Numerical simulation of quantum key distribution network based on wavelength division multiplexing technology

Shiju Sun[1], Jipeng Wang[2], Dan Su[1], Haiqiang Ma[2*]

[1.] School of Aircraft Engineering, Beijing Polytechnic, Beijing, China

[2.] School of Science, Beijing University of Posts and Telecommunication, Beijing, China

[*] E-mail: hqma@bupt.edu.cn

Abstract. Wavelength division multiplexing (WDM) technology can improve the networking level and overcome the shortcomings of low key rate under the existing technic background of measurement device independent quantum key distribution (MDI-QKD) protocol application. reference frame independent quantum key distribution (RFI-MDI-QKD) protocol cut down on the influence of the reference frame drift on the key distribution system . The decoy state protocol has important development prospects in the development of quantum communication networking. Combining the advantages of of the above protocols to realize RFI-MDI-QKD with WDM, the results show that the key distribution efficiency is improved with the increase in the number of WDM multiplexed channels, which promotes the further exploration and achievement of QKD networking application.

1. Introduction

The purpose of cryptography is to make communication between two authorized users incomprehensible to any third party. Privacy and confidentiality are the main goals of cryptography. Established on the difficulty of inverse solution of large prime factorization, the RSA algorithm public key encryption system has been widely used in various cryptography fields. However, the emergence of quantum computers can achieve exponentially increasing operating speeds[1]. Therefore, the mathematical problems based on the RSA encryption algorithm will be settled within a minute, leading to a security crisis. Therefore, in the era of quantum computers, how can the security of communication be ensured?

Based on quantum physics, quantum communication provides an unconditional security protocol on the physical level. It can resist the attack of possible eavesdroppers and achieve key distribution between two authorized users. the first and most widely recognized quantum key distribution protocol (QKD) is proposed in 1984 and named by the BB84 protocol[2]. Its security proofhas already been demonstrated by many former researches[3][4].

Theoretically, quantum communication can guarantee absolute information security. Unfortunately, when considering the actual situation, the limitations of current technology and the vulnerabilities in the actual system may lead to eavesdropping or attacks. Specifically, in actual experiments, most QKD systems are based on attenuated weak-coherent laser pulses. Thus, some pulse sequences may contain more than one photon. This defect provides the possibility for eavesdroppers to commit a so-called photon number separation attack[5]. The decoy scheme is an important weapon against this attack. By preparing some decoy states modulated by the different pulse intensities, Alice and Bob can find and defend against eavesdroppers via abnormal error rates. GLLP method[6] provides a rigorous security proof and compact security key estimation formula. It is proved that the two-decoy state scheme with vacuum and decoy state has the best practicality to achieve the QKD system[7][8][9]. Above all, the decoy scheme has become an indispensable part of QKD system.

The measurement device is one of the most vulnerable parts of the QKD system. Makarov proposed a black-blinding attack scheme for QKD system detectors[10], which successfully controls the measurement equipment of the QKD system. Fortunately, Lo et al. proposed measurement device-independent quantum key distribution (MDI-QKD)[11], which tactfully uses time-reversed entangled distribution protocols. the decoy method MDI-QKD protocol is considered the most secure QKD scheme at present. Relevant experimental verification is becoming more mature. The world's longest transmission distance under ultra-low loss fibre has been achieved at 404 km [12].

In the future, QKD is expected to be implemented in a quantum network, where many user nodes will work with central server through quantum channels[13]. First of all, the MDI-QKD construction architecture is very suitable for building a QKD network with a star architecture and a central relay. MDI allows the existence of untrusted relays which can also guarantee security. Nevertheless, MDI-QKD has its disadvantage in practicality and commercialization, which is lower key rate. The HOM interference play an important role in MDI-QKD system, which generally requires that two photons prepared by the two light sources are independent, in detail, and indistinguishable in polarization and time domain. Due to the influence of noise, temperature and vibration, a decrease in the interference contrast unavoidably affects the final key rate. Moreover, the low detection efficiency of the current commercial single photon detector limits the QKD channel security key rate. Against this background, considering multiplexing QKD channels into a feasible solution can be further discussed.

Photons can be routed to different parties by different wavelength channels using WDM, thereby supporting the requirement of multiple clients[14]. In terms of experimental implementation, Yoshino et al. used WDM technology to implement a three-channel QKD system, where interferometers of multiple wavelengths were used for encoding and decoding and achieved continuous running of key distribution of 45 km in fibre[15]. Above all, it is noted that QKD combined with WDM technology can support dozens of users at the same time. The combination of WDM technology and MDI protocol has great potential for higher key rate quantum communication networks[16].

