SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

August 2026, Vol. 69, Iss. 8, 180501:1–180501:8
https://doi.org/10.1007/s11432-025-4933-9

Special Topic: Quantum Information

Polarization self-compensation quantum key distribution system with 5 GHz modulation

Peng-Lei HAO[1,2,3], Wei CHEN[1,2,3,4*], Shuang WANG[1,2,3,4], Zhen-Qiang YIN[1,2,3,4], De-Yong HE[1,2,3,4], Fang-Xiang WANG[1,2,3,4], Shu-Feng LIU[5], Sheng ZHOU[5], Yu WANG[6], Guang-Can GUO[1,2,3,4] & Zheng-Fu HAN[1,2,3,4*]

[1]*Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China*
[2]*Anhui Province Key Laboratory of Quantum Network, University of Science and Technology of China, Hefei 230026, China*
[3]*CAS Center For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China*
[4]*Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China*
[5]*Anhui Asky Quantum Technology Co., Ltd., Wuhu 241002, China*
[6]*State Key Laboratory of Cryptology, Beijing 100878, China*

Received 11 November 2025/Revised 4 March 2026/Accepted 20 April 2026/Published online 21 July 2026

Abstract Quantum key distribution (QKD), which is based on the no-cloning theorem of quantum mechanics, provides information-theoretic security for private key distribution. Currently, QKD systems face limitations regarding cost, environmental adaptability, and secure key rates. Herein, we develop a time- and wavelength-division multiplexing (TWDM) method and demonstrate a practical 5 GHz phase modulation QKD system. This system, which is based on the Faraday-Michelson interferometer with adaptive polarization compensation, achieved a secure key rate of 4.084 ± 0.178 Mbps, operating continuously for over 30 h on a 50 km optical fiber channel.

Keywords quantum key distribution, adaptive polarization compensation, InGaAs/InP SPAD, 5 GHz modulation, time- and wavelength-division multiplexing

Citation Hao P-L, Chen W, Wang S, et al. Polarization self-compensation quantum key distribution system with 5 GHz modulation. Sci China Inf Sci, 2026, 69(8): 180501, https://doi.org/10.1007/s11432-025-4933-9

1 Introduction

Classical cryptography has traditionally been based on symmetric and asymmetric cryptographic algorithms that rely on computational complexity [1–3]. However, the rapid development of quantum computers poses a significant threat to the security of classical cryptographic systems, necessitating the development of quantum-resistant cryptosystems [4]. Quantum key distribution (QKD), which is based on the fundamental principles of quantum mechanics and generates a symmetric key [5, 6], is a promising solution for information-theoretic security. Since the first QKD protocol (BB84), which was proposed in 1984 [7], the performance of QKD has been continuously improved [8–10], the repetition frequency of QKD has increased to GHz levels, and superconducting nanowire single-photon detectors (SNSPDs) have been widely utilized in high-speed QKD experiments [7, 11–14], thereby significantly increasing the secure key rate (SKR). In 2020, Grünenfelder et al. [15] achieved SKR = 0.392 Mbps with a 20.2 dB channel attenuation using polarization encoding. In 2023, Li et al. [16] achieved SKR = 110 Mbps with a 2 dB channel attenuation by employing a transmitter-side polarization encoding chip. In 2022, Grünenfelder et al. [11] achieved SKR = 64 Mbps with a 1.58 dB channel attenuation using time-bin encoding.

However, their high cost and large physical size prevent the practical widespread deployment of SNSPDs [17, 18]. Therefore, QKD systems based on InGaAs/InP single-photon avalanche diodes (SPADs) are considered superior in practical deployment [19, 20]. An InGaAs/InP SPAD can be operated in either the free-running mode or the gated mode. Compared to the free-running SPAD, the high-frequency gated SPAD achieves a higher maximum count rate of several hundreds of Mcps. However, to the best of our knowledge, the highest reported gated frequency is 3 GHz [21], which can be attributed to the inherent bandwidth limitations of the SPAD. Consequently, single-wavelength 5 GHz photon pulse detection has not yet been achieved using InGaAs/InP SPADs, because the gated

* Corresponding author (email: weich@ustc.edu.cn, zfhan@ustc.edu.cn)

frequency restricts the performance of high-speed QKD. In 2018, Wang et al. [20] achieved SKR = 0.306 Mbps with a 10 dB channel attenuation using phase encoding and SPADs. Multiplexing techniques are commonly utilized in QKD systems to improve the SKR. For example, based on the polarization multiplexing approach, Yuan et al. [19] achieved SKR = 13.72 Mbps with a 2 dB channel attenuation using SPADs. Furthermore, Tanaka et al. [22] employed wavelength-division multiplexing, achieving SKR = 1 Mbps with a 10 dB channel attenuation using SPADs.

