Quantum Key Distribution System Immune to Polarization-Induced Signal Fading with Quarter-Wave Plate Reflector-Michelson Interferometers

Huaxing Xu*, Shaohua Wang*, Yang Huang, and Changlei Wang

China Academy of Electronics and Information Technology, Beijing 100041, China

Corresponding author*: andy_huaxingxu@126.com

Improvement of QKD performance, particularly on system stability, has been required to meet practical application. In this letter, we design a quarter-wave plate reflector-Michelson interferometer based one-way intrinsic-stabilization QKD system. By introducing quarter-wave plate reflector-Michelson interferometers, with the long and short arms comprising of polarization maintaining optical fiber, quarter-wave plate and total reflector, the QKD system can be free of polarization disturbances caused by quantum channel and optical devices in the system. The experimental result shows that the QKD system has long-term low quantum bit error rate, and the safe key rate is about 7.34 kbps over 50.4 km standard optical fiber in the lab.

Quantum key distribution (QKD) enables two authentic remote participants, the transmitter Alice and the receiver Bob, to share a secret key that is unknown to a potential eavesdropper Eve. The security of QKD protocol relies on quantum mechanics and information theory, and theoretically has been proved absolutely safe [1]. Since the first QKD protocol proposed by Bennett and Brassard in 1984 [2], various schemes different in the protocol used [2]–[6], the encoding type [7]–[9], one-way or round-trip propagation [10]–[14], discrete or continuous variable quantum source [15]–[18], over fiber [7], [19], [20] or free space [21]–[23], and so forth, have been realized and reported. In actual QKD application, besides the security of protocols and the loopholes of devices, another urgent problem in QKD over commercial optical fiber is the system stability, which is strongly dependent on encoding scheme. Among these schemes, the most popular encoding ways are polarization encoding, phase encoding and time-bin phase encoding. However, polarization encoding QKD system relies on complicated feedback compensation
when decoding quantum signal because of environmental disturbance in practice. While phase encoding or time-bin phase encoding QKD system, which is more competitive for overhead optical cable and tube optical cable along road or bridge, will also suffer from polarization-induced fading and increase quantum bit error rate (QBER).

A typical fiber QKD scheme is based on unbalanced-arm Faraday-Michelson (F-M) interferometers, which can automatically eliminate the polarization-induced signal fading by introducing Faraday Mirror [8]. According to Ref. [24], the anti-disturbance condition that unidirectional QKD system is free of polarized disturbance caused by both interferometers and transmission fiber is $L^+S=I$ or $L=S$, where $L$ and $S$ respectively represent the operators of the whole long and short arms of the F-M interferometer and are unitary. In the F-M based QKD system, $L$ and $S$ are corresponding to one of Pauli Matrices $\sigma_3$, where we adopt the same notation with the Ref. [25]. Here, we propose a new solution based on quarter-wave plate reflector-Michelson (Q-M) interferometer, which is corresponding to another Pauli Matrix $\sigma_2$ and makes QKD system immune to polarization-induced signal fading.

Fig. 1 presents an unbalanced-arm Michelson interferometer with quarter-wave plate reflectors (QWPRs) as mirrors, which we call Q-M interferometer. The Q-M interferometer is composed of a polarization maintaining coupler (PMC) and two unbalanced arms. Both the upper and lower arms are comprised of polarization maintaining (PM) optical fiber, quarter-wave plate (QWP) and reflector. Besides, there is a phase shifter (PS) in the upper arm as shown in Fig. 1. The slow and fast axes of the quarter-wave plate are along $x$ and $y$ direction and the slow and fast axes of the PM fiber are along $X$ and $Y$ direction, respectively. The angle between the slow axes of PM optical fiber and QWP is 45 degrees.

Physically, QWPR can turn $X$-direction linear polarization light to $Y$-direction, and vice versa, when the angle between the polarization direction of the linear light and the slow axis of QWP equals 45 degrees. As shown in Fig. 2 (a), a forward $X$ ($Y$) polarization incidence light along the slow (fast) axis of PM optical fibers can be transformed into a backward $Y$ ($X$) polarization output light along the fast (slow) axis of PM optical fiber after the reflection by QWPR. Due to the same phase accumulation during the round-trip transmission, only polarization state exchange
happens between the input and output light, namely, the output polarization state is independent of the PM optical fiber and can be expressed as the product of the incident polarization state and Pauli Matrix $\sigma_2$ (ignoring the phase factor $i$).

