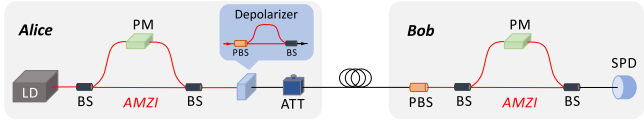
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Real-Time Phase Tracking Scheme With Mismatched-Basis Data for Phase-Coding Quantum Key Distribution

Volume 12, Number 3, June 2020

Dong Wang
Xiaotian Song
Liangjiang Zhou
Yibo Zhao



DOI: 10.1109/JPHOT.2020.2986343

Real-Time Phase Tracking Scheme With Mismatched-Basis Data for Phase-Coding Quantum Key Distribution

Dong Wang, Xiaotian Song, Liangjiang Zhou, and Yibo Zhao

National Key Laboratory of Microwave Imaging Technology, Institute of Electronics, Chinese Academy of Sciences, Beijing 100190, China

DOI:10.1109/JPHOT.2020.2986343

Manuscript received December 5, 2019; revised April 1, 2020; accepted April 3, 2020. Date of publication April 13, 2020; date of current version May 13, 2020. Corresponding authors: Xiaotian Song; Yibo Zhao. (e-mail: songxt@mail.ustc.edu.cn; zhaoyibo@mail.ustc.edu.cn).

Abstract: Phase drift is an inevitable problem in the practical implementation of phase-coding quantum key distribution (QKD) systems. Conventional active phase tracking and compensation solutions cannot be implemented during the key transmission process, resulting in reduced efficiency of the system. In this paper, we propose a single-photon level real-time phase tracking scheme using only the estimated quantum bit error rate (QBER) and mismatched-basis data to acquire the phase drift parameter instead of a phase scanning process or reference light pulses, without extra hardware or interrupting the transmission of quantum signals. This scheme is applied into a phase-coding QKD system with active phase disturbance and obtains an average QBER of 1.01% with a standard derivation of 0.37% over 50 h of continuous operation. Experimental results show that this scheme enables QKD systems to operate continuously with long-term stability and keep a low level of QBER even with rapid phase drift, suggesting its suitability for practical applications.

Index Terms: Quantum key distribution, phase tracking.

1. Introduction

Quantum key distribution (QKD) provides information-theoretic secure keys between two remote parties over a non-protected communication channel. Since the proposal of BB84 protocol [1], QKD has been extensively studied both theoretically and experimentally [2]–[7], even implemented in telecom networks [8]–[11]. To date, the practicality of QKD systems has been significantly improved and transferred from laboratory studies to applicable commercial products.

In real life implementations, it is highly demanded to maintain the long term stability and reliability of QKD systems to sustainedly support the encryption applications. While the deployment environments of QKD systems are usually complex and volatile, installed fibers and optical interferometers are sensitive to environmental fluctuations and drifts, leading to polarization and phase drifting. By utilizing the Faraday-Sagnac-Michelson interferometer (FSMI) [12] or Sagnac-Mach-Zehnder interferometer (SMZI) [13] in a phase-coding QKD system, the birefringence variations in installed fibers can be automatically compensated, thus eliminating the polarization effect of installed fibers. However, phase drift is still an inevitable problem for the interferometers in phase-coding QKD systems, which can directly increase the quantum bit error rate (QBER) and impact the stability of QKD systems. Phase drift mainly originates from the different response of Alice and Bob's

