Chinese Science Bulletin

Active phase compensation of quantum key distribution system

CHEN Wei[1,2], HAN ZhengFu[1†], MO XiaoFan[1], XU FangXing[1], WEI Guo[2] & GUO GuangCan[1]

[1] Key Lab of Quantum Information, University of Science and Technology of China, Hefei 230026, China;
[2] Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei 230026, China

Quantum key distribution (QKD) system must be robust enough in practical communication. Besides birefringence of fiber, system performance is notably affected by phase drift. The Faraday-Michelson QKD system can auto-compensate the birefringence of fiber, but phase shift is still a serious problem in its practical operation. In this paper, the major reason of phase drift and its effect on Faraday- Michelson QKD system is analyzed and an effective active phase compensation scheme is proposed. By this means, we demonstrate a quantum key distribution system which can stably run over 37-km fiber in practical working condition with the long-time averaged quantum bit error rate of 1.59% and the standard derivation of 0.46%. This result shows that the active phase compensation scheme is suitable to be used in practical QKD systems based on double asymmetric interferometers without additional devices and thermal controller.

quantum key distribution, Faraday-Michelson system, phase drift, active phase compensation

Quantum key distribution (QKD) systems, which are based on the fundamental principles of quantum mechanics, are the new generation of cryptography. Since the first scheme BB84 was proposed in 1984 by Bennet and Brassard[1], QKD systems have been remarkably developed theoretically and experimentally[2−7].

Many fiber QKD systems have been developed in the past few yeas for the rapid increasing demands of network security. Most of fiber QKD systems have been realized using phase-encoded methods because phase-encoded qubit is relatively more resistant to decoherence than polarize-encoded qubit in fiber[8]. In order to use QKD systems in practical conditions for long time operating, they must be resistant to birefringence and phase drift caused by environment variations in optical fiber. Although the effect of fiber birefringence on asymmetric Mach-Zehnder interferometer (AMZI) QKD system[9] was eliminated by Faraday-Michelson (F-M) system, which was proposed by Mo et al. in 2005[7], the phase drift is still an obstacle in actual QKD sessions.

Generally, there are three methods to solve phase drift problem in fiber QKD systems:

(1) Modify the structure of interferometers such as "plug-and-play" configuration to auto-compensate for the phase shift[10];

(2) Use passive compensation to reduce the negative effect of environment fluctuations by strict thermal and mechanical isolation;

(3) Acquire drift parameters by active phase tracking then performing compensation.

The "plug-and-play" system is very stable and can automatically compensate for both birefringence and phase drift. However, the configuration is more difficult than one-way systems in preventing from Trojan attack[4,11,12], and the raw bit rate is lower than those sin-

Received April 11, 2007; accepted July 17, 2007
doi: 10.1007/s11434-008-0023-0
†Corresponding author (email: zfhan@ustc.edu.cn)
Supported by the National Fundamental Research Program of China (Grant No. 2006CB921900), National Natural Science Foundation of China (Grant Nos. 60537020 and 60621064), and Knowledge Innovation Project of Chinese Academy of Sciences

gle-trip systems for its round-trip propagation. Interferometers made of low thermal factor materials[13] or integrated planar silica waveguide with thermal and mechanical isolation can be used in passive compensation[14,15]. Another improved way to passively compensate for phase drift is to find the environment temperature of interferometers, at which the difference between the modal phase shifts in the long and short arms of the AMZI ($\theta_L - \theta_S$) is multiples of 2π[16]. Although these measures can suppress the harmful temperature disturbance of environment, there must be accurate temperature controller with precision of 0.01℃ in the system. Even though the phase drift can be observed as the temperature of encoder AMZI and decoder AMZI changing independently, i.e., the phase shift of AMZI can not essentially be avoided. Townsend et al.[17] and Yuan et al.[18] used fiber stretcher to adjust fiber arm length to compensate for the phase drift. Yuan et al.[18] and Zavaryev et al.[19] use individual strong reference light to acquire phase shift parameters. Markarov et al.[20] used single photon counting and software algorithm to calculate phase drift parameters without actual QKD experiment result. The method of adjusting fiber length is not efficient to deal with practical QKD sessions and makes the system more complexity. Strong reference light increases the optical complexity due to additional devices and introduces more interference. In order to get enough counts, the tracking time in the single photon counting scheme will protract due to the increasing transmission distance and the maximum drift range which can be compensated is reduced.