Due to the birefringence effect in optical fibers, even when polarization correction techniques are employed, polarization-dependent QKD systems still suffer from instability during their operation [15, 16, 19, 23]. In contrast, time-bin or phase encoding QKD systems [11, 20, 24, 25] are inherently robust against channel polarization disturbance, providing a stable and reliable solution. Despite these developments, which demonstrate the rapid evolution of practical QKD technologies, exploiting multiplexing to improve the encoding and decoding rates of SPAD-based QKD systems has not yet been fully investigated.

In this study, we present a hybrid time- and wavelength-division multiplexing (TWDM) QKD system, which merges two 2.5 GHz photon pulses of different wavelengths into a combined 5 GHz pulse train, achieving a 5 GHz encoding rate using 2.5 GHz-gated SPADs. This system incorporates adaptive polarization compensation based on the Faraday-Michelson interferometer (FMI), ensuring simplicity and operational stability. Using this advanced setup, we achieved an average SKR = 4.084 ± 0.178 Mbps, operating continuously for over 30 h on a 50 km optical fiber channel.

2 Experimental setup

The QKD system adopts phase-coding BB84 protocol with one-decoy state; the schematic setup is illustrated in Figure 1. The 5 GHz photon pulse is generated by combining two 2.5 GHz photon pulses, based on a gain-switching distributed feedback (DFB) laser, and the 5 GHz trigger signal is subsequently divided into two 2.5 GHz trigger signals by the frequency division and delay circuit (FDDC). To minimize the phase difference caused by different wavelengths of electro-optical phase modulator (PM) under the same voltage modulation, lasers with adjacent wavelengths are selected, with central wavelengths of 1549.32 and 1550.12 nm, and the full widths at half maximum (FWHM) of photon pulses are 36.05 and 36.96 ps, respectively. By precisely adjusting the delay of the trigger signal and utilizing a dense wavelength-division multiplexer (DWDM), two 2.5 GHz photon pulses with a 200 ps interval are merged into a 5 GHz photon pulse. A lithium niobate electro-optical intensity modulator (IM) is employed to implement a decoy-state protocol against PNS attack. The system adopts a one-decoy intensity modulation scheme, whose finite-size key analysis has been well discussed [26, 27].

Quantum state encoding employs an asymmetric Mach-Zehnder interferometer (AMZI) with two cascaded PMs, and the AMZI is equipped with a 100 ps delay line to split a photon pulse into two photon pulses. As shown in Figure 2, the encoded signal is generated from the gigabit transceiver high-performance (GTH) interface of field-programmable gate array (FPGA), and is driven by variable gain amplifier (VGA) and power amplifier (PA) to PM, where the gain of VGA is controlled by a digital-to-analog converter (DAC), ultimately, the encoded signal with rise time of 61.77 ps and fall time of 69.15 ps is achieved. The first-stage PM modulates phases of 0 and $\pi/2$, while the second-stage PM modulates phases of 0 and π. This two-stage modulation scheme enables the generation of four distinct phases: 0, $\pi/2$, π, and $3\pi/2$. This encoding method not only reduces the driving power requirements for PA, but also eliminates signal distortion caused by input signal time deviation in an electrical adder. The encoded photon is attenuated by a variable optical attenuator (VOA) and then passes through dispersion-compensating fiber (DCF) to mitigate photon pulse broadening due to the chirp effect in the optical fiber channel.

The phase drift between synchronous and quantum photons during transmission via different fibers causes a phase shift in the gate signal of SPADs at Bob. To address this issue, the proposed QKD system adopts co-fiber transmission for synchronous and quantum photons. To suppress the crosstalk caused by the synchronous to quantum photons, a gain-switched DFB laser was used to compress the synchronous photon pulse to a FWHM = 50 ps. Additionally, a nonadjacent wavelength (center wavelength: 1552.52 nm) was selected for the synchronous laser. Furthermore, the same clock as that of the quantum photons was employed; its frequency is divided to reduce the frequency of the synchronous photons to 250 kHz. Finally, the gating characteristic of SPADs was utilized by transmitting the synchronous photons during the off-gate period; in this way, most of the Raman noise can be suppressed during the open-gate period. A DWDM was used to merge the quantum with the synchronous photons into the quantum channel.

