Computers, Materials & Continua CMC, vol.63, no.1, pp.369-387, 2020

Measurement Device Independent Quantum Key Distribution Based on Orbital Angular Momentum under Parametric Light Source

Meng Wang[1], Hong Lai[1,*] and Lei Pan[2]

Abstract: On the one hand, existing measurement device independent quantum key distribution (MDI-QKD) protocols have usually adopted single photon source (SPS) and weak coherent photon (WCP), however, these protocols have suffered from multi-photon problem brought from photon splitter number attacks. On the other hand, the orbital angular momentum (OAM)-MDI-QKD protocol does not need to compare and adjust the reference frame, solving the dependency of the base in the MDI-QKD protocol. Given that, we propose the OAM-MDI-QKD protocol based on the parametric light sources which mainly include single-photon-added-coherent (SPACS) and heralded single-photon sources (HSPS). Due to the stability of OAM and the participation of parametric light sources, the performance of MDI-QKD protocol gradually approaches the ideal situation. Numerical simulation shows that compared with WCP scheme, HSPS and SPACS schemes have increased the maximum secure transmission distance by 30 km and 40 km respectively.

Keywords: Measurement device independent, orbital angular momentum, parametric light sources, single-photon-added coherent state, heralded single-photon sources.

1 Introduction

Since quantum key distribution (QKD) was proposed by Bennett et al. in 1984 (BB84) [Bennett and Brassard (2014)], many researchers have developed their interest in the study of QKD [Renner (2008); Chan, Lucio-Martínez, Mo et al. (2017); Diamanti, Lo, and Qi (2016); Broadbent and Schaffner (2016)]. QKD can provide unconditional security according to the physical properties of quantum mechanics [Shor and Preskill (2000); Liu, Chen, Liu et al. (2018)]]. In the BB84 protocol, Alice and Bob share the key securely via the classical and quantum channels [Gleim, Egorov, Nazarov et al. (2016); Devetak and Winter (2005); Qu, Zhu, Wang et al. (2018)]. However, due to the limitation of the actual conditions, the security performance and the key rate of the protocol are not ideal. In order to address these problems fundamentally, measurement device independent quantum key distribution (MDI-QKD) [Xu, Curty, Qi et al. (2015)] has been

[1] School of Computer and Information Science, Southwest University, Chongqing, 400715, China.

[2] School of Information Technology, Deakin University, Geelong, VIC, 3220, Australia.

[*] Corresponding Author: Hong Lai. Email: hlai@swu.edu.cn.

Received: 14 May 2019; Accepted: 09 July 2019.

proposed by Xu et al. [Xu, Curty, Qi et al. (2013)]. The MDI-QKD protocol avoids the attacks on the measurement device, because the photons in the MDI-QKD protocol are not sent by one party Alice and received by the other party Bob for measuring. Instead, the measurement device is placed in a third party Charlie, and the photon states prepared by Alice and Bob are sent to Charlie for measuring, then Charlie publishes the measurement results.

In recent years, orbital angular momentum (OAM) [Allen, Beijersbergen and Spreeuw (1992)] has been widely used for QKD researches, and the OAM characteristics of photons have been paid more attention. Generally, the angular momentum of light can be divided into spin angular momentum (SAM) and OAM. SAM is generated by the polarization characteristics of light beams. Polarization is related to the direction of light vectors. OAM is generated by the helical phase structure of the beam. The eigenstates of OAM have a azimuthal $\exp(il\theta)$ proportional to rotation angle θ, since l is an arbitrary integer, OAM has an infinite number of eigenstates. The MDI-QKD protocols reduce the risk of being attacked on the detector sides, but there are still some problems in the photon preparation stages. The most important point is that it relies on the base calibration in the key production process [Tamaki, Lo, Fung et al. (2012)]. In the process of preparation and measurement, photon states of the reference frames need to be detected and adjusted in real time on both sides. At the same time, the polarization states may also drift during the propagation process, which adversely affects the performance of polarization coded MDI-QKD. In this paper, we add OAM to MDI-QKD to make full use of OAM's advantages, including the measurement value of photon's OAM which are not changed when the measured reference frame rotates and high dimension. In the systems that use the OAM, the measurement results do not depend on Alice's and Bob's reference frames, thus the defect of the base dependency is solved. The simulation results show that the OAM-MDI-QKD has a longer maximum transmission distance than polarization-encoded MDI-QKD.

Finally, considering most of the current OAM-MDI-QKD protocols are based on weak coherent photon (WCP) [Yan, Sun and Zhao (2014); Wu, Du, Wang et al. (2016); Zhang, Zhang, Guo et al. (2018)]. WCP is obtained by attenuating laser, but one of its problems is that the photon number distribution follows Poisson distribution, which makes it contain the vacuum state ratio of up to 60%, while the single photon ratio is less than 30%. Since the OAM-MDI-QKD protocol is limited to generate keys at a long distance. In contrast, parametric light sources including single-photon-added coherent state (SPACS) and heralded single-photon sources (HSPS) have better characteristics. SPACS not only has no vacuum state, but also the single photon ratio can reach 90%. SPACS can achieve the effect close to the ideal single photon source (SPS) if it is combined with the decoy state method. HSPS is sub-Poisson distribution light source with a small amount of vacuum states and the single photon ratio can be as high as 73%, which can improve the transmission distance of OAM-MDI-QKD. Therefore, in this paper, we propose an OAM-MDI-QKD protocol based on the parametric light sources, then analyze its key rate and the maximum transmission distance. Next, we compare the OAM-MDI-QKD protocols based on the different light sources. Through the numerical simulation, we conclude that the MDI-QKD protocols encoded by OAM under parametric light source

have a better performance than the protocols under WCP.

This paper is organized as follows. Section 2 mainly introduces the concepts, preparation and characteristics of two kinds of parametric light sources. Section 3 mainly introduces the protocol based on HSPS and present its security analysis. Section 4 describes our protocol that is the OAM-MDI-QKD based on SPACS and HSPS. We analyze the key rate and the maximum transmission distance of the protocol, and compare with the MDI-QKD protocol based on SPACS and HSPS. Section 5 describes the comparison between our protocol and the existing protocols based on WCP, then we compare three different light sources in detail. Finally, we present a summary.