The phase drift of QKD system is much more obvious in practical enviornment than on optical table, so a more effective compensation scheme must be adopted to keep system operating continuously with low QBER. In this paper, we analyze the major reason which causes system phase drift in field, and propose a novel effective phase compensating scheme. With this scheme, F-M system continuously can operate without any manual intervention in practical condition over 37-km optical fiber for more than 18 hours, while the system QBER is 1.59% with fluctuation less than 0.46%. Moreover, the scheme is also suitable for other QKD systems based upon M-Z interferometer.

P_{out1}, the output power of Faraday-Michelson interferometer (F-MI) can be derived from its simplified structure, as is shown in Figure 1[7].

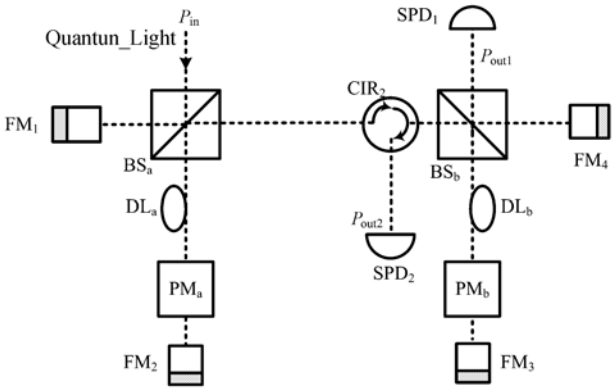

Figure 1 Simplified light path of F-M system. BS, 50/50 beam splitter; FM, Faraday mirror; SPD, single photon detector; CIR, circulator; DL, fiber delay line.

$$P_{out1} = \frac{\alpha}{8}[1 + \cos(\Delta\varphi_{pl} + \Delta\varphi_{pm})]E_{in}^{+}E_{in}. \quad (1)$$

Assuming that Δl_a and Δl_b are path differences of Alice and Bob's interferometers, respectively, and that wave vector is $k = \frac{2\pi}{\lambda}$, the phase difference between the two interfering light pulses is $\Delta\varphi_{pl} = k(\Delta l_b - \Delta l_a)$, where α is the optical attenuation factor. The phase differential value between Alice's and Bob's modulators is $\Delta\varphi_{pm}$. The output energy from P_{out1} will be the maximum when $\varphi_{pl} + \Delta\varphi_{pm} = 0$ and the minimum when $\Delta\varphi_{pl} + \Delta\varphi_{pm} = \pi$.

Without phase compensation, QBER caused by phase error is

$$QBER_{\Delta\varphi} = \sin^2\left(\frac{\Delta\varphi_e}{2}\right), \quad (2)$$

where $\Delta\varphi_e = \Delta\varphi_{epl} + \Delta\varphi_{epm}$, in which $\Delta\varphi_{epl}$ is caused by interferometer asymmetry of Alice and Bob, and $\Delta\varphi_{epm}$ is their reference phase difference. In theory, we can minimize $\Delta\varphi_e$ by adjusting $\Delta\varphi_{epm}$ precisely and supposing $\Delta\varphi_{epl}$ is constant, and then the count of SPD1 reaches its maximum and keeps stable. But the fluctuation of SPD counting oversteps the rational range in practical experiment, even if we have adjusted the modulation voltages of Alice and Bob to make $\Delta\varphi_e \to 0$. This illustrates that the phase drift exists in F-M QKD system. As the primary reason, environmental variations such as temperature fluctuation and mechanical vibration will change $\Delta\varphi_{pl}$, resulting in phase drift. During longtime operating, temperature fluctuation influences system performance much more than mechanical vibration, so the phase drift of F-M QKD system caused by

temperature is analyzed specifically in the next part.