In this paper,the time-phase encoded MDI-QKD protocol with WDM are investigated, which makes full use of the MDI protocol to ensure the security of key distribution as well as its strong networking and multiplexing capabilities, and makes up for previous shortcomings of the low key rate. More importantly, in this paper, the reference-frame-independent (RFI) protocol is utilized to ensure that the QKD system can withstand problems of unstable reference frames. In the end, the feasibility of the protocol based on WDM technology is demonstrated through numerical simulation.

2. MDI-QKD Protocol

We illuminate the process of the MDI-QKD system with WDM into five steps including the key length estimation method and display its schematic diagram in Figure 1. In the following, the realization of the RFI-MDI-QKD protocol is elaborated step by step.

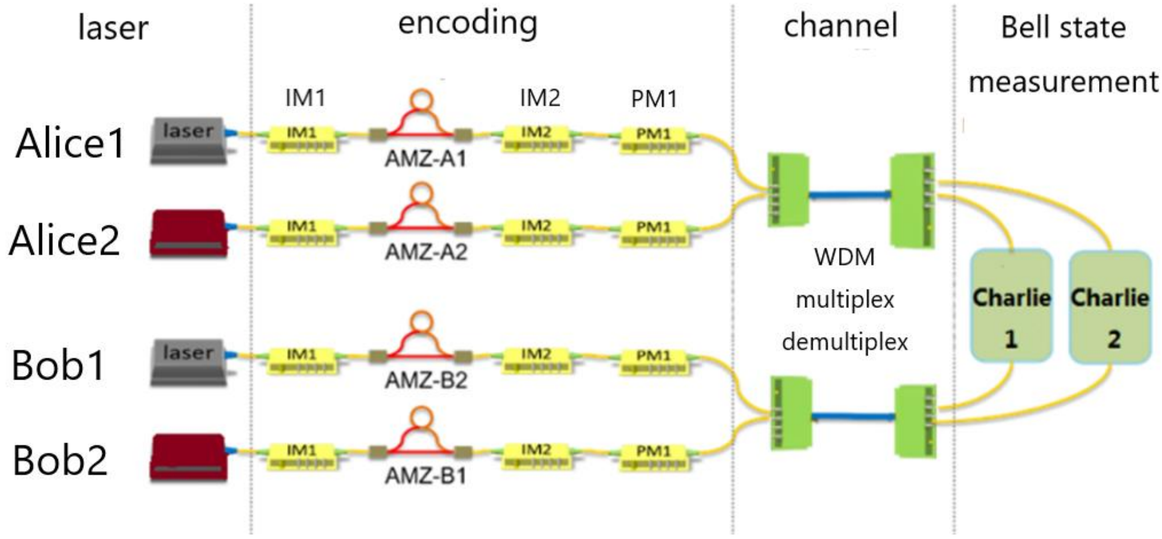

Figure 1: The schematic diagram of the time-bin phase encoded MDI-QKD with WDM in several channels: Two MDI-QKD systems are multiplexed in one fibre channel.
IM: Intensity modulator; PM: Phase modulator; AMZ: Asymmetric Mach–Zehnder interferometer; WDM: Wavelength division multiplexer.

2.1. Preparation with Z basis

In RFI-MDI-QKD, we suppose the aligned Z-basis between Alice and Bob. As shown in Figure 1, after the photons pass through the first asymmetric Mach–Zehnder interferometer, the photons are split into two adjacent optical pulses, and the intensity of either of the first and last two pulses will be reduced to 0 by IM2, corresponding to 0 bit and 1 bit respectively.

2.2. Preparation with X basis

IM1 does not work, that is, neither pulse is attenuated. PM1 is used to modulate one of two adjacent pulses with the phase of 0 or π corresponding to X_0 and X_1 respectively while π/2 and 3π/2 to Y_0 and Y_1.

2.3. Preparation of decoy-state

IM1 is used to modulate and implement decoy-state in MDI-QKD. In addition to the signal state, two other intensities will be used for a number of decoy states. The mean photon number is μ, ν and ω respectively, which correspond to signal state, decoy state and vacuum state respectively. The vacuum state is obtained by an empty triggering pulse.