2 Background

As the light sources in QKD, parametric light sources have certain advantages over general attenuation lasers. SPACS is a kind of non-classical state with the number of photon obeys sub-Poisson distribution, which can be obtained by the interaction between parametric down-conversion (PDC) photons and coherent states. In the HSPS, after targeting, the vacuum pulse can be largely eliminated and the single-photon ratio can be increased [Joshi, Farsi, Clemmen et al. (2018)]. The use of these light sources can improve photon utilization rate, thus improving the key rate and the maximum safe distance. In this section, we firstly introduce the concept and characteristics of SPACS light source, and then introduce the preparation and characteristics of HSPS.

2.1 Single-photon-added coherent state source

In 1991, Agarwal and Tara jointly proposed a protocol about photon-added coherent state $|\alpha, m\rangle$ also known as the excited coherent state [Dodonov, Marchiolli, Korennoy et al. (1998)]. It is the result of continuously increasing excitation of a single-photon by a classical coherent field. It can be obtained by continuously acting on the coherent state for *m* photon creation operators [Agarwal and Tara (1991)]. Its definition is as follow:

$$|\alpha, m\rangle = k_{\alpha,m}\hat{\alpha}^{\dagger m}|\alpha\rangle \tag{1}$$

where $|\alpha\rangle$ denotes the coherent state, and $\alpha^{\dagger}$ denotes the photon creation operator, $k_{\alpha,m} = [m!L_m(-|\alpha|^2)]^{-1/2}$ is the normalization factor. $L_m(x)$ is an m-order Laguerre polynomial and *m* is an integer. The properties of SPACS lie between the Fock states and the coherent states, so it shows some non-classical characteristics. If only one photon creation operator operation is performed on the coherent states, we can obtain SPACS [Zavatta, Viciani and Bellini (2004)]. SPACS can be defined as:

$$|\alpha, 1\rangle = \frac{\hat{a}^{\dagger}|\alpha\rangle}{\sqrt{1+|\alpha|^2}} \tag{2}$$

Coherent states are expanded by the Fock states as follow [Hofheinz, Weig, Ansmann et al. (2008)]:

$$|\alpha\rangle = e^{\frac{-|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{a^n}{\sqrt{n!}} |n\rangle \tag{3}$$

According to the commutation relation, the annihilation operator $\hat{a}$ and the creation operator $\hat{a}^{\dagger}$ can be used as ascending and descending operators of $|n\rangle$ as follows [Hofheinz, Weig, Ansmann et al. (2008)]:

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle, \hat{a}^{\dagger}|n\rangle = \sqrt{n+1}|n+1\rangle \tag{4}$$

Substituting Eqs. (3) and (4) into Eq. (2) to obtain

$$|\alpha,1\rangle = \frac{e^{\frac{-|\alpha|^2}{2}}}{1+\sqrt{|\alpha|^2}} \sum_{n=0}^{\infty} \frac{a^n}{\sqrt{n!}} \sqrt{n+1}|n+1\rangle \tag{5}$$

From Eq. (5), it can be seen that there is no contribution of vacuum term in SPACS, that is, SPACS has no vacuum state, and its density matrix can be obtained accordingly, thus obtaining the photon number distribution of SPACS [Wang, Li, Zhu et al. (2014)] as follow:

$$P_n = \frac{e^{-|\alpha|^2} |\alpha|^{2(n-1)} n}{(1+|\alpha|^2)(n-1)!}, n \geq 1 \tag{6}$$

2.2 Heralded single-photon sources

HSPS can generate photon pairs in the nonlinear optical process, such as spontaneous parametric down-conversion (SPDC) and spontaneous four-wave mixing. Here, we take the SPDC as an example to illustrate the principle of HSPS [Sun, Zhao and Dong (2016)].

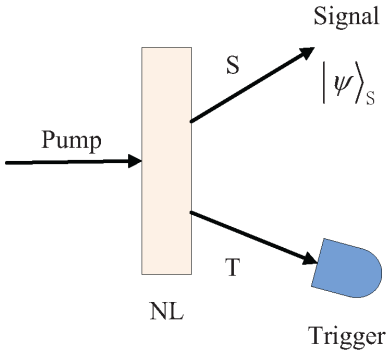


Figure 1: HSPS generation principle

As shown in Fig. 1, a pump photon is incident on a nonlinear crystal to generate two photons, a signal photon and an idle photon. Since this process is energy conservation and momentum conservation, the signal photon and idle photon are interrelated in energy, excitation time, momentum and polarization. At this time, we add a detector at the end of the idle photon. When Bob detects the idle photons, we can obtain the information of the signal photons through the correlation between the two photons. For example, when the

detector responds, it means that the signal photon exits. Thus, after marking the signal photon with the idle photon, a small proportion of vacuum states and a high proportion of single photons are generated.

According to the HSPS preparation process mentioned above, a dual-mode optical field is obtained as follow:

$$|\psi\rangle_{IS} = \sum_{n=0}^{\infty} \sqrt{P_n} \, |n\rangle_I \, |n\rangle_S \tag{7}$$

In HSPS, the signal mode (S mode) and the idle mode (I mode) have the same photon number distribution, and the relationship between the detector's time window δt_a and photon coherence time δt_c determines which distribution it is specifically subject to. When $\delta t_a \ll \delta t_c$, the photon number obeys the Thermal distribution, and when $\delta t_a \gg \delta t_c$, it obeys Poisson distribution. The photon number distributions are as follows respectively [Wang and Karlsson (2007)]:

$$P_n(x) = \frac{x^n}{(1+x)^{n+1}}, (\delta t_a \ll \delta t_c) \tag{8}$$

$$P_n(x) = e^{-x} \frac{x^n}{n!}, (\delta t_a \gg \delta t_c) \tag{9}$$

where x denotes the average photon number. Because the Poisson distribution has a higher single photon ratio than the specific heat distribution [Wang and Karlsson (2007)], we only study the case that obeys the Poisson distribution.

3 OAM-MDI-QKD protocol based on weak coherent photon

In the theoretical researches, most of the QKD protocols are under the ideal SPS. However, in reality, it is difficult to prepare ideal single photons, so researchers find WCP to replace SPS. When using this kind of non-ideal single photon sources, the case of multi-photon occurs [Chen, Yao, Yang et al. (2008)]. In order to solve the multi-photon problem, researchers put forward the decoy states [Ma, Qi, Zhao et al. (2005)]. This section introduces the OAM-MDI-QKD protocol based on the decoy states and WCP, then presents the security analyze.

