SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

October 2022, Vol. 65 200506:1–200506:7
https://doi.org/10.1007/s11432-022-3514-3

Special Focus on Quantum Information

Polarization-insensitive quantum key distribution using planar lightwave circuit chips

Guo-Wei ZHANG[1,2], Wei CHEN[1,2*], Guan-Jie FAN-YUAN[1,2], Li ZHANG[1,2,3], Fang-Xiang WANG[1,2], Shuang WANG[1,2], Zhen-Qiang YIN[1,2], De-Yong HE[1,2], Wen LIU[4], Jun-Ming AN[5,6], Guang-Can GUO[1,2] & Zheng-Fu HAN[1,2]

[1]*CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei* 230026*, China;*
[2]*CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026*, China;*
[3]*Hefei Quantachip Technology Co.,Ltd., Hefei* 230026*, China;*
[4]*USTC Center for Micro- and Nanoscale Research and Fabrication, University of Science and Technology of China, Hefei* 230026*, China;*
[5]*State Key Laboratory on Integrated Optoelectronics, Institute of Semiconductors, Chinese Academy of Sciences, Beijing* 100083*, China;*
[6]*Center of Materials Science and Optoelectronics Engineering, University of Chinese Academy of Sciences, Beijing* 100049*, China*

Received 6 June 2022/Accepted 14 June 2022/Published online 30 August 2022

Abstract Self-stabilizing the quantum key distribution (QKD) system is essential to evaluate eavesdroppers' information accurately. We develop and verify a polarization-insensitive time-bin decoder chip for QKD with the hybrid asymmetric Faraday-Michelson interferometer (AFMI) based on the planar lightwave circuit (PLC). Compared with existing chip-based QKD works, the scheme can intrinsically compensate for the polarization perturbation to quantum signals and thus work at arbitrary temperatures. We experimentally verify the chips in a time-bin QKD system at the clocking rate of 1.25 GHz and obtain an average secure key rate (SKR) of 1.34 Mbps over a 50 km fiber channel with an optimized analysis model. The steady variations of the quantum bit error and SKR with random polarization disturbance demonstrate that PLC-based AFMIs are available for developing self-stable QKD systems.

Keywords polarization insensitive, time-bin, asymmetric Faraday-Michelson interferometer, quantum key distribution, planar lightwave circuit

Citation Zhang G-W, Chen W, Fan-Yuan G-J, et al. Polarization-insensitive quantum key distribution using planar lightwave circuit chips. Sci China Inf Sci, 2022, 65(10): 200506, https://doi.org/10.1007/s11432-022-3514-3

1 Introduction

Quantum key distribution (QKD) enables two remote parties to share secret key bits by transmitting photons that follow the fundamental laws of quantum physics [1]. Since the first protocol was proposed by Bennett et al. [2] in 1984, QKD has developed rapidly both in theoretical and experimental fields [3–6], and has embarked on the road of engineering and robust implementations [6]. The essential security fundamental of QKD is to accurately evaluate the information leaked to eavesdroppers with the statistical results of the system. These results, like counting rate and the quantum bit error rate (QBER), heavily depend on the self-stability of the practical QKD systems. However, the polarization disturbance of the optical components and the channel caused by the environment will affect the stability of a QKD system, interrupting or even terminating the QKD procedure [7]. Many countermeasures have been proposed to overcome this problem, such as active compensating schemes [8, 9], "plug-and-play" systems [10], and Faraday-Michelson systems [11].

In recent years, the development of integrated photonics has promoted the evolution of QKD. Various platforms have been reported to implement on-chip QKD systems, such as the silicon-on-insulator

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

(SOI) [12,13], the III-V compounds [14,15], and the silica-on-silicon planar light-wave circuits (PLCs) [16–18]. Among these platforms, PLC is especially suitable for implementing optical decoders of QKD systems for their relatively lower insertion loss. Nevertheless, the remained intrinsic polarization dependence of PLC may reduce the performance of QKD systems due to the birefringence in fiber channels. Nambu et al. [19] and Li et al. [20] have proposed solutions to eliminate the polarization dependence by precisely controlling the chips' temperature to minimize the relative phase difference between the two polarization modes. The method requires the chip to work at a few specific points across a wide temperature range, putting strict requirements on the temperature control unit and increasing the power consumption. Zhang et al. [21] proposed a hybrid packaged asymmetric Faraday-Michelson interferometer (AFMI) consisting of a PLC chip and Faraday rotator mirrors (FMs), which can self-compensate the polarization perturbations of the device and channel over a wide temperature range. However, this method still demands a temperature control system to adjust and maintain the phase difference between the interferometer arms.

