doi:10.3788/gzxb20184703.0306007

基于脉冲位置调制的测量设备无关量子密钥分发

毛钱萍[1,2]，王乐[1]，马媛媛[3]，曾荣[3]，黄秀丽[3]，赵生妹[1]

（1 南京邮电大学 信号处理与传输研究院，南京 210003）
（2 南京工业大学 计算机科学与技术学院，南京 210009）
（3 全球能源互联网研究院，南京 210003）

摘　要：为了进一步提高测量设备无关量子密钥分发（MDI-QKD）系统的传输距离和密钥率，将脉冲位置调制（PPM）技术引入到MDI-QKD中，利用弱光源中的空脉冲和高维编码技术，提出了一种高效的测量设备无关量子密钥分发，即PPM-MDI-QKD协议.协议中，通信双方首先将M个连续的弱脉冲构建成一个PPM帧，然后利用BB84极化编码和PPM编码方案实现高维编码，最后根据合法PPM帧、成功贝尔态测量结果以及匹配基筛选出安全密钥.数值计算结果表明，当光源平均光强小于0.13时，PPM-MDI-QKD协议的性能优于MDI-QKD协议；与迄今为止报道的最远404 km的MDI-QKD协议相比，在相同条件下，本协议最远传输距离能够达到480 km，在404 km传输距离上的密钥率可达5.4×10^{-4} bps.

关键词：量子通信；量子密码；量子光学；信息安全；光纤通信

中图分类号：TN918；O431.2　　**文献标识码**：A　　**文章编号**：1004-4213(2018)03-0306007-8

Measurement-device-independent Quantum Key Distribution with Pulse-position Modulation

MAO Qian-ping[1,2], WANG Le[1], MA Yuan-yuan[3], ZENG Rong[3],
HUANG Xiu-li[3], ZHAO Sheng-mei[1]

(1 *Institute of Signal Processing and Transmission*, *Nanjing University of Posts and Telecommunications*, *Nanjing* 210003, *China*)
(2 *College of Computer Science and Technology*, *Nanjing Tech University*, *Nanjing* 210009, *China*)
(3 *Global Energy Interconnection Research Institute*, *Nanjing* 210003, *China*)

Abstract: In order to further enhance the transmission distance and secret key rate of the Measurement-Device-Independent Quantum Key Distribution (MDI-QKD) system, the Pulse Position Modulation (PPM) technique is introduced to the MDI-QKD protocol, and a new efficient quantum key distribution protocol, named PPM-MDI-QKD protocol, is proposed by utilizing the empty pulses of the weak source and high dimensional encoding technology. In the protocol, two communication parties firstly construct a PPM frame consisting of M consecutive weak pulses, then combine the BB84 polarization encoding and PPM encoding schemes to operate high dimensional encoding, and finally sift out the secure key with the legal PPM frame, the successful Bell-state measurement results, and matched bases. The numerical results show that the PPM-MDI-QKD protocol outperforms MDI-QKD protocol when the intensity of signals is less than 0.13. Moreover, compared with 404 km, the longest distance reported so far, the transmission distance can theoretically be extended to 480 km and the key rate up to 5.4×10^{-4} bps in

Foundation item: The National Natural Science Foundation of China (No. 61475075), the Science and Technology Project of State Grid (No. SGRIXTKJ[2017]459) and Postgraduate Research & Practice Innovation Program of Jiangsu Province(No.KYLX15-0832)

First author: MAO Qian-ping (1978－), female, lecturer, M.S. degree, mainly focuses on quantum key distribution and quantum communication. Email: maoqp@163.com

Supervisor(Contact author): ZHAO Sheng-mei (1968－), female, professor, Ph.D. degree, mainly focuses on quantum communication and information security. Email: zhaosm@njupt.edu.cn

Received: Aug.9, 2017; **Accepted**: Nov.13, 2017

404 km, with the same parameters.

Key words: Quantum communication; Quantum cryptography; Quantum optics; Security of information; Fiber optic communication

OCIS Codes: 060.5565; 270.5565; 270.5568; 270.5585

0 Introduction

Quantum Key Distribution (QKD) allows two distant parties, known as Alice and Bob, to securely exchange cryptographic keys even under the existence of an eavesdropper, Eve[1]. QKD, in principle, offers unconditional security based on quantum mechanics[2-4]. Since it is proposed, QKD has received considerable attentions and has made a great progress[5-10] recently.

But, in a practical QKD system, there are some defects of measurement devices[7], which results in the eavesdropping of Eve and affects the unconditional security of QKD. Recently, a Measurement Device Independent Quantum Key Distribution (MDI-QKD) protocol was proposed to avoid any possible side channels in detectors[11-12]. In the MDI-QKD protocol, both Alice and Bob send quantum signals to an untrusted third party, Charlie. He performs a Bell-State Measurement (BSM) and announces the results to Alice and Bob. With the announced information, Alice and Bob can distill a secret key between them. MDI-QKD protocol has been extensively studied both in experiment[13-18] and on theory[19-26] since it was proposed.

