Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum*

Wang Le(王 乐)[a], Zhao Sheng-Mei(赵生妹)[a)b)†], Gong Long-Yan(巩龙延)[c], and Cheng Wei-Wen(程维文)[a]

[a] *Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*

[b] *Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*

[c] *Information Physics Research Center and Department of Applied Physics, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*

(Received 28 May 2015; revised manuscript received 30 July 2015; published online 20 October 2015)

In this paper, we propose a measurement-device-independent quantum-key-distribution (MDI-QKD) protocol using orbital angular momentum (OAM) in free space links, named the OAM-MDI-QKD protocol. In the proposed protocol, the OAM states of photons, instead of polarization states, are used as the information carriers to avoid the reference frame alignment, the decoy-state is adopted to overcome the security loophole caused by the weak coherent pulse source, and the high efficient OAM-sorter is adopted as the measurement tool for Charlie to obtain the output OAM state. Here, Charlie may be an untrusted third party. The results show that the authorized users, Alice and Bob, could distill a secret key with Charlie's successful measurements, and the key generation performance is slightly better than that of the polarization-based MDI-QKD protocol in the two-dimensional OAM cases. Simultaneously, Alice and Bob can reduce the number of flipping the bits in the secure key distillation. It is indicated that a higher key generation rate performance could be obtained by a high dimensional OAM-MDI-QKD protocol because of the unlimited degree of freedom on OAM states. Moreover, the results show that the key generation rate and the transmission distance will decrease as the growth of the strength of atmospheric turbulence (AT) and the link attenuation. In addition, the decoy states used in the proposed protocol can get a considerable good performance without the need for an ideal source.

Keywords: measurement-device-independent quantum key distribution, orbital angular momentum, atmospheric turbulence, decoy states

PACS: 03.67.Hk, 03.67.Dd, 42.50.Ex **DOI:** 10.1088/1674-1056/24/12/120307

1. Introduction

Quantum key distribution (QKD)[1] enables two remote users to securely exchange cryptographic keys in the presence of an eavesdropper, and it has received a great deal of attention[2–7] since Bennett and Brassard proposed the first QKD protocol (BB84) in 1984.[1] Theoretically, it is unconditionally secure.[8,9] However, in a practical QKD system, an eavesdropper (Eve) might successfully eavesdrop some information of the key by utilizing the defects of measurement devices.[10–13] Recently, a measurement device independent quantum key distribution (MDI-QKD) protocol has been proposed to make the BB84 protocol free from any possible side-channels in detectors.[6] In the MDI-QKD protocol, neither Alice nor Bob performs any measurements, but an untrusted third party, called Charlie, detects photons. Alice and Bob distill a secret key according to Charlie's measurement results. It is shown that MDI-QKD protocol is free from side-channels because Alice and Bob do not employ photon detectors in the protocol. The MDI-QKD protocol has been extensively studied both experimentally[14–18] and theoretically[19–27] since it was proposed.

Most of the MDI-QKD protocols rely on either the polarization[6] or phase[18,19] of faint laser pulses as information carriers, and the use of polarization encoding limits the degree of a photon to encode information. Unlike the limited degree of freedom on polarization or phase states, orbital angular momentum (OAM) states have attracted a great deal of attention since there are infinite OAM eigenstates in a single-photon. Furthermore, OAM states are invariant under rotations about the propagation direction, which makes the sender and receiver to avoid the reference frame alignment.[28,29] These outstanding properties make OAM states that have been used in the BB84-type QKD protocol in free-space links.[30–32] However, the MDI-QKD with OAM states as information-carriers has been so far much less analyzed and reported.

In this paper, we propose an MDI-QKD protocol using OAM in the free-space link, named the OAM-MDI-QKD protocol. In the protocol, OAM states of photons are used

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61271238 and 61475075), the Specialized Research Fund for the Doctoral Program of Higher Education of China (Grant No. 20123223110003), the Natural Science Research Foundation for Universities of Jiangsu Province of China (Grant No. 11KJA510002), the Open Research Fund of Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, China (Grant No. NYKL2015011), and the Innovation Program of Graduate Education of Jiangsu Province, China (Grant No. KYLX0810). Gong Long-Yan is partially supported by Qinglan Project of Jiangsu Province, China.

†Corresponding author. E-mail: zhaosm@njupt.edu.cn

© 2015 Chinese Physical Society and IOP Publishing Ltd

as the information carriers. The decoy-state method[7] is adopted to overcome the security loophole caused by the weak coherent pulse source, together with a high efficient OAM sorter[33,34] that is employed to differentiate the different OAM states. Since OAM describes the spatial distributions of wavefunctions with helical phases,[35] the OAM-MDI-QKD protocol is inevitably sensitive to atmospheric turbulence (AT) interference.[36–39] The performance of the proposed protocol under atmospheric turbulence and link attenuation is further discussed.

The organization of the paper is arranged as follows. In Section 2, the decoy-state MDI-QKD protocol using orbital angular momentum states is presented. In Section 3, the key generation rate of the proposed protocol is analyzed, in conjunction with the influence on the performance by both AT and link attenuation in the free-space communications. Here, the general formulas for the contribution of single-photon pulses (gain Y_{11}^{OAM} and error rate e_{11}^{SUP}) and the contribution of signal states (total gain $Q_{\mu\nu}^{\mathrm{OAM}}$ and total QBER $E_{\mu\nu}^{\mathrm{OAM}}$) are derived. In Section 4, the security analysis is given. In Section 5, the performance of the OAM-MDI-QKD protocol is discussed by numerical simulations. Finally, Section 5 concludes the paper.

2. Decoy-state measurement-device-independent QKD protocol using orbital angular momentum states

Figure 1 shows the schematic diagram of the proposed OAM-MDI-QKD protocol. Both Alice and Bob produce a laser beam and modulate the photons to be the desired OAM states by illuminating the beam to a spatial light modulator (SLM) with a special hologram. Alice and Bob then obtain phase-randomized weak coherent states, including the decoy states and the signal state by using attenuators. Here, the intensity of the signal state for Alice and Bob is expressed as μ and ν, respectively. Assume both Alice and Bob could use infinite decoy states in the protocol. At a later moment, Alice and Bob send their pulses carrying OAM states to Charlie through a free-space communications link, which is disturbed by AT and link attenuation. In the protocol, Charlie is the only one who operates measurements. The measurement device comprises a beam-splitter (BS), two OAM-sorters and four single photon detectors. After Charlie's measurements, Alice and Bob could distill a secret key based on Charlie's successful measurement results.