In this paper, we develop a QKD decoder chip based on the AFMI structure mentioned above, which can passively fulfill the measurements of the time-bin encoding BB84 protocol [2]. An AFMI and an external intensity modulator (IM) act as the encoder to perform the time-bin encoding and the decoy-state modulation at a 1.25 GHz clocking rate. By taking advantage of the time-bin scheme and the self-stability of AFMI, the chips are intrinsically polarization-insensitive over a wide temperature range, and the temperature controllers of the substrate are not necessary. The feature is very different from previous polarization-insensitive QKD chips based on silica-on-silicon [19, 20], which controls the chip working at particular temperature points and can support more applications.

We also optimize the analytical model by considering the afterpulse effect of single-photon avalanche detectors (SPADs) when the QKD system operates with a high clocking rate. The experiment achieves an average secure key rate (SKR) of about 1.34 Mbps over a 50 km single-mode fiber (SMF) under the finite-size scenario. The stable results of the system with a random polarization scrambler in the channel demonstrate that the PLC-based setup is an effective way to implement self-stabilized QKD systems.

2 Experimental setups

The time-bin encoding of BB84 protocol with the one-decoy state method [22] is adopted for the design. The sender Alice and the receiver Bob deploy the time-bin basis (Z) and phase basis (X), which generate the raw key and estimate the eavesdropper's information, respectively. The Z basis consists of the quantum state $|\psi_0\rangle = |\alpha\rangle_E|0\rangle_L$ and $|\psi_1\rangle = |0\rangle_E|\alpha\rangle_L$, where E and L respectively represent the early and late time-bin of the temporal mode, and α represents the weak coherent state. Alice selects the Z or X basis with the probabilities of P_z^{A} and P_x^{A}. When selecting the Z basis, Alice prepares $|\psi_0\rangle$ or $|\psi_1\rangle$ according to its classical bits 0 or 1. In the X basis, Alice sends $|\psi_+\rangle = \frac{1}{\sqrt{2}}(|\psi_0\rangle + |\psi_1\rangle)$. The one-decoy state method [22] is used to defend against photon number splitting attacks [23]. In the receiver, Bob randomly chooses the Z or X basis for the measurement with probabilities of P_z^{B} and P_x^{B}. Bob directly measures the photon's arrival time to recover the bit value in the Z basis and evaluates the coherence between the two adjacent pulses by measuring their interference results in the X basis.

The structure of the decoder chip is shown in Figure 1(a), which includes two cascaded directional couplers (DCs) and a pair of asymmetric waveguides. DC1 of the PLC chip in Alice can be employed to monitor the quantum light source's optical power and play the role of randomly selecting the Z or X basis to measure the incident photons in Bob. The two arms on the PLC chip from DC2 with a 50:50 splitting ratio are coupled to two FMs to form an AFMI. There are two thermo-optic phase modulators (TOPM) on each waveguide of the two arms to tune the relative phase. A pair of AFMI can fulfill the measurement of the X basis by taking advantage of their polarization-insensitive stability [21].

The size of the silica-based PLC chips is about 38.5 mm $\times$ 24 mm. The primary fabrication procedure is as follows: thermal oxidation to form a lower cladding layer, plasma-enhanced chemical vapor deposition (PECVD) to grow the core waveguide layer, photolithography and inductively coupled plasma (ICP) to transfer the waveguide patterns, PECVD to form the upper cladding layer, and the magnetron sputtering to deposit Ti-W (titanium-tungsten) heaters and Ti-Pt-Au (titanium-platinum-gold) lead electrodes. The refractive index difference between the core and cladding is 0.75%, and the waveguide core size is 6 μm $\times$ 6 μm, which can achieve lower insertion loss. The PLC chip is coupled to the FMs and a fiber array (FA), and then the electrodes are wire-bonded to a printed circuit board (PCB), as shown in Figure 1(b).