In the implementation of MDI-QKD, Weak Coherent Source (WCS), which contains not only single-photon and multi-photon pulses, but also zero-photon (empty) pulses, is usually used to replace the idea single-photon source[11-12]. The decoy-state MDI-QKD scheme was presented to assure the security of QKD with WCS[11-12], and it has been developed rapidly. In 2014, Yan-Lin Tang et al. has experimentally implemented the key distribution over the 200km with a key rate of 0.018 bps[27]. Recently, many methods have been used to improve the performance of MDI-QKD. For example, Guang-Zhao Tang et al proposed a time-bin phase-encoding MDI-QKD scheme, the key rate was improved by reducing the Quantum Bit Error Rate (QBER) for the Z-basis to 0.8% over the 36 km standard optical fiber[28]. Yi-Heng Zhou et al presented a four-intensity decoy-state MDI-QKD protocol in which the final key rate is up to 0.98 bps[29], moreover, with the four-intensity decoy-state method, Hua-Lei Yin et al reported the results of MDI-QKD over 404 km of ultralow-loss optical fiber and 311 km of a standard optical fiber[30].

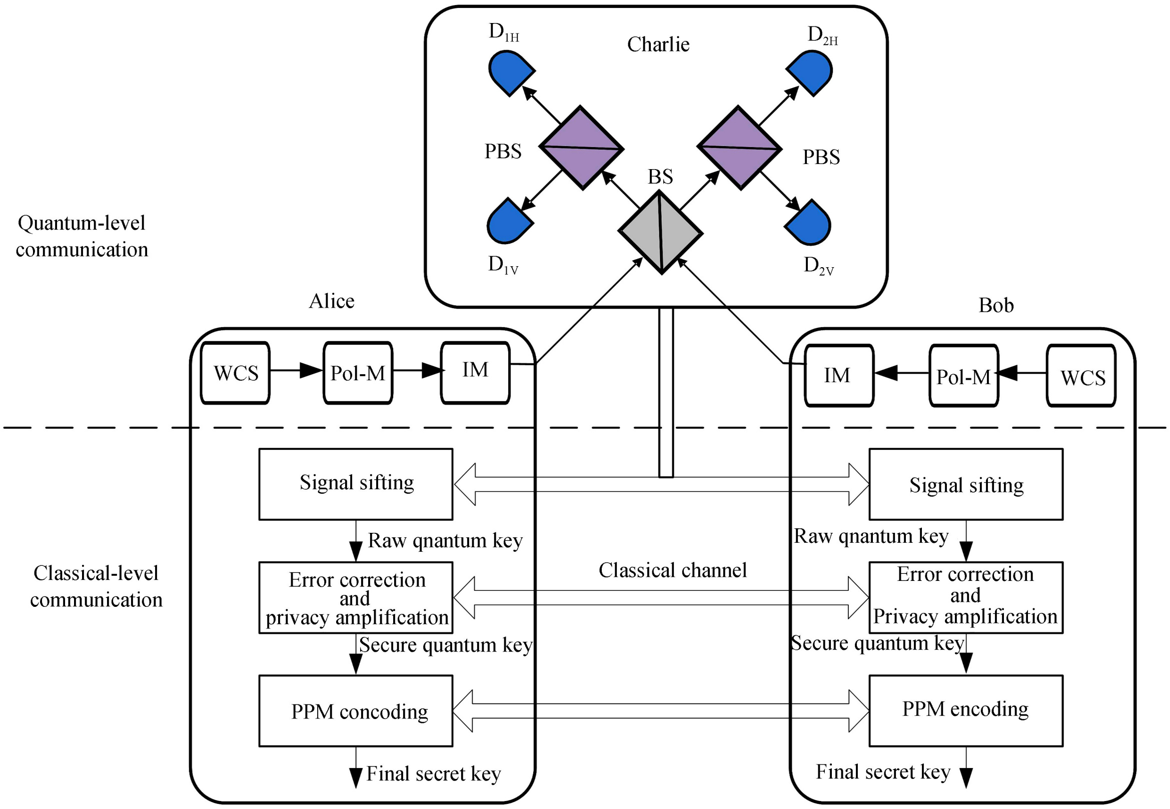
Accordingto the characteristic of WCS, Pulse-Position Modulation (PPM), a solution to photon-starved reception for classical optical communications[31], was adopted to BB84-style QKD system to achieve the higher secure key rate[32-34]. In Ref.[32], by employing PPM coding approach, the zero-photon and single-photon pulses were simultaneously utilized, 8-PPM-BB84 achieved the highest secret key rate at the intensity of 0.068, which outperformed that of BB84 QKD by 67.78% at the intensity of 0.1. Authors in Refs. [33] and [34] also showed the secret key rate was improved by utilizing the efficiency of WCS source in QKD. It was shown that the adaptive PPM-QKD scheme could avoid the photon detection losses or dark current in the system, and the performance of the system was close to the theoretical bound when the intensity λ was between 0.0039 and 0.1. Authors in Ref. [34] designed and demonstrated the PPM-QKD could achieve a throughput of 2.5 Mbit/s for loss equivalent to 25 km of fiber and the secret-key capacity was up to 4.0 bits per detected photon. However, the combination of PPM coding approach and MDI-QKD protocol still has not been discussed yet.

In this paper, we propose a MDI-QKD protocol based on PPM encoding, named as PPM-MDI-QKD protocol. In the protocol, M consecutive pulses are composed of a frame, and only one non-empty pulse is assumed in the frame, which results in that the empty pulses of the weak coherent source are utilized. Then, each pulse of the frame is modulated by one of the four BB84 polarization states. With the quantum-level and classical-level communications, the system outperforms a higher secret key rates for a long distance transmission.

