Passive measurement-device-independent quantum key distribution with orbital angular momentum and pulse position modulation*

WANG Lian (王潋), **ZHOU Yuan-yuan** (周媛媛)**, **ZHOU Xue-jun** (周学军), **and CHEN Xiao** (陈霄)
Electronic Engineering College, Naval University of Engineering, Wuhan 430033, China

(Received 26 October 2017; Revised 20 November 2017)

Based on the orbital angular momentum and pulse position modulation, we present a novel passive measurement-device-independent quantum key distribution (MDI-QKD) scheme with the two-mode source. Combining with the tight bounds of the yield and error rate of single-photon pairs given in our paper, we conduct performance analysis on the scheme with heralded single-photon source. The numerical simulations show that the performance of our scheme is significantly superior to the traditional MDI-QKD in the error rate, key generation rate and secure transmission distance, since the application of orbital angular momentum and pulse position modulation can exclude the basis-dependent flaw and increase the information content for each single photon. Moreover, the performance is improved with the rise of the frame length. Therefore, our scheme, without intensity modulation, avoids the source side channels and enhances the key generation rate. It has greatly utility value in the MDI-QKD setups.
Document code: A **Article ID:** 1673-1905(2018)02-0138-5
DOI https://doi.org/10.1007/s11801-018-7232-9

As an essential branch of quantum information, quantum key distribution (QKD)[1] has attracted considerable attention[2-4]. The unconditional security of QKD has been rigorously proved in theory[5], while there are conflictions between the theoretical proof and realistic setups. Specifically, imperfect physical devices, especially the detectors, introduce plenty of security loopholes in QKD system. To solve these conflictions, one countermeasure is a decoy state method[6] that can remove the photon number splitting (PNS) attack[7] caused by the non-ideal single photon source. The other is a measurement-device-independent quantum key distribution (MDI-QKD)[8] which can overcome all side channel attacks resulting from non-ideal detectors. In fact, MDI-QKD is generally integrated with the decoy state method to obtain more secure and efficient keys. Moreover, the active decoy state method introduces the side channel and leaks the information to eavesdroppers, while the passive decoy state method can solve these problems[9].

The studies show that the beam has two angular momentums, one is the spin angular momentum (SAM) generated by the polarization characteristic of the beam, and the other is the orbital angular momentum (OAM) produced by the helical phase structure of the beam. As for the setups of MDI-QKD, polarization coding[8] and phase coding[10] are two major coding methods, which are based on the SAM of photon to encode information. However, they suffer from the basis-dependent flaw[10] during the preparation and measurement of photons. Both users need to detect and adjust the reference system in real time, which brings adverse effect on the key generation rate. Luckily, Gibson[11] demonstrated the feasibility of OAM as an information carrier in quantum communication. Su[12] and Boyd[13] respectively achieved quantum cryptography by applying OAM and verified that OAM coding can exclude the basis-dependent flaw.

In addition, the weak coherent source (WCS) and the heralded single-photon source (HSPS)[14] are often used in the MDI-QKD setups. However, their single-photon pulse ratios are very low, which cause the poor key generation rate. Fortunately, pulse position modulation (PPM)[15] can modulate each pulse into a certain time slot within a PPM frame, thus increasing the information content carried by a single-photon pulse.

In this paper, on the basis of OAM coding and PPM technology, we put forward a novel passive MDI-QKD scheme with the two-mode source, called PPM-OAM-MDI-QKD. Besides, with the HSPS, we give the lower bound of the yield of single-photon pairs and the upper bound of the error rate of single-photon pairs as well as the modified formula of key generation rate. Furthermore, we numerically study the performance of this scheme.

Usually, OAM is described by the Laguerre-Gaussian (LG) mode, the OAM state is recorded as $|l\rangle$, and the topological value in the azimuth phase $\exp(il\alpha)$ is l. As

* This work has been supported by the National Natural Science Foundation of China (No.61302099).
** E-mail: 15623115746@163.com

for PPM, if the n-bit information is denoted as $m=(m_1,m_2,\ldots,m_n)$, the frame length is $M=2^n$ (i.e., the total number of slots). The slot position of the modulation pulse is written as L, and then the mapping coding relationship of PPM is

$$L = m_1 + 2m_2 + 2^2 m_3 + \ldots + 2^{n-1} m_n,$$
$$m_n \in \{0,1,\ldots,n-1\}. \quad (1)$$

Compared with a single photon just carrying one bit information in traditional MDI-QKD, the pulse carries $\log_2 M$ bits of information when the frame length of PPM signal is M, which greatly increases the information carried by the single photon.