The experimental setup is illustrated in Figure 2(a). Alice uses a 1550 nm distributed feedback (DFB)

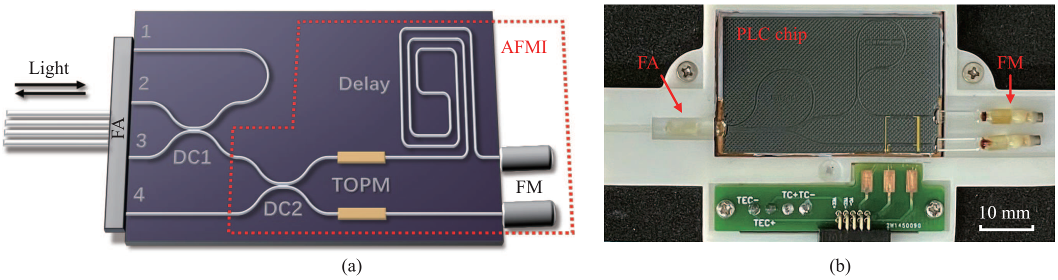

Figure 1 (Color online) PLC-based decoder chip. (a) The structure of the decoder. The part framed by the red dashed line is the AFMI; (b) the photograph of the decoder and its encapsulation.

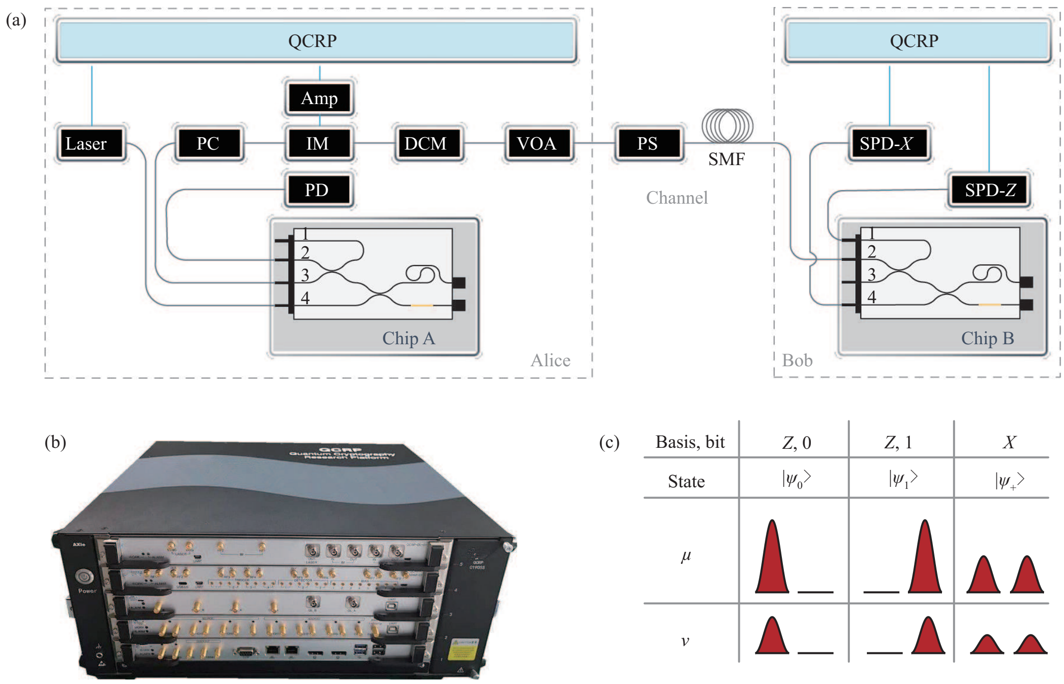

Figure 2 (Color online) Experimental setups. (a) Experimental setups to implement QKD. Laser: laser source; PC: polarization controller; IM: intensity modulator; Amp: RF amplifier; DCM: dispersion compensation module; VOA: variable optical attenuator; PS: polarization scrambler; SMF: single-mode fiber; SPD-X and SPD-Z: single-photon detectors for the X and Z basis; QCRP: quantum cryptography research platform. (b) The photograph of the QCRP. (c) Encoding of the states.

