OPEN ACCESS

Stable quantum key distribution with active polarization control based on time-division multiplexing

To cite this article: J Chen *et al* 2009 *New J. Phys.* **11** 065004

New Journal of Physics
The open-access journal for physics

Stable quantum key distribution with active polarization control based on time-division multiplexing

J Chen, G Wu, L Xu, X Gu, E Wu and H Zeng[1]

State Key Laboratory of Precision Spectroscopy, East China Normal University, Shanghai 200062, People's Republic of China
E-mail: hpzeng@phy.ecnu.edu.cn

New Journal of Physics **11** (2009) 065004 (13pp)
Received 29 November 2008
Published 16 June 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/6/065004

Abstract. Polarization-encoding provides a promising approach for the practical quantum key distribution (QKD) system due to the simple encoding and decoding method. Here we present a long-term stable polarization-encoding QKD with a real-time polarization control. The polarization of the signal photons in the optical fiber was maintained stable by using time-division-multiplexed reference pulses for feedback control. We implemented this technique in the QKD experiment in 50 km fiber to show that it could facilitate polarization-encoded quantum communication. The system operated stably for ~460 min, and the quantum bit error rate was ~5.27%. The raw key generating rate in this system was kept stable at ~500 bits s^{-1}. The advantages and disadvantages of the previous polarization-control schemes were also rigorously analyzed.

[1] Author to whom any correspondence should be addressed.

Contents

1. Introduction

Quantum key distribution (QKD) offers an unconditional secure communication between two parties (called Alice and Bob) and it is illegible to any unauthorized third party (called Eve) [1, 2]. Since the first protocol was proposed by Bennett and Brassard in 1984, various QKD experiments and protocols based on entangled photon pairs, continuous-variable, polarization-encoding and phase-encoding have been put forward [3]–[16]. However, in practical quantum communication systems, schemes using entangled photon pairs suffer from low key generation rates and quantum decoherence effects. The communication distance in the continuous-variable scheme is also limited. And in fiber-based QKD systems, both polarization-encoding and phase-encoding require compensation of the polarization fluctuations induced by the unpredictable birefringence changes in the telecom optical fiber. In order to meet this requirement, a 'plug and play' phase-encoding scheme in 'two-way' fiber QKD was put forward and a number of experimental demonstrations were reported [13], [17]–[19]. This scheme has been demonstrated so far as the most stable QKD system since any birefringence effects and polarization-dependent losses can be compensated automatically in the optical fibers. But the security of the 'two-way' QKD is at risk of Trojan attacks [20]. And the maximum communication distance is limited by the noise caused by the Rayleigh scatting during the round trip of signal pulses in fibers. Compared with phase-encoding, polarization-encoding needs no precise active modulation to overcome the instability and error rate caused by the phase shift in fibers. It can be easily implemented in a 'one way' fiber system with the decoy-state QKD protocol to enhance its security in the lossy transmission channels [21]–[25]. Nevertheless, the polarization-encoded QKD suffers from random fluctuation of polarization in a long-distance fiber. It is necessary to have a robust and efficient control on the polarization of the signal photons in the fiber. Researchers have tried different ways to achieve a stable polarization control, among which two methods are employed. One is called 'interruption' scheme, which relies on interrupting the communication between Alice and Bob for the polarization control [26]. The other is called 'real-time' scheme where the states of polarization (SOPs) of the signal pulses are monitored and actively recovered without interruption of the communication [27].

In this paper, we present a novel real-time polarization control system based on the time-division multiplexing (TDM) of the reference and signal pulses. The reference and signal photons of the same repetition rate and central wavelength but of different intensities are

multiplexed by different time delays and pass the same polarization devices. At the receiver, the reference and signal photons are distinguished by using different gate pulses for detection. The photon-count variation of the reference pulses on the single-photon detectors exactly displays the SOP transformation of the signal photons in the same long-distance fiber. According to the counts of the reference signals, the SOP of signal photons is monitored and the random change of the SOP can be compensated with electronic polarization controllers (EPC) in a real-time system. The feedback control system operates with extremely weak reference pulses to avoid detrimental influence caused by bright pulses. The optimization of the SOP and the key generation work simultaneously and independently.

This paper is arranged as follows. In section 2, we give a brief review of the previous QKD experiments utilizing polarization control. Section 3 presents the TDM-based polarization control system. And the QKD experimental results with the real-time polarization control are presented in section 4. The possible improvements of the present setup are discussed in section 5.

2. Polarization control and polarization-encoded QKD in optical fibers

2.1. Polarization control

In 1992, Bennett *et al* [29] used polarization encoding to experimentally demonstrate the first quantum communication in the open air over 30 cm distance. The SOP can be stable in space due to the isotropy of air. But the situation becomes complicated in fiber-based QKD systems. The environmental changes such as temperature drifts and unavoidable stress result in the unpredictable polarization transformation of the single photons between Alice and Bob. Therefore, Bob needs an active polarization feedback control to ensure a stable SOP in the transmission link for correct polarization decoding. This can be realized by using EPCs consisting of three piezoelectronic actuators R_1, R_2 and R_3, which press the fiber along different directions to produce a linear birefringence in the fiber [30, 31]. According to the applied voltages on R_1 and R_3, the SOP rotates around the OQ axis on the Poincaré sphere as shown in figure 1. And increasing or decreasing the voltage on R_2 directed 45° from R_1 makes the SOP rotate around the orthogonal axis (OH axis). In principle, an arbitrary output polarization state (Q′) can be adjusted to the target polarization state (Q) by properly processing at least two piezoelectronic actuators.