The system model for PPM-OAM-MDI-QKD is displayed in Fig.1. Based on the traditional MDI-QKD, our scheme adopts the two-mode source where one mode is the signal state, while the other is the trigger state. Alice and Bob execute OAM coding and PPM modulation on the signal states emitted by themselves, respectively. Then, the signal states are sent into the third party (Charlie) simultaneously to complete the separation and detection for extracting the secure key. The trigger state at Alice or Bob side is detected by local detector to predict the arrival of the signal state. According to the clicking and non-clicking events, the signal state is divided into two sets for parameter estimation and key extraction.

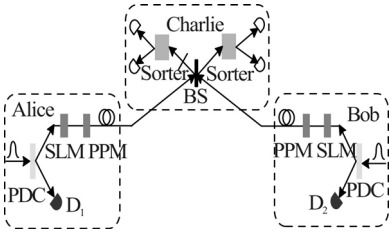

Fig.1 The model of PPM-OAM-MDI-QKD scheme

Our scheme combines OAM coding with PPM modulation coding to replace the normal polarization or phase coding, which is the essential difference form the traditional MDI-QKD. The implementation process of PPM-OAM-MDI-QKD is decomposed into four steps.

Step Ⅰ: Alice and Bob employ the OAM states to design two sets of unbiased bases, which are $B_1 = \{|l\rangle, |-l\rangle\}$ and $B_2 = \{(|l\rangle + |-l\rangle)/2, (|l\rangle - |-l\rangle)/2\}$. Alice (Bob) emits the two-mode source with the intensity μ. The trigger state is detected by the local detector to obtain two types of detection results. Meanwhile, the signal state is sent into the spatial light modulator (SLM) to prepare OAM states with different values of l, and then encoded in the base randomly chosen from the orthogonal bases B_1 and B_2.

Step Ⅱ: The encoded OAM states with different values of l are transmitted to the PPM modulator to produce PPM frames. For each PPM frame, only one particular time slot is occupied by a pulse, while the others are empty pulses without carrying information.

Step Ⅲ: Alice and Bob send the prepared PPM frames to Charlie. Then, Charlie performs the Bell-state measurements on the corresponding time slots of the two PPM frames synchronously. If the pulses are detected in the same slot of the two frames separately, the next measurement is continued. Instead, if not detected in a certain time slot, the slot is not measured. Note that the efficient OAM sorter is necessary to split the OAM states during Charlie's measurement process. Additionally, all of Charlie's detection results are recorded and divided into two types, the triggered and the untriggered events, depending on the clicking and non-clicking events of the trigger states at Alice and Bob sides.

Step Ⅳ: Repeat the above procedures to complete the measurements for all PPM frames, and the measurement results are published by Charlie. Alice and Bob determine whether the measurement results are correct. If incorrect, discard the data. Otherwise, if correct, temporarily retain this data and compare each base chosen by Alice and Bob individually. Afterwards, the data in the same base is kept and the corresponding bit flipping is conducted. After achieving these operations, this set of data is used as the raw key. Finally, the raw key is post-processed on the classic channel to obtain the final secure key.

In order to describe our scheme more clearly, we take five PPM frames and frame length of M=4 to illustrate how to prepare and encode quantum state of the sender, as shown in Tab.1.

Tab.1 4-PPM-OAM-MDI-QKD example

Parameter	Values				
Random numbers	1	0	1	0	0
l values	1	2	3	4	5
Base selection	B_1	B_2	B_1	B_1	B_2
OAM coding	$\|-1\rangle$	$\frac{\|2\rangle+\|-2\rangle}{2}$	$\|-3\rangle$	$\|4\rangle$	$\frac{\|5\rangle+\|-5\rangle}{2}$
PPM coding	01	00	10	00	11
Slot position	2 slot	0 slot	1 slot	0 slot	3 slot

In summary, the PPM-OAM-MDI-QKD scheme eliminates the basis-dependent flaw in MDI-QKD system by OAM coding. Besides, exploiting PPM technology, the scheme increases the information carried by the single photon to further improve the system performance. Furthermore, the passive decoy-state method with the two-mode source is used in our scheme to avoid the source side channel and solve the PNS attack.