2.4. Multiplex and demultiplex

On the one hand, the multiplexing WDM is used to integrate these signals of different wavelengths into a single-mode fibre for long-distance transmission. On the other hand, demultiplexing WDM was used to separate the optical signals with different wavelengths and transit them to the corresponding Charlie terminals for bell state measurement. As shown in the Figure.1, Alice-1 and Bob-1 constitute a communication group, and the wavelength of the two lasers denoted by identical color ensures the success of two-photon interference MDI-QKD measurement at the Charlie-1 site.

2.5. Measurement

A Successful Bell state measurement corresponds to the coincidence trigger of two detectors (associated with orthogonal polarization). For the case when both Alice and Bob prepare the same bit with Z basis, which means two photos are located at the same time-bin, after the interference in BS1 shown in Figure 2, the photons will all go into either BS2 or BS3. In another word, only one of the four detectors will be triggered. This is not a successful bell state measurement and can be discarded. For the case in a Z basis, if bits are prepared differently, two photons will go into BS2 and BS3 with equal possibility, which will cause the synchronous triggers of SPD1, 4 or SPD2, 3. Charlie announces the event of this successful bell state, Therefore, after bob and Alice share their basic choice, they know they prepare a different bit from each other, so an identical key bit can be generated. The analysis of the case in X and Y basis is similar.

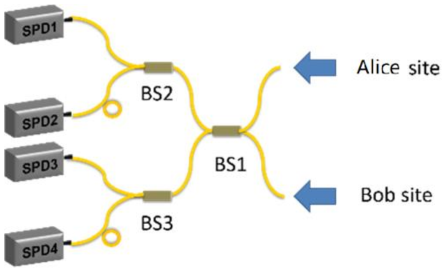

Figure 2: The structure of bell state measurement in the Charlie site. BS: Beam splitter; SPD: Single photon detector.

Charlie will record the measurement result. In this case, after subsequent logical and statistical calculations, Alice and Bob can share the same security key.

According to statistical data Q_w^{mn} and EQ_w^{mn}, which are the count rate and error rate corresponding to the successful case that the number of m photons (decoy or signal state by Alice) is sent by Alice and the number of n photons prepared by Bob, the upper and lower bound of the single photon yields denoted by superscript, L are deduced. The estimation formula group is as below[13]:

$$\begin{gathered} m^{11L} \geq (T_1 - T_2 - a_1' b_2' T_3)\big(a_1 a_1' (b_1 b_2' - b_1' b_2)\big)^{-1} \\ m^{1U} \leq (M^{v_i v_i} - T_3)(a_1 b_1)^{-1} \\ T_1 = a_1' b_2' \mathrm{Q}^{\mathrm{v_i v_i}} + a_1 b_2 a_0' \mathrm{Q}^{\mathrm{o}\mu_\mathrm{i}} + a_1 b_2 a_0' \mathrm{Q}^{\mu_\mathrm{i}\mathrm{o}} \\ T_2 = a_1 b_2 \mathrm{Q}^{\mu_\mathrm{i}\mu_\mathrm{i}} + a_1 b_2 a_0' b_0' \mathrm{Q}^{\mathrm{oo}} \\ T_3 = a_0 \mathrm{Q}^{\mathrm{ov_i}} + b_0 \mathrm{Q}^{\mathrm{v_i o}} - a_0 b_0 \mathrm{Q}^{\mathrm{oo}} \\ a'(b')_k = \mu_i^k e^{-\mu_i} (k!)^{-1} \\ a(b)_k = v_i^k e^{-v_i} (k!)^{-1} \\ M^{\lambda_A \lambda_B} \in \left[Q^{\lambda_A \lambda_B}, EQ^{\lambda_A \lambda_B}\right] \end{gathered} \tag{1}$$

Finally, the postprocessing including privacy amplification and correction are performed, and the final key is estimated by the Z-base single photon key rate, the information of Eve I_E and the key correction efficiency coefficient f (set as 1.16 in the simulation). The final formula is expressed as:

$$R = m_{ZZ}^{11}(1 - I_E) - Q_{ZZ}^{\mu\mu} f h\big(E_{ZZ}^{\mu\mu}\big) \tag{2}$$

I_E is estimated by the error gains of X basis in the original MDI-QKD protocol, However, as the X basis information is encoded by phase, it drifts periodically and leads to fluctuation or even fails to secure key generation. Therefore, an alternative method or protocol is needed to solve this system loophole.