An OAM state is associated with the azimuthal phase of a beam. It could be given as,[39]

$$|l\rangle = AW(r/R)\exp(\mathrm{i}l\theta), \tag{1}$$

where A denotes an amplitude of the beam, r and θ are the radial and azimuthal coordinates respectively, l is an OAM topological charge and it is an integer, and $W(r/R)$ is an aperture function with radius R. $W(r/R)$ can be expressed as,

$$W(r/R) = \begin{cases} 1, & \text{if } |r| \le R, \\ 0, & \text{else.} \end{cases} \tag{2}$$

It is shown that the OAM states do not need to align the shared reference frames as long as the z axis is synchronized in the QKD system since the spatial profile of the OAM states is rotational invariance.[28,29]

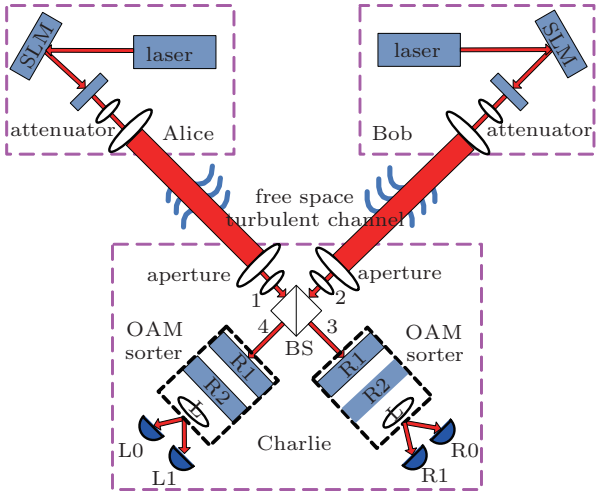


Fig. 1. (color online) A schematic diagram of the decoy-state MDI-QKD protocol using OAM states. SLM: spatial light modulator, to convert a Gaussian beam from a laser to a designed OAM state beam by a specific hologram. Attenuator: to produce weak coherent states, including decoy states or signal states. Aperture: the diameter of the receiver aperture is D. BS: beam splitter with 50:50. L0, L1, R0, and R1: detectors for single photon. OAM sorter: to sort OAM states, which employ two static optical elements (R1 and R2) and a lens (L) to efficiently differentiate the different OAM states.

For simplification and generality, a two-dimensional OAM-MDI-QKD protocol is discussed. One of the two two-dimensional OAM mutually unbiased bases for the proposed protocol could be defined as

$$\begin{aligned} |\Psi_{\mathrm{OAM}}^{n=0}\rangle &= |-l\rangle, \\ |\Psi_{\mathrm{OAM}}^{n=1}\rangle &= |l\rangle, \end{aligned} \tag{3}$$

where n represents the encoding bit, which can be taken an integer index from the set $\{0,1\}$. It is named OAM basis. The two states in OAM basis are orthogonal and rotational-invariant. The property of the rotational invariance enables quantum communication without alignment of shared reference frames and decreases the errors due to misalignment of shared reference frames.

Meanwhile, the other basis, called the superposition basis (SUP basis) is defined as

$$|\Psi_{\mathrm{SUP}}^{n}\rangle = \frac{1}{\sqrt{2}}(|l\rangle + \mathrm{e}^{\mathrm{i}n\pi}|-l\rangle), \tag{4}$$

where n is the encoding bit (0 or 1). The states in the SUP basis are a superposition of the $|l\rangle$ state and the $|-l\rangle$ state, and the two states in the SUP basis are orthogonal too. However, the two states in the SUP basis do not have the property

of the rotational invariance, thus alignment of shared reference frames is necessary.

Charlie is the only one who could operate measurements. His measurement device is composed of a beam-splitter (BS), two OAM-sorters, and four single photon detectors. When both the photons carrying OAM states arrive at the 50:50 BS, a Hong–Ou–Mandel (HOM) effect takes place.[40] Assume that the photon with the OAM state $|\Psi_m^n\rangle_1$ is sent from Alice and the photon with the OAM state $|\Psi_{m'}^{n'}\rangle_2$ is sent from Bob, where the subscript i of the ket represents the ith arm of BS. The action of the BS on the OAM state $|\Psi_m^n\rangle_1$ should be given by $\hat{a}_1^\dagger|\Psi_m^n\rangle = \frac{1}{\sqrt{2}}(|\Psi_m^n\rangle_3 + |\overline{\Psi_m^n}\rangle_4)$ and the action of the BS on the OAM state $|\Psi_{m'}^{n'}\rangle_2$ should be given by $\hat{a}_2^\dagger|\Psi_{m'}^{n'}\rangle = \frac{1}{\sqrt{2}}(|\overline{\Psi_{m'}^{n'}}\rangle_3 - |\Psi_{m'}^{n'}\rangle_4)$, where $\hat{a}_i^\dagger$ is the photon creation operator for the i-th input arm of the BS. Note that the reflection from BS will flip the sign of the OAM state. Hence, $|\overline{\Psi_m^n}\rangle$ is adopted to represent the state of $|\Psi_m^n\rangle$ reflecting from the BS. Hence, the output of the BS is

$$\begin{aligned}|\Psi_m^n\rangle_1|\Psi_{m'}^{n'}\rangle_2 \rightarrow\ & \frac{1}{\sqrt{2}}(|\Psi_m^n\rangle_3 + |\overline{\Psi_m^n}\rangle_4) \otimes \frac{1}{\sqrt{2}}(|\overline{\Psi_{m'}^{n'}}\rangle_3 - |\Psi_{m'}^{n'}\rangle_4) \\ =\ & \frac{1}{\sqrt{2}}(|\Sigma^+\rangle + |\Sigma^-\rangle), \end{aligned} \tag{5}$$

where

$$|\Sigma^+\rangle = \frac{1}{\sqrt{2}}(|\Psi_m^n\rangle_3|\overline{\Psi_{m'}^{n'}}\rangle_3 - |\overline{\Psi_m^n}\rangle_4|\Psi_{m'}^{n'}\rangle_4) \tag{6}$$

and

$$|\Sigma^-\rangle = \frac{1}{\sqrt{2}}(|\overline{\Psi_{m'}^{n'}}\rangle_3|\overline{\Psi_m^n}\rangle_4 - |\Psi_m^n\rangle_3|\Psi_{m'}^{n'}\rangle_4). \tag{7}$$

It is indicated that $|\Sigma^-\rangle$ will disappear if both Alice and Bob send the same photon states and choose the SUP basis (namely $|\Psi_{\rm SUP}^{n'}\rangle = |\Psi_{\rm SUP}^{n}\rangle$), or both of them send the opposite photon states and choose the OAM basis (namely $|\overline{\Psi_{\rm OAM}^{n'}}\rangle = |\Psi_{\rm OAM}^{n}\rangle$). Therefore, both photons appear in the same output arm of BS (3rd arm or 4th arm). Otherwise, $|\Sigma^+\rangle$ and $|\Sigma^-\rangle$ both exist.