3.1 Introduction of OAM-MDI-QKD protocol under WCP

WCP is a light source with poor temporal coherence and spatial coherence. It consists of a standard semiconductor laser and a calibrated optical attenuator. The equipment is simple and easy to implement. The photons generated by WCP obey the photon Poisson distribution as follow [Zhou and Zhou (2011)]:

$$P(n,u) = e^{-u} \frac{u^n}{n!} \tag{10}$$

where u represents the average photon number of the pulse, and n represents the photon number. When the WCP is adopted, two problems may be brought about, namely, the vacuum pulse leads to the reduction of counting rate and the multi-photon pulse leads to the PNS attack [Wang, Peng, Zhang et al. (2008); Zhao, Qi and Lo (2008); Peng, Jiang, Xu et al. (2008)]. The former can be compensated by using the modulation speed of the laser, while the latter can be solved by using the decoy technology.

Decoy state technology was firstly proposed by Lo et al. in 2005 [Ma, Qi, Lo et al. (2005)], and then it gradually developed into an important technology in QKD protocol under the research of Hoi-Kwang Lo's group. The idea of decoy state technology can be roughly described as: Alice prepares a series of signal states and decoy states with different photon numbers. The other characteristics of the two states are the same, such as wavelength, timing sequence and other information. For eavesdropper Eve, all she can obtain is the average photon number, which means that she can only rely on the distribution of the photon numbers. When Eve eavesdrops, she cannot be sure whether she obtains a signal state or a decoy state. When eavesdropping exists, the photon number distributions are affected, and the qubit error rate is only related to the photon number n, thus causing the qubit error rate to deviate from the expected threshold value, so the eavesdropping behavior is revealed. The core idea of decoy states can be summarized as follows [Zhao, Lo, Ma et al. (2007)]:

$$Y_n(signal) = Y_n(decoy) = Y_n \tag{11}$$

$$e_n(signal) = e_n(decoy) = e_n \tag{12}$$

Next, we learn from the literature [Yan, Zhao and Sun (2014)] that the protocol of WCP light source applied to MDI-QKD based on the OAM is shown in Fig. 2. In this protocol, Alice and Bob design two groups of mutually unbiased bases B_1 and B_2 based on the OAM states, namely [Bartkiewicz, Černoch, Lemr et al. (2015)]

$$B_1 = \{|l\rangle, |-l\rangle\} \tag{13}$$

$$B_2 = \{\frac{|l\rangle + |-l\rangle}{\sqrt{2}}, \frac{|l\rangle - |-l\rangle}{\sqrt{2}}\} \tag{14}$$

When detectors A and B respond at the same time, it indicates that Alice and Bob have chosen the same base, therefore, the results are correct and useful. These data can be kept as the raw key, and the final security key can be obtained after the process of data reconciliation and privacy amplification. However, when Alice and Bob choose different bases, the detection results are discarded.

In Fig. 2, the OAM states with different l values are prepared by a spatial light modulator (SLM), decoy states are prepared by a light intensity modulator (Decoy-IM), and are sent to Charlie, where photons enter a high-efficiency OAM state separation device through a beam splitter (BS) and finally reach a detector.

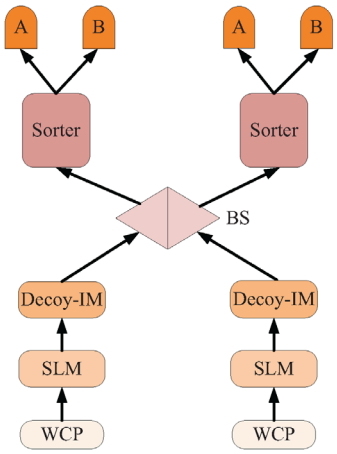


Figure 2: OAM-MDI-QKD based on decoy state under WCP

3.2 Security analysis

We perform the security analysis of our protocol which is based on the decoy state technology and OAM [Wang, Zhao, Gong et al. (2015)], following the GLLP principle, and we can obtain the key rate formula:

$$R = Q_{B_1}^{11}[1 - H(e_{B_2}^{11})] - Q_{B_1} f(E_{B_1}) H(E_{B_1}) \tag{15}$$

$$Q_{B_1}^{11} = u_A u_B e^{-(u_A + u_B)} Y_{B_1}^{11} \tag{16}$$

where $H(e_{B_2}^{11})$ is the process of privacy amplification, the latter half of the Eq. (15) indicates the data reconciliation and error correction process, f function is the efficiency of data reconciliation, and $H(x)$ is the Shannon entropy function. The $Q_{B_1}^{11}$ is the gain for Alice and Bob to select B_1 base and both send single photon states, $e_{B_2}^{11}$ is the quantum bit error rate when B_2 base is selected. The specific safety analysis under WCP has been implemented in Yan et al. [Yan, Zhao and Sun (2014)].

4 Our protocols

This section mainly introduces the MDI-QKD protocol based on OAM under SPACS and HSPS light sources. The protocol is combined with the decoy state technology, we can obtain the secure key rate of the OAM-MDI-QKD protocol. The key rate of MDI-QKD protocol with polarization coding and OAM-MDI-QKD protocol under the SPACS and HSPS light sources are simulated respectively, then we compare and analyze the characteristics and advantages of the OAM-MDI-QKD protocols based on SPACS and HSPS.

4.1 OAM-MDI-QKD protocol based on the SPACS with decoy states

It is known from Section 3.1 that when the initial coherent state intensity is small, SPACS theoretically has a high single photon ratio and has no vacuum state [Zhu, Wang, Liu et al. (2018)]. From Section 3, it can be seen that the key rate and the security are improved when we use the decoy technology in our OAM-MDI-QKD protocol which is based on the WCP source. Of course, when we use the SPACS light source, using decoy technology can also bring good effect. Therefore, we introduce the OAM into the MDI-QKD protocol based on SPACS light source to obtain the OAM-MDI-QKD protocol in two-intensity decoy states based on SPACS light source. The device diagram of the protocol is shown in Fig. 3.

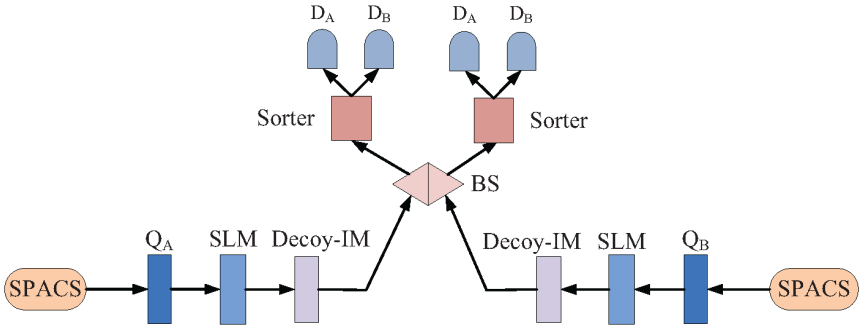


Figure 3: OAM-MDI-QKD based on SPACS

In Fig. 3, Q_A and Q_B denote the SPACS photons which are randomly prepared by Alice and Bob respectively. SLM represents a spatial light modulator, which are used to prepare OAM photons with different l values. Decoy-IM is an intensity modulator. BS stands for a beam splitter. Sorter is an efficient device for separating OAM states. It can separate two photons with different OAM values at the same time. In the measuring device, photons reach BS at the same time and pass through the Sorter to obtain the photons with different l values. We stipulate that detector A is placed at the exit position of $-lh$ photon and detector B is placed at the exit position of lh photon, so that when photons with different l values exit, different detectors respond. The flow chart of our OAM-MDI-QKD protocol based on the SPACS in Fig. 4.