2.6. Estimation of I_E in RFI protocol

In the QKD system, the basis for encoding photons at the Alice site is called the transmitting reference frame, and the basis for decoding the photons at the Bob site is called the receiving reference frame. If the reference frame shared by Alice and Bob is inconsistent, the correct bit value cannot be obtained with certainty. Therefore, calibrating the reference frame before the two parties communicate, or maintaining the consistency of the reference frame between the sending and receiving ends guarantees that the correct key is obtained, and the key distribution can perform continually. Therefore, most of the actual QKD systems need to calibrate the reference frames of both parties in real time. The current technology can achieve real-time phase compensation, but it will increase the system construction cost.

To cope with this problem, the reference frame-independent QKD protocol was proposed[17]. The Z basis is stable while the remaining two bases which are X and Y will drift with a variety of time. If X_A, X_B and Y_A, Y_B are used to denote the X, Y basis of Alice and Bob respectively, their relationship can be represented by:

$$\begin{gathered} X_B = X_A \cos\theta + Y_A \sin\theta \\ Y_B = Y_A \cos\theta - X_A \sin\theta \\ Z_B = Z_A \end{gathered} \tag{3}$$

where β characterize the degree of drift between the two reference frames. For instance, the circular polarization of light in free space channels, such as communications Earth-to-satellite QKD system, is less affected by the environment where the circular polarization of light is regarded as the Z base. Also, as to fibre or integrated optical chips, the time-bin information is stable and used to encode Z. The experimental applications of the RFI protocol have demonstrated this protocol has good performance[18][19][20][21]. The theoretical model in this paper is based on the time-bin phase encoded system where the time-bin is chosen as the Z basis and the phase is allowed to drift.

Different from protocols such as BB84, the two parties not only retain the same results, but also use the measurement results of different bases in combination with other information to estimate Eve's information obtained by. where the key parameter C is essential in RFI protocol,

$$C = \langle X_A X_B \rangle^2 + \langle X_A Y_B \rangle^2 + \langle Y_A X_B \rangle^2 + \langle Y_A Y_B \rangle^2 = \sum_{\alpha,\beta \in (X,Y)} (1 - 2E_{\alpha\beta})^2 \tag{4}$$

where $E_{\alpha\beta}$ is the bit error of X and Y basis. Here, C is independent of β and its theoretical maximum value of C is 2. The the key rate estimation divided into the single photon yield and the amount of Eve leakage. The security of the QKD protocol can be analyzed by the equivalent entanglement protocol. Alice to Bob QKD structure is equivalent to a pair of entanglement photons measured by Alice and Bob, which is $|\phi^+\rangle_{AB}$, the density matric of mixed state after a collective attack

$$\rho_{A\,B} = \lambda_1\, P_{\Phi^+} + \lambda_2\, P_{\Phi^-} + \lambda_3 P_{\Psi^+} + \lambda_4 P_{\Psi^-} \tag{5}$$

Then it can be deduced that $C = 2[(\lambda_1 - \lambda_2)^2 + (\lambda_3 - \lambda_4)^2]$. Here, those four non-negative parameters λ_i have three constraints: the sum of the four parameters is 1, and be related to the observed values of E_{ZZ}^{11}, C. Another free variable will be used to maximize the amount of information on Eve. According to the first two constraints, we introduce two parameters μ, $v \in [0,1]$, and $\lambda_1 =$

$(1 - E_{ZZ}^{11}\,)\frac{1+\mu}{2}$, $\lambda_2 = (1 - E_{ZZ}^{11})\frac{1-\mu}{2}$, $\lambda_3 = \frac{1+v}{2}E_{ZZ}^{11}$, $\lambda_4 = \frac{1-v}{2}E_{ZZ}^{11}$. At this time, Eve's information is estimated by,

$$I_E(E_{ZZ}^{11}, \mu, v) = (1 - E_{ZZ}^{11})h\left(\frac{1+\mu}{2}\right) + E_{ZZ}^{11}h\left(\frac{1+v(\mu)}{2}\right) \tag{6}$$

where $h(x)$ is the binary entropy function. Therefore, the equation of C will be written as

$$C = 2\left[(1 - E_{ZZ}^{11})^2\mu^2 + {E_{ZZ}^{11}}^2 v^2\right] \tag{7}$$

To maximize Eve's information, $I_E(E_{ZZ}^{11}, C) = \max\limits_{C} I_E\left(E_{ZZ}^{11,}, \mu, v\right)$. Note that $I_E(0, C) = h\left[\left(1 + (C/2)^{1/2}\right)/2\right]$. When $E_{ZZ}^{11,} > 0$, there is

$$v = \frac{\left(C/2 - \left(1 - E_{ZZ}^{11}\right)^2\mu^2\right)^{1/2}}{E_{ZZ}^{11}} \tag{8}$$