Moreover, high efficient OAM-sorters[33,34] are adopted to differentiate the different OAM states. For OAM basis states, they are converted to the different truncated plane waves with wavefront tilts which are proportional to the OAM charge l. For SUP basis states, they are transformed to two different truncated plane waves. In fact, the OAM-sorter has two static special optical transformations (unwrapper (R1) and phase corrector (R2) in Fig. 1) to map the azimuthal phase profile of an OAM mode to a tilted planar wavefront, and the plane waves are then separated and focused to specified lateral positions by a lens. The sorting is exclusively based on unitary transformations and in theory can achieve a power transmission efficiency of unity.

Four single photon detectors (L0, L1 or R0, R1) are placed in the focal planes of the lenses to detect two OAM states simultaneously (L0 or R0 for the OAM state $|l\rangle$, while R1 or L1 for the OAM state $|-l\rangle$). Assume that if and only if two of Charlie's four detectors are triggered at the same time (triggers both at L0 and L1, at R0 and R1, at L0 and R0, and at L1 and R1), Charlie gets a successful measurement result. After Charlie announces his measurement results, Alice and Bob tell each other what basis she or he chooses, and only keep the results with the same basis. Table 1 shows a probability distribution of the successful measurements for Charlie when both Alice and Bob choose the same basis. The results show that when Alice and Bob choose the SUP basis and Charlie announces that both L0 and R0, or both R1 and L1 are triggered at the same time, Alice and Bob have opposite bits; otherwise, Alice and Bob have the same bit. On the other hand, when Alice and Bob choose the OAM basis and Charlie announces a successful measurement, Alice and Bob have the same bit. Therefore, if Alice and Bob use the results with the OAM basis as the key bits and simultaneously use the results with the SUP basis as the testing bits, Alice and Bob can share a secret key after error correction and privacy amplification procedures.

Table 1. A probability distribution for Charlie's successful measurements when both Alice and Bob choose the same basis.

Basis	Alice	Bob	L0 L1	R0 R1	L0 R0	L1 R1
	$n=0$	$n=0$	0.25	0.25	0	0
$m=$ SUP	$n=1$	$n=0$	0	0	0.25	0.25
	$n=0$	$n=1$	0	0	0.25	0.25
	$n=1$	$n=1$	0.25	0.25	0	0
	$n=0$	$n=0$	0.25	0.25	0.25	0.25
$m=$ OAM	$n=1$	$n=0$	0	0	0	0
	$n=0$	$n=1$	0	0	0	0
	$n=1$	$n=1$	0.25	0.25	0.25	0.25

Correspondingly, the proposed protocol has some advantages. Firstly, the proposed protocol uses OAM states to carry information. It paves a way to exploit a high-dimensional MDI-QKD protocol for transmitting more than one bit per photon, so as to greatly enhance the key generation rate performance. Secondly, the property of the rotational invariance of the states in OAM basis has enabled quantum communication without alignment of shared reference frames and decreases the errors due to misalignment of shared reference frames, which slightly improves the performance and further simplifies the practical system. In addition, Alice and Bob can reduce the number of flipping bits in the secure key distillation.

The details of the proposed OAM-MDI-QKD protocol are listed below.

Step 1 Alice and Bob randomly choose a basis (OAM basis or SUP basis) and a bit ($n = \{0,1\}$). Then they display the corresponding hologram on their SLMs to convert a Gaussian beam to the desired OAM state beam. Subsequently, Alice and Bob randomly produce the signal states and the decoy states by attenuating the beam into various intensities. Then, Alice and Bob send the pulses carrying OAM states to Charlie through a free-space turbulent channel.

Step 2 Charlie receives the pulses and carries out OAM states measurements. If and only if two of the four detectors (L0, L1, R0, and R1) are triggered at the same time, i.e., the same click at L0 and L1, R0 and R1, L0 and R0, and L1 and R1, Charlie gets a successful measurement. Then Charlie announces his measurement results to Alice and Bob.

Step 3 Alice and Bob tell each other what basis she or he chooses, and only keep those results with the same basis corresponding to Charlie's successful measurements.

Step 4 Alice and Bob use the results with OAM basis as the key bits and the results with the SUP basis as the testing bits, and then they testify the security of the key distribution.

Step 5 If Alice and Bob make sure the key distribution is secure, they can obtain a raw key. After error correction and privacy amplification, they can distill a secure key.

3. Analysis on the key generation rate performance

The key generation rate for the proposed scheme can be written as follows according to the concepts in Ref. [6]

$$R = \mu\nu \mathrm{e}^{-(\mu+\nu)} Y_{11}^{\mathrm{OAM}} (1 - H(e_{11}^{\mathrm{SUP}})) - Q_{\mu\nu}^{\mathrm{OAM}} f H(E_{\mu\nu}^{\mathrm{OAM}}), \quad (8)$$

where Y_{11}^{OAM} is the gain when both Alice and Bob send single photons with the OAM basis, e_{11}^{SUP} is the quantum bit error rate (QBER) when Alice and Bob send single photons with the SUP basis, $Q_{\mu\nu}^{\mathrm{OAM}}$ is the total gain when both Alice and Bob send signal states with the OAM basis, and $E_{\mu\nu}^{\mathrm{OAM}}$ is the total QBER when both Alice and Bob send signal states with the OAM basis. In addition, $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is a binary Shannon entropy, and f is the error correction efficiency.

Unfortunately, the purity of OAM states is sensitive to AT and link attenuation,[36–38] and the key generation rate will be influenced by AT and link attenuation. Usually, the transmission probability η_0, which illustrates the probability of the received photon with the same OAM state as the input, and the transmission probability $\overline{\eta_0}$, which describes the probability of the received photon with the different OAM state to the input, are used to describe the aberration about AT and link attenuation.[39] η_0 and $\overline{\eta_0}$ are expressed as,

$$\eta_0 = \frac{\mathrm{e}^{-\alpha L}}{\pi} \int_0^1 \rho \mathrm{d}\rho \times \int_0^{2\pi} \exp\left[-3.44 \left(\frac{D}{r_0}\rho \sin(\frac{\theta}{2})\right)^{5/3}\right] \mathrm{d}\theta, \quad (9)$$

$$\overline{\eta_0} = \frac{\mathrm{e}^{-\alpha L}}{\pi} \int_0^1 \rho \mathrm{d}\rho \times \int_0^{2\pi} \exp\left[-3.44 \left(\frac{D}{r_0}\rho \sin(\frac{\theta}{2})\right)^{5/3}\right] \cos(2l\theta) \mathrm{d}\theta. \quad (10)$$

where D is the diameter of the receiver aperture, α is the coefficient caused by the atmospheric absorption and scattering loss (link attenuations), and r_0 is the Fried parameter (atmosphere turbulence),[41] which can be further described as,

$$r_0 = 0.1853 \left(\frac{\lambda^2}{C_n^2 L}\right)^{3/5}, \quad (11)$$

where C_n^2 is the refractive-index structure parameter, which is the strength of atmosphere turbulence, L is the propagation distance, and λ is the wavelength. The transmission probability of the states in the OAM basis is the same as that of the states in the SUP basis. Therefore, the whole transmission probability η is $\eta = \eta_0 + \overline{\eta_0}$, and the crosstalk probability is $t = \overline{\eta_0}/\eta$.