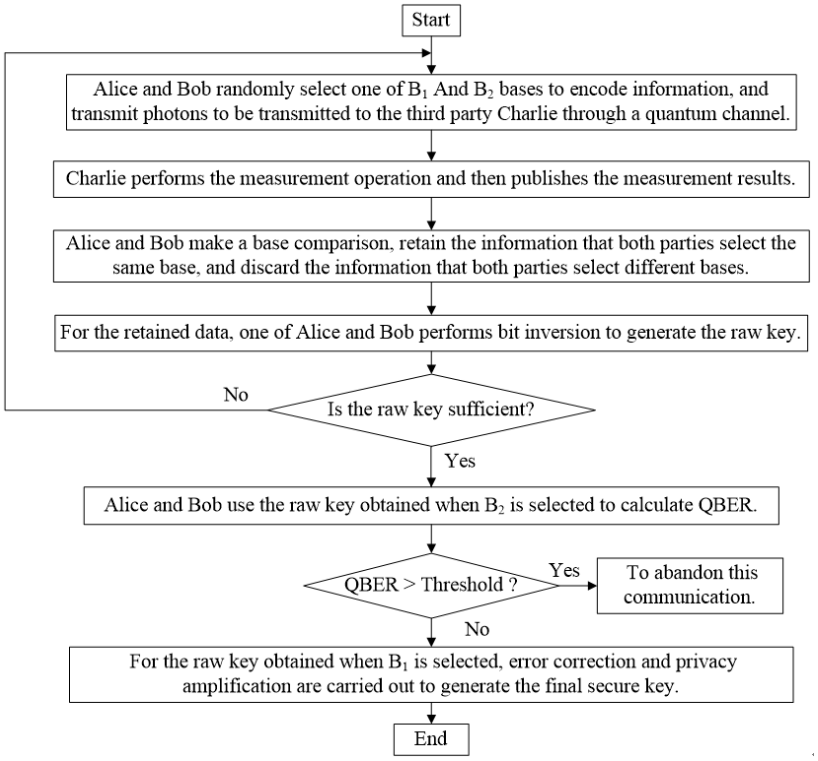


Figure 4: The flow chart of our OAM-MDI-QKD protocol based on the SPACS

4.2 Security analysis of two-intensity decoy OAM-MDI-QKD protocol based on SPACS

In this protocol, Alice and Bob send the photons to Charlie and project them onto a Bell state. When D_A and D_B respond simultaneously, which is regarded as a successful response. Then Charlie announces the successful events so that Alice and Bob can further generate the security key. In this protocol, Alice (Bob) randomly prepares two photon states with different intensities, namely, signal state $u_A(u_B)$ and decoy state $v_A(v_B)$. Let $u_A = u_B = u$, $v_A = v_B = v$, satisfying $u > v > 1$, we define Alice's and Bob's usage intensity as x and y respectively. When Alice and Bob send the photons with different intensities of x and y respectively, the total gain and QBER can be expressed as follows [Yin, Fung, Ma et al. (2013)]:

$$G_B^{xy} = \sum_{n,m=1}^{\infty} P_n(x) P_m(y) Y_B^{n,m} \tag{17}$$

$$E_B^{xy} G_B^{xy} = \sum_{n,m=1}^{\infty} P_n(x) P_m(y) e_B^{x,y} Y_B^{n,m} \tag{18}$$

where B represents B_1 or B_2, n and m represent the photon numbers sent by Alice and Bob respectively, $P_n(\cdot)$ represents the photon number distribution when different intensities are selected, $e_B^{x,y}$ and $Y_B^{x,y}$ represent the QBER and detector response rate when Alice and Bob send n and m photons to Charlie simultaneously under B respectively. To make the calculation easier, we omit the base B for calculation and use $G^{u,u}$ and $G^{v,v}$ to estimate the lower bound of Y^{11}.

According to Eq. (17), $G^{u,u}$ is expanded as follow:

$$\begin{aligned} G^{u,u} &= P_1^2(u)Y^{11} + P_1(u)\sum_{m=2}^{\infty} P_m(u)Y^{1m} \\ &+P_1(u)\sum_{n=2}^{\infty} P_n(u)Y^{n1} + \sum_{n,m=2}^{\infty} P_n(u)P_m(u)Y^{nm}. \end{aligned} \tag{19}$$

Similarly, by expanding $G^{v,v}$, we can obtain:

$$\begin{aligned} G^{v,v} &= P_1^2(v)Y^{11} + P_1(v)\sum_{m=2}^{\infty} P_m(v)Y^{1m} \\ &+P_1(v)\sum_{n=2}^{\infty} P_n(v)Y^{n1} + \sum_{n,m=2}^{\infty} P_n(v)P_m(v)Y^{nm}. \end{aligned} \tag{20}$$

According to the important conditions of decoy states:

$$\frac{P_n(u)}{P_n(v)} \geq \frac{P_2(u)}{P_2(v)} \geq \frac{P_1(u)}{P_1(v)} \tag{21}$$

In this paper, let $h = \frac{P_1(u)P_2(u)}{P_1(v)P_2(v)}$, from Eq. (20)$\times h -$ Eq. (19), the following results are obtained:

$$Y^{11} = \frac{hG^{v,v} - G^{u,u} + \tau}{hP_1^2(v) - P_1^2(u)} \tag{22}$$

where

$$\begin{aligned} \tau &= \sum_{m=2}^{\infty}[P_1(u)P_m(u) - hP_1(v)P_m(v)]Y^{1m} \\ &+\sum_{n=2}^{\infty}[P_1(u)P_n(u) - hP_1(v)P_n(v)]Y^{1n} \\ &+ \sum_{n,m=2}^{\infty}[P_n(u)P_m(u) - hP_n(v)P_m(v)]Y^{nm} \end{aligned} \tag{23}$$

According to Eq. (22), we can obtain:

$$hP_1^2(v) - P_1^2(u) \geq 0 \tag{24}$$

At the same time, $\tau \geq 0$ can also be obtained.