interferometers to the ever-changing ambient environment, such as the variation of temperature or mechanical vibration. To overcome this problem, several countermeasures are developed. For instance, passive schemes such as thermal and mechanical isolation are adopted in order to decrease the influence of the ambient environment [14], [15], just slowing down the speed of phase drift and increasing the complexity of systems. In some active schemes, a fiber-stretcher [16], [17] is placed in the receiver's interferometer to actively adjust the optical path difference, which is driven based on a feedback control algorithm. These schemes can continually compensate phase drift though, reference light pulses with higher intensity are required to obtain the feedback signal, resulting in an increase of the fabrication difficulty of interferometers and system complexity. A more common and effective measure adopted in recent years is the "scanning-and-transmitting" scheme, in which drift parameters used in phase compensation are obtained from a phase scanning process [18]–[20]. While in this scheme, the key transmission process has to be interrupted during the scanning process, since the light source, interferometers, and single-photon detectors (SPDs) in the QKD system are occupied during the acquisition time of the drift parameter. Therefore, the scanning process will occupy a proportion of the system time, and decrease the duty cycle [19] of the transmission process, resulting in a reduction of transmission efficiency and consequently the secure key generation rate of the QKD system. Most recently, an active phase compensation scheme based on the machine learning algorithm is proposed [21]. This scheme enables QKD systems to predict the parameter variations beforehand and actively perform real-time control on corresponding devices to perform the phase tracking, increasing the efficiency of the QKD system. Nevertheless, a large number of data points should be collected for the training algorithm in advance before predicting. In addition, the scanning process is still required to update the algorithm to eliminate the cumulative error in the prediction phase and keeping the QBER of the QKD system within an acceptable level. As a consequence, this scheme appears to be complicated and time-consuming.

In this paper, we present a real-time phase tracking scheme that removing the requirement of reference light pulses or phase scanning process, with which QKD systems can continuously run without being interrupted by the phase compensation process. Thus the duty cycle of the key transmission process can reach 1. The key point of our scheme is that the phase drift parameter can be directly calculated by utilizing only the estimated QBER and the raw key bits from the mismatched-basis measurements, where two parties use different bases that are normally discarded in the BB84 protocol. The estimation of phase drift parameter is quite simple and efficient and requires no extra hardware, thus significantly decreasing the complexity and increasing the total efficiency of QKD systems. When applied to a phase-coding BB84 QKD system, the effectiveness of this scheme is confirmed. Experimental results show that the system can be operated stably over 50 hours, the obtained average QBER is 1.01% with a standard deviation of 0.37%.

2. Real-Time Phase Tracking Scheme

In a typical asymmetric Mach-Zehnder interferometer (AMZI) based phase-coding BB84 QKD system, Alice and Bob randomly select one of the four phase shifts $\{0, \pi/2, \pi, 3\pi/2\}$ to perform the encoding and decoding operation, respectively. Since it is the relative phase between Alice and Bob that matters, the driving voltage of Alice's phase modulator (PM) for zero-phase (V_0^a) can be fixed as 0, then the driving voltage for other phases can be determined based on the half-wave voltage of PM. As for Bob, once the driving voltage of Bob's PM for π-phase (V_π^b) is ascertained, which has a phase difference of π with the corresponding phase of V_0^a, the working points of Bob's PM for other phases can be obtained [19] as well. Here we have assumed that the half-wave voltage value of PM is constant and the relationship between the phases and driving voltages is linear.

With the determined driving voltages of the four phase shifts, the key transmission process can be accomplished between Alice and Bob. However, the phase difference changes with phase drift, leading to an increase of QBER and variation of detection counts of SPD in consequence.

In order to compensate for the phase drift actively, it is common to perform a scan-operation to acquire V_{π}^{b}, then adjust voltage working points so that phases can be drawn back to their proper positions. To remove the requirement of scan-operation, we propose a continuously working phase tracking scheme to compensate for the phase drift. In our scheme, the phase drift parameter can be continually calculated using QBER and the mismatched-basis data. With the calculated phase drift parameter, the QKD system is allowed to perform real-time phase tracking by adjusting voltage working points. For instance, denoting $V_{\pi,i}^{b}$ as the driving voltage of π-phase of Bob and δ_i as the acquired phase drift parameter in the ith round of QKD session, the driving voltage for the next QKD session can be immediately obtained,

$$V_{\pi,i+1}^{b} = V_{\pi,i}^{b} + \frac{\delta_i}{\pi} V_{h}^{b}, \tag{1}$$

where V_{h}^{b} is the half-wave voltage of Bob's PM, which can be measured beforehand.

