Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

# Intrinsically stable phase-modulated polarization encoding system for quantum key distribution

Xiaobao Liu, Changjun Liao*, Jinglong Mi, Jindong Wang, Songhao Liu

*Laboratory of Photonic Information Technology, School for Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou 510006, China*

ARTICLE INFO

*Article history:*
Received 11 May 2008
Received in revised form 30 October 2008
Accepted 31 October 2008
Available online 6 November 2008
Communicated by P.R. Holland

*PACS:*
03.67.Dd

*Keywords:*
Sagnac interferometer
Polarizing interference
Phase modulation
Polarization encoding
Quantum key distribution

ABSTRACT

We demonstrate experimentally an intrinsically stable polarization coding and decoding system composed of optical-fiber Sagnac interferometers with integrated phase modulators for quantum key distribution. An interference visibility of 98.35% can be kept longtime during the experiment without any efforts of active compensation for coding all four desired polarization states.

A practical quantum key distribution system requires high bit rate and low bit error rate [1]. Polarization states encoded by phase modulation can provide high bit-rate operation [2]. Though the quantum bit error rate (QBER) is unavoidable, it is an important parameter in quantum key distribution system which is used to check whether the system is secure against eavesdropping problems [3]. A bound of QBER $\leqq 11\%$ is precisely obtained by Shor and Preskill following Mayers's proof [4] to guarantee security in a practical QKD system so that error correction and privacy application can be applied to the quantum sifted bits. Even the stable transmission of the polarization state of the photon in fiber has been considered [5], the polarization state is a favorable choice for free-space key exchange where there is essentially no birefringence at all, and various merits of using polarization encoding have been considered [6,7]. Therefore, the QBER has to be decreased to less than 11%. We have demonstrated direct private communication that can combine authentication and error correction altogether using quantum sifted keys with bit error rate less than 11% based on one-way communication [8]. The error bits due to experimental imperfections are mainly from detector dark counts [9] and imperfect interference that is considered as intrinsic errors existing in the coding system [10]. In this Letter, we demonstrate experimentally for the QKD an intrinsically stable phase-modulated polarization coding and decoding system. The system codes and decodes all four desired polarization states without any effort of pre-alignment for good performance and active compensation for stability during the experiment.

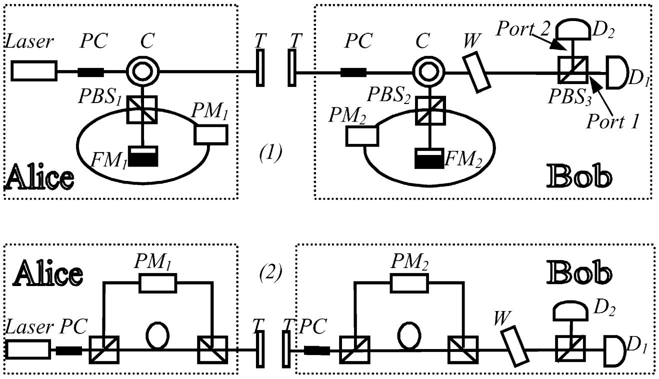

**Fig. 1.** (1) Phase-modulated polarization-code system with Sagnac interferometers. T stands for transmitting and receiving optics. PC stands for the polarization controller. C stands for the circular. (2) Phase-modulated polarization-code system with conventional polarizing interferometers.

The schematic of the system between Alice and Bob is sketched in Fig. 1(1). Both Alice and Bob are mainly based on the same structure of a Sagnac interferometer consisting of a polariza-

[*] Corresponding author. Tel.: +86 02085213862.
*E-mail address:* chliao@scnu.edu.cn (C. Liao).

0375-9601/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.physleta.2008.10.081

tion beam splitter PBS$_i$ $(i = 1, 2)$, an integrated electrically-driven waveguide-type phase modulator PM$_i$, and a Faraday mirror FM$_i$. The fiber loop with phase modulator is polarization-maintaining while standard single mode fiber is used to connect FM and PBS. All PBSs in our system are defined to transmits (reflect) the horizontally (vertically) linearly polarized component $P_x$ $(P_y)$ of a pulse to port 1 (2) in the states

$$P_x\colon\quad |H,1\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \qquad P_y\colon\quad |V,2\rangle = \begin{pmatrix}0\\1\end{pmatrix},$$

where the first position in the *kit* stands for its polarization state and the second one stands for from which port it comes out of the PBS.