laser working at the gain-switched mode to generate phase-randomized light pulses with a repetition rate of 1.25 GHz. The pulses enter and exit chip A (A represents Alice) from port A-4 and port A-3, respectively. The AFMI of the chip splits an incident light pulse into two pulses with a delay of 400 ps. An intensity modulator (IM, made by JDS Uniphase) with a bandwidth of 12 GHz is cascaded with the chip. The IM is utilized to modulate the pulses into one of the three states (as shown in Figure 2(c)) and control their intensities according to the time-bin encoding scheme and the decoy-state method. The equivalent extinction ratio of the IM is approximately 24 dB, which is mainly affected by the bandwidth and the pattern effect [24] of the signal generator and the radio-frequency amplifier (Amp). The light pulses are tuned to the intensity of the single-photon level by a variable optical attenuator (VOA) and sent to Bob as quantum signals. We add a dispersion compensation module (DCM) in the transmitter to precompensate the dispersion of the optical fiber since the widening and overlap of the pulse would significantly increase the QBER. We also place a polarization scrambler (PS) in the quantum channel and apply the active random polarization disturbance to evaluate the stabilization of the system.

On Bob's side, the measurement basis is passively selected by DC1-B (B represents Bob) with a splitting ratio of 73:27 (measured value) between the bar and cross ports, which corresponds to the unbalanced selection of the Z and X basis with the probabilities of 73% and 27%, respectively. The pulses exited from port B-1 of the chip B are directly sent to SPAD-Z to measure the Z basis, and the single-photon measurement results are sent to the time-to-digital converter (TDC) module to record the arriving time of the photons. SPAD-X is used to measure the pulses exiting from port B-4 after passing through the AFMI, which corresponds to the measurement results of X basis. The insertion loss of the PLC chip is approximately 0.98 and 3.89 dB for the Z and X basis, respectively. The extra insertion loss of the X basis is majorly due to the round-trip loss of the facet coupling, the DC, and the FMs.

The experimental system is controlled using a home-developed modular instrument named quantum cryptography research platform (QCRP), which follows the advanced telecommunications computing architecture extensions for instrumentation and test standard (AXIe). The kernel of the platform is a control board based on a field-programmable gate array (FPGA) (Xilinx Virtex-6). As shown in Figure 2(b), the QCRP includes the modules of the light source, the high-speed pulse generator, the adjustable current source, the high-bandwidth amplifier, the single-photon detectors, and the TDC, which are connected to the kernel control board via a rear panel. We use only one IM to fulfill the bit-base modulation and the decoy intensity modulation of each quantum light pulse. The high-speed driving signals of the IM are generated using an arbitrary waveform generator (AWG) (Tektronix AWG70002A), which is controlled and synchronized with the master clock of the QCRP.

The SPADs integrated into QCRP are based on InGaAs/InP negative feedback avalanche photodiodes and operate in Geiger mode. The typical detection efficiency, the dark count rate, and the overall afterpulse rate of the SPAD are about 21%, 6.6 kHz, and 1.9%, respectively. Since the delay between the early and the late time slots is 400 ps, the gating rate of the SPAD should be 2.5 GHz to measure the Z basis. We also used a SPAD with a gating rate of 2.5 GHz instead of two 1.25 GHz gating SPADs to simultaneously measure the QBER and the counting rate of the X basis. Thus, the system employ the pulses of $|\psi_+\rangle$ preceded by $|\psi_0\rangle$ and followed by $|\psi_1\rangle$ to estimate the total number of detections [25].

3 Afterpulse-compatible analysis model

In high-speed QKD systems, the afterpulse of the SPAD may cause the estimation of the theoretical model and parameters deviates from reality, which will finally reduce the SKR. Fan-yuan et al. [26] have proposed a QKD analytical model taking the afterpulse into account to gain better system performance. However, this model is aimed at the dual-detector model to measure the interference results of the phase-encoding, which is not precisely suitable for the time-bin scheme. We modify Fan's model to an afterpulse-compatible one adaptive to the time-bin QKD system. The afterpulse probability $P_{\rm ap}$ in a QKD system based on SPADs can be presented by [26, 27]

$$P_{\rm ap} = \frac{\hat{p}}{1-\hat{p}}\hat{Q}^d, \quad \hat{Q}^d = \sum_{\alpha=\mu,\nu} P_\alpha \widetilde{Q}_\alpha, \tag{1}$$

where $\hat{p} < 1$ is the overall afterpulse rate that can be measured by experiment, $\hat{Q}^d$ is the weighted average of the gain of varying states, P_α and $\widetilde{Q}_\alpha$ are the selecting probability and the response probability of the state of intensity α, respectively ($\alpha = \mu, \nu$ for signal and decoy state).