Because $v \in [0,1]$, so $\mu \in [\mu_{min}, \mu_{max}]$, where

$$\mu_{min} = \frac{1}{1-E_{ZZ}^{11}}\left(\max\left[C/2 - {E_{ZZ}^{11}}^2, 0\right]\right)^{1/2} \tag{9}$$

$$\mu_{max} = \min\left(\frac{1}{1-E_{ZZ}^{11}}\left(\frac{C^L}{2}\right)^{1/2}, 1\right) \tag{10}$$

The single photon yield is obtained through the statistic of gains in both signal and decoy states, and used to estimate the C value in the RFI protocol[22]. In summary, the reference frame-independent protocol can tolerate the drift of the reference frame without adding extra devices, which greatly promotes the robustness and stability of QKD.

3. Simulation Result

We establish a symmetric theoretical model for RFI-MDI-QKD with wavelength division multiplexing technology. Supposing Alice and Bob are at the same distance from Charlie and share the same signal intensities, the decoy state intensity is set to 0.01 while the optimized value of signal states changes with distance tofind out optimized key rate. In the simulation, the dark count rate of the detector is set to 3×10^{-6} while the detection efficiency is 15%. The loss in fibre derives mainly from two aspects, Rayleigh scattering and material absorption. As for the wavelength larger than the C band (1530 nm – 1565 nm), the attenuation due to strong absorption from materials of fibre is significantly increasing, thereby unavailable for long-distance fibre communication. In the C-band range, Rayleigh scattering can be considered as the biggest influence on the attenuation coefficient which can be reckoned by $\alpha[dB/km] = 1.7({}^{0.85}/_{\lambda[\mu m]})^4$. Furthermore, considering other factors of attenuation, such as the injection loss of WDM, 4dB is additionally included in the simulation of channel loss. Finally, we can get the key length and compare the situation of multiplexing of 10 and 20 channels which has the same wavelength interval between each other in the C band.

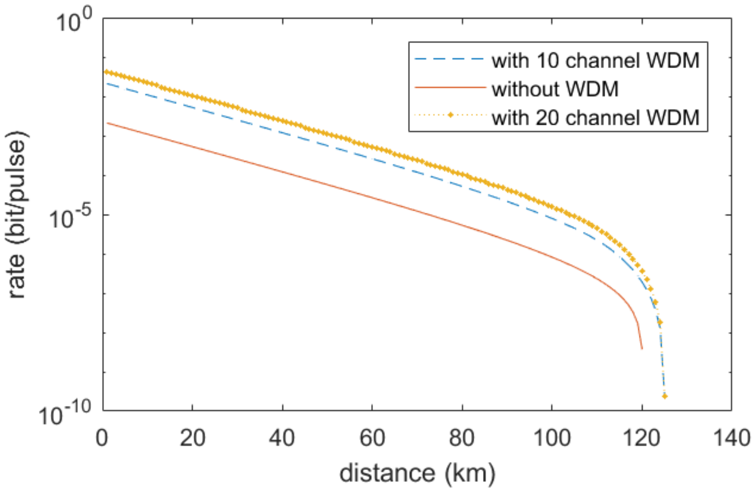

Figure 3. Simulation result of RFI-MDI-QKD with WDM

As shown in Figure 3, it can be seen that more multiplex channels used for QKD communication slightly affect the longest transmission distance, but the relationship between the key lengths with and without WDM is presented as an obvious multiplication relationship with the increase of the multiplexed channels number. Besides, we compare the key length beneath phase drift of 0 and π/4. As result, the misalignment of the reference frame has no influence on key length (not shown since the equality of the key length between different phase drifts). The results show that RFI-MDI-QKD based on WDM is an effective method to improve the key rate and the network construction capability of QKD.

4. Conclusion

In this paper, the scheme of WDM RFI-MDI-QKD in multiplex channel by is proposed. Its scheme diagram and performance through numerical simulation are illustrated and researched. The result shows that RFI-MDI-QKD can resist unstable reference frames and improve the shortcoming of low-key rates of MDI-QKD. In the future, we will further explore how WDM channels affect the performance of MDI-QKD to promote its feasibility in the real world.

Acknowledgments

We would like to express our gratitude for financial support from the Key Topics of Beijing Polytechnic NO. 2021Z016-KXZ, the State Key Laboratory of Information Photonics and Optical Communications (Beijing University of Posts and Telecommunications) No. IPOC2021ZT10, BUPT Innovation and Entrepreneurship Support Program (Grant No. 2022-YC-T051), the Fundamental Research Funds for the Central Universities No. 2019XD-A02.