2.2. Polarization-encoded QKD with interruption

A standard polarization-encoded BB84 protocol requires four linear polarization states in the horizontal (H), vertical (V), +45° (Q) and −45° (R) directions. Alice randomly sends signal photons polarized in HV or QR base. At Bob's site, he also randomly selects one of the two bases to measure the SOPs. But the SOPs of the photons change after a long-distance propagation in the fiber. To decode the polarization information correctly, Bob needs two EPCs to recover the SOP of the HV and QR bases, respectively. In the experimental setup, the polarization controls for the two selected bases are independent of each other. Once the decoding base is chosen, Bob only focuses on the polarization control of the orthogonal polarizations in that base. The polarization drifts in the other bases are disregarded since they produce no useful information in the selected base.

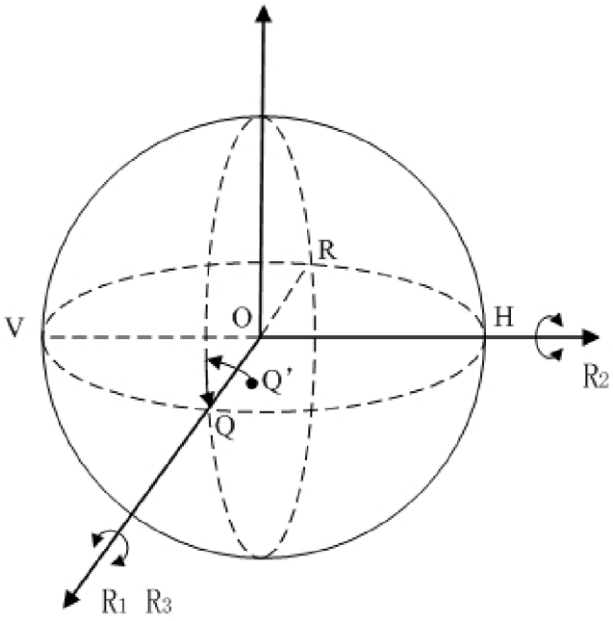

Figure 1. Photon polarization represented in the Poincaré sphere. The polarization directions of +45°, −45°, 0° and 90° are represented, respectively, by the points Q, R, H and V on the Poincaré sphere.

The conventional active polarization-control approach contains two operation cycles: the polarization-control cycle where Alice sends reference pulses containing large amounts of photons to adjust the compensating system to correct the slow polarization drifts, and the key-generation cycle where the average photon number is reduced to the single-photon level for the communication and Alice uses these photons for the key generation. The system periodically interrupts the key generation cycle to check the SOP with reference pulses. Polarization control is launched to compensate for the polarization offset if it become worse. After the SOP is recovered, the system switches back to the key-generation cycle and continues QKD [25, 26].

The experimental setup of the polarization control with 'interruption', mentioned above, is shown in figure 2. The signal and reference pulses are emitted from the same laser diodes (LDs) and polarized along the same direction. Therefore, the SOP of the signal and reference pulses transform in the same way in the long-distance fiber. The optical switch in the setup works from time to time according to the alternation of the two operation cycles. The attenuator $Attn_1$ is used to adjust the loss to increase the photon counts of the reference pulses in polarization-control cycle to enhance the count stability of reference photons. In this way, Bob can analyze the SOPs accurately and rapidly.

Based on this scheme, a 'one-way' polarization-encoded QKD with long-term stability was demonstrated [26]. Obviously, in this scheme, the key generation efficiency is reduced due to the periodic interruption by the polarization control.

2.3. Real-time polarization control based on wavelength-division multiplexing (WDM)

Compared with the 'interruption' scheme, the real-time polarization control is more applicable for the practical QKD system with an increased key generation rate. The polarization stability

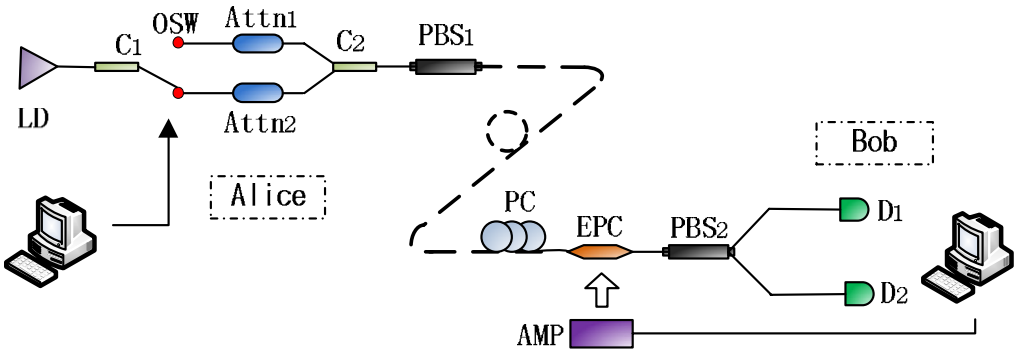

Figure 2. Experimental setup of the polarization control with 'interruptions'. LD: laser diode with central wavelength at 1550 nm; OSW: optical switch; $C_{1\sim2}$: optical couplers; $Attn_{1\sim2}$: variable optical attenuators; $PBS_{1\sim2}$: polarization beam splitters; EPC: electronic polarization controller; $D_{1\sim2}$: single-photon detectors; AMP: voltage amplifier; PC: manual polarization controller.