Similarly, the driving voltages for the other three phase shifts can be adjusted in the same way. As a result, the modulated phase in each session can be modified by using data from the previous session, thus enabling the system to track the phase continuously. The highlight of this scheme is the way to accurately calculate the phase drift parameter δ by using QBER and the mismatched-basis data. In the following, we demonstrate the derivation of δ.

According to the model of Ref. [22], the detection probability of one SPD in a phase-coding QKD system can be expressed as

$$\begin{aligned} P(\Delta\varphi) &= 1 - (1 - P_d) e^{-m(1+V\cos\Delta\varphi)} \\ &\approx P_d + m\,(1 - P_d)\,(1 + V\cos\Delta\varphi), \end{aligned} \tag{2}$$

where $m = \frac{1}{2}\mu\eta_b\eta_c\eta_d$ satisfying the condition of $m \ll 1$, μ is the mean photon number per pulse emitted by Alice, η_b (η_c) is the transmittance of the receiver(fiber channel), η_d (P_d) is the detection efficiency (dark count probability) of SPD, $\Delta\varphi = \varphi_a - \varphi_b$ is the phase difference between Alice and Bob, V is the interference fringe visibility of the system. If the phase drift of the system is δ, then Eq. (2) is modified as

$$P(\Delta\varphi) = P_d + m\,(1 - P_d)\,[1 + V\cos(\Delta\varphi + \delta)]. \tag{3}$$

Considering a QKD system with unbiased-basis choice, the repetition frequency of which is f, we can obtain the counting rate of one SPD,

$$C(\Delta\varphi) = \frac{f}{4} P(\Delta\varphi), \tag{4}$$

where $\Delta\varphi = 0, \pi, \pm\pi/2$, and the counts $C(0)$ and $C(\pi)$ ($C(\pm\pi/2)$) correspond to the matched-basis (mismatched-basis) events, meaning that Alice and Bob have selected the same (different) bases.

From Eq. (3) and (4), we can obtain the following formulae,

$$\begin{aligned} C(-\pi/2) - C(\pi/2) &= \frac{f}{2} m\,(1 - P_d)\,V\sin\delta, \\ C(-\pi/2) + C(\pi/2) &= \frac{f}{2}\,[P_d + m\,(1 - P_d)]\,. \end{aligned} \tag{5}$$

According to the definition of QBER, and combining Eq. (5), we can derive the relationship between QBER and the phase drift parameter and the mismatched-basis photon counts as

$$\begin{aligned} QBER &= \frac{C(\pi)}{C(0) + C(\pi)} = \frac{1}{2}\left[1 - \frac{m\,(1 - P_d)\,V\cos\delta}{P_d + m\,(1 - P_d)}\right] \\ &= \frac{1}{2}\left\{1 - \frac{C(-\pi/2) - C(\pi/2)}{\tan\delta\,[C(\pi/2) + C(-\pi/2)]}\right\}. \end{aligned} \tag{6}$$

If the QBER and mismatched-basis photon counts of the system are available, the phase drift parameter can be directly calculated from Eq. (6), which can be used in the phase compensation.

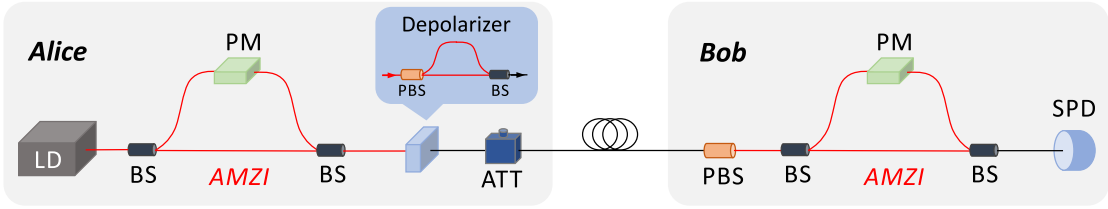


Fig. 1. Experimental setup of QKD system. (LD, laser diode; BS, beam-splitter; PM, phase modulator; ATT, attenuator; PBS, polarization beam splitter; SPD, single-photon detector). The red lines represent polarization-maintaining fibers (PMFs), and the black ones are single-mode fibers (SMFs).