If the thermal expansion coefficient of fiber is α_T, the fiber length is l, and temperature variation is Δ_T, then the fiber length changed by temperature is $\Delta L = \alpha_T \cdot l \cdot \Delta_T$. We define the reference temperature T_0 at which interferometers are made up. When the system is operating, the temperature variations of Alice and Bob are $\Delta T_a = T_a - T_0$ and $\Delta T_b = T_b - T_0$, respectively, and the phase difference between the two interfering optical pulses can be described as

$$\Delta\varphi = \Delta\varphi_{pm} + k(\Delta l_b - \Delta l_a) + \alpha_T k(\Delta l_b \Delta T_b \Delta l_a \Delta T_a), \quad (3)$$

where $\Delta\varphi_{pm}$ is the phase difference of the two phase modulators of Alice and Bob, and the third part of the equation is temperature impact on QKD system. If we define $l = (\Delta l_a + \Delta l_b)/2$ and $T = (\Delta T_a + \Delta T_b)/2$, then the inherent asymmetry can be written as $\Delta l = \Delta l_b - \Delta T_a$. Practically, the ambient temperatures of Alice and Bob are not the same. If $\Delta T = \Delta l_b - \Delta T_a$, the equation (3) can be modified as

$$\begin{aligned}\Delta\varphi &= \Delta\varphi_{pm} + k\Delta l + k\alpha_T T\Delta l + k\alpha_T l\Delta T \\ &= \Delta\varphi_{pm} + \Delta\varphi_0 + \Delta\varphi_{T1} + \Delta\varphi_{T2} \\ &= \Delta\varphi_{pm} + \Delta\varphi_0 + \Delta\varphi_{\text{var}}, \end{aligned} \quad (4)$$

where $\Delta\varphi_0$ is the constant phase difference caused by intrinsic asymmetry of interferometers. $\Delta\varphi_{T1}$ and φ_{T2} have relationship with ambient thermal variation and can be merged into phase drift $\Delta\varphi_{\text{var}}$. For example, the interferometer used in our experiment is made of silica fiber with thermal expansion coefficient of 5.4×10^{-7}℃. If the long arm of interferometer is 3 m longer than the short arm, then 0.03℃ difference in temperature can result in 1% QBER.

Active phase modulation with integrated electro-optic modulator is often used in phase-encoded QKD systems. Modulation scheme must be correlated with QKD protocol such as BB84, B92 and so on. For example, in order to use BB84, which is well known as an absolutely secure protocol, user must determine the four driving voltage operating points of phase modulator corresponding to optical phases of 0, π/2, π and 3π/2. If we can acquire phase drift parameters, then phases can be drawn back to their proper positions by adjusting voltage working points.

The two steps of active phase compensation scheme are parameter acquisition and active compensation. QKD system performs "scan" operation to acquire phase drift parameters before crypto key transfer[21]. At the beginning of the scan process, the driving voltage of PM_a, the modulator of Alice, is fixed at V_{a0}. φ_{a0} is the phase determined by V_{a0}, which is used as Bob's reference phase. Because only the relative phase between Alice and Bob is significant, we can set $V_{a0}=0$ and $\varphi_{a0}=0$. Bob increases PM_b's driving voltage from $V_{\min}$ to $V_{\max}$ with voltage step of ΔV. The scan range of phase must be more than 2π. At each voltage step, system waits for N synchronization pulses, and accumulates the count of SPD to get C_i. The voltage-count couples of $\{V_i, C_i\}$ can be plotted as interference fringe. As shown in Figure 2, the fringe is coincident with a sinusoidal pattern. Phase difference between PM_a and PM_b is zero on the top of the sinusoidal curve, while π at the bottom. By measuring the difference between V_{c_max} and V_{c_min}, which are according to the maximum and minimum count positions, respectively, we can get the half-wave voltage of modulator.

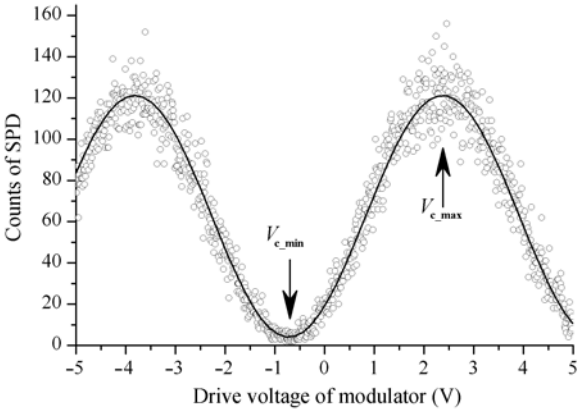

Figure 2 Interference fringe. driving voltage from −5 to +5 V, each point is accumulated from 1000 optical signal pulses. The real line is sinusoidal fitting of the fringe.