1 PPM-MDI-QKD protocol

1.1 PPM-MDI-QKD protocol

The scheme of the proposed protocol is depicted in Fig.1, which includes quantum-level and classical-level communication. Here, the polarization-encoding method is used. In the quantum-level communication, both Alice and Bob prepare Weak Coherent Pulses (WCPs) and modulate quantum information on each pulse in four polarization states (i.e., vertical, horizontal, 45 °, and 135 °polarized states) by polarization modulators (Pol-M). The decoy and signal states are randomly generated by using an Intensity Modulator (IM), and are sent to Charlie. Then, Charlie performs a Bell State Measurement (BSM) and publicly announces the detection results.



WCS: Weak coherent source; Pol-M: polarization modulator; IM: Decoy states intensity modulator; BS: Beam splitter with 50:50 ; PBS: Polarizing beam splitter; D: Single-photon detector

Fig.1 Schematic diagram of PPM-MDI-QKD protocol

After quantum-level communication, the classical-level communication is started. According to Charlie's successful results, Alice and Bob operate data sifting to obtain raw quantum keys by recognizing whether the successful results is belong to an eligible PPM frame. Here, the eligible PPM frame means that Alice and Bob send exactly one non-empty pulse within the M consecutive pulses while there is no photon at any other pulse slots. Hence, the information bits can be carried by the position of non-empty pulse of a PPM frame and each PPM frame can carry $m=\log_2 M$ bits information. Then, error correction and privacy amplification are performed to extract the secure quantum keys. Finally, the final secret key is achieved by PPM encoding.

The differences between the proposed protocol and the conventional MDI-QKD protocol are in the phase of data sifting and PPM encoding.

Fig. 2 shows the process of data sifting in the proposed protocol. Firstly, Alice and Bob judge whether the frames they have are eligible. For M-PPM, a frame consists of M time slots. If there is exactly one time slot has a single-photon pulse, and the other M-1 time slots are empty pulses, the frame is regarded as an eligible frame. Based on it, they keep successful measurement results according to the announced results from Charlie. With the eligible PPM frame and successful measurement, Alice and Bob broadcast their bases and they keep the data only when the bases match. After that, the raw quantum keys are achieved.

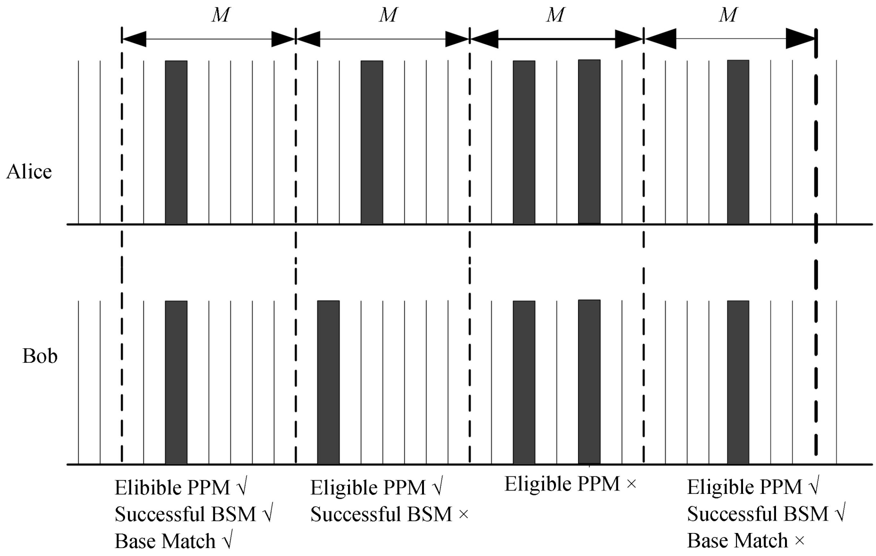


Fig.2 The process of data sifting

The progress of PPM encoding could convert the secure quantum key of L bits into a final secret key of $L\times\log_2 M$ bits by combing the pulse-position information. It includes two steps. The first one is PPM coding, where the information bits are naturally encoded on an effective M-PPM frame. Taking the M-PPM as an example, the $\log_2 M$ information bits are carried by a PPM frame. The second step is bit-flipping. If the secure quantum key bit is "0", the information bits are kept, otherwise, the bit-flipping is operated on the information bits.

For example,the secure quantum key is $S_1S_2\cdots S_L$, where the length is L. Firstly, every bit S_i is encoded into m information bits according PPM coding. Taking the M-PPM with $M=8$ as an example, the $m=3$ information bits, which is carried by a PPM frame with a pulse at the position $p=6$, are interpreted as $b_{i1}b_{i2}\cdots b_{im}=110$. Secondly, by bit-flipping, the m information bits $b_{i1}b_{i2}\cdots b_{im}$ is maintained if S_i is "0", while the $b_{i1}b_{i2}\cdots b_{im}$ is converted into $\overline{b_{i1}b_{i2}}\cdots\overline{b_{im}}$ by complementary operation if the bit S_i is "1". With the insertion of complementary operation, if a eavesdropper want to eavesdrop, Eve has to perform quantum measurement to obtain the quantum information as in BB84. So the quantum PPM encoding can avoid the situation in which eavesdropper learns the information bits only by knowing the pulse position. Hence, by quantum PPM encoding, each valid quantum bit S_i of a secure quantum key is encoded into m final secure bits, which compose a final secret key.