In fact, after basis sifting, a portion of sifted key bits that are matched-basis are revealed to estimate the QBER to be further used and discarded during the error correction procedure of QKD. Nevertheless, the key bits of mismatched-basis are discarded in the original BB84 protocol. In our scheme, these mismatched-basis key bits can be used to calculate the phase drift parameter. When the basis sifting is accomplished, Alice announces the phase choices of these mismatched-basis data, then Bob collects the corresponding statistical counts $C(\pm\pi/2)$ of SPD. It's worth stressing that, the resources cost by this procedure are rather limited, which can be neglected compared to the whole time cost by post-processing. Moreover, this procedure won't cause any security problem of the system. Thus with the estimated QBER and mismatched-basis data, the phase drift parameter can be easily obtained with Eq. (6),

$$\delta = \arctan \frac{C(-\pi/2) - C(\pi/2)}{(1-2QBER)\,[C(-\pi/2) + C(\pi/2)]}, \tag{7}$$

which can be used in Eq. (1) to accomplish the phase tracking task.

As for the case of rapid phase drift, the calculation of phase drift parameter with this scheme could be inaccurate, thus a modification of the calculated value is required. According to the concept of proportional-integral-derivative (PID) control algorithm, taking account of the current and history of phase drift, one can obtain the correction of phase drift parameter,

$$\Delta\delta_i = k_1\delta_{i-1} + k_2\sum_{n=0}^{i-1}\delta_n,\ i \geqslant 1, \tag{8}$$

where k_1, and k_2 are the coefficients. Then the corresponding driving voltage in Eq. (1) can be adjusted to be

$$V^b_{\pi,i+1} = V^b_{\pi,i} + \frac{(\delta_i + \Delta\delta_i)}{\pi}V^b_h. \tag{9}$$

3. Experiment and Results

The proposed real-time phase tracking scheme is tested on a phase-coding BB84 QKD system as shown schematically in Fig. 1. The system works at a repetition frequency of 1 MHz. The laser pulse duration is about 50 ps and the output pulse intensity of Alice is set to be $\mu = 0.6$. The detection efficiency and the dark count rate of the SPD are 10% and 5×10^{-6}/gate, respectively.

In order to obtain high and stable interference fringe visibility, we have added a depolarizer [23] after Alice's AMZI, and a polarization beam splitter (PBS) before Bob's. The inset of Fig. 1 shows the configuration of depolarizer, which consists of a polarization-maintaining BS and a PBS. The input pulse is first split into two beams with identical polarization in the PMFs, then combined at the PBS with orthogonal polarization. One output arm is delayed with respect to the other so that the recombined beams are incoherent and cannot be time-resolved with the detectors. Therefore the depolarizer randomizes the polarization of the photons before entering the quantum channel, and the PBS at Bob's input polarizes these depolarized photons with a 50% loss. Furthermore,