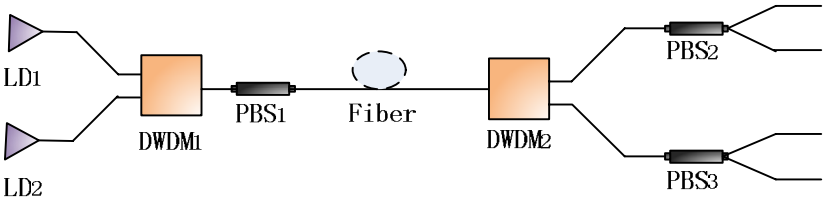

Figure 3. Test experiment setup for the QKD with WDM-based single-photon polarization control. The wavelengths of the LD_1 and LD_2 were 1549.3 and 1552.5 nm, respectively. The wavelength tuning is realized by adjusting the temperature of the LDs. Photons at different wavelengths are multiplexed and demultiplexed by $DWDM_1$ and $DWDM_2$.

can be further improved because the SOP in the fiber channel is uninterruptedly monitored by the real-time polarization control system during the whole communication. The multiplexing technique is a simple and efficient tool to realize real-time polarization control independent of the signal photon transmission. Recently, Xavier *et al* [27] have employed WDM to demonstrate that the polarization control could be realized by using non-orthogonal reference signals counter-propagating with the single-photon information carriers, leading to non-intercepted key generation. The propagation distance might be nevertheless limited by the Rayleigh scatting of the counter-propagating reference signals in this scheme. And the qubit polarization cannot be sufficiently controlled due to the wavelength-dependent polarization changes in a long-distance fiber channel. We tested the evolution of the polarization in the time domain at different central wavelengths (1549.3 and 1552.5 nm) in 3 and 18 km fiber, and the test duration was 1h. The test setup is shown in figure 3. By monitoring the output powers after PBS_1 and PBS_2, we obtained the respective visibilities $V_{1549.3}$ and $V_{1552.5}$ and the ratio $R = V_{1549.3}/V_{1552.5}$. In this WDM scheme, the polarization evolution for the signal and reference photons at different wavelengths

is supposed to be the same and the standard deviation (SD) of R should remain 0. But our test result revealed that the SD of R was dependent on the communication distance. With the 3-km fiber, we got the SD of R as 0.60%. But with the 18-km fiber, it increased to 1.53%. The SD of R might increase further with an increase of the propagation length, which brings about the major obstacle to control the polarization by using the WDM technique. The obstacle mainly originated from wavelength-dependent fiber birefringence. Different central wavelengths led to different polarization mode dispersion (PMD), which results in significant depolarization. As the PMD changes randomly, the average differential group delay $\langle\tau\rangle$ is typically used to describe the PMD [28]:

$$\langle\tau\rangle = \frac{h}{\sqrt{2}}\left(\frac{\partial W}{\partial \omega}\right)\left(\frac{2L}{h} - 1 + \exp\left[\frac{-2L}{h}\right]\right)^{1/2}, \tag{1}$$

where W is the average total birefringence, ω is the angular frequency of the light, h is the average polarization mode-coupling length due to random disturbances and L is the length of the fiber. Obviously, $\langle\tau\rangle$ is a function of the wavelength, and thus PMDs differ at different working wavelengths. Moreover, with the increase of the propagation distance, the difference of the PMDs for different wavelengths increases. If one chooses two wavelengths very close to each other, the wavelength-dependent polarization changes in fiber may decrease. But at present, limited by the channel bandwidth of the dense wavelength-division multiplexer (DWDM) device, the smallest gap between the two wavelengths we can implement in the laboratory is typically about 0.8 nm. In this case, the wavelength-dependent polarization changes cannot be ignored, especially in a long-distance fiber. As a result, the SOP of the reference photons could not represent the SOP evolution of signal photons. Such a WDM scheme cannot guarantee stable polarization control for polarization encoding in long-distance fiber.