To obtain the key generation rate, the gain Y_{11}^{OAM} in the OAM basis, the error rate e_{11}^{SUP} in the SUP basis, the total gain $Q_{\mu\nu}^{\mathrm{OAM}}$ in the OAM basis, and the total QBER $E_{\mu\nu}^{\mathrm{OAM}}$ in the OAM basis should be deduced[19] first. To estimate Y_{11}^{OAM}, two cases should be considered. One is the case where both Alice and Bob choose the same encoding bit, so that $n - n' = 0$. The other is the case where both Alice and Bob choose different encoding bits where $n - n' = \pm 1$. Fortunately, the two cases are symmetric so that only one of them should be considered.

Without loss of generality, the case where both Alice and Bob send a single photon carrying $|-l\rangle$ is analyzed, which means that both Alice and Bob choose the same encoding bit $n = 0$. The joint states after BS are

$$\begin{aligned} |-l\rangle_1|-l\rangle_2 \rightarrow & \frac{1}{\sqrt{2}}(|-l\rangle_3 + |l\rangle_4) \otimes \frac{1}{\sqrt{2}}(|l\rangle_3 - |-l\rangle_4) \\ = & \frac{1}{2}(|-l\rangle_3|l\rangle_3 - |-l\rangle_3|-l\rangle_4 \\ & + |l\rangle_3|l\rangle_4 - |l\rangle_4|-l\rangle_4), \end{aligned} \quad (12)$$

where the subscript $i = \{1,2,3,4\}$ represents the ith arm of BS. If Charlie receives a vacuum state from Alice (or Bob) because of the losses in the aberration links, the joint states are changed to

$$\begin{aligned} |-l\rangle_1|0\rangle_2 \rightarrow & \frac{1}{\sqrt{2}}(|-l\rangle_3 + |l\rangle_4)|0\rangle, \\ |0\rangle_1|-l\rangle_2 \rightarrow & \frac{1}{\sqrt{2}}(|l\rangle_3 - |-l\rangle_4)|0\rangle. \end{aligned} \quad (13)$$

Hence, the gain for two of four of Charlie's detectors (L0, L1, R0, and R1) triggered at the same time when both Alice and Bob choose $n = 0$ is

$$\begin{aligned} & Y_{11}^{l_3 - l_3\, n=n'=0} = Y_{11}^{l_4 - l_4\, n=n'=0} \\ = & Y_{11}^{l_3 l_4\, n=n'=0} = Y_{11}^{-l_3 - l_4\, n=n'=0} \\ = & (1-P_{\mathrm{d}})^2 \left[\frac{\eta_{\mathrm{a}}\eta_{\mathrm{b}}}{4} + \frac{\eta_{\mathrm{a}}(1-\eta_{\mathrm{b}})}{2} P_{\mathrm{d}} \right. \\ & \left. + \frac{(1-\eta_{\mathrm{a}})\eta_{\mathrm{b}}}{2} P_{\mathrm{d}} + (1-\eta_{\mathrm{a}})(1-\eta_{\mathrm{b}}) P_{\mathrm{d}}^2\right], \end{aligned} \quad (14)$$

where $Y_{11}^{l_3 - l_3\, n=n'=0}$ is defined as the gain of a single photon for Charlie's detectors R0 and R1 are triggered at the same time when both Alice and Bob choose $n = 0$. Similarly,

$Y_{11}^{l_4-l_4\,n=n'=0}$, $Y_{11}^{l_3l_4\,n=n'=0}$, and $Y_{11}^{-l_3-l_4\,n=n'=0}$ are defined as the gain of a single photon are triggered at the same time when both Alice and Bob choose $n=0$ for Charlie's detectors L0 and L1, Charlie's detectors R0 and L0, and Charlie's detectors R1 and L1, respectively. $P_{\rm d}$ is the background count rate of a detector, and $\eta_{\rm a}$ ($\eta_{\rm b}$) is the transmission probability between Alice (Bob) and Charlie.

Similarly, the gains when both Alice and Bob choose $n=1$, and Alice and Bob choose different encoding bits ($n-n'=\pm1$) could be expressed as

$$\begin{aligned} & Y_{11}^{l_3-l_3\,n=n'=1}=Y_{11}^{l_4-l_4\,n=n'=1} \\ =\ & Y_{11}^{l_3l_4\,n=n'=1}=Y_{11}^{-l_3-l_4\,n=n'=1} \\ =\ & (1-P_{\rm d})^2\left[\frac{\eta_{\rm a}\eta_{\rm b}}{4}+\frac{\eta_{\rm a}(1-\eta_{\rm b})}{2}P_{\rm d}\right. \\ & \left.+\frac{(1-\eta_{\rm a})\eta_{\rm b}}{2}P_{\rm d}+(1-\eta_{\rm a})(1-\eta_{\rm b})P_{\rm d}^2\right], \end{aligned} \tag{15}$$

and

$$\begin{aligned} & Y_{11}^{l_3-l_3\,n=0\&n'=1}=Y_{11}^{l_4-l_4\,n=0\&n'=1} \\ =\ & Y_{11}^{l_3l_4\,n=0\&n'=1}=Y_{11}^{-l_3-l_4\,n=0\&n'=1} \\ =\ & Y_{11}^{l_3-l_3\,n=1\&n'=0}=Y_{11}^{l_4-l_4\,n=1\&n'=0} \\ =\ & Y_{11}^{l_3l_4\,n=1\&n'=0}=Y_{11}^{-l_3-l_4\,n=1\&n'=0} \\ =\ & (1-P_{\rm d})^2\left[\frac{\eta_{\rm a}\eta_{\rm b}}{2}P_{\rm d}+\frac{\eta_{\rm a}(1-\eta_{\rm b})}{2}P_{\rm d}\right. \\ & \left.+\frac{(1-\eta_{\rm a})\eta_{\rm b}}{2}P_{\rm d}+(1-\eta_{\rm a})(1-\eta_{\rm b})P_{\rm d}^2\right]. \end{aligned} \tag{16}$$