A reference voltage is necessary in order to calculate working points of Bob. For example, if we choose V_{ref} which has the phase difference of π with V_{a0}, then from eq. (4) we can deduce

$$\pi = \pi\frac{V_{\text{ref}}}{V_{\text{half}}} + \Delta\varphi_0 + \Delta\varphi_{\text{var}}, \quad (5)$$

where V_{half} is half-wave voltage of modulator and $\Delta\varphi_{\text{var}}$ is phase drift. Then during crypto key transfer, the four voltage operating points of Alice are

$$\begin{aligned}&\{V_{a,0}, V_{a,1}, V_{a,2}, V_{a,3}\} = \{V_{a,0}, V_{a,\pi/2}, V_{a,\pi}, V_{a,3\pi/2}\} \\ &= \{0, \tfrac{1}{2}V_{\text{half}}, V_{\text{half}}, \tfrac{3}{2}V_{\text{half}}\}. \end{aligned} \quad (6)$$

The working points of Bob can be obtained by adding V_{half} to V_{ref} as follows,

$$\{V_{b,0},V_{b,1},V_{b,2},V_{b,3}\} = \{V_{b,0},V_{b,\pi/2},V_{b,\pi},V_{b,3\pi/2}\}$$
$$= \{V_{ref} - V_{half},\ V_{ref} - \tfrac{1}{2}V_{half},\ V_{ref},\ V_{ref} + \tfrac{1}{2}V_{half}\}. \quad (7)$$

In the real system the voltage saturation must be considered in equation (7).

When Alice and Bob set their modulation voltages at $V_{a,j}$ and $V_{b,j}$, their phase difference is

$$\Delta\varphi = \pi\frac{V_{b,j} - V_{a,i}}{V_{half}} + \Delta\varphi_0 + \Delta\varphi_{var} = \frac{j-i}{2}\pi. \quad (8)$$

This result shows that the coherent error and phase drift can be compensated through adjustment of driving voltage operating points.

Figure 3 illustrates the diagram of the F-M system and the real devices is shown in Figure 4. Light from 1550 DFB laser is divided into sync light and quantum light by a 1∶99 fiber optic splitter. The 1% output of splitter is quantum signal, and the 99% output acts as the sync signal. Quantum signal transfers through F-MI in Alice and is attenuated by an electronic optical attenuator. Signal pulses transmit over 37.2-km telecom fiber and are fed into another part of F-MI. Detection results of SPD are sent to host by data acquisition device