References

[1] Rivest R L, Shamir A and Adleman L J 1978 A method for obtaining digital signatures and public-key cryptosystems *Communications of the ACM*. **21(2)** 120-6
[2] Bennett C H and Brassard G 1984 Quantum Cryptography: Public Key Distribution, and Coin-Tossing *Proc 1984 IEEE International Conference on Computers, Systems, and Signal Processing*. 175-9
[3] Shor P W and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol *Phys. Rev. Lett.* **85** 441–4
[4] Koashi M and Preskill J 2003 Secure Quantum Key Distribution with an Uncharacterized Source *Phys. Rev. Lett.* **90** 4
[5] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 Limitations on practical quantum

cryptography *Phys. Rev. Lett.* **85** 1330–3

[6] Gottesman D, Hoi-Kwonglo L O, Lütkenhaus N and Preskill J 2004 Security of quantum key distribution with imperfect devices *Quantum Inf. Comput.* **4** 325–60

[7] Wang J Y, *et al* 2013 Direct and full-scale experimental verifications towards ground-satellite quantum key distribution *Nat. Photonics* **7** 387–93

[8] Wang, S, et al 2015 Experimental demonstration of a quantum key distribution without signal disturbance monitoring *Nature Photonics*. **9(12)** 832-6

[9] Boaron A, Boso G, Rusca D, Vulliez C, Autebert C, Caloz M, Perrenoud M, Gras G, Bussières F, Li M J, Nolan D, Martin A and Zbinden H 2018 Secure Quantum Key Distribution over 421 km of Optical Fibre *Phys. Rev. Lett.* **121** 1–5

[10] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 Hacking commercial quantum cryptography systems by tailored bright illumination *Nat. Photonics* **4** 686–9

[11] Lo H K, Curty M and Qi B 2012 Measurement-device-independent quantum key distribution *Phys. Rev. Lett.* **108** 1–7

[12] Yin H L, *et al* 2016 Measurement-Device-Independent Quantum Key Distribution over a 404 km Optical Fibre *Phys. Rev. Lett.* **117**

[13] Liu H, *et al* 2019 Experimental Demonstration of High-Rate Measurement-Device-Independent Quantum Key Distribution over Asymmetric Channels *Phys. Rev. Lett.* **122** 1–20

[14] Brassard G, Bussieres F, Godbout N and Lacroix S 2003 Multiuser quantum key distribution using wavelength division multiplexing *Applications of Photonic Technology* **6** 149-53

[15] Yoshino K, Fujiwara M, Tanaka A, Takahashi S, Nambu Y, Tomita A, Miki S, Yamashita T, Wang Z, Sasaki M and Tajima A 2012 High-speed wavelength-division multiplexing quantum key distribution system *Opt. Lett.* **37** 223

[16] Mao Q, Zhao S, Wang L, Qian C and Chen H 2017 Measurement-device-independent quantum key distribution based on wavelength division multiplexing technology *Chinese Journal of Quantum Electronics* **34(1)** 46

[17] Laing A, Scarani V, Rarity J G and O'Brien J L 2010 Reference-frame-independent quantum key distribution *Phys. Rev. A - At. Mol. Opt. Phys.* **82** 1–5

[18] Liu H, Wang J, Ma H and Sun S 2018 Polarization-multiplexing-based measurement-device-independent quantum key distribution without phase reference calibration *Optica* **5** 902

[19] Liang W Y, Wang S, Li H W, Yin Z Q, Chen W, Yao Y, Huang J Z, Guo G C and Han Z F 2014 Proof-of-principle experiment of reference-frame-independent quantum key distribution with phase coding *Sci. Rep.* **4** 0–5

[20] Wang C, Song X T, Yin Z Q, Wang S, Chen W, Zhang C M, Guo G C and Han Z F 2015 Phase-Reference-Free Experiment of Measurement-Device-Independent Quantum Key Distribution *Phys. Rev. Lett.* **115** 1–5

[21] Chun H, Choi I, Faulkner G, Clarke L, Barber B, George G, Capon C, Niskanen A, Wabnig J, O'Brien D and Bitauld D 2017 Handheld free space quantum key distribution with dynamic motion compensation *Opt. Express* **25** 6784

[22] Zhang C M, Zhu J R and Wang Q 2017 Practical decoy-state reference-frame-independent measurement-device-independent quantum key distribution *Phys. Rev. A* **95** 1–5