The details of the proposed protocol is listed as follows.

1) Both Alice and Bob prepare weak coherent states with different intensity: the signal states and decoy states. Then they modulate their information on each pulses in four BB84 polarization states(i.e., vertical, horizontal, 45 °, and 135 °polarized states)[1], and send them to an untrusted relay Charlie located in the middle through the quantum channel.

2)Charlie performs BSM and announce her measurement results through the classical channel.

3)Then Alice and Bob proceed to signal siftings. According to the successful measurement results, they recognize the eligible PPM frames, then sift out and keep the results of using the same bases as a raw quantum key.

4)Alice and Bobperform error correction and privacy amplification to extract a secure quantum key by the classical channel.

5)Alice and Bob get the final secret key by quantum PPM encoding.

Based on the principle of PPM encoding approach, the proposed protocol has only changes in the post-processing of the sifted data. It makes no difficulty for the implementations.

1.2 Analysis of secret key rate

Accordingto Refs.[11] and [32], the secure quantum key rate per frame, R_{PPM}, is

$$R_{\mathrm{PPM}}\geqslant Q_{\mathrm{rect,PPM}}^{1,1}[1-H(e_{\mathrm{diag}}^{1,1})]-Q_{\mathrm{rect}}fH(E_{\mathrm{rect}}) \tag{1}$$

where $Q_{\mathrm{rect,PPM}}^{1,1}$ means the gain for Alice and Bob to generate eligible frames with a single-photon pulse in the rectilinear basis. $e_{\mathrm{diag}}^{1,1}$ represents the Quantum Bit Error Rate (QBER) of the single-photon states in the diagonal basis sent by Alice and Bob. f is the error correction inefficiency, and $H(x)=-x\log_2 x-(1-x)\log_2(1-x)$ is the binary Shannon entropy function. Q_{rect} and E_{rect} denote the total gain and total QBER in the rectilinear basis, where

$$Q_{\mathrm{rect}}=\sum\nolimits_{n,m}Q_{\mathrm{rect}}^{n,m} \tag{2}$$

and

$$E_{\mathrm{rect}}=\sum\nolimits_{n,m}Q_{\mathrm{rect}}^{n,m}e_{\mathrm{rect}}^{n,m}/Q_{\mathrm{rect}} \tag{3}$$

According to the principle of PPM encoding approach, the final secret key rate per pulse is

$$R\geqslant\frac{\log_2 M}{M}\{Q_{\mathrm{rect,PPM}}^{1,1}[1-H(e_{\mathrm{diag}}^{1,1})]-Q_{\mathrm{rect}}fH(E_{\mathrm{rect}})\} \tag{4}$$

Hence, $Q_{\mathrm{rect,\,PPM}}^{1,1}$, $e_{\mathrm{diag}}^{1,1}$, Q_{rect} and E_{rect} play important roles in estimating the final secret key rate R. Note that Q_{rect} and E_{rect}, the two parameters can be measured in experiment, here we use the results in Ref. [12]

$$Q_{\mathrm{rect}}=Q_{\mathrm{rect}}^{\mathrm{C}}+Q_{\mathrm{rect}}^{\mathrm{E}} \tag{5}$$

$$E_{\mathrm{rect}}Q_{\mathrm{rect}}=e_{\mathrm{d}}Q_{\mathrm{rect}}^{\mathrm{C}}+(1-e_{\mathrm{d}})Q_{\mathrm{rect}}^{\mathrm{E}} \tag{6}$$

where

$$Q_{\mathrm{rect}}^{\mathrm{C}}=2\ (1-p_{\mathrm{d}})^2e^{-\mu'/2}\ [1-(1-p_{\mathrm{d}})^{-\eta_{\mathrm{A}}\mu_{\mathrm{A}}/2}]*[1-(1-p_{\mathrm{d}})^{-\eta_{\mathrm{B}}\mu_{\mathrm{B}}/2}] \tag{7}$$

$$Q_{\mathrm{rect}}^{\mathrm{E}}=2p_{\mathrm{d}}\ (1-p_{\mathrm{d}})^2e^{-\mu'/2}\ [I_0(2x)-(1-p_{\mathrm{d}})e^{-\mu'/2}] \tag{8}$$

and e_{d} represents the misalignment probability. In Eq.(8), $I_0(x)$ is the modified Bessel function of the first kind, p_{d} is the background count rate per detector, and $\eta_{\mathrm{A}}(\eta_{\mathrm{B}})$ is the transmission efficiency of Alice (Bob), and $\mu'=\eta_{\mathrm{A}}\mu_{\mathrm{A}}+\eta_{\mathrm{B}}\mu_{\mathrm{B}}$, and $x=\sqrt{\eta_{\mathrm{A}}\mu_{\mathrm{A}}\eta_{\mathrm{B}}\mu_{\mathrm{B}}}/2$.