Therefore, the gain of single-photon pulses in the OAM basis for two of four of Charlie's detectors triggered at the same time is

$$\begin{aligned} & Y_{11}^{l_3-l_3}=Y_{11}^{l_4-l_4}=Y_{11}^{l_3l_4}=Y_{11}^{-l_3-l_4} \\ =\ & \frac{1}{4}(Y_{11}^{l_3-l_3\,n=n'=0}+Y_{11}^{l_3-l_3\,n=n'=1} \\ & +Y_{11}^{l_3-l_3\,n=0\&n'=1}+Y_{11}^{l_3-l_3\,n=1\&n'=0}) \\ =\ & (1-P_{\rm d})^2\left[\frac{\eta_{\rm a}\eta_{\rm b}}{8}+\frac{\eta_{\rm a}\eta_{\rm b}}{4}P_{\rm d}\right. \\ & +\frac{\eta_{\rm a}(1-\eta_{\rm b})}{2}P_{\rm d}+\frac{(1-\eta_{\rm a})\eta_{\rm b}}{2}P_{\rm d} \\ & \left.+(1-\eta_{\rm a})(1-\eta_{\rm b})P_{\rm d}^2\right], \end{aligned} \tag{17}$$

and the gain $Y_{11}^{\rm OAM}$ of single-photon pulses in the OAM basis is

$$\begin{aligned} Y_{11}^{\rm OAM} &= Y_{11}^{l_3-l_3}+Y_{11}^{l_4-l_4}+Y_{11}^{l_3l_4}+Y_{11}^{-l_3-l_4} \\ &= (1-P_{\rm d})^2\left[\frac{\eta_{\rm a}\eta_{\rm b}}{2}+(2\eta_{\rm a}+2\eta_{\rm b}-3\eta_{\rm a}\eta_{\rm b})P_{\rm d}\right. \\ &\quad \left.+4(1-\eta_{\rm a})(1-\eta_{\rm b})P_{\rm d}^2\right]. \end{aligned} \tag{18}$$

Likely, the gain $Y_{11}^{\rm SUP}$ in the SUP basis can also be estimated with similar steps,

$$Y_{11}^{\rm SUP}=Y_{11}^{\rm OAM}. \tag{19}$$

$Y_{11}^{\rm SUP}$ can be written as $Y_{11}^{\rm SUP}=Y_{11}^{\rm SUP+}+Y_{11}^{\rm SUP-}$, and

$$\begin{aligned} Y_{11}^{\rm SUP+} &= (1-P_{\rm d})^2\left[\frac{\eta_{\rm a}\eta_{\rm b}}{2}+(\eta_{\rm a}+\eta_{\rm b}-1.5\eta_{\rm a}\eta_{\rm b})P_{\rm d}\right. \\ &\quad \left.+2(1-\eta_{\rm a})(1-\eta_{\rm b})P_{\rm d}^2\right] \\ Y_{11}^{\rm SUP-} &= P_{\rm d}(1-P_{\rm d})^2[\eta_{\rm a}+\eta_{\rm b}-1.5\eta_{\rm a}\eta_{\rm b} \\ &\quad +2(1-\eta_{\rm a})(1-\eta_{\rm b})P_{\rm d}], \end{aligned} \tag{20}$$

where $Y_{11}^{\rm SUP+}$ describes the gain of single-photon pulses in the SUP basis when the states of the pulses received by Charlie are different from those sent by Alice and Bob, and $Y_{11}^{\rm SUP-}$ describes the gain of single-photon pulses in SUP basis when the states of the pulses received by Charlie are the same as those sent by Alice and Bob.

On the other hand, errors are induced by misalignment and crosstalk between states in the SUP basis when Alice and Bob choose different encoding bits while L0 and L1 (or R1 and R0) are triggered simultaneously, or when Alice and Bob choose the same encoding bit while R0 and L0 (or R1 and L1) are triggered simultaneously. According to the crosstalk between different states induced by AT, Charlie receives the different states with the probability $t_+=(t_{\rm a}(1-t_{\rm b})+(1-t_{\rm a})t_{\rm b})(1-e_{\rm d})+((1-t_{\rm a})(1-t_{\rm b})+t_{\rm a}t_{\rm b})e_{\rm d}$ and the same states with the probability $t_-=(t_{\rm a}(1-t_{\rm b})+(1-t_{\rm a})t_{\rm b})e_{\rm d}+((1-t_{\rm a})(1-t_{\rm b})+t_{\rm a}t_{\rm b})(1-e_{\rm d})$. So the $e_{11}^{\rm SUP}$ can be given as

$$e_{11}^{\rm SUP}=\frac{t_-Y_{11}^{\rm SUP-}+t_+Y_{11}^{\rm SUP+}}{Y_{11}^{\rm SUP}}, \tag{21}$$

where $t_{\rm a}$ and $t_{\rm b}$ are the crosstalk probability for the states sent by Alice and Bob to Charlie, respectively, and $e_{\rm d}$ represents the misalignment-error probability.

The total gain $Q_{\mu\nu}^{\rm OAM}$ in the OAM basis can be derived[19] as follows. Alice and Bob separately prepare the phase-randomized weak coherent states with intensities of μ and ν, respectively, so Alice and Bob's joint state is

$$(|{\rm e}^{{\rm i}\theta_{\rm a}}\sqrt{\mu}\rangle\otimes|\Psi_{\rm OAM}^{n}\rangle)_1(|{\rm e}^{{\rm i}\theta_{\rm b}}\sqrt{\nu}\rangle\otimes|\Psi_{\rm OAM}^{n'}\rangle)_2, \tag{22}$$

where $\theta_{\rm a}$ and $\theta_{\rm b}$ are randomized phases. After the pulses pass through two lossy channels between Alice or Bob and Charlie with transmission probability $\eta_{\rm a}$ and $\eta_{\rm b}$, the joint state can then be written as

$$(|{\rm e}^{{\rm i}\theta_{\rm a}}\sqrt{\mu\eta_{\rm a}}\rangle\otimes|\Psi_{\rm OAM}^{n}\rangle)_1(|{\rm e}^{{\rm i}\theta_{\rm b}}\sqrt{\nu\eta_{\rm b}}\rangle\otimes|\Psi_{\rm OAM}^{n'}\rangle)_2. \tag{23}$$

Then, two cases should be considered. One is both Alice and Bob choose the same encoding bit ($n-n'=0$) and the other case is they choose different encoding bits ($n-n'=\pm1$). Let us consider the gain $Q_{\mu\nu}^{{\rm OAM}\,n\neq n'}$ that both Alice and Bob choose the different encoding bits ($n-n'=\pm1$) first. Alice is assumed to choose $n=0$ and Bob is assumed to choose $n'=1$. So after passing through the BS of Charlie, the joint state can be transformed into the detection modes as follows:

$$\left|\mathrm{e}^{\mathrm{i}\theta_\mathrm{a}}\sqrt{\mu\eta_\mathrm{a}/2}+\mathrm{e}^{\mathrm{i}\theta_\mathrm{b}}\sqrt{\nu\eta_\mathrm{b}/2}\right\rangle_{\mathrm{R0}}\left|\mathrm{e}^{\mathrm{i}\theta_\mathrm{a}}\sqrt{\mu\eta_\mathrm{a}/2}-\mathrm{e}^{\mathrm{i}\theta_\mathrm{b}}\sqrt{\nu\eta_\mathrm{b}/2}\right\rangle_{\mathrm{L1}}, \tag{24}$$

then the detection probabilities of the single-photon detector R0 and L1 should be