In a time-bin encoding QKD system using the IM to chop the pulses, the IM's finite extinction ratio is a significant source for the QBER of the Z basis. Assuming that the extinction ratio of the IM is κ (in dB), the response probability in the Z basis $\widetilde{Q}_{\alpha,Z}$ can be expressed as

$$\widetilde{Q}_{\alpha,Z} = P_Z^{\rm A} P_Z^{\rm B}\left[1 - \frac{1}{2}\left({\rm e}^{-\alpha\eta} + {\rm e}^{-\mu\eta\eta_{\rm er}}\right)(1-Y_0)\right] + P_X^{\rm A} P_Z^{\rm B}\left[1 - {\rm e}^{-\alpha\eta/2}(1-Y_0)\right], \tag{2}$$

where $P_X^{\rm A}$ and $P_Z^{\rm A}$ are the probabilities of selecting the basis (X and Z) for preparation, $P_Z^{\rm B}$ represents the probabilities of selecting the Z basis for measurement, η is the overall transmission and detection efficiency between Alice and Bob, Y_0 is the background counting rate, and $\eta_{\rm er} = 10^{-\kappa/10}$ is the efficiency of leaking light when considering the extinction ratio.

Since we use one IM for both the information encoding and the decoy-state modulating, the QBER of the signal and decoy states will be affected by the intensity of the signal state. Therefore, We use the intensity of the signal state (μ) rather than the corresponding quantum state (α) in the term ${\rm e}^{-\mu\eta\eta_{\rm er}}$ to calculate the overall yield and QBER in the Z basis more precisely, which are given by

$$\begin{aligned} Q_{\alpha,Z} &= 1 - {\rm e}^{-\alpha\eta}(1-Y_0)(1-P_{\rm ap}^Z), \\ E_{\alpha,Z}Q_{\alpha,Z} &= 1 - {\rm e}^{-\mu\eta\eta_{\rm er}}(1-Y_0)(1-P_{\rm ap}^Z). \end{aligned} \tag{3}$$

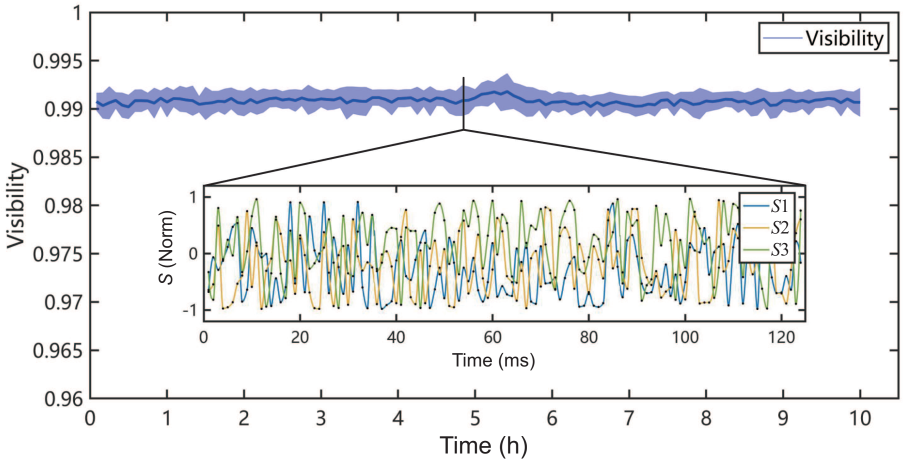

Figure 3 (Color online) Interference results for a long-term test without the temperature control of the substrate. Shadow areas represent the 3-σ error bar. Inset: the diagram of normalized Stokes parameters during the test in a short time segment.