Afterwards, we analyze the performance of this scheme with HSPS that is generated by the parametric down-conversion (PDC) process. HSPS has a two-mode state with identical characteristics, written as

$$|\Psi\rangle_{\mathrm{TS}} = \sum_{n=0}^{\infty} \sqrt{P_n} |n\rangle_{\mathrm{T}} |n\rangle_{\mathrm{S}}, \quad (2)$$

where $|n\rangle$ denotes the n-photon state and P_n is the probability of the photon number distribution. Here, we use the Poisson distribution of HSPS to study system performance. Thus, we have $P_n(\mu)=\mu^n e^{-\mu}/n!$, and μ is the

average intensity.

When Alice or Bob emits n-photon state, the probability that the signal state is encoded as the PPM frame with M time slots is

$$P_{n,\mathrm{PPM}}(\mu)=MP_n(P_0)^{M-1}=M\frac{\mu^n}{n!}\mathrm{e}^{-M\mu}. \tag{3}$$

The trigger state is sent into the detector at Alice or Bob side, and the probability of the local detector clicking is

$$\begin{cases} q_n=1-(1-d_v)(1-\eta_v)^n, & n\geq 1 \\ q_0=d_v, & n=0. \end{cases} \tag{4}$$

Assuming the detectors at Alice and Bob sides are identical, d_v and η_v represent their dark count rate and detection efficiency, respectively. The probability of the local detector not clicking is $(1-q_n)$.

According to the clicking and non-clicking results of the local detector at Alice (Bob) side, the signal pulse is divided into two types, triggered event ρ_μ^{nt} and untriggered event ρ_μ^{t}, whose density operators are

$$\rho_\mu^{nt}=\sum\nolimits_n c_n^t|n\rangle\langle n|=\sum\nolimits_n q_n P_{n,\mathrm{PPM}}(\mu)|n\rangle\langle n|, \tag{5}$$

$$\rho_\mu^{t}=\sum\nolimits_n c_n^{nt}|n\rangle\langle n|=\sum\nolimits_n (1-q_n) P_{n,\mathrm{PPM}}(\mu)|n\rangle\langle n|. \tag{6}$$

The corresponding photon number distributions are

$$c_n^{nt}=q_n\mathrm{P}_{n,\mathrm{PPM}}=M\left[1-(1-d_\mathrm{A})(1-\eta_\mathrm{A})^n\right]\frac{\mu^n}{n!}\mathrm{e}^{-M\mu}, \tag{7}$$

$$c_n^{t}=(1-q_n)\mathrm{P}_{n,\mathrm{PPM}}=M(1-d_\mathrm{A})(1-\eta_\mathrm{A})^n\frac{\mu^n}{n!}\mathrm{e}^{-M\mu}, \tag{8}$$

where c=a, b.

Thus, the triggered and untriggered events are used to describe the decoy state nt and the signal state t, separately. Eqs.(7) and (8) also represent the photon number distributions of signal state and decoy state, respectively.

When Alice and Bob transmit the signal state or decoy state in B_1 or B_2 base, the total gains and error rate can be expressed as

$$S_{l,r}^w=\sum_{j,k\geq 0} a_j^l b_k^r Y_{jk}^w, \quad l,r=t,nt, \tag{9}$$

$$E_{l,r}^w S_{l,r}^w=\sum_{j,k\geq 0} a_j^l b_k^r e_{jk}^w Y_{jk}^w, \quad l,r=t,nt, \tag{10}$$

where $w=B_1$ or B_2, Y_{jk}^w and e_{jk}^w denote the yield and error rate when the j-photon from Alice and the k-photon from Bob select the w base. According to the estimation method in Ref.[16], we can give the lower bound of the yield of single-photon pairs Y_{11} and the upper bound of the error rate of single-photon pairs e_{11}.