When photons arrive at Bob, they pass through the DWDM to separate the synchronous from the quantum photons. The synchronous photon is converted to an electrical signal of the same frequency using an avalanche

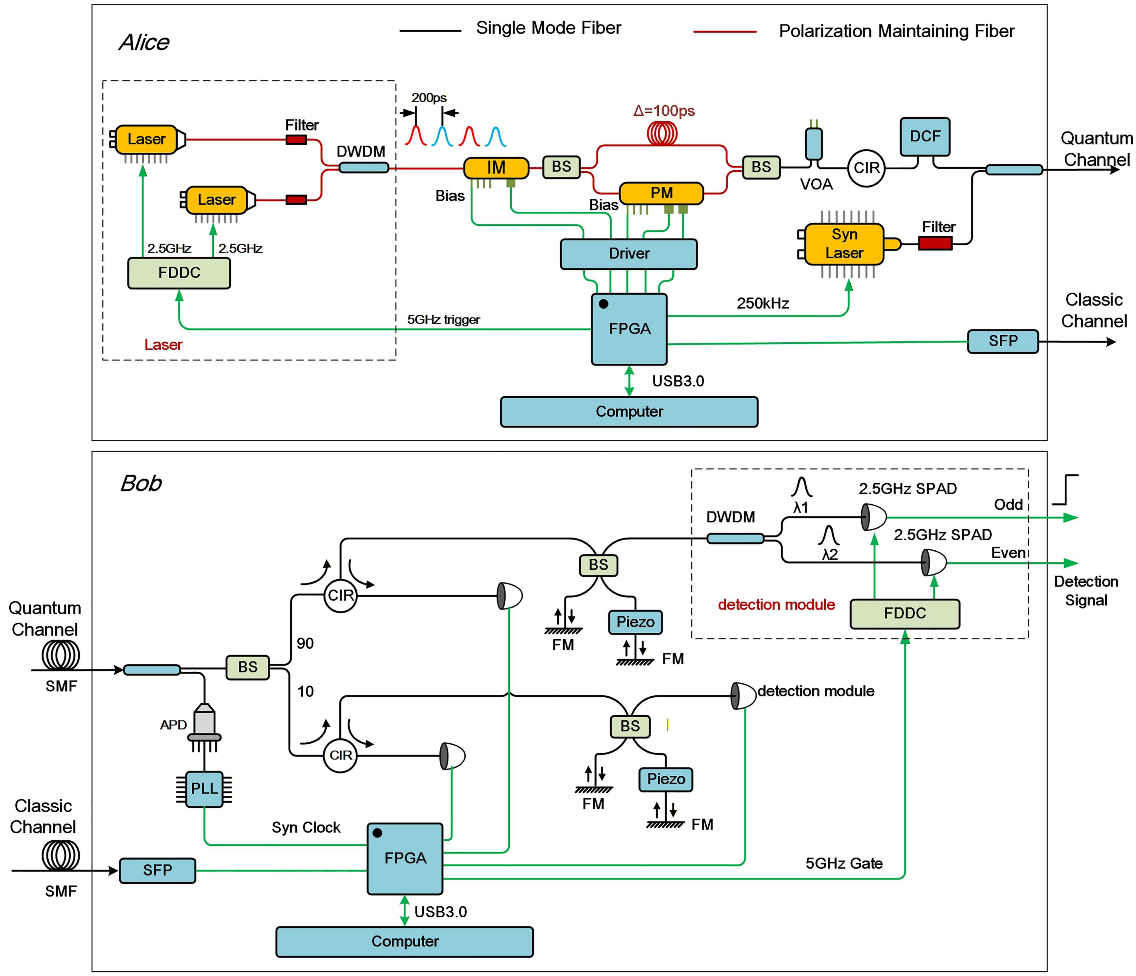

Figure 1 (Color online) Schematic of 5 GHz QKD system. AMP: RF amplifier; CIR: circulator; FM: Faraday mirror; SMF: single-mode fiber.

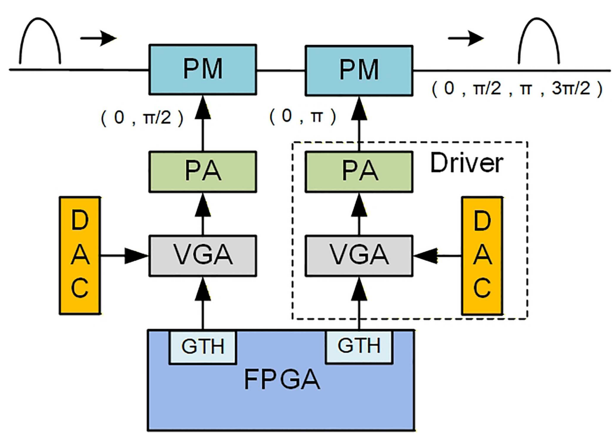

Figure 2 (Color online) Encode driver circuit.