The situation in the X basis is similar to that in [28]. Considering the experimental scenario with only one SPAD and the relationship of light intensity, the response probability in the X basis $\widetilde{Q}_{\alpha,X}$ can be expressed as

$$\widetilde{Q}_{\alpha,X} = P_X^{\mathrm{A}} P_X^{\mathrm{B}} \left[1 - \frac{1}{2}\left(\mathrm{e}^{-\alpha\eta\eta_X/2} + \mathrm{e}^{-\alpha\eta(1-\eta_X)/8}\right)(1-Y_0)\right] + P_Z^{\mathrm{A}} P_X^{\mathrm{B}} \left[1 - \mathrm{e}^{-\alpha\eta/4}(1-Y_0)\right], \quad (4)$$

where η_X is the leakage light ratio in the X basis. The overall yield in the X basis is estimated by the detections in the non-interfering peaks (Q_α^{ni}) in the conclusive events. So we have

$$\begin{aligned} Q_{\alpha,X} &= 4Q_{\alpha,X}^{\mathrm{ni}}/P_Z^{\mathrm{A}} - E_{\alpha,X}Q_{\alpha,X}, \\ Q_\alpha^{\mathrm{ni}} &= 1 - \mathrm{e}^{-\alpha\eta/8}(1-Y_0)(1-P_{\mathrm{ap}}^X), \\ E_{\alpha,X}Q_{\alpha,X} &= 1 - \mathrm{e}^{-\alpha\eta\eta_X/2}(1-Y_0)(1-P_{\mathrm{ap}}^X). \end{aligned} \quad (5)$$

Taking the finite-size effects into account, the secure key rate can be calculated by [22, 25]

$$l \leqslant s_{Z,0} + s_{Z,1}\left(1 - h\left(\phi_Z\right)\right) - \lambda_{\mathrm{EC}} - 6\log_2\left(19/\epsilon_{\mathrm{sec}}\right) - \log_2\left(2/\epsilon_{\mathrm{cor}}\right), \quad (6)$$

where $s_{Z,0}$ and $s_{Z,1}$ are the lower bounds on the number of vacuum and single-photon events in the Z basis respectively, ϕ_Z is the upper bound on the phase error rate, $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function, λ_{EC} is the consumption of the information in error correction, and $\varepsilon_{\mathrm{sec}} = 10^{-9}$ and $\varepsilon_{\mathrm{cor}} = 10^{-15}$ are the security parameters.

4 Results

Before conducting the QKD experiments, we first verified the polarization-independent properties of the AFMIs without temperature control. Using the experimental setups described in Figure 2(a) and keeping the IM unmodulated, the interference results can be detected at SPD-X. The current driving the TOPMs in the AFMI is initialized to ensure that the two interferometers are at their maximum interference position and the detector counts are minimized. The phase compensation technique commonly used in fiber optic QKD [29, 30] is employed for current feedback to maintain the phase difference between interferometers during the 10 h experiment. The PS was randomly scrambled at a rate of 1 kHz to demonstrate the polarization-independent performance of the AFMIs. The average value and the standard deviation (SD) of the visibility are calculated using the data collected every 5 min, as shown in Figure 3. It can be seen that the visibility is 99.08% $\pm$ 0.05% during the test.

According to the modified analysis model, we optimized the primary parameters in the transmitter for different quantum channel distances, including the probability of selecting the Z and X bases, the mean photon number, and the selecting probabilities of the signal and the decoy states. The QKD experiment

Table 1 Experimental parameters and performance at different distances

Distance (km)	μ	ν	P_μ	P_X^A	$QBER_Z$ (%)	ϕ_Z (%)	SKR (bps)
50[a)]	0.42	0.15	0.77	0.08	1.50	4.63	1.34×10^6
75	0.41	0.14	0.77	0.09	1.47	5.89	3.81×10^5
100	0.39	0.11	0.78	0.11	1.85	6.55	9.00×10^4
125	0.35	0.08	0.80	0.19	3.28	7.21	7.32×10^3

a) The result at this distance are tested under SMF, while the results in other distances are using VOA.

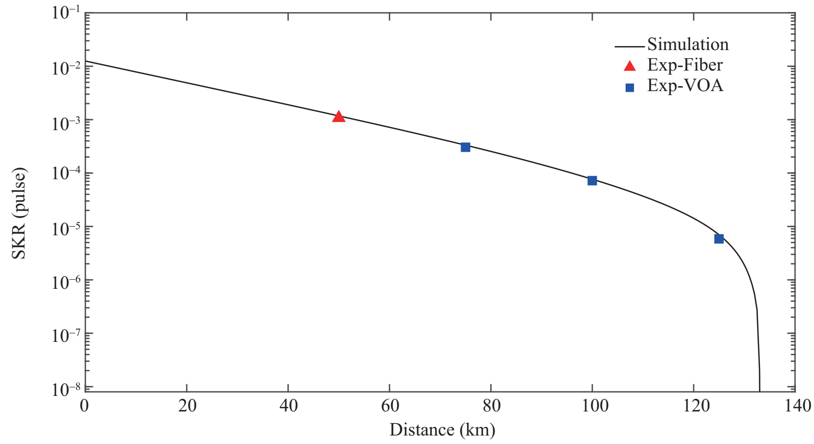

Figure 4 (Color online) Secure key rate (per pulse) as a function of transmission distance. The black line indicates the simulation result. The red triangle is the result using the actual SMF channel, and the blue squares are the result of simulating the fiber length by VOA.