Since B_1 is used to generate the key and B_2 is used to detect and estimate the error rate, we first calculate the detector response rate under B_1 as follow:

$$\begin{aligned} Y_{B_1}^{11} &\geq \frac{hG_{B_1}^{v,v} - G_{B_1}^{u,u}}{hP_1^2(v) - P_1^2(u)} \\ &= \frac{P_1(u)P_2(u)G_{B_1}^{v,v} - P_1(v)P_2(v)G_{B_1}^{u,u}}{P_1(u)P_1(v)[P_1(v)P_2(u) - P_1(u)P_2(v)]} \end{aligned} \tag{25}$$

By the same token, we calculate the bit error rate under B_2, which can be seen from the expansion of Eq. (18) under B_2,

$$\begin{aligned} E_{B_2}^{v,v}G_{B_2}^{v,v} &= \sum_{n,m=1}^{\infty} P_n(v)P_m(v)e_{B_2}^{n,m}Y_{B_2}^{nm} \\ &= P_1^2(v)Y_{B_2}^{11}e_{B_2}^{11} + d \\ &\geq P_1^2(v)Y_{B_2}^{11}e_{B_2}^{11}. \end{aligned} \tag{26}$$

Therefore, the upper bound of the available key bit error rate is

$$e_{B_2}^{11} \leq \frac{E_{B_2}^{v,v}G_{B_2}^{v,v}}{P_1^2(v)Y_{B_2}^{11}e_{B_2}^{11}} \tag{27}$$

From the analogy of the key rate formula mentioned in Section 3, it can be seen that:

$$R \geq -G_{B_1}^{u,u} fH(E_{B_1}^{u,u}) + P_1^2(u)Y_{B_2}^{11}[1 - H(e_{B_2})] \tag{28}$$

where f is the key agreement coefficient and $H(x)$ is the binary information entropy.

According to the above analysis of OAM-MDI-QKD based on SPACS light source and comparison with MDI-QKD based on polarization in Jiang et al. [Jiang, Yu and Wang (2016)], we conduct a numerical simulation, and the results are shown in Fig. 5.

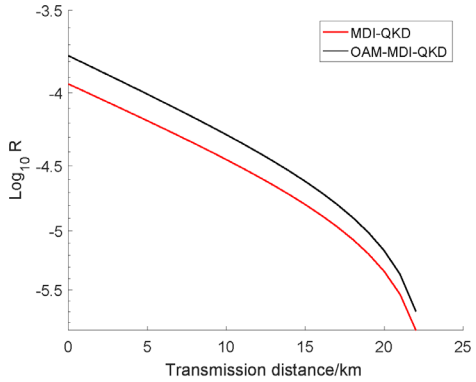


Figure 5: Comparison of the MDI-QKD protocol with or without OAM based on SPACS

In Fig. 5, it shows that the MDI-QKD protocol comparison with or without OAM based on SPACS. It can be seen that the key rate of OAM-MDI-QKD protocol is higher than of MDI-QKD, which indicates that the introduction of OAM increases the key rate and the transmission distance compared with traditional MDI-QKD.

4.3 HSPS-based OAM-MDI-QKD protocol and security analysis

When using coherent states, if the transmission distance exceeds 100 km, the influence of dark counting becomes very significant, so we need to use HSPS to reduce the influence of dark counting [Zhang, Zhang, Guo et al. (2018)]. Therefore, this section analyzes the security of MDI-QKD protocol based on OAM and HSPS. From the understanding of HSPS, we know that the photon numbers are highly correlated, and the targeting of HSPS can be realized through this characteristic. Similarly we use decoy states technology to improve the gain and bit error rate of the single photon signal states of the protocol. The device diagram of our OAM-MDI-QKD with HSPS and decoy state technology is shown in Fig. 6.

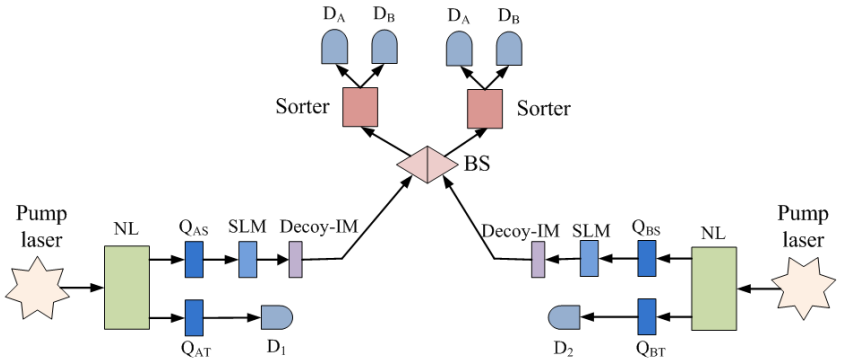


Figure 6: OAM-MDI-QKD protocol under HSPS light source

In Fig. 6, Alice uses pump laser to generate signal photon Q_{AS} and idle photon Q_{AT} through non-linear crystal. The D_1 is used to detect Q_{AT}. At the same time, the signal photon Q_{AS} exits the beam splitter (BS) through the spatial light modulator (SLM) and the intensity modulator (IM), and then passes through the OAM efficient separation device (Sorter) to reach the detectors D_A and D_B. Bob operates the same way with Alice. The specific protocol flow is similar to Fig. 4 and will not be repeated here.

Next, we estimate the single photon key rate Y^{11} and key bit error rate e^{11} of OAM-MDI-QKD protocol when the labeled single photon source obeys Poisson distribution.

$$k_0 = d \tag{29}$$

$$k_n = 1-(1-d)(1-\gamma) \tag{30}$$

where d indicates the detection efficiency, γ indicates the dark count, and k_n indicates the response efficiency of Alice and Bob detectors when sending n photons.