3. Real-time polarization control based on TDM

To avoid the problems caused by the wavelength difference, we propose to employ TDM of the signal and reference pulses at the same wavelength to realize a real-time polarization feedback control. As figure 4 shows, the photon pulses were of the same repetition rate (1 MHz) and central wavelength (1550 nm). An asymmetric Mach–Zehnder interferometer with 10 m arm-length difference between the long and short arms was used to induce 50 ns time difference between the reference and signal pulses. At Bob's site, no special demultiplexing devices were used. After a 50/50 coupler, the signal and reference pulses could be easily distinguished according to their arrival times if we set the gate pulses of the corresponding single-photon detectors with different time delays. The signal photons were detected by D_1 and D_3. The polarization state was monitored by the photon counts of the reference pulses in D_2 and D_4, of which the synchronous gate was delayed 50 ns later than that of D_1 and D_3. Bob used a data acquisition card to record the photon counts of the detectors and sent the counting rate to the computer. After appropriate algorithmic processing, the data acquisition card generated two analog signals (V_1 and V_2) to drive the squeezers of the EPC by a high voltage amplifier. Then the squeezers pressed the fiber in different directions to induce additional birefringence to compensate for the random polarization fluctuations.

The feedback control program is detailed as follows. The program set three polarization-visibility thresholds T_1, T_2 and T_3 ($T_1 > T_2 > T_3$) to control the state of the program, where

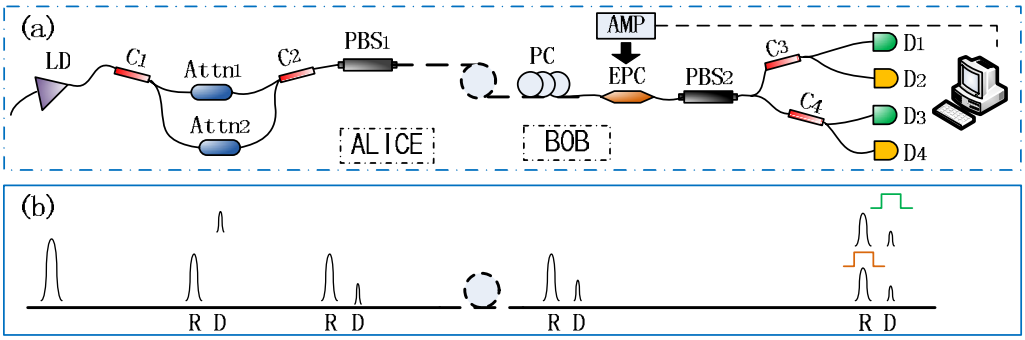

Figure 4. (a) Schematic diagram of the single-photon polarization-control system based on TDM. LD: DFB laser diode at 1550 nm; $Attn_{1\sim2}$: variable optical attenuators; $C_{1\sim4}$: optics couplers; $PBS_{1\sim2}$: polarization beam splitters; EPC: electronic polarization-controller; $D_{1\sim4}$: single-photon detectors; AMP: voltage amplifier. (b) Temporal distribution of the single and reference pulses. D: data pulse; R: reference pulse.

T_1 is the target visibility, T_2 is the visibility that polarization-control should start and T_3 is the tolerable limit visibility for the useful data. At first, V_1 and V_2 were set at the mean value of the EPC operation voltage range (0–150 V). We denote the visibility of each time as C which was monitored synchronously to judge whether the polarization was optimized. If $C < T_2$, the program produced two proper offset analog voltages for V_1 and V_2 to drive the piezoelectronic actuators R_1 and R_2 of the EPC, respectively. There were four possible changes of V_1 and V_2: ($V_1\pm$, $V_2\pm$, $V_1 \pm / V_2\pm$ and $V_1 \pm / V_2\mp$) ('+' for increase and '−' for decrease). If the changes on the V_1 and V_2 in one mode did not optimize the SOP, the other modes would be attempted until the SOP was recovered. Once $C > T_1$, which meant that the polarization in the fiber came back to the expected state, the values of V_1 and V_2 were maintained and the system was switched to the free running state until the next $C < T_2$ was recorded. The condition $C < T_3$ occasionally happened due to the sudden change of environment or the misjudgement of the program. In this instance, the generated keys were tagged as useless data. We tested the TDM-based polarization control in 50 km fiber. The result is shown in figure 5. The chosen values of T_1, T_2 and T_3 were 0.99, 0.98 and 0.97, respectively. In most cases, the polarization control worked with an acceptable polarization visibility. The red points below the tolerable limit (green dashed line) represent that the deteriorated SOP went out of the acceptable range. The useless data in our QKD result were about 2%.

The single-photon detectors used in the experiment were based on InGaAs/InP avalanche photodiodes (APD) operated in gated Geiger mode. The amplitude of the gate pulses was about 1.8 V. Once the applied reverse bias voltage reached the breakdown voltage, the APD experienced an avalanche at single-photon clicks. If single-photon pulses were caught within the 'gate', the APD produced coincidence count signals, while the photons arriving outside the 'gate' were not recorded. As in D_1 and D_3, almost all of the reference pulses were ignored due to the 50 ns delay from the gate pulses. Nevertheless, the response carriers generated by the reference photons on the APD could still be reserved for a period of time. If these carriers were