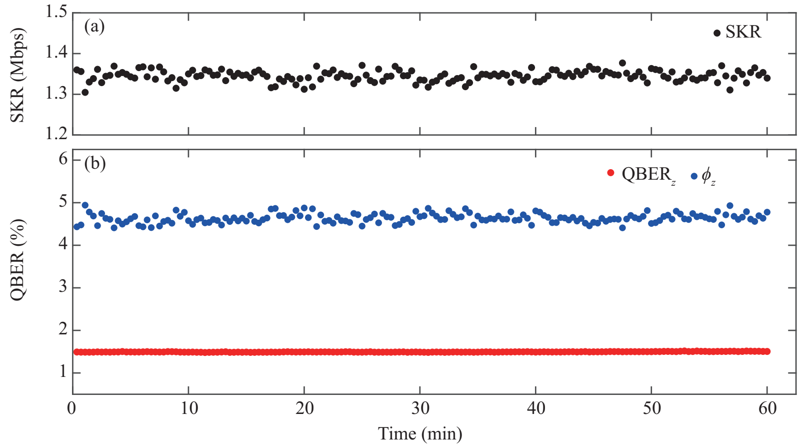

Figure 5 (Color online) System stability over 60 min with 50 km SMF and additional polarization scrambling. (a) The SKR and (b) corresponding $QBER_Z$ and ϕ_Z as a function of time.

is fulfilled in a 50 km standard SMF with a loss of about 0.2 dB/km and obtained an average SKR of about 1.34×10^6 bps. The block size for privacy amplification is 1×10^8. The dispersion of the light pulses and the synchronization signal shifting due to the fiber length variations can be compensated with a DCM module and a timing monitor feedback loop, respectively. The system performance in 75, 100, and 125 km fiber channels is evaluated with an optical variable attenuator. The operating parameters and results are summarized in Table 1. The experimental results are marked in Figure 4, which agree well with the numerical simulation results shown with the black line in Figure 4.

The system's stability is evaluated by applying a random polarization disturbance in the quantum channel using a polarization scrambling module. The QBER of the Z basis, ϕ_Z deduced from the QBER of the X basis, and the SKR are recorded within 60 min, in which the collecting interval for each data point is about 22 s, as shown in Figure 5. The 3-σ deviation of the SKR is approximately 2.9% of the average value, and the standard deviation of the Z-basis QBER is less than 0.01%. The slight fluctuations of the system performance in the polarization disturbance condition indicate that the time-bin QKD system implemented with the PLC chips is polarization-insensitive and intrinsically stable.

5 Conclusion

In conclusion, we design and verify the hybrid packaged QKD decoder chips based on PLC. With an optimized analytical model, the actual system can be portrayed more accurately, and a higher SKR can be achieved. The experimental results demonstrate that the PLC-based AFMI is available for realizing intrinsic stable QKD systems. Further efforts can be made to achieve better performance and compatibility, such as reducing the insertion loss of the chip, adding adjustable units like Mach-Zehnder interferometers to the chip, and combining with universal simulation frameworks [31].

Acknowledgements This work was supported by National Key Research and Development Program of China (Grant No. 2018YFA0306400), National Natural Science Foundation of China (Grant Nos. 61627820, 61622506, 61822115), Anhui Initiative in Quantum Information Technologies (Grant No. AHY030000). This work was partially carried out at the USTC Center for Micro and Nanoscale Research and Fabrication.