Single photon pulses in 45° linearly polarization state are emitted by the semiconductor laser and delivered to the coding system at Alice side. Each of the pulses splits at PBS$_1$ into two orthogonal components, $P_x$ and $P_y$. The transmitted $P_x$ is directly reflected back by the FM$_1$ with its state rotated to $|V,1\rangle$ so that it will be reflected by PBS$_1$ to go anticlockwise through the loop before recombined with the other component at PBS$_1$; while the reflected $P_y$ goes clockwise through the loop, reflected again by PBS$_1$ and then reflected by FM$_1$ with rotation to the state $|H,1\rangle$ so that it can pass through PBS$_1$ where $P_x$ and $P_y$ reunite. The polarizing interference between $P_x$ and $P_y$ results in a new polarization state as the output of the Sagnac interferometer. As PM$_1$ is set in such a proper place of the loop that the time $P_x$ reaches the PM$_1$ is much later than that $P_y$ does, PM$_1$ works in time-division mode: It applies no phase shift on $P_y$ and the phase shift $\varphi_1$ is exclusively applied on $P_x$ during its passage through PM$_1$. That is to say, PM$_1$ introduces additional phase shift $\varphi_1$ between $P_x$ and $P_y$ before they reunite. The Sagnac interferometer at Bob's side works in the same way.

We now present further analysis of the polarization states during the whole encoding process. The input pulse at Alice's coding system in 45° linearly polarized state can be described by wave function

$$|in\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\end{pmatrix}.$$

The beam split operators are $T = \left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$ for the transmitted and $R = \left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$ for the reflected, so that

$$P_x\colon\quad T|in\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix} = |H,1\rangle;$$

$$P_y\colon\quad R|in\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\end{pmatrix} = |V,2\rangle.$$

$P_x$ is sent on a round trip through an optical fiber (a length $l_{BF}$ between PBS$_1$ and FM$_1$) terminated by a Faraday mirror. The transfer function of this process can be describe as

$$\begin{aligned} F &= \begin{pmatrix} e^{ik_H l_{BF}} & 0\\ 0 & e^{ik_V l_{BF}}\end{pmatrix}\begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}\begin{pmatrix} e^{ik_H l_{BF}} & 0\\ 0 & e^{ik_V l_{BF}}\end{pmatrix}\\ &= \begin{pmatrix} 0 & e^{ik_H l_{BF}+ik_V l_{BF}}\\ e^{ik_V l_{BF}+ik_H l_{BF}} & 0\end{pmatrix},\end{aligned}$$

where $k_H$ and $k_V$ are wave vectors for horizontal and vertical components. $P_x$ is then reflected by PBS$_1$, and guided through the loop (a length of $l$) anticlockwise back to PBS$_1$ with phase shift $\varphi_1$ added by PM$_1$ to the vertical component. The transmission operator is

$$L = \begin{pmatrix} e^{ik_H l} & 0\\ 0 & e^{ik_V l+i\varphi_1}\end{pmatrix}.$$

**Table 1**
Output polarization states at Alice side and the photon-count situations at Bob side.

| | | | Bob ($\varphi_2$) | | | |
|---|---|---|---|---|---|---|
| | | | 0 | $\pi$ | $3\pi/2$ | $\pi/2$ |
| | | | diagonal polarized analyzers | | circular polarized analyzers | |
| Alice ($\varphi_1$) | 0 | ⤢ | D$_1$ | D$_2$ | 50% | 50% |
| | $\pi$ | ⤡ | D$_2$ | D$_1$ | 50% | 50% |
| | $3\pi/2$ | ↺ | 50% | 50% | D$_1$ | D$_2$ |
| | $\pi/2$ | ↻ | 50% | 50% | D$_2$ | D$_1$ |