For the proposed protocol, $Q_{\mathrm{rect,PPM}}^{1,1}$ and $e_{\mathrm{diag}}^{1,1}$ are given as

$$Q_{\mathrm{rect,PPM}}^{1,1}=p_{1,1,\mathrm{PPM}}Y_{\mathrm{rect}}^{1,1} \tag{9}$$

$$e_{\mathrm{diag}}^{1,1}Y_{\mathrm{diag}}^{1,1}=e_0Y_{\mathrm{diag}}^{1,1}-(e_0-e_{\mathrm{d}})\ (1-p_{\mathrm{d}})^2\ \frac{\eta_{\mathrm{A}}\eta_{\mathrm{B}}}{2} \tag{10}$$

where $p_{1,1,\mathrm{PPM}}$ is the probability of eligible PPM frame with single-photon pulse, e_0 is the error rate of background, and the yield $Y_w^{1,1}$ ($w=$ rect, diag) is the total probability to have a successful measurement result when Alice and Bob use the same basis.

The probability for Alice and Bob to generate an eligible PPM frame with a single photon pulse is expressed as

$$p_{1,1,\mathrm{PPM}}=Mp_1(\mu_{\mathrm{A}})(p_0(\mu_{\mathrm{A}}))^{M-1}p_1(\mu_{\mathrm{B}})(p_0(\mu_{\mathrm{B}}))^{M-1} \tag{11}$$

where $p_k(\lambda)$ is the probability of the k-photons pulses from the WCS with the intensity λ, and

$$p_k(\lambda)=e^{-\lambda}\lambda^k/k! \tag{12}$$

According to the result in Ref. [21], $Y_w^{1,1}$ can be estimated as

$$Y_{\mathrm{rect}}^{11}=Y_{\mathrm{diag}}^{11}=(1-p_{\mathrm{d}})^2[\frac{\eta_{\mathrm{A}}\eta_{\mathrm{B}}}{2}+(2\eta_{\mathrm{A}}+2\eta_{\mathrm{B}}-3\eta_{\mathrm{A}}\eta_{\mathrm{B}})p_{\mathrm{d}}+4(1-\eta_{\mathrm{A}})(1-\eta_{\mathrm{B}})p_{\mathrm{d}}^2] \tag{13}$$

Finally, the final secret key rate per pulse R is

$$\begin{aligned}R\geqslant&\frac{\log_2 M}{M}\{p_{1,1,\mathrm{PPM}}\{(1-p_{\mathrm{d}})^2[\frac{\eta_{\mathrm{A}}\eta_{\mathrm{B}}}{2}+(2\eta_{\mathrm{A}}+2\eta_{\mathrm{B}}-3\eta_{\mathrm{A}}\eta_{\mathrm{B}})p_{\mathrm{d}}+4(1-\eta_{\mathrm{A}})(1-\eta_{\mathrm{B}})p_{\mathrm{d}}^2]\}\cdot\\ &\{1-H(e_0-\frac{(e_0-e_{\mathrm{d}})\eta_{\mathrm{A}}\eta_{\mathrm{B}}}{\eta_{\mathrm{A}}\eta_{\mathrm{B}}+2(2\eta_{\mathrm{A}}+2\eta_{\mathrm{B}}-3\eta_{\mathrm{A}}\eta_{\mathrm{B}})p_{\mathrm{d}}+8(1-\eta_{\mathrm{A}})(1-\eta_B)p_{\mathrm{d}}^2})\}-\{2\ (1-p_{\mathrm{d}})^2\cdot\\ &e^{-(\eta_{\mathrm{A}}\mu_{\mathrm{A}}+\eta_{\mathrm{B}}\mu_{\mathrm{B}})/2}\ [1-(1-p_{\mathrm{d}})^{-\eta_{\mathrm{A}}\mu_{\mathrm{A}}/2}]*[1-(1-p_{\mathrm{d}})^{-\eta_{\mathrm{B}}\mu_{\mathrm{A}}/2}]+2p_{\mathrm{d}}\ (1-p_{\mathrm{d}})^2e^{-(\eta_{\mathrm{A}}\mu_{\mathrm{A}}+\eta_{\mathrm{A}}\mu_{\mathrm{A}})/2}\cdot\\ &[I_0(\sqrt{\eta_{\mathrm{A}}\mu_{\mathrm{A}}\eta_{\mathrm{B}}\mu_{\mathrm{B}}})-(1-p_{\mathrm{d}})e^{-(\eta_{\mathrm{A}}\mu_{\mathrm{A}}+\eta_{\mathrm{B}}\mu_{\mathrm{B}})/2}]\}\cdot f\cdot H(e_{\mathrm{d}}\cdot 2\ (1-p_{\mathrm{d}})^2e^{-(\eta_{\mathrm{A}}\mu_{\mathrm{A}}+\eta_{\mathrm{B}}\mu_{\mathrm{B}})/2}\cdot\\ &[1-(1-p_{\mathrm{d}})^{-\eta_{\mathrm{A}}\mu_{\mathrm{A}}/2}]*[1-(1-p_{\mathrm{d}})^{-\eta_{\mathrm{B}}\mu_{\mathrm{B}}}/2]+(1-e_{\mathrm{d}})\cdot 2p_{\mathrm{d}}\ (1-p_{\mathrm{d}})^2e^{-(\eta_{\mathrm{A}}{}^{\mathrm{A}}\mu_{\mathrm{A}}+\eta_{\mathrm{B}}\mu_{\mathrm{B}})/2}\cdot\\ &[I_0(\sqrt{\eta_{\mathrm{A}}\mu_{\mathrm{A}}\eta_{\mathrm{B}}\mu_{\mathrm{B}}})-(1-p_{\mathrm{d}})e^{-(\eta_{\mathrm{A}}\mu_{\mathrm{A}}+\eta_{\mathrm{B}}\mu_{\mathrm{B}})/2}])\}\end{aligned} \tag{14}$$