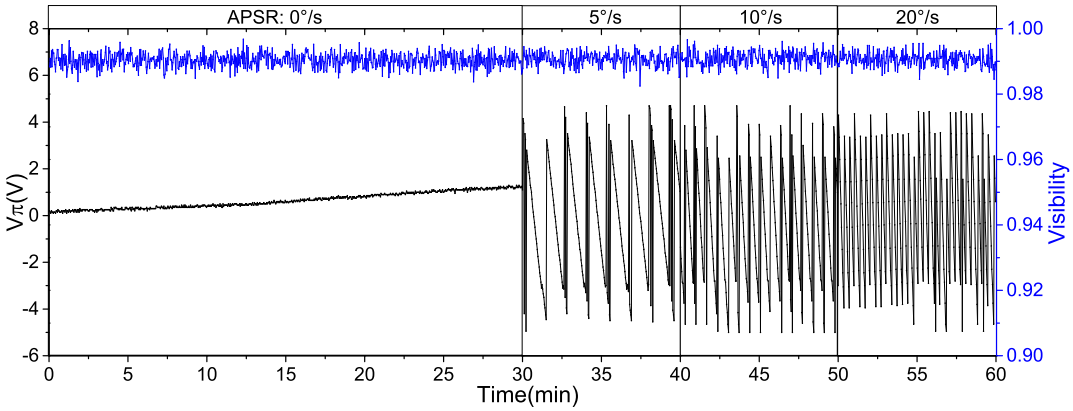


Fig. 2. Variations of interference fringe visibility of our system and driving voltage for π-phase of Bob at different value of APSR. The corresponding value of APSR are displayed in the box for different measurement time.

all the components of AMZI are polarization-maintaining elements, ensuring the photons have the same polarization in each arm. Consequently, this QKD system can continuously operate without intervention.

Usually, phase drift is more rapid and irregular in the field than that in the laboratory. In order to evaluate the practical performance of the proposed phase tracking scheme, an active phase disturbance achieved by changing V_0^a with time is added in the QKD system. The total phase drift in the experiment is a joint effect of the active phase disturbance and laboratory environment variations, which can simulate the realistic situation of the field to some extent. Considering the phase drift rate reported by Makarov [18] and Chen [19] are $2^\circ/s$ and $4^\circ/s$, respectively, we chose four rational value of the active phase scrambling rate (APSR) in the experiment, i.e., $0^\circ/s$, $5^\circ/s$, $10^\circ/s$, and $20^\circ/s$.

Through a scanning process, the corresponding driving voltages for π-phase of Bob's PM at different APSR, as well as the interference fringe visibility of the AMZIs are recorded, as shown in Fig. 2. Within a measurement time of 60 minutes, the duration for APSR of $0^\circ/s$ is 30 minutes, and that for $5^\circ/s$, $10^\circ/s$, and $20^\circ/s$ are all 10 minutes, respectively.

As can be seen from Fig. 2 that, the interference fringe visibility of the system remains stable over 60 minutes at different APSR, the calculated value of which is $99.07 \pm 0.21\%$. Fig. 2 also demonstrates that phase drift rates agree well with the APSR.

In the following we set the channel loss of our QKD system to be 3 dB, resulting in a 927.1 of mean total mismatched-basis counts per second. Denoting M1 as the driving voltages adjustment method with Eq. (1), and M2 the method with Eq. (9). Our phase tracking scheme is applied into the QKD system, both of M1 and M2 are tested at four APSR. For M1 (M2) we measured the QBER over 2.5 hours at each APSR. Fig. 3 displays the corresponding experimental results over the total measurement time of 20 hours.

Fig. 3 including the inset indicates that our phase tracking scheme with M1 and M2 can both continuously compensate phase drift and keep the QBER within an acceptable level. At low phase drift rate, say less than $5^\circ/s$, the performances of our scheme with M1 and M2 are comparable. While in the case of rapid phase drift, QBER and its standard deviation increase with APSR when M1 is applied. As for M2, the results show a slight increase of QBER and its standard deviation with APSR, demonstrating a significant enhancement.

We also investigated the long-term stability of the system by applying the phase tracking scheme with M2. The system continuously operated with active phase disturbance ($20^\circ/s$) over 50 hours, Fig. 4 shows the QBER and corresponding statistical distribution. The obtained QBER is $1.01 \pm 0.37\%$ and keeps relatively stable during the whole measurement period.