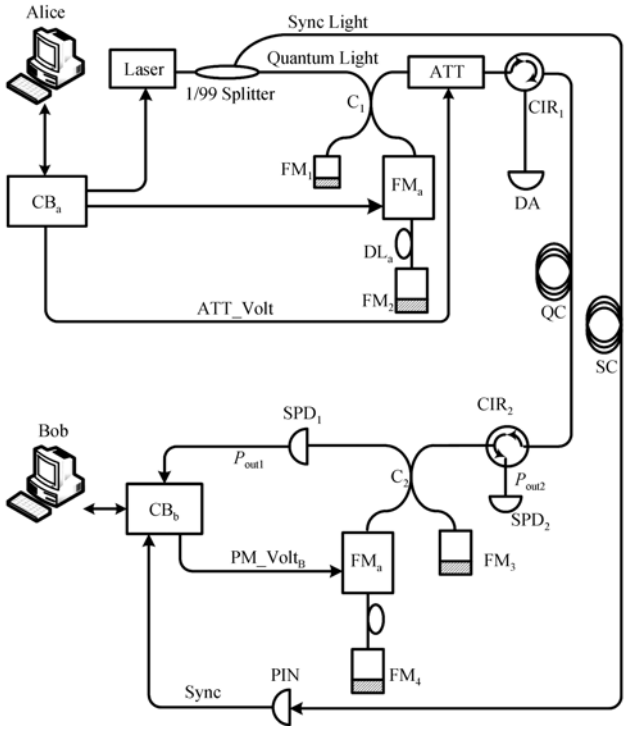

Figure 3 Schematic of Faraday-Michelson QKD experiment system. Laser, 1550-nm DFB laser; CB, system control board; FM, Faraday mirror; PM, optical phase modulator; C, optical coupler; DL, fiber delay line; ATT, optical attenuator; SPD, single photon detector; PIN, detector for sync optical pulse; QC, quantum channel; SC, sync channel; DA, intruding detector; PM_Volt, driving voltage for modulator; Att_Volt, driving voltage for attenuator.

Figure 4 Practical QKD system. Each part of the system was compacted into a 5U-height (225 mm) rack mounts without temperature controller.

through USB2.0 interface. Host calculates the phase drift parameter and controls phase modulator to perform active compensation. The system pulse repetition rate is 1 MHz and BB84 protocol for QKD is used. Mean photon number per pulse of quantum signal light is set to μ=0.1. Transmission loss of the link is 7.4 dB. The InGaAs SPD (id200 made by id Quantique) with dark count probability of 1.5×10^{-5} was used in this experiment.

The system phase drift rate can be estimated by continuously monitoring the count of SPD while PM_a and PM_b keep constant driving voltages. Phase drift is commonly rapid and irregular in the operating environment. In our experiment the phase drift rate can exceed 4.2 rad/min in average, as shown in Figure 5, while the phase drift rate reported by Townsend[15] and Makarov[18] is 0.6 rad/min and 2.0 rad/min respectively with the experiment equipments on the optical table. Figure 6 illustrates the data recording over 18 hours without manual adjustment. Every QBER sample was a statistical value of 1 M-bit block. In our system, the raw key generation rate is 800 bps with single SPD.

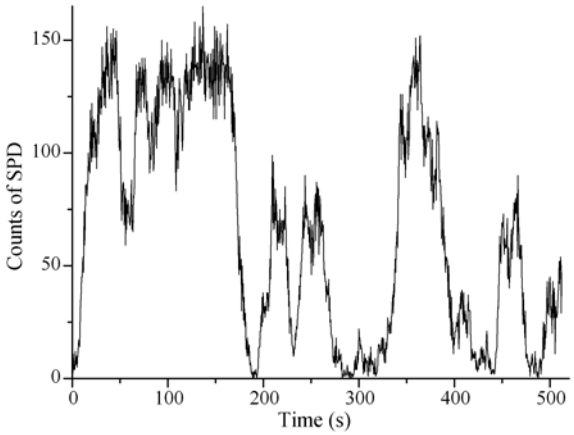

Figure 5 Long time phase drift of QKD system.

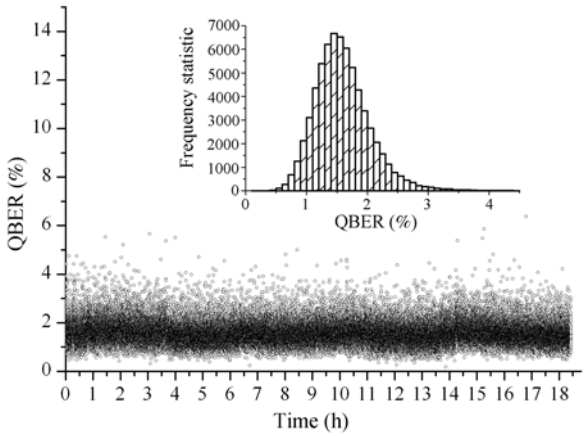

Figure 6 QBER of F-M system with phase compensation. The inset shows the distribution of different values for the QBER.

The QBER due to the residual phase mismatch between two F-MI is an important parameter to evaluate the active compensation scheme. QBER over the whole QKD session is 1.59%, and the standard derivation of QBER is 0.46%. System fringe visibility is 98.98% which infers the QBER due to the optical imperfection is 0.51%. The QBER from detector's dark count is 0.28%, thus the QBER made by phase error and others is 0.8%. This result illustrates that we can control phase error within 0.2rad according to equation (2). By comparing Figures 5 and 6, it can be seen that there is no continuous high QBER arising with large-scale phase drift. This result demonstrates the active phase compensation scheme is powerful for practical QKD sessions. Some points with QBER higher than 4% in Figure 6 are probably relative to the contingent strong vibration which causes sharp phase drift that exceeds the compensation range of the scheme.