2 Numerical results

In this section, the numerical experiments for our PPM-MDI-QKD protocol are presented. For simplicity, the symmetric scenario is adopted, hence Alice and Bob both use the same intensity of signal states, i.e., $\mu=\mu_{\mathrm{A}}=\mu_{\mathrm{B}}$, and have the same transmission efficiency $\eta=\eta_{\mathrm{A}}=\eta_{\mathrm{B}}=10^{-\alpha L_s/10}$, where the loss coefficient of the channel $\alpha$is 0.2 dB/km, and L_S is the distance of quantum channel between Alice (Bob) and Charlie. The other parameters used in simulations are listed in Table 1.

Table1 List of some parameters for numerical simulations

	p_d	f	e_0	e_d
a[21]	3×10^{-6}	1.16	0.5	1.5%
b[30]	7.2×10^{-8}	1.16	0.5	1%

Fig.3 shows the secret key rates versus the intensity of signal for the proposed protocol with M= 2, 4, 8, 16, 32, together with that of MDI-QKD protocol, where the distance between Alice and Bob is 100 km. The results show that the PPM-MDI-QKD protocol outperforms MDI-QKD when the intensity of signals is less than 0.13. When the intensity is between 0.13 and 0.01, the maximal key rate can be obtained by selecting an appropriate M. While the intensity is smaller than 0.01, the larger the M is, the greater the final secret key rate is.

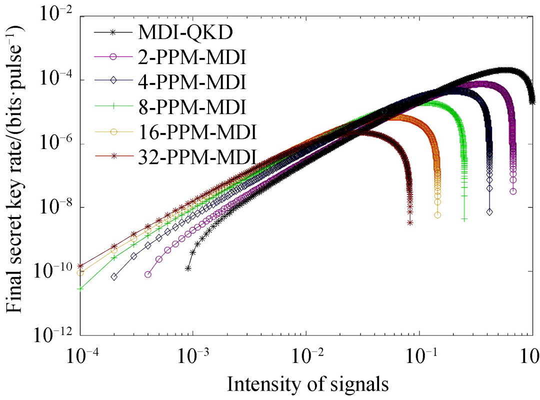
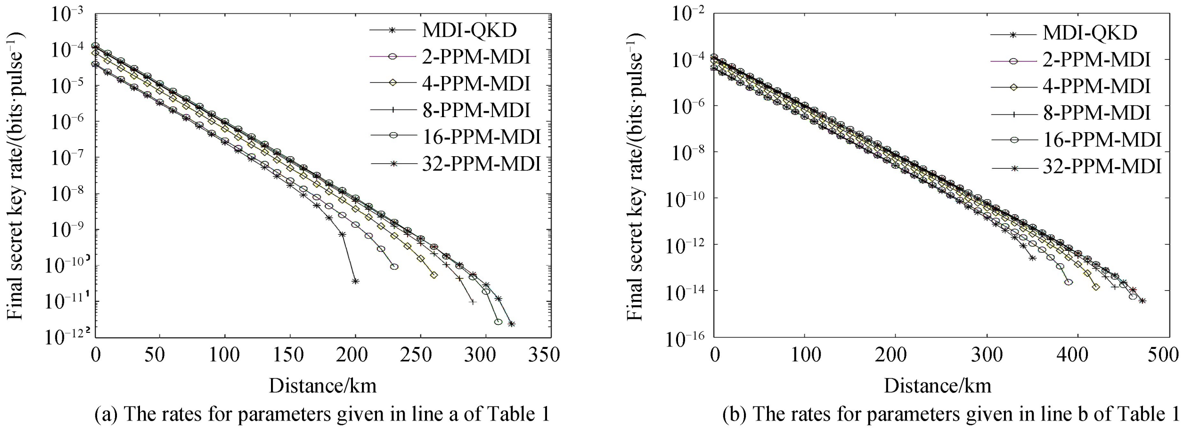


Fig.3 Final secret key rate versus the intensity performances of MDI-QKD and PPM-MDI-QKD with the parameters given in line a of Table 1

Fig.4 shows the final secret key rates versus the transmission distance , here the intensity of source μ is 0.01. It can be seen that the secret key rates decrease with the increasing distance in either MDI-QKD or PPM-MDI-QKD protocol. By comparing the curves in Fig.4, it is shown that the PPM-MDI-QKD scheme outperforms the MDI-QKD both in the transmission distance and the key rate, and the performance of PPM-MDI-QKD are increased with the increasing M. In addition, the maximal distances of MDI-QKD and PPM-MDI-QKD are 200 km and 320 km in Fig.4(a), while they are 340 km and 480 km in Fig.4(b), respectively. Hence, the result is obtained that the PPM-MDI-QKD protocol can improve the secret key rate and extend the transmission distance.