Then we use $Y_{m,n}^{B}$, $G_{m,n}^{B}$, $E_{m,n}^{B}$ to express the key rate, key gain and QBER respectively. Then, m and n represent the number of photons sent by Alice and Bob respectively. Similarly, B_1 is used to generate the key and B_2 is used to detect the bit error rate. In this protocol, Alice (Bob) randomly prepares two photon states with different intensities, namely, signal state $u_A(u_B)$ and decoy state $v_A(v_B)$. Assume that $u_A = u_B = u$, $v_A = v_B = v$, the density matrix can be expressed as follow:

$$\begin{aligned}\rho_{xy} &= (\sum_{n=0}^{\infty} k_n P_n(x) \mid n\rangle\langle n \mid) \otimes (\sum_{n=0}^{\infty} k_n P_n(y) \mid n\rangle\langle n \mid) \\ &= (\sum_{n=0}^{\infty} k_n e^{-x} \frac{x^n}{n!} \mid n\rangle\langle n \mid) \otimes (\sum_{n=0}^{\infty} k_n e^{-y} \frac{y^n}{n!} \mid n\rangle\langle n \mid).\end{aligned} \tag{31}$$

According to the Eqs. (32) and (33) of key gain and key bit error rate:

$$G_{x,y}^{B} = \sum_{n,m=1}^{\infty} P_n(x) P_m(y) Y_{nm}^{B} \tag{32}$$

$$E_{x,y}^{B} G_{x,y}^{B} = \sum_{n,m=1}^{\infty} P_n(x) P_m(y) e_{x,y}^{B} Y_{nm}^{B} \tag{33}$$

We can obtain

$$\begin{aligned}G_{x,y} &= G'_{0,0} + \gamma_A \gamma_B x e^{-x} y e^{-y} Y_{11} \\ &+ \gamma_A x e^{-x} \sum_{n=2}^{\infty} [1-(1-\gamma_B)^n] e^{-y} \frac{y}{n!} Y_{1n} \\ &+ \gamma_B y e^{-y} \sum_{m=2}^{\infty} [1-(1-\gamma_A)^n] e^{-x} \frac{x}{m!} Y_{m1} \\ &+ \sum_{n,m=2}^{\infty} e^{-x} \frac{x}{m!} Y_{m1} e^{-y} \frac{y}{n!} Y_{1n} [1-(1-\gamma_A)^n][1-(1-\gamma_B)^n] Y_{m,n}\end{aligned} \tag{34}$$

where $G_{0,0}^{'} = G_{x,0} + G_{0,y} - G_{0,0}$.

Using $G_{u,u}$ and $G_{v,v}$ to estimate Y_{11}:

$$
\begin{aligned}
G_{u,u} &= G'_{0,0} + \gamma_A \gamma_B u e^{-u} u e^{-u} Y_{11} \\
&+ \gamma_A u e^{-u} \sum_{n=2}^{\infty} [1-(1-\gamma_B)^n] e^{-u} \frac{u}{n!} Y_{1n} \\
&+ \gamma_B u e^{-u} \sum_{m=2}^{\infty} [1-(1-\gamma_A)^n] e^{-u} \frac{u}{m!} Y_{m1} \\
&+ \sum_{n,m=2}^{\infty} e^{-u} \frac{u}{m!} Y_{m1} e^{-u} \frac{u}{n!} Y_{1n} [1-(1-\gamma_A)^n][1-(1-\gamma_B)^n] Y_{m,n}
\end{aligned} \tag{35}
$$

Similarly,

$$
\begin{aligned}
G_{v,v} &= G'_{0,0} + \gamma_A \gamma_B v e^{-v} v e^{-v} Y_{11} \\
&+ \gamma_A v e^{-v} \sum_{n=2}^{\infty} [1-(1-\gamma_B)^n] e^{-v} \frac{v}{n!} Y_{1n} \\
&+ \gamma_B v e^{-v} \sum_{m=2}^{\infty} [1-(1-\gamma_A)^n] e^{-v} \frac{v}{m!} Y_{m1} \\
&+ \sum_{n,m=2}^{\infty} e^{-v} \frac{v}{m!} Y_{m1} e^{-v} \frac{v}{n!} Y_{1n} [1-(1-\gamma_A)^n][1-(1-\gamma_B)^n] Y_{m,n}
\end{aligned} \tag{36}
$$

Let $k = \frac{(1-\gamma_A)(1-\gamma_B)^2}{\gamma_A[1-(1-\gamma_B)^2]} (\frac{u}{v})^3 e^{2v-2u}$ and obtain Y_{11} through Eq. (35) $\times h$ - (36):

$$
Y_{11} = \frac{h(G_{v,v} - G'_{0,0}) - (G_{u,u} - G'_{0,0}) + \tau}{h\gamma_A \gamma_B v^2 e^{-2v} - (1-\gamma_A)(1-\gamma_B)^2 u^2 e^{-2u}} \tag{37}
$$

It is easy to prove the following inequality:

$$
\frac{\tau}{h\gamma_A \gamma_B v^2 e^{-2v} - (1-\gamma_A)(1-\gamma_B)^2 u^2 e^{-2u}} \geq 0 \tag{38}
$$

By the same token, we can obtain:

$$
e_{11}^{B_2} \leq \frac{E_{v,v}^{B_2} G_{v,v}^{B_2} - E_{v,0}^{B_2} G_{v,0}^{B_2} - E_{0,v}^{B_2} G_{0,v}^{B_2} + E_{0,0}^{B_2} G_{0,0}^{B_2}}{G_{11}^{B_2}} \tag{39}
$$

Finally, according to the key rate formula of OAM-MDI-QKD, the key rate of HSPS light source under Poisson distribution is obtained as follows:

$$
R \geq \gamma_A \gamma_B u^2 e^{-2u} Y_{11}^{B_1} [1 - H(e_{11}^{B_2})] - G_{u,u}^{B_1} f(E_{u,u}^{B_1}) H(E_{u,u}^{B_1}) \tag{40}
$$

Based on the above analysis, similarly, we compare the MDI-QKD with and without OAM under HSPS light source and obtain results shown in Fig. 7 through numerical simulations. As seen from Fig. 7, the black curve is higher than the red curve, which indicates that the introduction of OAM not only improves the key rate of MDI-QKD protocol, but also increases the transmission distance under HSPS light source.

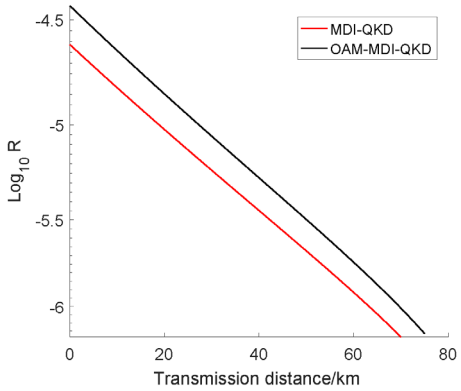


Figure 7: The comparison of MDI-QKD protocols with or without OAM under HSPS

4.4 Protocol comparisons

In the fourth section, we can know that the probability of producing single-photon and multi-photon of SPACS can be calculated when $u = 1.10$. As shown in Tab. 1, as a comparison, we give the probability of the vacuum state, the single-photon and the multi-photon using WCP and HSPS light source when the average photon number is 0.5 [Sun, Zhao and Dong (2016)]. Tab. 1 shows the probability of producing single-photon and multi-photon in SPACS, WCP and HSPS light sources. The average photon number of SPACS is 1.10, the average photon number of WCP and HSPS is 0.5, the dark count of HSPS labeled detector is 10^{-6}, and the detection efficiency is 0.75.