$$\begin{aligned} D_{\mathrm{R0}} &= 1-(1-P_\mathrm{d})\exp\left(-\left|\mathrm{e}^{\mathrm{i}\theta_\mathrm{a}}\sqrt{\frac{\mu\eta_\mathrm{a}}{2}}+\mathrm{e}^{\mathrm{i}\theta_\mathrm{b}}\sqrt{\frac{\nu\eta_\mathrm{b}}{2}}\right|^2\right)=1-(1-P_\mathrm{d})\,\mathrm{e}^{-\mu'/2}\,\mathrm{e}^{-x\cos\Delta\theta},\\ D_{\mathrm{L1}} &= 1-(1-P_\mathrm{d})\exp\left(-\left|\mathrm{e}^{\mathrm{i}\theta_\mathrm{a}}\sqrt{\frac{\mu\eta_\mathrm{a}}{2}}-\mathrm{e}^{\mathrm{i}\theta_\mathrm{b}}\sqrt{\frac{\nu\eta_\mathrm{b}}{2}}\right|^2\right)=1-(1-P_\mathrm{d})\,\mathrm{e}^{-\mu'/2}\,\mathrm{e}^{x\cos\Delta\theta}, \end{aligned} \tag{25}$$

where P_d is the background count rate per detector, $x=\sqrt{\eta_\mathrm{a}\eta_\mathrm{b}\mu\nu}$, $\Delta\theta=\theta_\mathrm{a}-\theta_\mathrm{b}$, and $\mu'=\eta_\mathrm{a}\mu+\eta_\mathrm{b}\nu$. Due to symmetry, the case when Alice chooses $n=1$ and Bob chooses $n'=0$ is the same result as above, so the gain $Q_{\mu\nu}^{\mathrm{OAM}\,n\neq n'}$ is given by taking the integral of $\Delta\theta$ over 0 to 2π,

$$Q_{\mu\nu}^{\mathrm{OAM}\,n\neq n'}=2P_\mathrm{d}(1-P_\mathrm{d})\frac{1}{2\pi}\int_0^{2\pi}\mathrm{d}\Delta\theta[D_{\mathrm{R0}}(1-D_{\mathrm{L1}})+(1-D_{\mathrm{R0}})D_{\mathrm{L1}}]=4P_\mathrm{d}(1-P_\mathrm{d})^2\,\mathrm{e}^{-\mu'/2}[\mathrm{I}_0(x)-(1-P_\mathrm{d})\,\mathrm{e}^{-\mu'/2}], \tag{26}$$

where $\mathrm{I}_0(x)$ is the modified Bessel function of the first kind.

Similarly, the gain $Q_{\mu\nu}^{\mathrm{OAM}\,n=n'}$ that both Alice and Bob choose the same encoding bits in the OAM basis can be derived by the same methods[19] as

$$Q_{\mu\nu}^{\mathrm{OAM}\,n=n'}=4(1-P_\mathrm{d})^2\,\mathrm{e}^{-\mu'/2}[1-(1-P_\mathrm{d})\,\mathrm{e}^{-\mu\eta_\mathrm{a}/2}][1-(1-P_\mathrm{d})\,\mathrm{e}^{-\nu\eta_\mathrm{b}/2}]. \tag{27}$$

Due to equal probability, the $Q_{\mu\nu}^{\mathrm{OAM}}$ is given by

$$Q_{\mu\nu}^{\mathrm{OAM}}=\frac{1}{2}(Q_{\mu\nu}^{\mathrm{OAM}\,n=n'}+Q_{\mu\nu}^{\mathrm{OAM}\,n\neq n'}). \tag{28}$$

Because the rotational invariance of OAM states enables quantum communication without alignment of shared reference frames, the $E_{\mu\nu}^{\mathrm{OAM}}$ is only caused by turbulence-induced crosstalk and is given by

$$E_{\mu\nu}^{\mathrm{OAM}}=\frac{(t_\mathrm{a}(1-t_\mathrm{b})+(1-t_\mathrm{a})t_\mathrm{b})Q_{\mu\nu}^{\mathrm{OAM}\,n=n'}+((1-t_\mathrm{a})(1-t_\mathrm{b})+t_\mathrm{a}t_\mathrm{b})Q_{\mu\nu}^{\mathrm{OAM}\,n\neq n'}}{Q_{\mu\nu}^{\mathrm{OAM}\,n=n'}+Q_{\mu\nu}^{\mathrm{OAM}\,n\neq n'}}. \tag{29}$$

4. Security analysis

In this section, we will discuss the unconditional security proof of the proposed protocol, which is determined by the EPR-based QKD protocol[7] and the decoy state method.[42] In the protocol, both Alice and Bob use the decoy state method, resulting in the protocol that can avoid a photon number splitting attack.[43] Moreover, Alice and Bob could obtain that gain and QBER when the photons sent to Charlie are single photons. On the other hand, with the help of the virtual qubit idea proposed in Ref. [44], the OAM photon sent from Alice (Bob) to Charlie could be considered as the one real photon of a virtual entangled OAM photons pair, where the virtual OAM photon is kept by Alice (Bob). According to the principles of quantum swapping,[45] the virtual photons kept by Alice and Bob are entangled after Charlie finishes his Bell measurements and announcements. At this time, Alice and Bob are sharing virtual Bell-entangled OAM photons. Therefore, a secure key could be generated by performing the measurements on the virtual Bell-entangled OAM photons. It is indicated that the security of the proposed protocol is equivalent to that of the EPR-based QKD protocol. It has been shown that there is an unconditional security analysis for the EPR-based QKD protocol.[8] Hence, our proposed protocol is an unconditional secure protocol.

5. Numerical Simulations for the performance

In this section, we discuss the performance of the proposed protocol by numerical simulations. The parameters for the numerical simulation are the following. The background count rate for the detector P_d is 3×10^{-6}. The misalignment-error probability in the SUP basis e_d is 1.5%. The error correction efficiency f is 1.16. The OAM charge l is 10. The diameter of the receiver aperture D is 15cm and the wavelength λ is 1550 nm. Assume that the distance between Alice and Charlie is equivalent to the distance between Bob and Charlie ($L_\mathrm{a}=L_\mathrm{b}$), the transmission probability from Alice to Charlie is the same as that of Bob to Charlie ($\eta_\mathrm{a}=\eta_\mathrm{b}$), and the crosstalk probability of Alice (t_a) is equal to that of Bob (t_b), where $t_\mathrm{a}=t_\mathrm{b}=\overline{\eta_0}/\eta$.

Figure 2 shows the key generation rate performance of the

OAM-MDI-QKD protocol against the transmission distance, in comparison with that of the polarization-based MDI-QKD protocol with the same experimental parameters. The results show that the key generation rate performance of the proposed protocol is slightly better than that of the polarization-based MDI-QKD protocol, because Alice and Bob need not align their reference frames when both Alice and Bob use the OAM basis in the proposed protocol, which results in a lower error rate e_{11}^{OAM}. It is shown that the MDI-QKD using OAM states is feasible, and a high-dimensional MDI-QKD protocol using OAM states could be supposed for a significant improvement of the key generation rate.