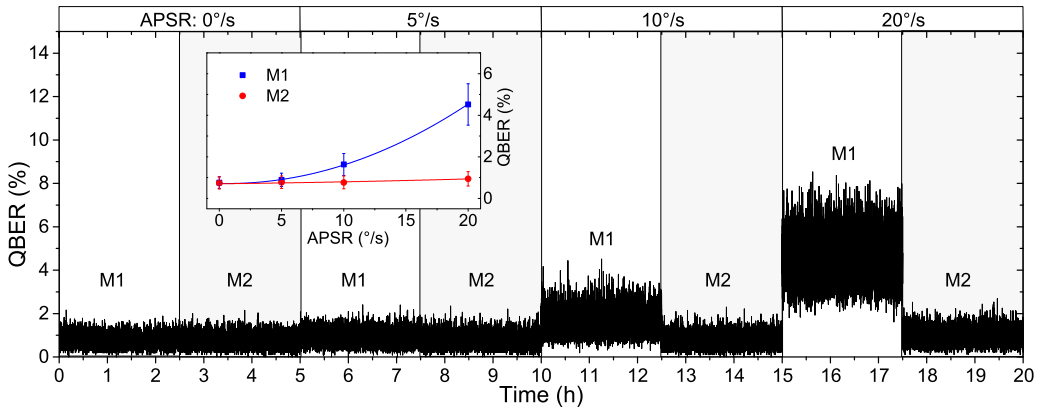


Fig. 3. Obtained QBERs of the system by applying the proposed phase tracking scheme with M1 (white areas) or M2 (grey areas) at different value of APSR. The inset shows the mean values and standard deviations of QBER with different APSR.

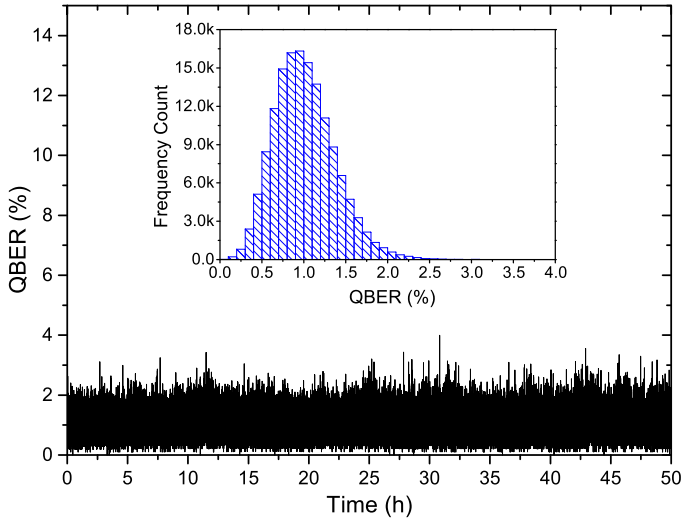


Fig. 4. QBER of our system over 50 hours of continuously running, the inset shows its statistical distribution.

4. Conclusion

In conclusion, we have proposed a real-time phase tracking scheme for phase-coding QKD systems. By exploiting the estimated QBER and mismatched-basis data, this scheme allows the QKD system to track phase drift without being interrupted. Compared to the traditional active phase compensation scheme, the requirement of reference light pulses or scanning process is removed in our scheme, leading to an improvement of practicality of QKD systems. Our scheme is applied into a phase-coding BB84 QKD system, allowing it to operate continuously and stably. Experimental results indicate the effectiveness of our scheme even with rapid phase drift. Noted that the repetition frequency of the system is 1 MHz, the calculation of phase drift parameter is easily affected by statistical fluctuation when the total mismatched-basis data are insufficient, resulting in a deterioration of the performance. We must achieve a balance between the speed and accuracy of phase drift parameter estimation. This can be ameliorated by improving the system repetition frequency of the QKD system, thus the accuracy and efficiency of phase tracking can be significantly promoted accordingly. Actually, in our recent work [13], this scheme has been

applied in a 40 MHz phase-coding QKD system, which was tested over a 50-km fiber channel for 10 days, and showed excellent long-term stability. We believe that our scheme is suitable for practical application, especially for systems with high repetition frequency.

Acknowledgment

The authors would like to thank Dr. Xiao-Ming Lu and Dr. Di Jiang for enlightened discussions and technical supports.