Table 1: Probability of single-photon and multi-photon in SPACS, WCP and HSPS

Sources	SPACS	WCP	HSPS
vacuum	0	0.60653	1.94×10^{-6}
Single-photon	0.90593	0.30326	0.72735
Multi-photon	0.09407	0.09024	0.27265
$g^2(0)$	0.16808	1	0.43634

The MDI-QKD protocol under SPACS and HSPS light source is introduced in detail in document [Zhang, Zhang, Guo et al. (2018)] and document [Jiang, Yu and Wang (2016)] and its safety is analyzed. In this paper, we use the OAM and analyze the OAM-MDI-QKD protocol under these two different parametric light sources, and then compare them with MDI-QKD based on polarization. Finally, we compare OAM-MDI-QKD under the parametric light sources with the OAM-MDI-QKD based on WCP in the reference [Yan, Zhao and Sun (2014)]. Because the parametric light sources have a lower dark count rate and the probability of producing the vacuum state, the single-photon ratio in the protocol is increased. We compare the simulation result of the three light sources under the same parameter conditions as shown in Figs. 8 (a) and 8(b), and the parameters are shown in Tab. 2. In Fig. 8(a), it shows the single photon counting rate of three different light

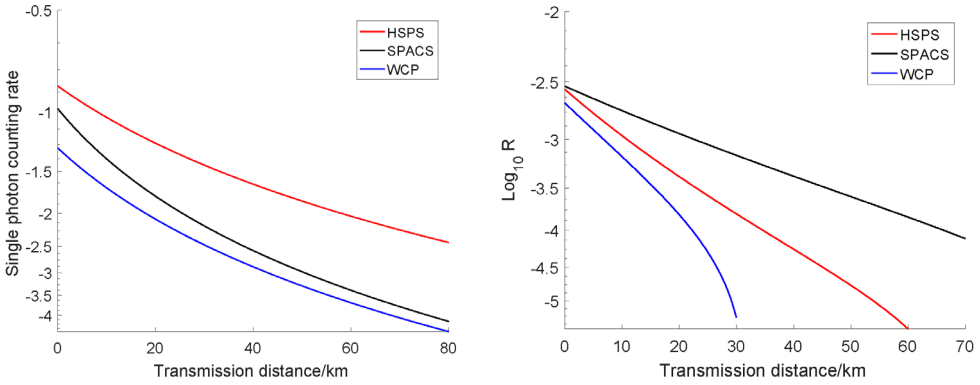
sources under the same parameters. The higher the single photon counting rate, the higher the key rate is, thus achieving the goal of saving resources such as human and material resources. As can be seen from Fig. 8(a), the single photon counting rate of parametric light sources HSPS and SPACS are higher than that of WCP. Among them, HSPS is the best one. The Fig. 8(b) shows the key rate and transmission distance of three different light sources under the same parameters. We can see that the transmission distance of OAM-MDI-QKD protocol based on parametric light source is at least double that of WCP, and HSPS has the longest transmission distance.

Table 2: Simulation parameters

Parameters	u	f	d_B	v	η_{Bob}
values	0.1	1	2×10^{-6}	0.01	0.145

5 Conclusion

In this paper, we have introduced OAM-MDI-QKD protocol based on two kinds of parametric light sources, and carried out safety analysis and numerical simulation, then compared them with the OAM-MDI-QKD protocol based on WCP respectively. The simulation results show that the OAM-MDI-QKD protocol based on the parametric light sources has a higher photon utilization rate and longer transmission distance than the protocol based on the WCP light source. Among them, SPACS light source has obvious advantages over the other two kinds of light sources in terms of key rate and transmission distance. Accumulating keys requires relatively shorter time and can be realized under the existing technical conditions. Therefore, we think SPACS is very promising for the OAM-MDI-QKD protocol in the future with the miniaturization and maturity of the light source.



(a) (b)

Figure 8: (a) Single-photon counting rate of the protocol under different light sources. (b) Comparison simulation results of three different light sources

Acknowledgement: Hong Lai has been supported by the National Natural Science Foundation of China (No. 61702427) and the Chongqing innovation project (No. cx2018076), the Fundamental Research Funds for the Central Universities

(XDJK2018C048), and the financial support in part by the 1000-Plan of Chongqing by Southwest University (No. SWU116007).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Agarwal, G. S.; Tara, K. (1991): Nonclassical properties of states generated by the excitations on a coherent state. *Physical Review A*, vol. 43, no. 1, pp. 492-497.

Allen, L.; Beijersbergen, M. W.; Spreeuw, R. J. C.; Woerdman, J. P. (1992): Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes. *Physical Review A*, vol. 45, no. 11, pp. 8185-8189.

Bartkiewicz, K.; Černoch, A.; Lemr, K.; Miranowicz, A.; Nori, F. (2015): Experimental temporal steering and security of quantum key distribution with mutually-unbiased bases. *Physical Review A*, vol. 93, no. 6, 062345.

Bennett, C. H.; Brassard, G. (2014): Quantum cryptography: public key distribution and coin tossing. *Theoretical Computer Science*, vol. 560, pp. 7-11.

Broadbent, A.; Schaffner, C. (2016): Quantum cryptography beyond quantum key distribution. *Designs Codes and Cryptography*, vol. 78, no. 1, pp. 351-382.

Chan, P.; Lucio-Martínez, I.; Mo, X.; Tittel, W. (2017): Quantum key distribution. *III-Vs Review*, vol. 17, no. 5, pp. 24.

Chen, Y.; Yao, Z.; Yang, H.; Deng, K. (2008): The secure transmission criterion of practical polarization coding QKD systems under PNS attacks. *Proceedings of SPIE-the International Society for Optical Engineering*, vol. 7137, 71372Z.

Devetak, I.; Winter, A. (2005): Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 461, no. 2053, pp. 207-235.

Diamanti, E.; Lo, H. K.; Qi, B. (2016): Practical challenges in quantum key distribution. *NPJ Quantum Information*, vol. 2, no. 16025.