photodiode (APD), and the synchronous clock is generated using a phase-locked loop (PLL) frequency multiplier. The quantum photon passes through a beam splitter (BS) with a splitting ratio of 90:10 to achieve an unbalanced passive basis selection, the corresponding selection ratio of the Z- to the X-basis is 90:10. To minimize the optical insertion loss (OIL) at Bob and enhance SKR, a piezoelectric fiber stretcher (Piezo) was used in the FMI to perform phase modulation, reducing OIL to only 0.1 dB. For the Z- and X-basis, Piezo was modulated to the phase of 0 and $\pi/2$, respectively. The Faraday-Sagnac-Michelson interferometer (FSMI) [20] can also adaptively compensate for the birefringence effect of the fiber channel; however, the FMI was selected because it reduces OIL and achieves

Table 1 Parameters of QKD system. Att is optical fiber channel attenuation; μ_1 and P_{μ_1} are the average photon number of the signal state and its generation ratio; μ_2 and $P_{\mu_2} = 1-P_{\mu_1}$ are the average photon number of the decoy state and its generation ratio; $P_{Z,A}$ and $P_{Z,B}$ are the probabilities of Alice and Bob choosing the Z-basis, respectively.

Fiber length (km)	Att (dB)	μ_1	μ_2	P_{μ_1}	$P_{Z,A}$	$P_{Z,B}$	$e^z_{1,p}$ (%)	QBER_Z (%)	SKR (Mbps)
50	8	0.3305	0.0762	0.844	0.906	0.9	3.67	2.34	4.07

a simple implementation.

The detection module was based on the InGaAs/InP SPAD operating in the gated Geiger mode. The photons were divided into odd- and even-sequence photons using a DWDM with a center wavelength of 1549.32 nm; the transmission and reflection isolations of the DWDM were 30.78 dB and 20.19 dB, respectively. Although 1% of the transmitting wavelength photon exits the reflection port, it reaches SPAD during the off-gate period; thus, the error count caused by this photon can be ignored. The FDDC divides the 5 GHz gate signal into two 2.5 GHz gate signals, which trigger two 2.5 GHz SPADs [28] in the gated Geiger mode, to detect the odd- and even-sequence photons, respectively. The 2.5 GHz SPADs employ a sinusoidal gating scheme by incorporating a specifically designed low-pass filter and a zero-crossing discriminator to effectively reduce the timing jitter. The detection efficiency was 20%, and the dark count probability was $< 3 \times (10^{-6})$ per gate. The detection signals exited according to odd- and even-sequence photons, and raw key data were acquired via sampling before being transmitted to the computational platform for postprocessing.

To maintain system stability with a low quantum bit error rate (QBER), a continuous reference phase alignment is necessary. The phase of the Z-basis at Bob was used as a reference, and the phase at Alice was adjusted by increasing the voltage through the bias port of the phase modulator (PM), as shown in Figure 1, with the phase scanning range exceeding 2π. Starting from 0 V, Alice sends 10^6 of photon pulses after setting the bias port voltage each time, and Bob records the corresponding detected signal. By comparing the detection count rates, the voltage value corresponding to the maximum detection count rate was identified and configured, indicating that the phase reference between the transmitter and the receiver had been successfully aligned. Postprocessing was performed on an Intel Core$^{\text{TM}}$ i9-10900TE platform and included sifting, error correction (EC), and privacy amplification (PA). To minimize information leakage, a cascade reconciliation was adopted [29], achieving an EC efficiency of 1.032 at QBER = 3%. Moreover, a universal class hash function was utilized for PA [30]. To increase SKR, it is necessary to enhance the duty cycle of the photon transmission time by implementing a multithreading approach in the QKD system, which enables the parallel execution of processes. The entire process was organized into three dedicated threads. The first thread handles the photon transmission, data exchange, and reference phase alignment. The second thread manages sifting. Once the computational platform receives raw key data, the sifting process begins, and the sifted key data are transferred to the next thread. The third thread handles EC and PA, with speeds of 80 and 26.6 Mbps, respectively. This multithreading approach significantly optimizes system performance, ensuring the efficient and stable operation of the QKD system.

3 Results and discussion

Based on the above setup, the QKD system operates on a 50 km link with the loss of 8 dB optical fiber, while accounting for the finite-key-length effect [26, 27, 31], and the finite block size is $n = 10^9$. The secure key length, denoted as l_z, is calculated using the following formula [31]:

$$l_z = s_0^z + s_1^z(1 - H_2(e^z_{1,p})) - \lambda_{\text{EC}} - 6\log_2\frac{19}{\epsilon_{\text{sec}}} - \log_2\frac{2}{\epsilon_{\text{cor}}}, \tag{1}$$

where s_0^z and s_1^z represent the lower bounds on the number of vacuum events and single-photon events in the Z-basis, respectively. $e^z_{1,p}$ represents the upper bound on phase error rate. λ_{EC} quantifies leakage of EC stage and secrecy parameter is $\epsilon_{\text{sec}} = 10^{-9}$, correctness parameter is $\epsilon_{\text{cor}} = 10^{-15}$.