References

[1] C.-H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst., Signal Process.*, pp. 175–179, 1984.
[2] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Physical Rev. Lett.*, vol. 91, no. 5, Aug. 2003, Art. no. 057901.
[3] X.-F. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Rev. A*, vol. 72, no. 1, Jul. 2005, Art. no. 012326.
[4] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical Rev. Lett.*, vol. 108, no. 13, Mar. 2012, Art. no. 130503.
[5] T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," *Nature*, vol. 509, pp. 475–478, May 2014.
[6] D. Rosenberg *et al.*, "Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber," *Physical Rev. Lett.*, vol. 98, no. 1, Jan. 2007, Art. no. 010503.
[7] S. Wang *et al.*, "Experimental demonstration of a quantum key distribution without signal disturbance monitoring," *Nature Photon.*, vol. 9, pp. 832–836, Nov. 2015.
[8] M. Peev *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, Jul. 2009, Art. no. 075001.
[9] D. Stucki *et al.*, "Long-term performance of the Swiss Quantum quantum key distribution network in a field environment," *New J. Phys.*, vol. 13, Dec. 2011, Art. no. 123001.
[10] M. Sasaki *et al.*, "Field test of quantum key distribution in the tokyo QKD network," *Opt. Express*, vol. 19, no. 11, pp. 10387–10409, May 2011.
[11] S. Wang *et al.*, "Field and long-term demonstration of a wide area quantum key distribution network," *Opt. Express*, vol. 22, no. 18, pp. 10387–10409, Sep. 2014.
[12] S. Wang *et al.*, "Practical gigahertz quantum key distribution robust against channel disturbance," *Opt. Lett.*, vol. 43, no. 9, pp. 2030–2033, May 2018.
[13] X. T. Song *et al.*, "Phase-coding quantum-key-distribution system based on Sagnac-Mach-Zehnder interferometers," *Physical Rev. A*, vol. 101, no. 3, Mar. 2020, Art. no. 032319.
[14] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, "Single-photon interference over 150 km transmission using silica-based integrated-optic interferometers for quantum cryptography," *Japanese J. Appl. Phys.*, vol. 43, no. 9A/B, pp. L1217–L1219, Sep. 2004.
[15] T. Honjo, K. Inoue, and H. Takahashi, "Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer," *Opt. Lett.*, vol. 29, no. 23, pp. 2797–2799, Dec. 2004.
[16] Z. L. Yuan and A. J. Shields, "Continuous operation of a one-way quantum key distribution system over installed telecom fibre," *Opt. Express*, vol. 13, no. 2, pp. 660–665, Jan. 2005.
[17] A. R. Dixon *et al.*, "High speed prototype quantum key distribution system and long term field trial," *Opt. Express*, vol. 23, no. 6, pp. 7583–7592, Mar. 2015.
[18] V. Makarov, A. Brylevski, D. R. Hjelme, "Real-time phase tracking in single-photon interferometers," *Appl. Opt.*, vol. 43, no. 22, pp. 4385–4392, May 2004.
[19] W. Chen, Z. F. Han, X. F. Mo, F. X. Xu, G. Wei, and G. C. Guo, "Active phase compensation of quantum key distribution system," *Chin. Sci. Bull.*, vol. 53, no. 9, pp. 1310–1314, May 2008.
[20] L. J. Zhang *et al.*, "Real-time compensation of phase drift for phase-encoded quantum key distribution systems," *Chin. Sci. Bull.*, vol. 56, no. 22, pp. 2305–2311, Aug. 2011.
[21] J. Y. Liu, H. J. Ding, C. M. Zhang, S. P. Xie, and Q. Wang, "Practical Phase-Modulation Stabilization in Quantum Key Distribution via Machine Learning," *Physical Rev. Appl.*, vol. 12, no. 1, Jul. 2019, Art. no. 014059.
[22] S. P. Kulik and S. N. Molotkov, "Decoy state method for quantum cryptography based on phase coding into faint laser pulses," *Laser Phys. Lett.*, vol. 14, Nov. 2017, Art. no. 125205.
[23] P. J. Clarke, R. J. Collins, P. A. Hiskett, P. D. Townsend, and G. S. Buller, "Robust gigahertz fiber quantum key distribution," *Appl. Phys. Lett.*, vol. 98, no. 13, Mar. 2011, Art. no. 131103.