As a result, the overall combined effect on the $P_x$ before it leaves the interferometer can be described by the matrix $RLRFT$, and $P_x$ becomes

$$\begin{aligned} RLRFT|in\rangle &= \begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix} e^{ik_H l} & 0\\ 0 & e^{ik_V l+i\varphi_1}\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix}\\ &\quad\times\begin{pmatrix} 0 & e^{ik_H l_{BF}+ik_V l_{BF}}\\ e^{ik_V l_{BF}+ik_H l_{BF}} & 0\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix}\\ &= \frac{1}{\sqrt{2}}\begin{pmatrix}0\\ e^{ik_V l+i\varphi_1+ik_V l_{BF}+ik_H l_{BF}}\end{pmatrix}.\end{aligned}$$

The reflected $P_y$ will not be phase-modulated. Its whole transmission matrix in the interferometer is $TFRLR$, and $P_y$ becomes

$$\begin{aligned} TFRLR|in\rangle &= \begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix} 0 & e^{ik_H l_{BF}+ik_V l_{BF}}\\ e^{ik_V l_{BF}+ik_H l_{BF}} & 0\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix}\\ &\quad\times\begin{pmatrix} e^{ik_H l} & 0\\ 0 & e^{ik_V l}\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\end{pmatrix}\\ &= \frac{1}{\sqrt{2}}\begin{pmatrix}e^{ik_V l+ik_H l_{BF}+ik_V l_{BF}}\\ 0\end{pmatrix}.\end{aligned}$$

Now that the two components recombine and interfere, the wave function at the output becomes

$$\begin{aligned} |out\rangle_A &= \frac{1}{\sqrt{2}}\begin{pmatrix}0\\ e^{ik_V l+i\varphi_1+ik_V l_{BF}+ik_H l_{BF}}\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}e^{ik_V l+ik_H l_{BF}+ik_V l_{BF}}\\ 0\end{pmatrix}\\ &= \frac{1}{\sqrt{2}}e^{ik_H l_{BF}+ik_V(l_{BF}+l)}\begin{pmatrix}1\\ e^{i\varphi_1}\end{pmatrix} = \frac{1}{\sqrt{2}}e^{i\Phi}\begin{pmatrix}1\\ e^{i\varphi_1}\end{pmatrix}\end{aligned}$$

where $\Phi = ik_H l_{BF} + ik_V(l_{BF}+l)$.

This suggests the polarization state of the pulse out of the interferometer is only determined by the phase shift $\varphi_1$ applied by the PM$_1$, either as 45° linearly polarized, 135° linearly polarized, left-circular polarized or right-circular polarized (see Table 1). The coded pulse is then transmitted to the Bob. Its orthogonal components $P'_x$ for transmission and $P'_y$ for reflection go through similar changes in Bob's interferometer and become:

$$\begin{aligned} P'_x\colon\quad & R'L'R'F'T'|out\rangle_A\\ &= \begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix} e^{ik_H l'} & 0\\ 0 & e^{ik_V l'+i\varphi_2}\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix}\\ &\quad\times\begin{pmatrix} 0 & e^{ik_H l'_{BF}+ik_V l'_{BF}}\\ e^{ik_V l'_{BF}+ik_H l'_{BF}} & 0\end{pmatrix}\frac{1}{\sqrt{2}}e^{i\Phi}\begin{pmatrix}1\\0\end{pmatrix}\\ &= \frac{e^{i\Phi}}{\sqrt{2}}\begin{pmatrix}0\\ e^{ik_V l'+i\varphi_2+ik_V l'_{BF}+ik_H l'_{BF}}\end{pmatrix},\end{aligned}$$

$$\begin{aligned} P'_y\colon\quad & T'F'R'L'R'|out\rangle_A\\ &= \begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix} 0 & e^{ik_H l'_{BF}+ik_V l'_{BF}}\\ e^{ik_V l'_{BF}+ik_H l'_{BF}} & 0\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix}\end{aligned}$$

$$\times \begin{pmatrix} e^{ik_H l'} & 0 \\ 0 & e^{ik_V l'} \end{pmatrix} \frac{1}{\sqrt{2}} e^{i\Phi} \begin{pmatrix} 0 \\ e^{i\varphi_1} \end{pmatrix}$$
$$= \frac{e^{i\Phi}}{\sqrt{2}} \begin{pmatrix} e^{ik_V l' + ik_H l'_{BF} + ik_V l'_{BF} + i\varphi_1} \\ 0 \end{pmatrix}.$$