The QKD system operates continuously for over 30 h, with the parameters summarized in Table 1. QBER and SKR are shown in Figure 3. e_z and e_x represent the average QBER in the Z-basis and X-basis, respectively, where e_z=2.34 % and e_x = 2.49 %. Phase tracking of the X-basis adopts a gradient descent algorithm, due to the slow drift of the reference phase and hysteresis of the phase tracking in the gradient descent algorithm, e_x is slightly higher than e_z. Further details of the setup and phase tracking approach are provided in Appendix A.

To achieve a 5 GHz photon pulse detection using 2.5 GHz-gated SPADs, the high-speed optical switches employed for path selection require picosecond-scale switching times. However, such switches introduce high OIL.

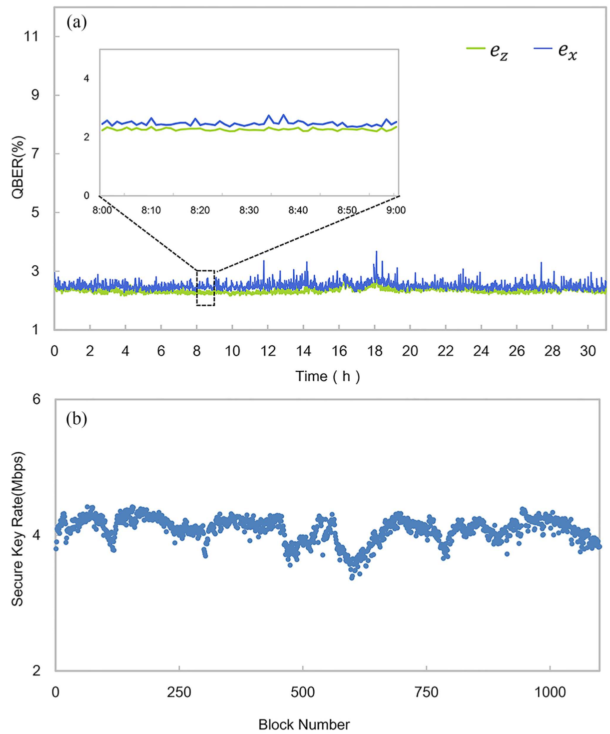

Figure 3 (Color online) The QBER (a) and secure key rate (b) for over 24 h of continuous run.

Jiang et al. [32] demonstrated an optical switch with a switching time below 28 ps and an OIL of 4.3 dB. In contrast, the wavelength-division multiplexing enables passive path selection without the need for high-speed optical switches. In our system, the DWDM exhibits transmission and reflection OILs of only 0.54 dB and 0.14 dB, respectively. Therefore, this approach increases SKR. Compared to a single-wavelength phase encoding QKD system, our system employs phase encoding, but only with alternating odd and even optical pulses at distinct wavelengths. Since time-division multiplexing inherently ensures temporal distinguishability between odd and even optical pulses, the additional wavelength distinguishability introduced by wavelength-division multiplexing does not compromise system security. Notably, our control and modulation schemes are fully compatible with a 5 GHz QKD system, constituting a crucial step toward implementing a true 5 GHz QKD system. However, TWDM requires two lasers and two SPADs, resulting in increased system complexity and cost compared to a single-wavelength scheme. Nevertheless, future advanced integration technologies, such as hybrid integration and microassembly, are expected to improve the integration of lasers and detectors, thereby mitigating and resolving these issues.

To assess the duty cycle of the quantum photon transmission time, which is controlled by a multithreaded approach, a one-hour statistical analysis of data was performed. The first thread exhibited the longest execution time, where the quantum photon transmission time accounted for 93.9%. The execution times of the second and third threads were 47.1% and 44.8%, respectively, of that of the first thread. Consequently, postprocessing can be performed synchronously with the execution of the first thread; the duty cycle of the quantum photon transmission time was 93.9%.

To assess the performance of the proposed QKD system against polarization disturbance, a 1 kHz polarization disturbance was applied to the quantum channel using a polarization scrambling module. The e_x distributions, which are shown in Figure 4, were statistically analyzed without and with a polarization disturbance for five hours. After introducing the polarization disturbance, the average e_x increased slightly from 2.12% to 2.27%, and the standard deviation increased from 0.11 to 0.19, which can be attributed to the imperfections of the FM devices.