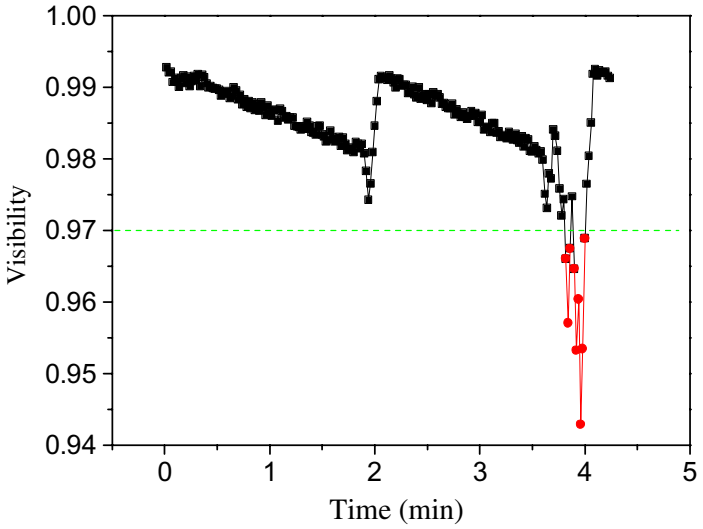

Figure 5. Polarization extinction ratio of the signal photons with the TDM-based polarization control in 50 km fiber.

not released when the next gate pulse started, they would possibly be recorded in this gate and this count would be added to the error of the key generation. This possibility was related to the intensity of the reference pulses and the delay between the gate and reference pulses.

We measured the reference photon counts within the signal gate pulses to check the influence of the reference power on the error counts of the key generation. The half-widths of reference and gate pulses were set to be 1 and 2 ns, respectively. The reference pulses were delayed by 50 ns from the signal gate pulses. The APD (JDSU Co.) was Peltier cooled at $-65\,^{\circ}$C and the quantum efficiency was 10%. As shown in figure 6(a), when the power of the reference pulse was lower than 1.6 pW (at 1 MHz), the photon counts of the single-photon detector were produced dominantly by the dark counts of the APDs and the reference pulses produced negligible effects on the detection of the signal photons. Above 1.6 pW, the photon counts increased obviously. These photon counts were from the carriers caused by the reference pulses that were not released when the next gate pulse began, as mentioned above. The result of the test showed that the influence of reference pulses was negligible at low powers (<1.6 pW) and, accordingly, the polarization-control and polarization-encoding could operate in the same optical fiber with negligible cross-interference. In our QKD experiment, a reference power of 0.013 pW (namely, 0.1 photon per pulse at 1 MHz) was sufficient to monitor the polarization change to produce accurate feedback signal. With such reference pulses, the monitoring detectors could obtain enough counts to analyze the SOP and the influence of the dark counts in the detectors could be minimized. We also measured the reference photon counts with different delays between the reference and gate pulses, keeping the reference pulse power at 0.013 pW. As shown in figure 6(b), when the gap from the reference pulse to the following gate pulse was larger than 2.7 ns (reference ahead), the carriers caused by the reference could be neglected and there were almost no error counts from the unreleased carriers. The above test indicated that the TDM-based polarization-control could facilitate a repetition rate of up to $\sim$400 MHz at 0.1 photon per reference pulse.

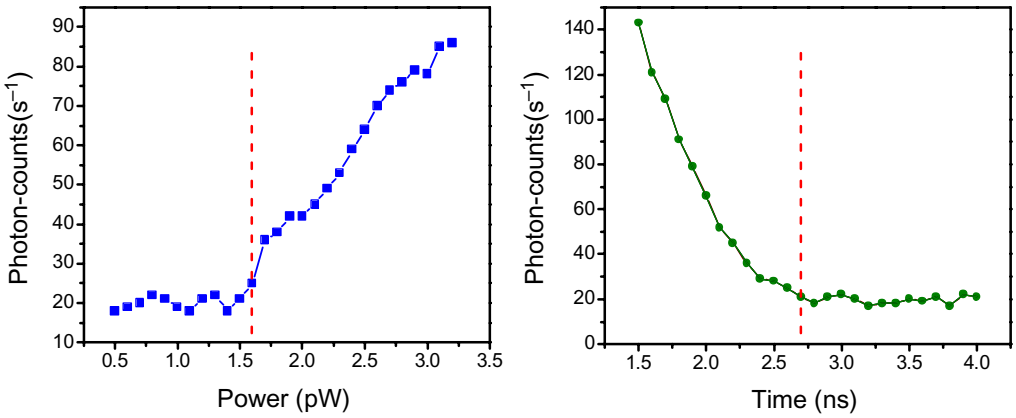

Figure 6. (a) Counting rate of the reference pulses detected by the data signal gate pulses as a function of the reference pulse power. (b) Statistics of the reference pulse counting rate with different delays between the reference and gate pulses.