Thus, the polarization state of the pulse leaving $PBS_2$ through port 0 is

$$|out\rangle_b = |H,1\rangle' + |V,2\rangle'$$
$$= \frac{e^{i\Phi}}{\sqrt{2}} \begin{pmatrix} 0 \\ e^{ik_V l' + i\varphi_2 + ik_V l'_{BF} + ik_H l'_{BF}} \end{pmatrix}$$
$$+ \frac{e^{i\Phi}}{\sqrt{2}} \begin{pmatrix} e^{ik_V l' + ik_H l'_{BF} + ik_V l'_{BF} + i\varphi_1} \\ 0 \end{pmatrix}$$
$$= \frac{1}{\sqrt{2}} e^{i\Phi} e^{i\Phi'} \begin{pmatrix} e^{i\varphi_1} \\ e^{i\varphi_2} \end{pmatrix},$$

where $\Phi' = ik_V(l' + l'_{BF}) + ik_H l'_{BF}$.

The pulse then goes through a $\lambda/2$ wave plate with its fast axis at an angle of $+22.5°$ to the horizontal axis,

$$W = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

and the pulse becomes

$$|out\rangle'_b = W|out\rangle_b = \frac{1}{2} e^{i\Phi} e^{i\Phi'} \begin{pmatrix} e^{i\varphi_1} + e^{i\varphi_2} \\ e^{i\varphi_1} - e^{i\varphi_2} \end{pmatrix}.$$

Its polarization state is only determined by phase shift $\varphi_1$ and $\varphi_2$ that have been randomly selected by Alice and Bob in their own PMs. As a result, the photon-count situations at Bob's detectors vary according to different selections of phase shift $\varphi_1$ and $\varphi_2$ as follows: take selection $\varphi_1 = 0$ for example which means Alice sends a 45° linearly polarized pulse to Bob. When Bob selects $\varphi_2 = 0$,

$$|out\rangle'_b = e^{i\Phi} e^{i\Phi'} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = e^{i\Phi} e^{i\Phi'} |H,1\rangle,$$

which means the pulse will come out of $PBS_3$ from port 1 ($D_1$) with 100% possibility; When Bob selects $\varphi_2 = \pi$,

$$|out\rangle'_b = e^{i\Phi} e^{i\Phi'} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = e^{i\Phi} e^{i\Phi'} |V,2\rangle,$$

which means pulse will come out of $PBS_3$ from port 2 ($D_2$) with 100% possibility. However, when Bob selects $\varphi_2 = 3\pi/2$ and $\pi/2$, $|out\rangle'_b = \frac{1}{2}[(1-i)|H,1\rangle + (1+i)|V,2\rangle]$ and $|out\rangle'_b = \frac{1}{2}[(1+i)|H,1\rangle + (1-i)|V,2\rangle]$, respectively. This means the pulse will come out of $PBS_3$ from either port with 50% possibility. That is to say, in the situation of $\varphi_2 = 0$ and $\varphi_2 = \pi$, Bob functions as diagonal polarized analyzers, distinguishing pulses in 45° and 135° linearly polarized states. For the same reason, in situation of $\varphi_2 = 3\pi/2$ and $\varphi_2 = \pi/2$, Bob functions as circular polarized analyzers, distinguishing pulses in left and right circular polarized states (see Table 1).

As these four states belong to two nonorthogonal bases, the diagonal basis (45° and 135° linearly polarized) and the circular one (left-circularly and right-circularly polarized), this phase-modulated polarization-code system can be used to implement polarization-code BB84 QKD protocol. The expressions of $|out\rangle_a$ and $|out\rangle'_b$ also suggest that the polarization states prepared at Alice's coding system and the photon-count situations at Bob's side are only determined by phase shift $\varphi_1$ and $\varphi_2$ in their PMs that are randomly selected by Alice and Bob.