Table 2 shows a comparison between the results of our system and those of high-speed QKD experiments reported in recent years. In optical fiber communication networks, apart from ducted and buried fibers, aerial fibers are also extensively used. Vibration and environmental changes in the optical fiber channel are unavoidable. Therefore, QKD systems that are robust against channel polarization disturbance are particularly suitable for maintaining operational stability [23, 33]. In [19], to enable noninterference peaks to contribute to information extraction, each photon pulse was split into a pair of pulses with orthogonal polarizations. Although this approach improves SKR, the introduced polarization degree of freedom makes the system vulnerable to channel polarization distur-

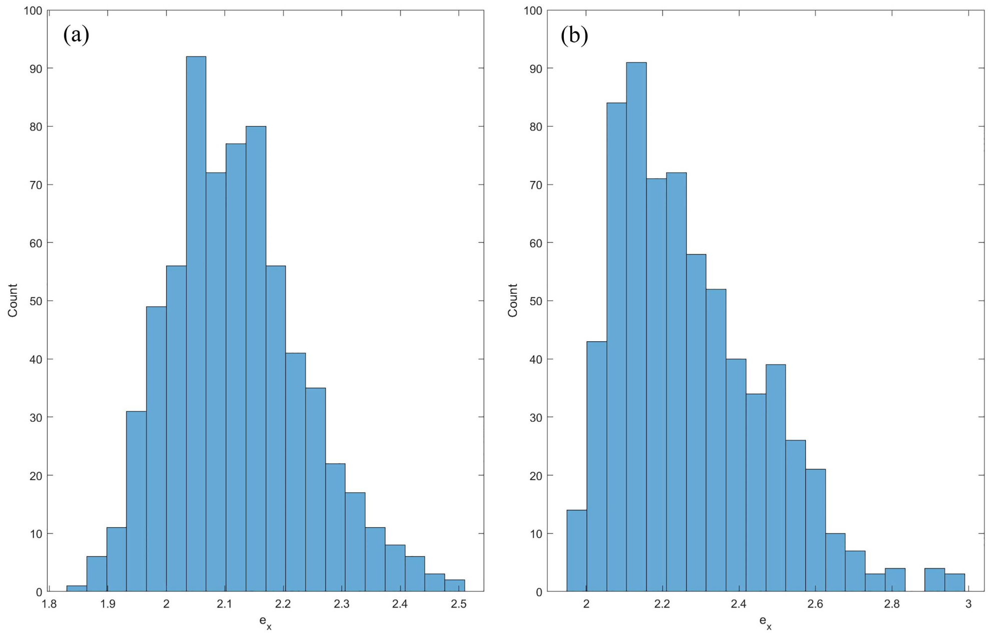

Figure 4 (Color online) The QKD system stability test (a) without polarization disturbance and (b) with polarization disturbance.

Table 2 Comparison of high-speed QKD experiments.

Ref.	Repetition frequency (GHz)	QBER (%)	Detector type	Att (dB)	Resistant to channel polarization disturbance	SKR (Mbps)	Encoding	SKR normalized to 10 dB (Mbps)
[15]	5	1.93	SNSPD	20.2	No	0.392	Polarization	4.08
[16]	2.5	0.61	SNSPD	2.2	No	115.8	Polarization	19.22
[11]	2.5	0.4	SNSPD	1.58	Yes	64	Time-bin	9.21
[19]	1	3.0	InGaAs/InP	2.0	No	13.72	Phase	2.17
[25]	2.5	2.03	InGaAs/InP	20.2	Yes	0.014	Time-bin	0.15
[20]	1	2.17	InGaAs/InP	10	Yes	0.306	Phase	0.306
This work	5	2.34	InGaAs/InP	8.0	Yes	4.08	Phase	2.57

bance. In [25], InGaAs/InP SPADs performed a free-running operation, where the dark count rates were as low as 1 count/s. However, the 20 μs of deadtime reduced SKR [34].

The detection efficiency of the SNSPDs used in the aforementioned experiments reached 80% [15]. The SNSPDs are unaffected by the afterpulse effect and exhibit low dark count rates, thus reducing QBER. However, their detection efficiency is polarization-dependent, leading to SKR fluctuations. In contrast, the detection efficiency of InGaAs/InP SPADs is polarization-independent. Notably, although our system employs eight SPADs, its total cost is below one-fifth of that of the SNSPDs. Furthermore, considering the limitations of SNSPDs in size and readiness for deployment, commercial QKD systems mainly employ InGaAs/InP SPADs [35, 36]. Because of the differences in attenuation, all the results were normalized to an optical fiber channel attenuation of 10 dB to facilitate the comparison of SKR. Our study shows that improved performance can be achieved by utilizing InGaAs/InP SPADs while maintaining robustness against channel polarization disturbance. Therefore, our system is a promising solution for large-scale deployment.