References

1 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. Rev Mod Phys, 2002, 74: 145–195
2 Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of International Conference on Computers, Systems & Signal Processing, 1984. 175–179
3 Bennett C H, Bessette F, Brassard G, et al. Experimental quantum cryptography. J Cryptology, 1992, 5: 3–28
4 Li L L, Li J, Chang Y, et al. Quantum key distribution based on single-particle and EPR entanglement. Sci China Inf Sci, 2020, 63: 169501
5 Yang Y G, Yang J J, Zhou Y H, et al. Quantum network communication: a discrete-time quantum-walk approach. Sci China Inf Sci, 2018, 61: 042501
6 Xu F, Ma X, Zhang Q, et al. Secure quantum key distribution with realistic devices. Rev Mod Phys, 2020, 92: 025002
7 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
8 Dixon A R, Dynes J F, Lucamarini M, et al. High speed prototype quantum key distribution system and long term field trial. Opt Express, 2015, 23: 7583–7592
9 Ding Y Y, Chen W, Chen H, et al. Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits. Opt Lett, 2017, 42: 1023–1026
10 Zbinden H, Gautier J D, Gisin N, et al. Interferometry with Faraday mirrors for quantum cryptography. Electron Lett, 1997, 33: 586–588
11 Wang S, Chen W, Yin Z Q, et al. Field and long-term demonstration of a wide area quantum key distribution network. Opt Express, 2014, 22: 21739–21756
12 Sibson P, Kennard J E, Stanisic S, et al. Integrated silicon photonics for high-speed quantum key distribution. Optica, 2017, 4: 172
13 Geng W, Zhang C, Zheng Y L, et al. Stable quantum key distribution using a silicon photonic transceiver. Opt Express, 2019, 27: 29045
14 Sibson P, Erven C, Godfrey M, et al. Chip-based quantum key distribution. Nat Commun, 2017, 8: 13984
15 Semenenko H, Sibson P, Hart A, et al. Chip-based measurement-device-independent quantum key distribution. Optica, 2020, 7: 238
16 Honjo T, Inoue K, Takahashi H. Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer. Opt Lett, 2004, 29: 2797–2799
17 Choe J S, Ko H, Choi B S, et al. Silica planar lightwave circuit based integrated 1 × 4 polarization beam splitter module for free-space BB84 quantum key distribution. IEEE Photon J, 2018, 10: 1–8
18 Takesue H, Sasaki T, Tamaki K, et al. Experimental quantum key distribution without monitoring signal disturbance. Nat Photon, 2015, 9: 827–831
19 Nambu Y, Yoshino K, Tomita A. Quantum encoder and decoder for practical quantum key distribution using a planar lightwave circuit. J Modern Opt, 2008, 55: 1953–1970
20 Li X, Ren M Z, Zhang J S, et al. Interference at the single-photon level based on silica photonics robust against channel disturbance. Photon Res, 2021, 9: 222–228
21 Zhang G W, Ding Y Y, Chen W, et al. Polarization-insensitive interferometer based on a hybrid integrated planar light-wave circuit. Photon Res, 2021, 9: 2176–2181
22 Rusca D, Boaron A, Grünenfelder F, et al. Finite-key analysis for the 1-decoy state QKD protocol. Appl Phys Lett, 2018, 112: 171104
23 Brassard G, Lütkenhaus N, Mor T, et al. Limitations on practical quantum cryptography. Phys Rev Lett, 2000, 85: 1330–1333
24 Roberts G L, Pittaluga M, Minder M, et al. Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution. Opt Lett, 2018, 43: 5110
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 Fan-Yuan G J, Wang C, Wang S, et al. Afterpulse analysis for quantum key distribution. Phys Rev Appl, 2018, 10: 064032
27 Wang F X, Chen W, Li Y P, et al. Non-Markovian property of afterpulsing effect in single-photon avalanche detector. J Lightwave Technol, 2016, 34: 3610–3615
28 Fan-Yuan G J, Wang S, Yin Z Q, et al. Modeling alignment error in quantum key distribution based on a weak coherent source. Phys Rev Appl, 2019, 12: 064044
29 Chen W, Han Z F, Mo X F, et al. Active phase compensation of quantum key distribution system. Sci Bull, 2008, 53: 1310–1314
30 Zhang L J, Wang Y G, Yin Z Q, et al. Real-time compensation of phase drift for phase-encoded quantum key distribution systems. Chin Sci Bull, 2011, 56: 2305–2311
31 Fan-Yuan G J, Chen W, Lu F Y, et al. A universal simulating framework for quantum key distribution systems. Sci China Inf Sci, 2020, 63: 180504