4. QKD experiment

A real-time polarization-encoded QKD system employing TDM-based polarization control was experimentally realized. The setup is shown in figure 7. The repetitive pulses from LD_5 were used to synchronize the sender and receiver during the whole communication period. This separate channel for the clock signal can avoid the influence of its Raman scattering. At Alice's site, the linearly polarized single-photon pulses with +45° (Q), −45° (R), 0° (H) and 90° (V) along the optical axis of the system were emitted by LD_1, LD_2, LD_3 and LD_4, respectively. For the HV base, the laser pulses from LD_4 were separated into signal pulses (through up path) and reference pulses (through down path). After $Attn_5$ and $Attn_7$, the signal pulses were attenuated to 0.2 photon per pulse. By comparison, the average photon number of the reference pulses was attenuated to ∼4 photons per pulse after $Attn_6$ and $Attn_7$ and delayed by 50 ns from the signal photons. After PBS_2, all the photons exhibited the same polarization. As the reference and signal photons of the same wavelength propagated in the same long-distance fiber, the SOPs of both transformed in the same way. The polarization-control for the QR base in BB84 protocol was similar to that for the HV base. The only difference was that the reference pulses of QR-base were delayed for 90 ns in order to guarantee that the reference pulses of HV and QR bases were detected independently by the corresponding detectors D_6 and D_5. At Bob's site, the Q, R, H and V polarized photons were detected by D_2, D_1, D_4 and D_3, respectively. Each arriving photon had 50% probability of choosing the correct decoding base after the fiber coupler. For the HV base, the reference SOP was set in the vertical direction (V) and the transformation of polarization could be monitored by D_6 detecting along the H-direction. In principle, there should be another detector 'D_7' to monitor the reference photons separated from D_4 channel (V-direction) in order to measure the accurate polarization in the HV base. However, if the total number of reference photons remains stable, the SOP of the original V-direction can be estimated depending on the detection along the orthogonal direction (H). Actually, the final intention of the polarization-control system was to keep the counts of D_6 below a threshold value, and then Bob could approximately maintain linear V polarization. Based on such a

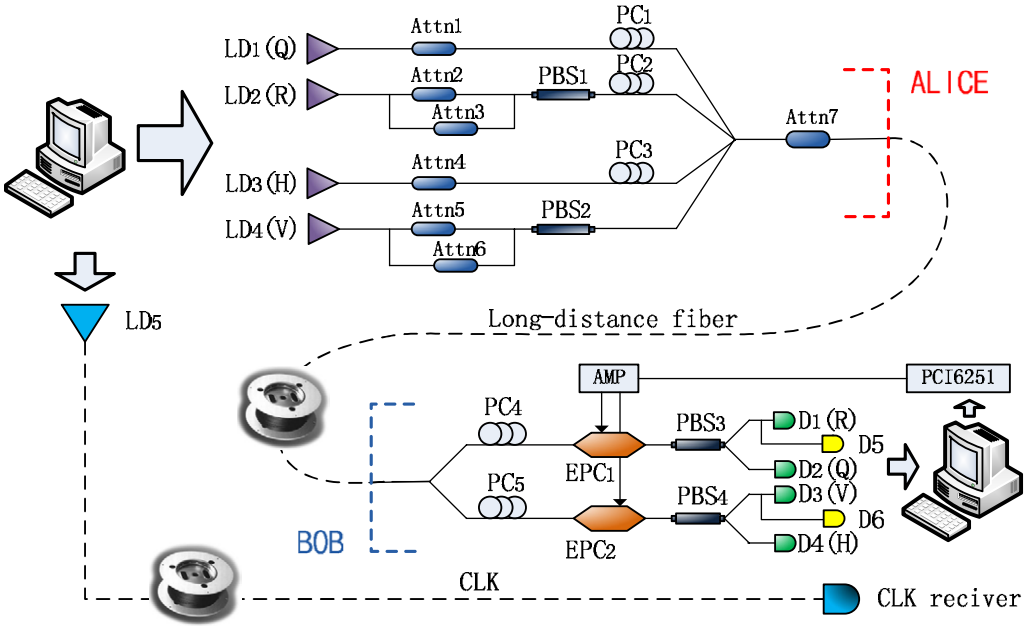

Figure 7. Experimental setup of QKD system under TDM-based polarization control. $LD_{1\sim5}$: DFB laser diodes at 1550 nm; $Attn_{1\sim7}$: variable optical attenuators; $PBS_{1\sim4}$: polarization beam splitters; $EPC_{1\sim2}$: electronic polarization-controllers; $D_{1\sim6}$: single-photon detectors; AMP: voltage amplifier; $PC_{1\sim5}$: manual polarization-controllers.

real-time control, a long-term stable QKD system could be realized in the long-distance fiber channel.

The polarization-encoded QKD experiment with polarization-control was demonstrated in 50 km fiber. The average 0.2 photon per signal pulse in our experiment was set to defeat possible photon-number-splitting attack. According to the simple inequality $P_{\text{exp}} > P_{\text{multi}}$ that is a necessary condition for an error-free QKD system [32], we choose the average photon number of 0.2 for 50 km fiber. P_{exp} is the probability of the number of non-empty signals as expected given by the lossy channel, and P_{multi} is the probability of the multiphoton signals. In our experimental setup, 50 km fiber provided 10 dB loss. We had $P_{\text{exp}} = 0.2 \times 10\% = 0.02$ and $P_{\text{multi}} = 1 - P_1 - P_0$ (P_1 and P_0 are the probability of containing 1 photon and 0 photon in one pulse, respectively). According to the Poissonian distribution, $P_{\text{multi}} \approx 0.0175$. Of course, a QKD system with unconditional security would better employ the decoy-state protocol to cover a longer distance of absolutely secure communication. The raw key generation rate was $\sim$500 bits s^{-1}. The secure key generation rate R can be calculated by the following equation [33, 34]:

$$R = \tfrac{1}{2} Y_{\text{exp}} I_{\text{AB}}, \tag{2}$$

$$I_{\text{AB}} = 1 + D\log_2(D) + (1 - D)\log_2(1 - D), \tag{3}$$

where Y_{exp} is Bob's expected click of single-photon pulses per second, in our experiment, $Y_{\text{exp}} = 1000$ bit s^{-1}. I_{AB} is the mutual information between Alice and Bob. D is Bob's bit error rate (5.27% in our experiment). We obtain $R \approx 350$ bit s^{-1}. The secure keys can be generated