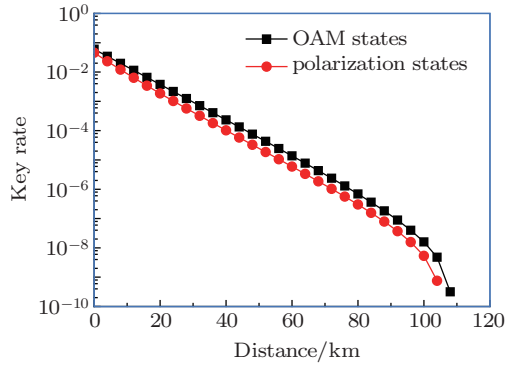


Fig. 2. (color online) The key generation rate performance of the OAM-MDI-QKD protocol against the transmission distance, in comparison with that of the polarization-based MDI-QKD protocol. Here, link attenuation α is 1.38×10^{-4} (0.6 dB/km) and no atmospheric turbulence.

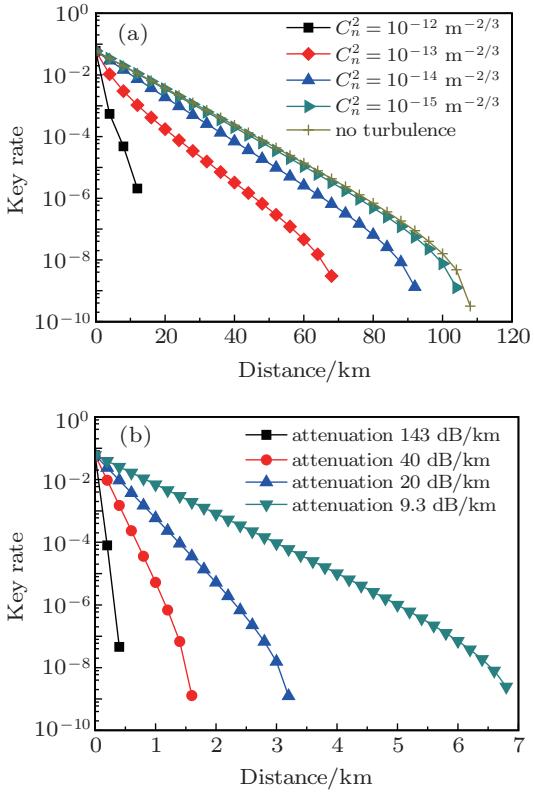


Fig. 3. (color online) The key generation rate against the transmission distance with different strength of AT and different link attenuations. Panel (a) is for different AT and the same atmospheric attenuation, where α is 1.38×10^{-4} (0.6 dB/km). Panel (b) is for different link attenuations and the same AT, where C_n^2 is set to 10^{-15} m$^{-2/3}$.

In order to demonstrate the key generation rate performance influenced by AT and link attenuation, figure 3 illustrates the key generation rate against the transmission distance with different strength of AT (C_n^2) and different link attenuations (α). Figure 3(a) is for different AT and the same link attenuation, where α is setup to 1.38×10^{-4} (0.6 dB/km), in addition to the performance of the proposed protocol without turbulence. Figure 3(b) is for different link attenuation and the same AT, where C_n^2 is set to 10^{-15} m$^{-2/3}$. Here, the four different link attenuations in Ref. [46] are discussed to illustrate the different weather conditions. The results show that the key generation rate decreases with the increase of the transmission distance under AT and link attenuation. In other words, AT and link attenuation decrease the transmission distance of the proposed QKD protocol. The stronger AT and higher link attenuation make the key generation rate performance drop quickly. Furthermore, the key generation rate performance is influenced heavily by the different weather conditions.

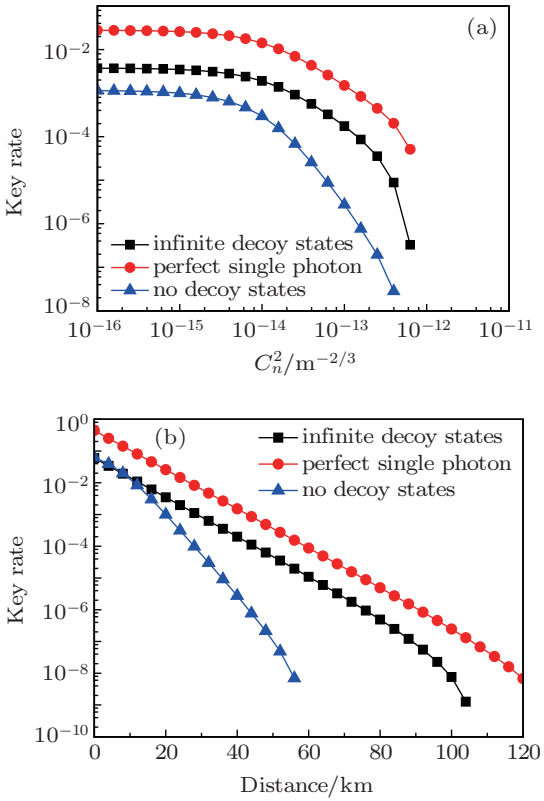


Fig. 4. (color online) The key generation rate of the proposed protocol using the infinite decoy states, the weak coherent states without decoy states, and the perfect single photon source. Panel (a) is the performance as a function of the strength of AT (C_n^2), where the distance between Alice (Bob) and Charlie is setup to 10 km, and α is set to 1.38×10^{-4} (0.6 dB/km). Panel (b) is the performance as a function of the distance between Alice and Bob, where $C_n^2 = 10^{-15}$ m$^{-2/3}$, and $\alpha = 1.38 \times 10^{-4}$.

In order to display the benefits of using decoy states, figure 4 shows the key generation rate of the proposed protocol using the weak coherent states without decoy states, the weak coherent states with the infinite decoy states, and the perfect single photon source. Figure 4(a) is the performance

as a function of the strength of AT (C_n^2), where the distance between Alice (Bob) and Charlie is setup to 10 km, and α is set to 1.38×10^{-4} (0.6 dB/km). Figure 4(b) is the performance as a function of the distance between Alice and Bob, where $C_n^2 = 10^{-15}$ m$^{-2/3}$ and $\alpha = 1.38 \times 10^{-4}$. It is shown that the key generation rate with the infinite decoy states is higher than that without decoy states, and it is still much lower than that with the perfect single photon source. With the increase of the strength of AT and the transmission distance, the key generation rate performance falls down quickly. For the same key generation rate, for example, $R = 10^{-5}$, the transmission distance for the three different sources are 36 km, 60 km, and 76 km, respectively. The results imply that the proposed protocol with the decoy-state could get a considerable good performance without the need of an ideal source.