In the demonstration experiment, laser pulses of 50 ps at wavelength of 1550 nm from laser PDL808 are encoded in Alice's security zone and attenuated to a level of 0.1 photon/pulse as single photon sources. The encoded pulses are directed into a single mode fiber for delivery to transmitting optics, and emitted towards Bob's receiver. The coupling efficiency between transmitter and receiver for 20 centimeter transmission distance is −2.3 dB. At Bob's side, the qubits are collected by receiving optics and recovered by polarization controller to their initial polarization states and directed into Bob's interferometer. The id200 single-photon detectors (id Quantique, Switzerland) are used to detect single photon signal, with a dark count rate of $10^{-6}$ per gate. The gate pulses of 2.5 ns are synchronized with the arriving of the laser pulses. Insertion loss of the interferometers is −11.0 dB. The half-wave voltage of the PMs is 5.3 V. Interference visibility of higher than 30 dB for Sagnac interferometers of both Alice and Bob are obtained.

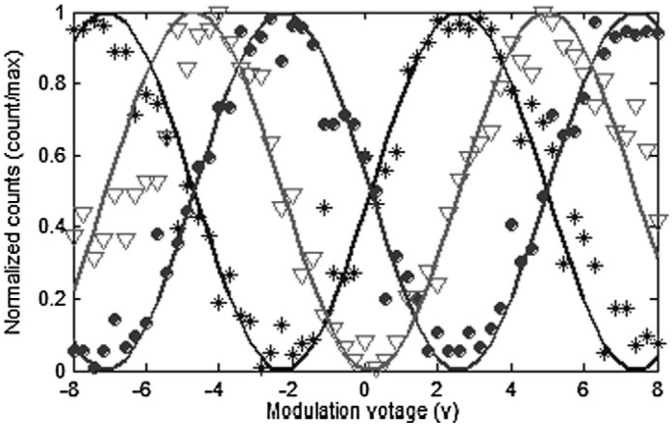

**Fig. 2.** Interference curves of the system. Phase shift of $PM_2$ is scanned while phase shift of $PM_1$ is fixed at 0, $\pi$ and $3\pi/2$ (corresponding to the circled, asterisked and triangled dots). The solid lines stand for the theoretical situations.

In a typical situation we scan the phase shift of $PM_2$ from 0 to $2\pi$ while we fix the phase shift of $PM_1$ at 0, $\pi$ and $3\pi/2$, respectively. Data curves are showed in Fig. 2. The mean visibility of interference fringes showed at output 1 and output 2 are kept stable at 98.35% for an hour's performance. This implies a 0.82% QBER for QKD sifted bits, which is fairly tolerable within the bound of 11%. The system noise comes from the detection noise of the single photon detectors that are caused mainly by dark counts and the after pulses [9]. This would be improved by the detection technology. Also, with the implementation of high speed single photon detection [11], this scheme can be used to achieve a high bit rate QKD, as the coding speed of our system is only limited by the PMs' modulation speed, which can be up to GHz.

We also compare the stability of two phase-modulated polarization-encoding schemes, one is our system which uses Sagnac interferometers (Fig. 1(1)); The other uses conventional polarizing interferometers (Fig. 1(2)). Both schemes prepare and distinguish polarization states on the principle of polarizing interference, however, their stabilities differ. In the same condition, the data from both systems are recorded for one hour, during which all the PMs in both system apply no phase shifts. The room temperature is about 25 °C ± 1 °C. Results (Fig. 3) show that the polarization-code system with Sagnac interferometers is intrinsically stable while the one with conventional polarizing interferometers fluctuates as a function of time. As a result, no phase adjustment need be used to compensate for the phase drift in the interferometers to keep our system stable.