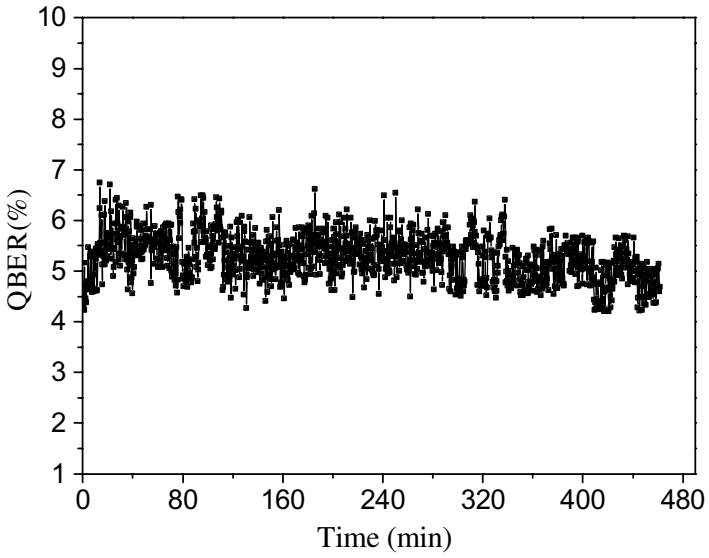

Figure 8. Evolution of the QBER in 50 km fiber polarization-encoded QKD within ∼460 min.

after classical data processing (error correction, privacy amplification for instance). In this paper, we focus on the scheme of the QKD with real-time polarization control. We did not employ sequential data processing after raw key generation. The dark counts of the detectors were 1.7×10^{-5} (D_1), 1.2×10^{-5}(D_2), 1.8×10^{-5}(D_3), and 1.3×10^{-5}(D_4), 3.4×10^{-5}(D_5), 4.1×10^{-5}(D_6) and the corresponding quantum efficiencies were 14, 7, 14% and 7, 7, 7%. The high efficiency of D_1 and D_3 was set to compensate for the separated signal photons that were received by D_5 and D_6, respectively, as shown in figure 7. The trade-off between quantum efficiency and dark count rate of the single-photon detectors lies in the signal-to-noise rate. Since all the single-photon detectors were designed by ourselves, the breakdown voltage of APD could be easily adjusted to find the best balance point between quantum efficiency and dark count rate [35]. By experimental comparison, the best signal-to-noise ratio was obtained when the quantum efficiency was about 10%. In the experiment, we set the quantum efficiency to 7% and 14% (around 10%) for the single-photon detectors to balance the photon count since half of the signal photons were detected by the reference single-photon detectors in the TDM scheme. Figure 8 displays the evolution of quantum bit error rate (QBER) within a long-term operation of ∼460 min, and the mean value of QBER is 5.27%.

5. Discussion and conclusion

Actually the TDM technique has been widely used in classical optical communication to increase the transmission bandwidth. But different from the classical optical communication, the QKD handles the SOP of single photons, which requires special designs for polarization control. This is the first time, as far as we know, that the TDM technique is used for polarization control at the single-photon level. The TDM technique supports real-time polarization control independent of the raw key generation processing. No additional noise is induced by the reference pulses with appropriately selected low powers and delays. It improves the key-generation efficiency without intentional interruption of the key-generation cycles. In the

standard 'interruption' scheme, the polarization control process occupied ∼9% of the whole communication duration, where the key generation was not available [26].

In this TDM scheme, the QBER mainly consists of two parts: the dark noise of the single-photon detectors (∼3.3%) and the imperfect polarization control (∼2.0%). Some improvements can be applied to decrease the QBER. For example, if the APDs are operated in liquid nitrogen environment at −95 °C, the detectors can obtain the best signal-to-noise ratio [35]. In this way, the estimated QBER of the system may decrease to 3.0% due to the suppression of the dark noise. Moreover, it will be better if the TDM system operates at a higher repetition rate to increase the counts of reference pulses [36, 37]. Because the polarization control is based on the accumulation of photon counts, to analyze the SOP on the extremely faint light intensity level, increased counts of the reference detection can increase the bandwidth of the feedback control system to enhance its reliability and accuracy. Another possible improvement of the system lies in the optimization of the feedback program to enhance the analysis ability and the control precision. By this means, the polarization recovering process will speed up and its occupation in the whole communication duration will be much shortened, leading to a decrease of the useless data. And the average polarization extinction ratio can be increased as well, further decreasing the QBER. Meanwhile, the stability of the system might be improved if the program could be optimized for more powerful capability against disturbances such as sudden changes of the environment, which usually force the communication to be stopped.

