experimental technology. In addition, the realization of the optimal POVMs was proved to be feasible in our previous work,[23] so we think our scheme of unambiguous quantum state comparison is feasible in a real experiment.

References

[1] Wootters W K and Zurek W H 1982 *Nature* (London) **299** 802

[2] Helstrom C W 1976 *Quantum Detection and Estimation Theory* (New York: Academic)

[3] Ivanovic I D 1987 *Phys. Lett.* A **123** 257
Dieks D 1988 *Phys. Lett.* A **126** 303
Peres A 1988 *Phys. Lett.* A **128** 19

[4] Jaeger G and Shimony A 1995 *Phys. Lett.* A **197** 83

[5] Croke S, Andersson E, Barnett S M, Gilson C R and Jeffers J 2006 *Phys. Rev. Lett.* **96** 070401

[6] Sciarrino F, Ricci M, Martini F De, Filip R and Mišta Jr. L 2006 *Phys. Rev. Lett.* **96** 020408

[7] Holevo A S 1998 *IEEE Trans. Inf. Theory* **IT-44** 269

[8] Nielsen M N and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)

[9] Chefles A 1998 *Phys. Lett.* A **239** 339

[10] Feng Y, Duan R Y and Ying M S 2004 *Phys. Rev.* A **70** 012308

[11] Barnett S M, Chefles A and Jex I 2003 *Phys. Lett.* A **307** 189

[12] Andersson E, Curty M and Jex I 2006 *Phys. Rev.* A **74** 022304

[13] Buhrman H, Cleve R, Watrous J and de Wolf R 2001 *Phys. Rev. Lett.* **87** 167902

[14] Gottesman D and Chuang I L 2001 arXiv:quant-ph/0105032

[15] Horn R T, Babichev S A, Marzlin K P, Lvovsky A I and Sanders B C 2005 *Phys. Rev. Lett.* **95** 150502

[16] Rudolph T, Spekkens R M and Turner P S 2003 *Phys. Rev.* A **68** 010301(R)

[17] Herzog U and Bergou J A 2005 *Phys. Rev.* A **71** 050301(R)

[18] Kleinmann M, Kampermann H and Bruß D 2005 *Phys. Rev.* A **72** 032308

[19] Zhang C W 2004 *Phys. Rev.* A **69** 014304

[20] Wei T C, Altepeter J B, Branning D, Goldbart P M, James D F V, Jeffrey E, Kwiat P G, Mukhopadhyay S and Peters N A 2005 *Phys. Rev.* A **71** 032329

[21] Lin Q, Li J and Guo G C 2007 *Chin. Phys. Lett.* **24**(7) 1809

[22] Ahnert S E and Payne M C 2006 *Phys. Rev.* A **73** 022333

[23] Lin Q, Li J and Guo G C 2006 *J. Phys.* B*: At. Mol. Opt. Phys.* **39** 3649

[24] Lükenhaus N, Calsamiglia J and Suominen K A 1999 *Phys. Rev.* A **59** 3295

[25] Calsamiglia J and Lükenhaus N 2001 *Appl. Phys.* B **72** 67

[26] de Beaudrap J Niel 2004 *Phys. Rev.* A **69** 022307

[27] Lu C Y, Zhou X Q, Gühne O, Gao W B, Zhang J, Yuan Z S, Goebel A, Yang T and Pan J W 2007 *Nature Physics* **3** 91