Since Eqs.(9) and (10) are independent of base selection, the superscript w is omitted during subsequent calculation. Eq.(9) is transformed as

$$\begin{aligned} S_{l,r}=&a_0^l b_0^r Y_{00}+a_0^l\sum_{k=1}^{\infty} b_k^r Y_{0k}+b_0^r\sum_{j=1}^{\infty} a_j^l Y_{j0}+a_1^l b_1^r Y_{11}+\\ &a_1^l\sum_{k=2}^{\infty} b_k^r Y_{1k}+b_1^r\sum_{j=2}^{\infty} a_j^l Y_{j1}+\sum_{j,k=2}^{\infty} a_j^l b_k^r Y_{jk}, \quad l,r=t,nt. \end{aligned} \tag{11}$$

Thus, we get

$$\begin{aligned} &a_0^{nt}b_0^{nt}S_{t,t}-a_0^t b_0^{nt}S_{nt,t}-a_0^{nt}b_0^t S_{t,nt}+a_0^t b_0^t S_{nt,nt}=\\ &\left(a_0^{nt}a_1^t-a_0^t a_1^{nt}\right)\left(b_0^{nt}b_1^t-b_0^t b_1^{nt}\right)Y_{11}+\\ &\left(a_0^{nt}a_1^t-a_0^t a_1^{nt}\right)\sum_{k=2}^{\infty}\left(b_0^{nt}b_k^t-b_0^t b_k^{nt}\right)Y_{1k}+\\ &\left(b_0^{nt}b_1^t-b_0^t b_1^{nt}\right)\sum_{j=2}^{\infty}\left(a_0^{nt}a_j^t-a_0^t a_j^{nt}\right)Y_{j1}+\\ &\sum_{j,k=2}^{\infty}\left(a_0^{nt}a_j^t-a_0^t a_j^{nt}\right)\left(b_0^{nt}b_k^t-b_0^t b_k^{nt}\right)Y_{jk}. \end{aligned} \tag{12}$$

It is easy to prove that $c_j^{nt}c_k^t-c_j^t c_k^{nt}\geq 0$ is correct when $j\leq k$, then

$$\frac{c_0^{nt}c_j^t-c_0^t c_j^{nt}}{c_0^{nt}c_j^{nt}+c_0^t c_j^t}\geq\frac{c_0^{nt}c_2^t-c_0^t c_2^{nt}}{c_0^{nt}c_2^{nt}+c_0^t c_2^t}, \quad j\geq 2, c=a,b. \tag{13}$$

Therefore, Eq.(12) can be rewritten as

$$\begin{aligned} &a_0^{nt}b_0^{nt}S_{t,t}-a_0^t b_0^{nt}S_{nt,t}-a_0^{nt}b_0^t S_{t,nt}+a_0^t b_0^t S_{nt,nt}\geq\\ &A_1B_1\left(a_0^{nt}a_1^{nt}+a_0^t a_1^t\right)\left(b_0^{nt}b_1^{nt}+b_0^t b_1^t\right)Y_{11}+\\ &A_1B_2\left(a_0^{nt}a_1^{nt}+a_0^t a_1^t\right)\sum_{k=2}^{\infty}\left(b_0^{nt}b_k^{nt}+b_0^t b_k^t\right)Y_{1k}+\\ &A_2B_1\left(b_0^{nt}b_1^{nt}+b_0^t b_1^t\right)\sum_{j=2}^{\infty}\left(a_0^{nt}a_j^{nt}+a_0^t a_j^t\right)Y_{j1}+\\ &A_2B_2\sum_{j,k=2}^{\infty}\left(a_0^{nt}a_j^{nt}+a_0^t a_j^t\right)\left(b_0^{nt}b_k^{nt}+b_0^t b_k^t\right)Y_{jk}\geq\\ &A_1B_1\left(a_0^{nt}a_1^{nt}+a_0^t a_1^t\right)\left(b_0^{nt}b_1^{nt}+b_0^t b_1^t\right)Y_{11}+\\ &Ca_0^t b_0^t\left(S_{t,t}-a_0^t S_{0,t}-b_0^t S_{t,0}+a_0^t b_0^t S_{0,0}-a_1^t b_1^t Y_{11}\right)+\\ &Ca_0^t b_0^{nt}\left(S_{t,nt}-a_0^t S_{0,nt}-b_0^{nt}S_{t,0}+a_0^t b_0^{nt}S_{0,0}-a_1^t b_1^{nt}Y_{11}\right)+\\ &Ca_0^{nt}b_0^t\left(S_{nt,t}-a_0^{nt}S_{0,t}-b_0^t S_{nt,0}+a_0^{nt}b_0^t S_{0,0}-a_1^{nt}b_1^t Y_{11}\right)+\\ &Ca_0^{nt}b_0^{nt}\left(S_{nt,nt}-a_0^{nt}S_{0,nt}-b_0^{nt}S_{nt,0}+a_0^{nt}b_0^{nt}S_{0,0}-a_1^{nt}b_1^{nt}Y_{11}\right), \end{aligned} \tag{14}$$