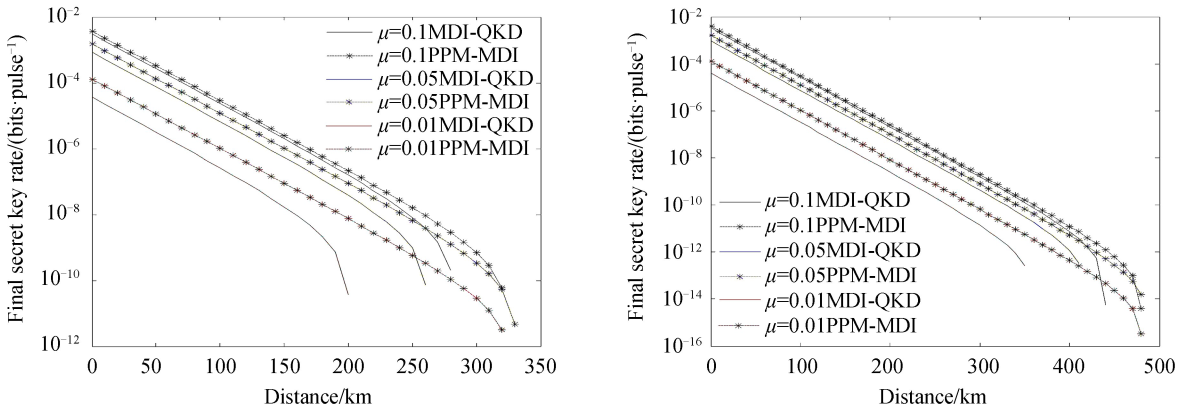


(a) The rates for parameters given in line a of Table 1

(b) The rates for parameters given in line b of Table 1

Fig.4 Final secret key rate versus the distance for MDI-QKD and PPM-MDI-QKD

Fig.5 shows the key rates against the transmission distance for μ=0.1, μ=0.05 and μ=0.01. Here, the key rates for PPM-MDI-QKD are maximized by optimizing the value of M for a given transmission distance. For MDI-QKD and PPM-MDI-QKD protocol, the larger the μ is, the greater the final secret key rate is. Moreover, the PPM-MDI-QKD protocol outperforms the MDI-QKD both in the key rate and transmission.



(a) The rates for parameters given in line a of Table 1

(b) The rates for parameters given in line b of Table 1

Fig.5 The optimal key rates with different intensity of source

Table 2 lists the comparison between our work and Ref.[30] with the same device parameter, which has been given in line b of Table 1. Compared to the Ref.[30], the longest distance of our work is extended to 1.2 times, and the rate is raised to 1.7 times.

Table 2 Comparison of performance for different protocol

	The longest distance	The key rate at the distance 404 km
Ref.[30]	404 km	3.2×10^{-4} bps
Our work	480km	5.4×10^{-4} bps

Therefore, PPM-MDI-QKD is a better candidate for long-distance and high-key-rate QKD with weak coherent sources.

3 Conclusion

In the paper, we have proposed a PPM-MDI-QKD protocol to improve the secret key rate and the transmission distance. By adopting PPM encoding approach, the efficiency of utilizing weak laser source is enhanced, and multi-dimension information can be transferred over a single-photon pulse in an eligible frame. Moreover, we can implement a quantum key distribution of longer distant transmission without adding additional setup. Hence the protocol has the advantages of both MDI-QKD and PPM. The numerical simulations also demonstrate that the proposed protocol can achieve higher secret key rate in long-distance when the intensity of source is less than 0.13. Comparing with the experimentally implementation of 404 km[30], the longest distance reported by far, we can theoretically extend the transmission distance to 480 km with the same parameters. Lastly, although PPM is only adopted into MDI-QKD in this paper, it can be easily applied into other QKD protocols with WCS.

References

[1] BENNETT C H, BRASSARD G. Quantum cryptography: Public key distribution and coin tossing[J]. *Theoretical Computer Science*, 2014, **560**(1): 7-11.

[2] LO H. Unconditional security of quantum key distribution over arbitrarily long distances[J].*Science*, 1999, **283**(5410): 2050-2056.

[3] SHOR P W, PRESKILL J. Simple proof of security of the BB84 quantum key distribution protocol[J]. *Physical Review Letters*, 2000, **85**(2): 441-444

[4] MAYERS D. Unconditional security in quantum cryptography[J]. *Journal of the Acm*, 2001,**48**(3):351-406.

[5] WANG Le, ZHAO Sheng-mei. Round-robin differential-phase-shift quantum key distribution with heralded pair-coherent sources[J]. *Quantum Information Processing*, 2017, **16**(4): 100.

[6] YANG Rong-huan, HE Guang-qiang. The influence of Faraday mirror's imperfection in Continuous variable quantum key distribution system[J].*Acta Photonica Sinica*, 2015, **44**(2): 0227001.

[7] LI Jian, PAN Ze-shi, ZHENG Jun, *et al*. The security analysis of quantum "SAGR04" protocol in collective-rotation noise channel[J]. *Chinese Journal of Electronics*, 2015,**24**(4): 689-693.

[8] SUN Yong-mei, CHENG Xian-zhu, JI Yue-feng. A differentialized service providing scheme on trusted relay quantum key distribution networks[J].*Acta Photonica Sinica*, 2014, **43**(7): 0706009.

[9] ZHAO Sheng-mei, GONG Long-yan, LI Yong-qiang, *et al*. A large-alphabet quantum key distribution protocol using

orbital angular momentum entanglement[J]. *Chinese Physics Letters*, 2013, **30**(6): 060305.