4 Conclusion

By developing a hybrid TWDM approach, we have successfully implemented a QKD system with 5 GHz modulation. The system demonstrated exceptionally remarkable stability, operating continuously for over 30 h on a 50 km optical fiber channel, achieving SKR $= 4.084 \pm 0.178$ Mbps and $e_z = 2.34\%$. To address the polarization instability in long-distance fiber transmission, we employed an FMI to achieve adaptive polarization compensation, thus significantly improving system robustness. Furthermore, the integration of low-cost InGaAs/InP SPADs ensures high performance while enhancing practical feasibility, which is critical in scalable, high-performance quantum communication networks. Future optimizations in system stability and deployability can be achieved by integrating key functional modules [12–14, 37].

Acknowledgements This work was supported by National Key Research and Development Program of China (Grant No. 2018YFA0306400), Prospect and Key Core Technology Projects of Jiangsu Provincial Key Research and Development Program (Grant No. BE2022071), and Quantum Science and Technology-National Science and Technology Major Project (Grant No. 2021ZD0300701).

References

1 Koblitz N. Elliptic curve cryptosystems. Math Comp, 1987, 48: 203–209
2 Rudnytskyi V, Korchenko O, Lada N, et al. Cryptographic encoding in modern symmetric and asymmetric encryption. Procedia Comput Sci, 2022, 207: 54–63
3 Alharbi M F, Aldosari F, Alharbi N F. Review of some cryptographic algorithms in cloud computing. Int J Comput Sci Netw Secur, 2021, 21: 41–50
4 Preskill J. Quantum computing in the NISQ era and beyond. 2018. arXiv: 1801.00862
5 Nicolas, Gisin, Grégoire, et al. Quantum cryptography. Rev Mod Phys, 2002, 74: 145–195
6 Ekert A K. Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67: 661–663
7 Bennett C H. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE Symposium on Foundations of Computer Science, Singer Island, 1984. 175–179
8 Ma X. Security of quantum key distribution with realistic devices. 2005. arXiv: 0503057
9 Diamanti E, Lo H K, Qi B, et al. Practical challenges in quantum key distribution. npj Quantum Inf, 2016, 2: 1–2
10 Lu Q H, Wang F X, Chen W, et al. Quantum key distribution over a mimicked dynamic-scattering channel. Sci China Inf Sci, 2024, 67: 142503
11 Grünenfelder F, Boaron A, Resta G V, et al. Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems. Nat Photon, 2023, 17: 422–426
12 Sibson P, Erven C, Godfrey M, et al. Chip-based quantum key distribution. Nat Commun, 2017, 8: 13984
13 Beutel F, Gehring H, Wolff M A, et al. Detector-integrated on-chip QKD receiver for GHz clock rates. npj Quantum Inf, 2021, 7: 40
14 Geng W, Zhang C, Zheng Y, et al. Stable quantum key distribution using a silicon photonic transceiver. Opt Express, 2019, 27: 29045–29054
15 Grünenfelder F, Boaron A, Rusca D, et al. Performance and security of 5 GHz repetition rate polarization-based quantum key distribution. Appl Phys Lett, 2020, 117: 144003
16 Li W, Zhang L, Tan H, et al. High-rate quantum key distribution exceeding 110 Mbs^{-1}. Nat Photon, 2023, 17: 416–421
17 Perrenoud M, Caloz M, Amri E, et al. Operation of parallel SNSPDs at high detection rates. Supercond Sci Technol, 2021, 34: 024002
18 Wang Z, Miki S, Fujiwara M. Superconducting nanowire single photon detectors for quantum information and communications. IEEE J Sel Top Quantum Electron, 2009, 15: 1741–1747
19 Yuan Z, Murakami A, Kujiraoka M, et al. 10-Mb/s quantum key distribution. J Lightwave Technol, 2018, 36: 3427–3433
20 Wang S, Chen W, Yin Z Q, et al. Practical gigahertz quantum key distribution robust against channel disturbance. Opt Lett, 2018, 43: 2030–2033
21 Yuan Z L, Sharpe A W, Dynes J F, et al. Multi-gigahertz operation of photon counting InGaAs avalanche photodiodes. Appl Phys Lett, 2010, 96: 071101
22 Tanaka A, Fujiwara M, Yoshino K-I, et al. High-speed quantum key distribution system for 1-Mbps real-time key generation. IEEE J Quantum Electron, 2012, 48: 542–550
23 Ding Y Y, Chen H, Wang S, et al. Polarization variations in installed fibers and their influence on quantum key distribution systems. Opt Express, 2017, 25: 27923–27936
24 Mo X F, Zhu B, Han Z F, et al. Faraday-Michelson system for quantum cryptography. Opt Lett, 2005, 30: 2632
25 Boaron A, Korzh B, Houlmann R, et al. Simple 2.5 GHz time-bin quantum key distribution. Appl Phys Lett, 2018, 112: 171108
26 Lim C C W, Curty M, Walenta N, et al. Concise security bounds for practical decoy-state quantum key distribution. Phys Rev A, 2014, 89: 022307
27 Zhou Y L, Ortner M, Rabl P. Long-range and frustrated spin-spin interactions in crystals of cold polar molecules. Phys Rev A, 2011, 84: 052332
28 He D Y, Wang S, Chen J L, et al. 2.5 GHz gated InGaAs/InP single-photon avalanche diode with 44 ps time jitter. Adv Devices Instrum, 2023, 4: 0020
29 Mao H K, Li Q, Hao P L, et al. High performance reconciliation for practical quantum key distribution systems. Quantum Inf Process, 2021, 20: 1–15
30 Zhang C M, Li M, Huang J Z, et al. Fast implementation of length-adaptive privacy amplification in quantum key distribution. Chin Phys B, 2014, 23: 090310
31 Ho W W, Jonay C, Hsieh T H. Ultrafast variational simulation of nontrivial quantum states with long-range interactions. Phys Rev A, 2019, 99: 052332
32 Jiang Y, Han X, Li Y, et al. High-speed optical mode switch in lithium niobate on insulator. ACS Photonics, 2023, 10: 2257–2263
33 Liu R, Yu H, Zan J, et al. Analysis of polarization fluctuation in long-distance aerial fiber for QKD system design. Optical Fiber Tech, 2019, 48: 28–33
34 Korzh B, Walenta N, Lunghi T, et al. Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency. Appl Phys Lett, 2013, 104: 081108
35 Zhang J, Itzler M A, Zbinden H, et al. Advances in InGaAs/InP single-photon detector systems for quantum communication. Light Sci Appl, 2015, 4: 286
36 Walenta N, Lunghi T, Guinnard O, et al. Sine gating detector with simple filtering for low-noise infra-red single photon detection at room temperature. J Appl Phys, 2012, 112: 175–179
37 Pelucchi E, Fagas G, Aharonovich I, et al. The potential and global outlook of integrated photonics for quantum technologies. Nat Rev Phys, 2022, 4: 194–208