The duty cycle of system is an important parameter for assessing the efficiency of QKD schemes. The system duty cycle is defined as the ratio of time which is actually used for key transmission to the total time, i.e., $\tau = t_{\text{tran}}/t_{\text{total}}$. In our system, the duty rate is 96.4% and keeps constant during the whole session.

In summary, we have analyzed in detail the major reason which causes phase drift of Faraday-Michelson QKD system in practical environment and realized an efficient active phase compensation scheme to solve the problem. The compensation scheme gives a QBER of 1.59% averaged over 18 hours practical key distribution session and a system duty cycle of 96.4% without any additional devices or thermal controller. The results demonstrate that actively compensated QKD systems are suitable for practical applications.

1 Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of International Conference on Computers, Systems and Signal Processing, 1984. 175－179
2 Bennett C H, Bessette F, Brassard G, et al. Experiment quantum cryptography. J Crypto, 1992, 5(3): 3－28
3 Hughes R, Morgan G, Peterson C. Practical quantum key distribution over a 48-km optical fiber network. J Mod Opt, 2000, 47, 533－547
4 Stucki D, Gisin N, Guinnard O, Ribordy G., and Zbinden H., Quantum key distribution over 67 km with a plug & play system. New J Phys, 2002, 4: 41.1－41.8
5 Huges R, Nordholt J, Derkacs D, et al. Practical free-space quantum key distribution over 10 km in daylight and night. New J Phys, 2002, 4: 43.1－43.14
6 Gobby C, Yuan Z L, Shields A J, Quantum key distribution over 122 km of standard telecom fiber. Appl Phys Lett, 2004, 84: 3762－3764
7 Mo X F, Zhu Bing, Han Z F, et al. Faraday-Michelson system for quantum cryptography. Optics Letters, 2005, 30(19): 2632－2634
8 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. Rev Modern Phys, 2002, 74: 145－195
9 Han Z F, Mo X F, et al. Stability of phase-modulated quantum key distribution systems. App Phys Lett, 2005, 86: 221103.1－221103.3
10 Zbinden H, Gautier J D, Gisn N, et al. Interferometry with Faraday mirrors for quantum cryptography. Electron Lett, 1997, 33: 586－588
11 Muller A, Herzog T, Hutter B, et al. "Plug and play" systems for quantum cryptography. Appl Phys Lett, 1997, 70: 793－795
12 Vakhitov A, Mkarov V, et al. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. J Mod Opt, 2001, 48: 2023－2038
13 Ribordy G., Brendel J, Gautier J D, et al. Long-distance entanglement-based quantum key distribution. Phys Rev A, 2001, 63, 012309.1－012309.12
14 Nambu Y, Hatanaka T, Nakamura K. BB84 quantum key distribution system based on silica-based planar lightwave circuits. Jpn J Appl Physm, 2004, 43: L1109－L1110
15 Hongjo T, Inoue K, Takahashi H. Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer. Opt Letts, 2004, 29: 2797－2799
16 Nambu Y, Yoshino K, Tomita A. One-way quantum key distribution system based on planar lightwave circuits. Jpn J Appl Phys, 2006, 45: 5344－5348
17 Townsend P D, Rarity J G, Tapster P R. Single photon interferometer in 10 km long optical fibre interferometer. Elect Letts, 1993, 29: 634－635
18 Yuan Z L, Shields A J. Continuous operation of a one-way quantum key distribution system over installed telecom fibre. Opt Exp, 2005, 13(2): 660－665
19 Zavriyev A, Leverrier A, Denchev V, et al. Improving the performance of quantum key distribution apparatus. J Mod Opt, 2007, 54: 305－313
20 Makarov V, Brylevski A, Hjelme D R. Real-time phase tracking in single-photon interferometer. Appl Opt, 2004, 43(22): 4385－4392
21 Mo X F. Experimental research on quantum cryptography. Thesis for PhD Degree. University of Science and Technology of China, 2006