[10] HWANG W-Y. Quantum key distribution with high loss: toward global secure communication[J]. *Physical Review Letters*, 2003, **91**(5): 057901.

[11] LO H K, CURTY M, QI B. Measurement-device-independent quantum key distribution[J]. *Physical Review Letters*, 2012, **108**(13): 130503.

[12] MA Xiong-feng, RAZAVI M. Alternative schemes for measurement-device-independent quantum key distribution[J]. *Physical Review A*, 2012, **86**(6): 062319.

[13] TANG Zhi-yuan, WEI Ke-jin, BEDROYA O, *et al*. Experimental measurement-device-independent quantum key distribution with imperfect sources[J]. *Physical Review A*, 2016, **93**(4): 042308.

[14] TANG Guang-zhao, SUN Shi-hai, XU Fei-hu, *et al*. Experimental asymmetric plug-and-play measurement-device-independent quantum key distribution[J]. *Physical Review A*, 2016, **94**(3): 032326.

[15] WANG Chao, WANG Shuang, YIN Zhen-qiang, *et al*. Experimental measurement-device-independent quantum key distribution with uncharacterized encoding[J]. *Optics Letters*, 2016, **41**(23): 5596-9.

[16] TANG Zhi-yuan, LIAO Zhong-fa, XU Fei-hu, *et al*. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution[J]. *Physical Review Letters*, 2014, **112**(19): 190503.

[17] TANG Yan-lin, YIN Hua-lei, CHEN Si-jing, *et al*. Field test of measurement-device-independent quantum key distribution[J]. *IEEE Journal of Selected Topics in Quantum Electronics*, 2015, **21**(1): 6600407.

[18] TANG Yan-lin, YIN Hua-lei, CHEN Si-jing, *et al*. Measurement-device-independent quantum key distribution over 200 km[J]. *Physical Review Letters*, 2015, **114**(6): 069901.

[19] WU Cheng-feng, DU Ya-nan, WANG Jin-dong, *et al*. Analysis on performance optimization in measurement-device-independent quantum key distribution using weak coherent states[J]. *Acta Physica Sinica*, 2016, **65**(10): 100302.

[20] HWANG W Y, SU Hong-yi, BAE J. N-dimensional measurement-device-independent quantum key distribution with N +1 un-characterized sources: zero quantum-bit-error-rate case[J]. *Scientific Reports*, 2016, **6**: 30036.

[21] MA Xiong-feng, FUNG C H F, RAZAVI M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution[J]. *Physical Review A*, 2012, **86**(5): 052305.

[22] CHOI Y, KWON O, WOO M, *et al*. Plug-and-play measurement-device-independent quantum key distribution[J]. *Physical Review A*. 2016, **93**(3): 032319.

[23] ZHANG Chun-mei, ZHU Jian-rong, WANG Qin. Practical decoy-state reference-frame-independent measurement-device-independent quantum key distribution[J]. *Physical Review A*. 2017, **95**(3): 032309.

[24] WANG Qin, WANG Xiang-bin. Simulating of the measurement-device independent quantum key distribution with phase randomized general sources[J]. *Scientific Reports*, 2014, **4**: 4612.

[25] ZHOU Yi-heng, YU Zong-wen, WANG Xiang-bin. Tightened estimation can improve the key rate of measurement-device-independent quantum key distribution by more than 100%[J]. *Physical Review A*, 2014, **89**(5): 052325.

[26] ZHOU Chun, BAO Wan-sun, ZHANG Hai-long, *et al*. Biased decoy-state measurement-device-independent quantum key distribution with finite resources[J]. *Physical Review A*, 2015, **91**(2): 022313.

[27] TANG Yan-lin, YIN Hua-lei, CHEN Si-jing, *et al*. Measurement-device-independent quantum key distribution over 200 km[J]. *Physical Review Letters*, 2014, **113**(19): 190501.

[28] TANG Guang-zhao, SUN Shi-hai, CHEN Huan, *et al*. Time-bin phase-encoding measurement-device-independent quantum key distribution with four single-photon detectors[J]. *Chinese Physics Letters*, 2016, **33**(12): 120301.

[29] ZHOU Yi-heng, YU Zong-wen, WANG Xiang-bin. Making the decoy-state measurement-device-independent quantum key distribution practically useful[J]. *Physical Review A*, 2016, **93**(4): 042324.

[30] YIN Hua-lei, CHEN Teng-yun, YU Zong-wen, *et al*. Measurement-device-independent quantum key distribution over a 404 km optical fiber[J]. *Physical Review Letters*, 2016, **117**(19): 190501.

[31] ROBINSON B S, KERMAN A J, DAULER E A, *et al*. 781 Mbit/s photon-counting optical communications using a superconducting nanowire detector[J]. *Optics Letters*, 2006, **31**(4): 444-446.

[32] ZHANG Ye-qun, DJORDJEVIC I B. Generalized PPM-based BB84 QKD protocol[C]. ICTON, 2014, paper Tu.B1.5.

[33] ZHOU Hong-chao, WORNELL G. Adaptive pulse-position modulation for high-dimensional quantum key distribution [C]. ISIT, 2013: 359-363.

[34] ZHONG Tian, XU Fei-hu, ZHANG Zhe-shen, *et al*. Photon-efficient quantum cryptography with pulse-position modulation[J/OL]. (2015-10-21)[2015-10-21]. https://arxiv.org/abs/1510.06126.