In conclusion, we demonstrated long-term stable polarization-encoded QKD with an active and non-interruption polarization control based on a TDM technique. The SOP transformation was monitored by detecting reference pulses appropriately delayed from the signal pulses. By using EPC to control the polarization of the reference photons, real-time polarization feedback control was achieved in a long-distance fiber, and the SOP of signal photons could remain stable for hours. This scheme provides a quite simple but robust method to realize real-time 'one way' polarization-based QKD, which is also suitable for the implementation of the decoy-state protocol against photon-number-splitting attack with enhanced security in long-distance fiber. Such a scheme can be used as a robust technique for a polarization-encoded QKD system.

Acknowledgments

This work was funded in part by National Natural Science Fund (grant nos. 10525416, 10774045, 10804032 and 60807027), National Key Project for Basic Research (grant nos. 2006CB921105 and 2006CB806005), Projects from Shanghai Science and Technology Commission (grant no. 8530708200), Shanghai Leading Academic Discipline Project (grant no. B408), and Key Project Sponsored by the National Education Ministry of China (grant no. 108058), and ECNU PhD Research Fund.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India)* (New York: IEEE) p 175–9
[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145–95
[3] Ribordy G, Brendel J, Gautier J, Gisin N and Zbinden H 2000 *Phys. Rev.* A **63** 012309
[4] Jennewein T, Simon C, Weihs G, Weinfurter H and Zeilinger A 2000 *Phys. Rev. Lett.* **84** 4729
[5] Enzer D G, Hadley P G, Hughes R J, Peterson C G and Kwiat P G 2002 *New J. Phys.* **4** 45

[6] Ma X, Fung C F and Lo H K 2007 *Phys. Rev.* A **76** 012307
[7] Hübel H, Vanner M R, Lederer T, Blauensteiner B, Lorünser T, Poppe A and Zeilinger A 2007 *Opt. Express* **15** 7853–62
[8] Ralph T C 1999 *Phys. Rev.* A **61** 010303
[9] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[10] Muller A, Zbinden H and Gisin N 1996 *Europhys. Lett.* **33** 335–40
[11] Franson J D and Jacobs B C 1995 *Electron. Lett.* **31** 232–4
[12] Townsend P 1998 *Opt. Fiber Technol.: Mater. Devices Syst.* **4** 345
[13] Zbinden H, Gautier J D, Gisin N, Huttner B, Muller A and Tittel W 1997 *Electron. Lett.* **33** 586–8
[14] Marand C and Townsend P D 1995 *Opt. Lett.* **20** 1695
[15] Hughes R, Morgan G and Peterson C 2000 *J. Mod. Opt.* **47** 533–47
[16] Zhao Y, Qi B and Lo H K 2007 *Appl. Phys. Lett.* **90** 044106
[17] Muller A, Herzog T, Huttner B, Tittel W, Zbinden H and Gisin N 1997 *Appl. Phys. Lett.* **70** 793
[18] Ribordy G, Gautier J D, Gisin N, Guinnard O and Zbinden H 2000 *J. Mod. Opt.* **47** 517–31
[19] Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 *New J. Phys.* **4** 41
[20] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev.* A **73** 022320
[21] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[22] Wang X 2005 *Phys. Rev. Lett.* **94** 230503
[23] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[24] Hayashi M 2007 *New J. Phys.* **9** 284
[25] Peng C, Zhang J, Yang D, Gao W, Ma H, Yin H, Zeng H, Yang T, Wang X and Pan J 2007 *Phys. Rev. Lett.* **98** 010505
[26] Chen J, Wu G, Li Y, Wu E and Zeng H 2007 *Opt. Express* **15** 17928–36
[27] Xavier G B, Vilela de Faria G, Temporão G P and von der Weid J P 2008 *Opt. Express* **16** 1867–73
[28] de Lignie M C, Nagel H G J and Oskar van Deventer M 1994 *J. Lightwave Technol.* **12** 1325–9
[29] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 *J. Cryptol.* **5** 3
[30] Ulrich R 1979 *Appl. Phys. Lett.* **35** 840–42
[31] Noe R, Heidrich H and Hoffmann D 1988 *J. Lightwave Technol.* **6** 1199–208
[32] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[33] Wyner A D 1975 *Bell Syst. Tech. J.* **54** 1355
Csiszár I and Körner J 1978 *IEEE Trans. Inf. Theory* **24** 339
[34] Wu G, Chen J, Li Y, Xu L and Zeng H 2006 *Phys. Rev.* A **74** 062323
[35] Wu G, Zhou C, Chen X and Zeng H 2006 *Opt. Commun.* **265** 126
[36] Fernandez V, Collins R J, Gordon K J, Townsend P D and Buller G S 2007 *Proc. SPIE* **6780** 678004
[37] Yuan Z L, Dixon A R, Dynes J F, Sharpe A W and Shields A J 2008 *Appl. Phys. Lett.* **92** 201104