where $C=\min\{A_1B_2, A_2B_1, A_2B_2\}$ and

$$A_1=\frac{a_0^{nt}a_1^t-a_0^t a_1^{nt}}{a_0^{nt}a_1^{nt}+a_0^t a_1^t}, \qquad A_2=\frac{a_0^{nt}a_2^t-a_0^t a_2^{nt}}{a_0^{nt}a_2^{nt}+a_0^t a_2^t},$$

$$B_1=\frac{b_0^{nt}b_1^t-b_0^t b_1^{nt}}{b_0^{nt}b_1^{nt}+b_0^t b_1^t}, \qquad B_2=\frac{b_0^{nt}b_2^t-b_0^t b_2^{nt}}{b_0^{nt}b_2^{nt}+b_0^t b_2^t}. \tag{15}$$

Then, $(C-A_1B_1)\left(a_0^{nt}a_1^{nt}+a_0^t a_1^t\right)\left(b_0^{nt}b_1^{nt}+b_0^t b_1^t\right)>0$ is always true, thereby deducing the lower bound of Y_{11} as

$$\begin{aligned} \underline{Y}_{11}=&\frac{g_{t,t}S_{t,t}+g_{t,nt}S_{t,nt}+g_{nt,t}S_{nt,t}+g_{nt,nt}S_{nt,nt}}{(C-A_1B_1)\left(a_0^{nt}a_1^{nt}+a_0^t a_1^t\right)\left(b_0^{nt}b_1^{nt}+b_0^t b_1^t\right)}+\\ &\frac{g_{0,0}S_{0,0}-g_{t,0}S_{t,0}-g_{nt,0}S_{nt,0}-g_{0,t}S_{0,t}-g_{0,nt}S_{0,nt}}{(C-A_1B_1)\left(a_0^{nt}a_1^{nt}+a_0^t a_1^t\right)\left(b_0^{nt}b_1^{nt}+b_0^t b_1^t\right)}, \end{aligned} \tag{16}$$

where the corresponding coefficients for total gains are

$$g_{t,t}=Ca_0^t b_0^t-a_0^{nt}b_0^{nt}, \qquad g_{t,0}=Ca_0^t\left[\left(b_0^t\right)^2+\left(b_0^{nt}\right)^2\right],$$

$$g_{t,nt}=Ca_0^t b_0^{nt}+a_0^{nt}b_0^t, \qquad g_{nt,0}=Ca_0^{nt}\left[\left(b_0^t\right)^2+\left(b_0^{nt}\right)^2\right],$$

$$g_{nt,t}=Ca_0^{nt}b_0^t+a_0^t b_0^{nt}, \qquad g_{0,t}=Cb_0^t\left[\left(a_0^t\right)^2+\left(a_0^{nt}\right)^2\right],$$

$$g_{nt,nt}=Ca_0^{nt}b_0^{nt}-a_0^{t}b_0^{t},\quad g_{0,nt}=Cb_0^{nt}\left[\left(a_0^{t}\right)^2+\left(a_0^{nt}\right)^2\right],$$
$$g_{0,0}=C\left[\left(a_0^{t}\right)^2+\left(a_0^{nt}\right)^2\right]\left[\left(b_0^{t}\right)^2+\left(b_0^{nt}\right)^2\right]. \tag{17}$$

Similarly, according to Eq.(10), the total error rate of the system can be rewritten as

$$\begin{aligned}&E_{nt,nt}S_{nt,nt}=-a_0^{nt}b_0^{nt}e_{00}Y_{00}+a_1^{nt}b_1^{nt}e_{11}Y_{11}+\\&a_0^{nt}\sum_{k=0}^{\infty}b_k^{nt}e_{0k}Y_{0k}+b_0^{nt}\sum_{j=0}^{\infty}a_j^{nt}e_{j0}Y_{j0}+a_1^{nt}\sum_{k=2}^{\infty}b_k^{nt}e_{1k}Y_{1k}+\\&b_1^{nt}\sum_{j=2}^{\infty}a_j^{nt}e_{j1}Y_{j1}+\sum_{j,k=2}^{\infty}a_j^{nt}b_k^{nt}e_{jk}Y_{jk}\geq\\&-a_0^{nt}b_0^{nt}e_{00}Y_{00}+a_1^{nt}b_1^{nt}e_{11}Y_{11}+\\&a_0^{nt}\sum_{k=0}^{\infty}b_k^{nt}e_{0k}Y_{0k}+b_0^{nt}\sum_{j=0}^{\infty}a_j^{nt}e_{j0}Y_{j0}=\\&-a_0^{nt}b_0^{nt}E_{0,0}S_{0,0}+a_1^{nt}b_1^{nt}e_{11}Y_{11}+a_0^{nt}E_{0,nt}S_{0,nt}+\\&b_0^{nt}E_{nt,0}S_{nt,0}.\end{aligned} \tag{18}$$