6. Conclusion

We have proposed a decoy-state MDI-QKD protocol using orbital angular momentum states in this paper. In the protocol, the mutually unbiased bases of OAM states are prepared, and the modes of different OAM states in the MUBs are represented for different information. In order to overcome the security loophole caused by the weak coherent pulse source, the decoy states are used. A highly efficient OAM-sorter is adopted in the measurement device to obtain the output OAM state. We analyzed the key generation rate performance of the proposed protocol through a free-space atmospheric turbulent link, and discussed the performance by numerical simulations. The results show that the protocol has a slightly improved performance in comparison with that of the polarization-based MDI-QKD protocol with the same experimental condition. Moreover, the MDI-QKD protocol based on OAM states with higher dimensions could further enhance the key generation rate performance. In addition, AT and link attenuation have influenced on the key generation rate performance and the transmission distance. The stronger AT and higher link attenuation make the key generation rate performance drop quickly, and the transmission distance decreases straightway. Finally, the results demonstrate that the proposed protocol with the decoy states could get a considerably good performance without the need of an ideal source.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India) p. 175
[2] Zhao L Y, Li H W, Yin Z Q, Chen W, You J and Han Z F 2014 *Chin. Phys. B* **23** 0100304
[3] Quan D X, Zhu C H, Liu S Q and Pei C X 2015 *Chin. Phys. B* **24** 050309
[4] Huang W, Wen Q Y, Liu B and Gao F 2015 *Chin. Phys. B* **24** 070308
[5] Wang Y, Bao W S, Li H W, Zhou C and Li Y 2014 *Chin. Phys. B* **23** 080303
[6] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[7] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[8] Lo H K and Chau H F 1999 *Science* **283** 2050
[9] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[10] Xu F, Qi B and Lo H K 2010 *New J. Phys.* **12** 113026
[11] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 686
[12] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C and Makarov V 2011 *Nat. Commun.* **2** 349
[13] Burenkov V, Qi B, Fortescue B and Lo H K 2014 *Quantum Inform. Comput.* **14** 217
[14] Liu Y, Chen T Y, Wang L J, Liang H, Shentu G L, Wang J, Cui K, Yin H L, Liu N L, Li L, Ma X F, Pelc J S, Fejer M M, Peng C Z, Zhang Q and Pan J W 2013 *Phys. Rev. Lett.* **111** 130502
[15] Ferreira da Silva T, Vitoreti D, Xavier G B, do Amaral G C, Temporão G P and von der Weid J P 2013 *Phys. Rev. A* **88** 052303
[16] Rubenok A, Slater J A, Chan P, Lucio-Martinez I and Tittel W 2013 *Phys. Rev. Lett.* **111** 130501
[17] Tang Y L, Yin H L, Chen S J, Liu Y, Zhang W J, Jiang X, Zhang L, Wang J, You L X, Guan J Y, Yang D X, Wang Z, Liang H, Zhang Z, Zhou N, Ma X F, Chen T Y, Zhang Q and Pan J W 2014 *Phys. Rev. Lett.* **113** 190501
[18] Tang Y L, Yin H L, Chen S J, Liu Y, Zhang W J, Jiang X, Zhang L, Wang J, You L X, Guan J Y, Yang D X, Wang Z, Liang H, Zhang Z, Zhou N, Ma X F, Chen T Y, Zhang Q and Pan J W 2015 *IEEE J. Sel. Top. Quantum Electron.* **21** 6600407
[19] Ma X F and Razavi M 2012 *Phys. Rev. A* **86** 062319
[20] Song T T, Wen Q Y, Guo F Z and Tan X Q 2012 *Phys. Rev. A* **86** 022332
[21] Tamaki K, Lo H K, Fung C H F and Qi B 2012 *Phys. Rev. A* **85** 042307
[22] Yu Z W, Zhou Y H and Wang X B 2015 *Phys. Rev. A* **91** 032318
[23] Zhou C, Bao W S, Zhang H L, Li H W, Wang Y, Li Y and Wang X 2015 *Phys. Rev. A* **91** 022313
[24] Shan Y Z, Sun S H, Ma X C, Jiang M S, Zhou Y L and Liang L M 2014 *Phys. Rev. A* **90** 042334
[25] Yin H L, Cao W F, Fu Y, Tang Y L, Liu Y, Chen T Y and Chen Z B 2014 *Opt. Lett.* **39** 5451
[26] Zhou Y Y, Zhang H Q, Zhou X J and Tian P G 2013 *Acta Phys. Sin.* **62** 200302 (in Chinese)
[27] Sun Y, Zhao S H and Dong C 2015 *Acta Phys. Sin.* **64** 140304 (in Chinese)
[28] Spedalieri F M 2006 *Opt. Commun.* **260** 340
[29] Li J L and Wang C 2010 *Chin. Phys. Lett.* **27** 110303
[30] Malik M, O'Sullivan M, Rodenburg B, Mirhosseini M, Leach J, Lavery M P J, Padgett M J and Boyd R W 2012 *Opt. Express* **20** 13195
[31] Zhao S M, Gong L Y, Li Y Q, Yang H, Sheng Y B and Cheng W W 2013 *Chin. Phys. Lett.* **30** 060305
[32] Mafu M, Dudley A, Goyal S, Giovannini D, McLaren M, Padgett M.J, Konrad T, Petruccione F, Lütkenhaus N and Forbes A 2013 *Phys. Rev. A* **88** 032305
[33] Berkhout G C G, Lavery M P J, Courtial J, Beijersbergen M W and Padgett M J 2010 *Phys. Rev. Lett.* **105** 153601
[34] Mirhosseini M, Malik M, Shi Z M and Boyd R W 2013 *Nat. Commun.* **4** 2781
[35] Allen L, Beijersbergen M W, Spreeuw R J C and Woerdman J P 1992 *Phys. Rev. A* **45** 8185
[36] Zhao S M, Leach J, Gong L Y, Ding J and Zheng B Y 2012 *Opt. Express* **20** 452
[37] Zhao S M, Yang H, Li Y Q, Cao F, Sheng Y B, Cheng W W and Gong L Y 2013 *Opt. Commun.* **294** 223
[38] Zhao S M, Wang B, Gong L Y, Sheng Y B, Cheng W W, Dong X L and Zheng B Y 2013 *J. Lightwave Technol.* **31** 2823
[39] Tyler G A and Boyd R W 2009 *Opt. Lett.* **34** 142
[40] Nagali E, Sansoni L, Sciarrino F, De Martini F, Marrucci L, Piccirillo B, Karimi E and Santamato E 2009 *Nat. Photon.* **3** 720
[41] Fried D L 1965 *J. Opt. Soc. Am.* **55** 1427
[42] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[43] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev. A* **51** 1863
[44] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum. Inform. Comput.* **5** 325
[45] Pan J W, Bouwmeester D, Weinfurter H and Zeilinger A 1998 *Phys. Rev. Lett.* **80** 3891
[46] Awan M S, Horwath L C, Muhammad S S, Leitgeb E, Nadeem F and Khan M S 2009 *J. Commun.* **4** 533