Appendix A Phase tracking method for X-basis

The phase drift of Piezo in the interferometer at Bob is influenced by environmental factors. While the phase drift of Z-basis can be compensated by tracking reference phase, the phase drift of X-basis also requires active tracking. To address this, we adopt a gradient descent algorithm to determine the compensation voltage of Piezo by identifying the minimum e_x, as shown in Algorithm A1.

Algorithm A1 Processing flowchart.

```
Step 1: Initialization.
volt_signal ⇐ 1;
ρ ⇐ 125; {value according to the device characteristics}
err_thld ⇐ 1%; {set ideal reference value}
Step 2: Calculate the step size of voltage value regulation according to the gradient of QBER difference, and calculate the QBER err_currt.
if (err_currt > err_thld) then
    if (err_currt > err_old) then
        volt_signal ⇐ volt_signal × (−1); {change sign}
    end if
    volt_step ⇐ |err_currt − err_thld| × 100 × ρ; {step size}
    volt_new ⇐ volt_currt + volt_signal × volt_step; {regulate voltage value}
    err_old ⇐ err_currt; {update QBER}
    volt_currt ⇐ volt_new; {update voltage value}
    set(volt_new); {configure voltage value}
else
    set(volt_currt); {configure voltage value}
end if
```

The current Piezo voltage value is denoted as *volt_currt*, while updated voltage value resulting from tracking algorithm is denoted as *volt_new*, current QBER is denoted as *err_currt*, and previous QBER is denoted as *err_old*, voltage regulation direction is indicated by *volt_signal*, step size for voltage adjustment is denoted as *volt_step*, QBER threshold for Piezo voltage tracking is denoted as *err_thld* is QBER, and gradient regulation factor is denoted as ρ.

To mitigate erroneous fluctuation of X-basis phase drift compensation voltage caused by inaccuracies in reference phase tracking, we take an average of 10 consecutive e_x values as reference, and the gradient descent algorithm is then applied to phase tracking for the Piezo phase drift once per iteration. However, this phase tracking method for X-basis has two limitations. First, the time interval for Piezo phase drift compensation is approximately 22 s, since the compensation voltage is calculated according to the previous average QBER, phase drift cannot be compensated in real time, leading to e_x higher than e_z. Second, the gradient descent algorithm can get trapped in local minima; when this occurs, the algorithm fails to identify the global minimum e_x at that stage. Although the reference phase and optimal values continuously evolve during operation, making the local minimum trap temporary, it still leads to elevated e_x during the process. To address the precision of X-basis Piezo phase tracking, future efforts will focus on stabilizing the environmental conditions of the interferometer and refining the algorithm. These enhancements aim to reduce phase drift and improve the overall stability and performance of the QKD system.