Thus, we can deduce the upper bound of e_{11} as

$$\bar{e}_{11}=\frac{E_{nt,nt}S_{nt,nt}-a_0^{nt}E_{0,nt}S_{0,nt}-b_0^{nt}E_{nt,0}S_{nt,0}+a_0^{nt}b_0^{nt}E_{0,0}S_{0,0}}{a_1^{nt}b_1^{nt}\underline{Y}_{11}}. \tag{19}$$

Here, *t* and *nt* (the superscript or subscript) respectively represent the signal state and the decoy state prepared by Alice or Bob. The subscript 0 means a vacuum state. Since we mostly take advantage of the laser diode driven by the electrical pulse to generate the light pulse, the vacuum state can be produced by turning off the electrical pulse. This process is reasonable and secure. Therefore, the signal state and the decoy state used in our scheme can be considered to be passively produced, and our scheme still belongs to the passive decoy state scheme without modulated vulnerabilities.

At last, we modify the classical formula of key generation rate given in Ref.[8], and the key generation rate of our scheme can be calculated as

$$R\geq\log_2 Mq_1^2\mu^2\mathrm{e}^{-2\mu}\underline{Y}_{11}^{B_1}\left[1-H\left(\bar{e}_{11}^{B_2}\right)\right]-S_{t,t}^{B_1}fH\left(E_{t,t}^{B_1}\right), \tag{20}$$

where $S_{t,t}^{B_1}$ and $E_{t,t}^{B_1}$ are the total gains and error rate of the triggered event in B_1 base, which can be measured in experiments[17]. $H_2(x)=-x\log_2(x)-(1-x)\log_2(1-x)$ is the binary Shannon function. *f* is the actual error correction efficiency. In particular, due to the application of PPM technology, a single photon pulse in our scheme carries $\log_2 M$ bits of information, which means that the yield of the single-photon pairs in B_1 base is $\log_2 M$ times as the MDI-QKD with traditional coding methods.

Now, using Eqs.(16), (19) and (20), we numerically study the performance of our scheme. We set the parameters primarily from Ref.[17]: e_d=1.5%, f=1.16, η_v=0.75, $d_v=1.0\times10^{-6}$ and α=0.2 dB/km is the channel loss. Because OAM coding solves the basis-dependent flaw, the misalignment-error probability in our scheme is $e_d=0$.

The simulation results are presented in Figs.2 and 3, where the curves display the traditional passive MDI-QKD scheme with polarization coding, the OAM-MDI-QKD scheme (without PPM modulation), and the PPM-OAM-MDI-QKD schemes with different frame lengths of *M*, such as $M=2,4,8,16$.

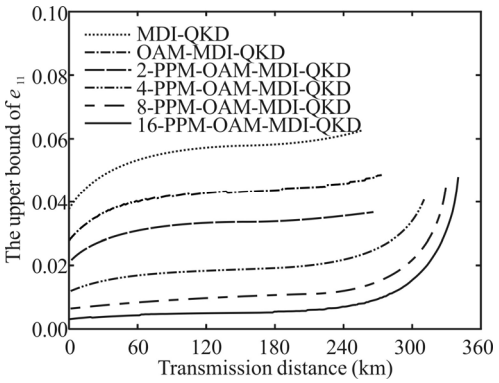

Fig.2 Upper bound of e_{11} under different MDI-QKD schemes

Fig.2 reveals that the upper bound of e_{11} in the OAM-MDI-QKD scheme is clearly below that in the traditional MDI-QKD scheme with polarization coding. It depends on the rotation invariance of OAM state, which can solve the basis-dependent flaw resulting from the polarization coding or phase coding to decline the error rate. Moreover, adding the PPM technology to OAM-MDI-QKD scheme can further decrease the error rate. For the PPM-OAM-MDI-QKD schemes, longer frame length makes the error rate lower.