Also, no effort is needed to pre-alignment for good interference visibility in our system, which intrinsically promises a low contribution to QBER. However, the system with conventional interferometers need great effort of careful alignment of the optical path to achieve a mean visibility of 91.82% (showed in Fig. 3), because discrepancy which comes from the insertion loss of the waveguide-type phase modulators in one arm and the asymme-

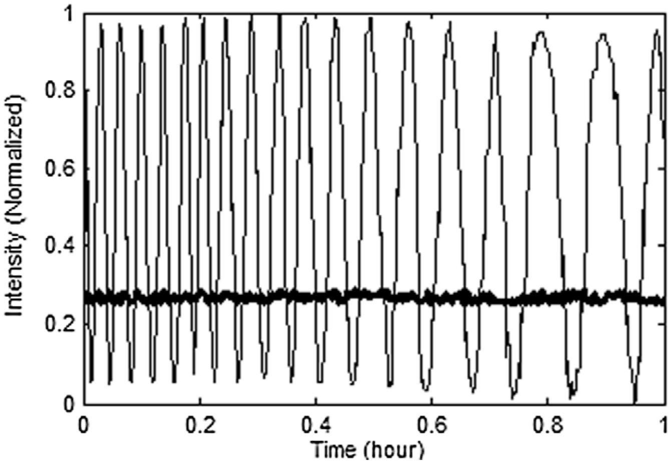

**Fig. 3.** Stability of both schemes in Fig. 1. The sinusoid curve shows the dates from system with conventional polarizing interferometers in Fig. 1(1) and the other curve shows the dates from system with Sagnac interferometers in Fig. 1(2).

try of two optical paths would decrease the interfering visibility [9]. However, the Sagnac interferometer automatically solves this problem since both interfering components cover the same path in the interferometer.

In conclusion, we have demonstrated an intrinsically stable phase-modulated polarization-code system for QKD between Alice and Bob. Experiments show that without any effort of active phase compensation for stability, Alice can correctly prepare four desired polarization states with the polarization Sagnac interferometer while Bob will correctly distinguish these states with similar device according to their protocol. The mean visibility of the system is counted at 98.35%. This system has advantages as follows: 1, the system is intrinsically stable, which promise a low contribution to the error bits. 2, Alice and Bob have similar structure of Sagnac interferometers, which provides convenience and economization in practical application. 3, adoption of phased-modulation mode to implement polarization encoding suggests potential of high bit rate QKD. As a result, the phase-modulated polarization-code system with Sagnac interferometers is worth of wide application in polarization-code QKD.

## References

[1] C. Liao, L. Zhen, S. Liu, Practical quantum key distribution system for high-speed optical fiber communications, in: Challenging Optics in Science & Technology, 21–26 August 2005, Proc. SPIE 6025 (2006) 602517.

[2] X. Liu, Z. Tang, C. Liao, Y. Lu, F. Zhao, S. Liu, Phys. Lett. A 358 (2006) 386;
Z.L. Tang, M. Li, Z.J. Wei, F. Lu, C.J. Liao, S.H. Liu, Acta Phys. Sin. 54 (2) (2005) 517.

[3] U.M. Maurer, S. Wolf, IEEE Trans. Inf. Theory 45 (1999) 499;
H.-K. Lo, H.F. Chau, Science 283 (1999) 2050.

[4] P.W. Shor, J. Preskill, Phys. Rev. Lett. 85 (2000) 441.

[5] G. Wu, J. Chen, Y. Li, H.P. Zeng, quant-ph/0606108.

[6] D. Bruß, Phys. Rev. Lett. 81 (1998) 3018.

[7] C.Z. Peng, J. Zhang, D. Yang, W.B. Gao, H.X. Ma, H. Yin, H.P. Zeng, T. Yang, X.-B. Wang, J.W. Pan, Phys. Rev. Lett. 98 (2007) 010505.

[8] C. Liao, S. Liu, L. Zheng, Acta Sin. Quantum Opt. 14 (2) (2008) 165.

[9] P. Zhou, Z. Wei, C. Liao, C. Li, S. Yuan, J. Phys. D: Appl. Phys. 41 (2008) 155101;
Z. Wei, P. Zhou, J. Wang, C. Liao, J. Guo, R. Liang, S. Liu, J. Phys. D: Appl. Phys. 40 (2007) 6922.

[10] X.F. Mo, B. Zhu, Zh.F. Han, Y.Zh. Gui, G.C. Guo, Opt. Lett. 30 (19) (2005) 2632.

[11] Z.L. Yuan, B.E. Kardynal, A.W. Sharpe, A.J. Shield, Appl. Phys. Lett. 91 (2007) 041114.