Dodonov, V. V.; Marchiolli, M. A.; Korennoy, Y. A.; Man'ko, V. I.; Moukhin, Y. A. (1998): Parametric excitation of photon-added coherent states. *Physica Scripta*, vol. 58, no. 5, pp. 469-480.

Gleim, A. V.; Egorov, V. I.; Nazarov, Y. V.; Smirnov, S. V.; Chistyakov, V. V. et al. (2016): Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference. *Optics Express*, vol. 24, no. 3, pp. 2619.

Hofheinz, M.; Weig, E. M.; Ansmann, M.; Bialczak, R. C.; Lucero, E. et al. (2008): Generation of Fock states in a superconducting quantum circuit. *Nature*, vol. 454, no. 7202, pp. 310-314.

Jiang, C.; Yu, Z. W.; Wang, X. B. (2016): Measurement-device-independent quantum key distribution with source state errors in photon number space. *Physical Review A*, vol. 94, no. 6, 062323.

Joshi, C.; Farsi, A.; Clemmen, S.; Ramelow, S.; Gaeta, A. L. (2018): Frequency multiplexing for quasi-deterministic heralded single-photon sources. *Nature Communications*, vol. 9, no. 1, pp. 847.

Liu, W.; Chen, Z.; Liu, J.; Su, Z.; Chi, L. (2018): Full-Blind Delegating Private Quantum Computation. *Computer, Materials & Continua*, vol. 56, no. 2, pp. 211-223.

Long, Y.; Hao, S.; Zhao, S. M. (2014): Study on decoyed measurement device independent quantum key distribution protocol using orbital angular momentum. *Journal of Signal Processing*.

Ma, X. F.; Qi, B.; Zhao, Y.; Lo, H. K. (2005): Practical decoy state for quantum key distribution. *Physical Review A*, vol. 72, no. 1, 012326.

Peng, X.; Jiang, H.; Xu, B.; Ma, X. F.; Guo, H. (2008): Experimental quantum-key distribution with an untrusted source. *Optics Letters*, vol. 33, no. 18, pp. 2077-2079.

Qu, Z.; Zhu, T.; Wang, J.; Wang, X. (2018): A novel quantum stegonagraphy based on brown states. *Computers, Materials & Continua*, vol. 56, no. 1, pp. 47-59.

Renner, R. (2008): Security of quantum key distribution. *International Journal of Quantum Information*, vol. 6, no. 1, pp. 1-127.

Shor, P. W.; Preskill, J. (2000): Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, vol. 85, no. 2, pp. 441-444.

Sun, Y.; Zhao, S. H.; Dong, C. (2016): Memory-assisted measurement device-independent quantum key distribution with parametric down-conversion sources. *Journal of Modern Optics*, vol. 1-6.

Tamaki, K.; Lo, H. K.; Fung, C. H. F.; Qi, B. (2012): Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw. *Physical Review A*, vol. 85, no. 4, 042307.

Wang, D.; Li, M.; Zhu, F.; Yin, Z. Q.; Chen, W. et al. (2014): Quantum key distribution with the single-photon-added coherent source. *Physical Review A*, vol. 90, no. 6, 062315.

Wang, L.; Zhao, S. M.; Gong, L. Y.; Chen, W. W. (2015): Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum. *Chinese Physics B*, vol. 24, no. 12, 238-245.

Wang, Q.; Karlsson, A. (2007): Performance enhancement of a decoy-state quantum key distribution using a conditionally prepared down-conversion source in the Poisson distribution. *Physical Review A*, vol. 76, no. 1, 014309.

Wang, X. B.; Peng, C. Z.; Zhang, J.; Yang, L.; Pan, J. W. (2008): General theory of decoy-state quantum cryptography with source errors. *Physical Review A*, vol. 77, no. 4, pp. 1912-1917.

Wu, C. F.; Du, Y. N.; Wang, J. D.; Wei, Z. J.; Qin, X. J. et al. (2016): Analysis on performance optimization in measurement-device-independent quantum key distribution using weak coherent states. *Acta Physica Sinica*, vol. 65, no. 10.

Xu, F.; Curty, M.; Qi, B.; Lo, H. K. (2013): Practical aspects of measurement-device-independent quantum key distribution. *New Journal of Physics*, vol. 15, no. 11.

Xu, F.; Curty, M.; Qi, B.; Lo, H. K. (2015): Measurement-device-independent

quantum cryptography. *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 148-158.

Yan, L.; Sun, H.; Zhao, S. M. (2014): Study on decoyed measurement device independent quantum key distribution protocol using orbital angular momentum. *Journal of Signal Processing*, vol. 30, no. 11.

Yin, Z. Q.; Fung, C. H. F.; Ma, X.; Zhang, C. M.; Li, H. W. et al. (2013): Measurement-device-independent quantum key distribution with uncharacterized qubit sources. *Physical Review A*, vol. 88, no. 6, 062322.

Zavatta, A.; Viciani, S.; Bellini, M. (2004): Quantum-to-classical transition with single-photon-added coherent states of light. *Science*, vol. 306, no. 5696, pp. 660-662.

Zhang, C. H.; Zhang, C. M.; Guo, G. C.; Wang, Q. (2018): Biased three-intensity decoy-state scheme on the measurement-device-independent quantum key distribution using heralded single-photon sources. *Optics Express*, vol. 26, no. 4, pp. 4219-4229.

Zhang, C. H.; Zhang, C. M.; Guo, G. C.; Wang, Q. (2018): Biased three-intensity decoy-state scheme on the measurement-device-independent quantum key distribution using heralded single-photon sources. *Optics Express*, vol. 26, no. 4, pp. 4219-4229.

Zhao, Y.; Lo, H. K.; Ma, X.; Qi, B.; Chen, K. et al. (2007): Decoy state quantum key distribution: theory and practice. *Aps Meeting Abstracts*.

Zhao, Y.; Qi, B.; Lo, H. K. (2008): Quantum key distribution with an unknown and untrusted source. *Physical Review A*, vol. 77, no. 5, 052327.

Zhou, Y. Y.; Zhou, X. J. (2011): Nonorthogonal passive decoy-state quantum key distribution with a weak coherent state source. *Acta Physica Sinica*, vol. 60, no. 10, pp. 687-709.

Zhu, J. R.; Wang, C. Y.; Liu, K.; Zhang, C. M.; Wang, Q. (2018): Decoy-state reference-frame-independent quantum key distribution with the single-photon-added coherent source. *Quantum Information Processing*, vol. 17, no. 11, pp. 294.