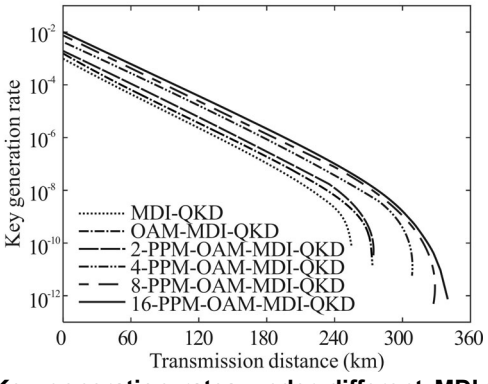

Fig.3 Key generation rates under different MDI-QKD schemes

Fig.3 points out that the performance of OAM-MDI-QKD scheme whether in key generation rate or secure transmission distance is better than that of traditional MDI-QKD scheme with polarization coding. Besides, the OAM-MDI-QKD scheme provides a performance comparable to the 2-PPM-OAM-MDI-QKD scheme, and they have identical maximum transmission distance that is 273.4 km. Moreover, the PPM-OAM-MDI-QKD schemes with different frame lengths exceed the OAM-MDI-QKD scheme in performance. As the frame length *M* of

PPM-QAM-MDI-QKD increases, the key generation rate and secure transmission distance are both improved. For example, the maximum transmission distance can reach 340.2 km when M=16.

In conclusion, we have proposed a passive decoy-state MDI-QKD scheme based on OAM coding and PPM technology, called PPM-OAM-MDI-QKD, in which both Alice and Bob emit the two-mode source without intensity modulation. Especially, combining with the OAM and PPM, our scheme can exclude the basis-dependent flaw and increase the information content for the single photon. Besides, we have given the lower bound of the yield of single-photon pairs and the upper bound of the error rate of single-photon pairs to tightly estimate the key generation rate. Based on this, we numerically study the performance of this scheme with HSPS. The results demonstrate that the PPM-OAM-MDI-QKD scheme supplies a performance superior to the OAM-MDI-QKD scheme and the traditional MDI-QKD. For the PPM-OAM-MDI-QKD schemes with different frame lengths, longer frame length makes the performance of corresponding scheme better. Specifically, when the frame length is 2, the maximum secure distance is 273.4 km that is identical to that of the OAM-MDI-QKD scheme. And it can reach 340.2 km when the frame length is 16. Therefore, our scheme avoids the source side channels and significantly optimizes the system performance. It seems promising in the future development for MDI-QKD.

References

[1] C. H. BENNETT and G. BRASSARD, Quantum Cryptography: Public Key Distribution and Coin Tossing, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing **560**, 175 (1984).

[2] Y. Y. Zhou, X. J. Zhou and B. B. Su, Optoelectron. Lett. **12**, 0148 (2016).

[3] L. Wang and S. M. Zhao, Quantum Inf. Process. **16**, 100 (2017).

[4] L. Li and F. Z. Guo, Sci. Rep. **7**, 11370 (2017).

[5] D. Mayers, Journal of the ACM **48**, 351 (2001).

[6] W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[7] G. Brassard, N. Ltttkenhaus and T. Mor, Phys. Rev. Lett. **85**, 1330 (2000).

[8] H. K. Lo, M. Curty and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[9] Q. C. Sun, W. L. Wang and Y. Liu, Laser Phys. Lett. **11**, 085202 (2014).

[10] K. Tamaki, H. K. Lo and C. H. F. Fung, Phys. Rev. A **85**, 042307 (2012).

[11] G. Gibson, J. Courtial and M. J. Padgett, Opt. Express **12**, 5448 (2004).

[12] Z. K. Su, F. Q. Wang and Y. Q. Lu, Acta Phys. Sin. **56**, 3016 (2008). (in Chinese)

[13] R. W. Boyd, A. Jha and M. Malik, SPIE OPTO **79480**, 79480L-6 (2011).

[14] M. Schiavon, G. Vallone, F. Ticozzi and P. Villoresi, Phys. Rev. A **93**, 012331 (2016).

[15] Y. Q. Zhang and B. D. Ivan, ICTON, 1 (2014).

[16] Y. Z. Shan, S. H. Sun, X. C. Ma and M. S. Jiang, Phys. Rev. A **90**, 042334 (2014).

[17] Q. Wang and X. B. Wang, Sci. Rep. **4**, 4612 (2014).