For Faraday mirror, there will be an additional phase $\pi$ besides the polarization state exchange. As shown in Fig. 2 (b), when a forward light with $X$-direction and $Y$-direction components is incident on a Faraday mirror at any angle, the output light will be a backward light with $Y$-direction and $(-X)$-direction components. So the polarization direction of the incident light and the output light after the reflection by Faraday mirror are always orthogonal and F-M based QKD scheme will be free of polarization disturbances in the system, which is shown in Fig. 2(b). Unlike the Q-M interferometer, the operators of the long and short arms of F-M interferometer correspond to Pauli Matrix $\sigma_3$.

![Fig. 1. Unbalanced-arm Michelson interferometer with two quarter-wave plate reflectors (QWPRs) as mirrors, a polarization maintaining coupler (PMC), a phase shifter (PS) and PM optical fibers.](image1)

![Fig. 2. (a) The forward light (incident) and backward light (output) after the reflection by QWPR, where the angle between the direction of $X$ polarization state and the slow axis of QWP (x-direction) is](image2)
45 degrees. (b) The forward light (incident) and backward light (output) after the reflection by Faraday mirror. The solid and dashed lines respect forward and backward light after the reflection, respectively.

To describe the change of polarization more intuitive, we take the coordinate system as right handed and the light propagation direction as +z direction when the light propagates to the QWPR along PM optical fiber, and the coordinate system is left handed after the reflection by the reflector. For the convenience of theoretical analysis, we use the same notations with those in Ref. [25]. For Q-M interferometer, the operator of PM optical fiber in long arm is \( l = U(\delta/2,1,0,0) \), where \( \delta \) is the birefringence strength of the PM fiber, and the operator of QWPR is \( QR_{\lambda/4} = U(\pi/4,0,1,0)^t \). \( U(\pi/4,0,1,0) = U(\pi/2,0,1,0) \), where:

\[
U(\gamma, s_1, s_2, s_3) = \sigma_0 \cos \gamma + i(s_1\sigma_1 + s_2\sigma_2 + s_3\sigma_3) \sin \gamma,
\]

\[
s_1^2 + s_2^2 + s_3^2 = 1
\]

\[
\sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},
\]

\[
\sigma_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_3 = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}.
\]

Then the long arm operator \( L \) will be:

\[
L = \overline{I} \cdot QR_{\lambda/4} \cdot \overline{I} = U(\delta/2,1,0,0)^t \cdot U(\pi/2,0,1,0) \cdot U(\delta/2,1,0,0) = U(\delta/2,1,0,0) \cdot U(\pi/2,0,1,0) \cdot U(\delta/2,1,0,0) = i\sigma_2.
\]

Where the arrows ← and → indicate the backward and forward propagation and the index t designates the transposed matrix. For reciprocal optical element, the backward propagation notation equals the transposed matrix of the notation in forward coordinate system. The conclusion also applies to the short arm operator \( S \).

Considering double Q-M interferometers \( a \) and \( b \) connected with each other by optical fiber channel, there will be two paths for the pulse to interfere:

Path 1: \( L_a \rightarrow \text{channel} \rightarrow S_b \);
Path 2: \( S_a \rightarrow \text{channel} \rightarrow L_b \);

The transformation matrices of the two paths can be described respectively by:
where \( l_i \) and \( s_i \) \((i=a, b)\) represent the operators of the long and short PM optical fiber in the arms of Q-M interferometer, \( \alpha_i \) and \( \beta_i \) are the phase caused by the long and short arm of interferometers, respectively, \( \phi \) is the phase of transmission fiber, and \( \phi \) is the phase shift from the PS. Supposing input Jones vector is \( E_{in} \) at Alice’s side, the output of Bob’s interferometer can be written as:

\[
P_i : (s_b \cdot Q_R_{s/4} \cdot s_b) \cdot C : (I_b \cdot Q_R_{s/4} \cdot I_b) e^{i\phi} = e^{i\beta} \cdot Q_R_{s/4} \cdot C : e^{i\alpha} \cdot Q_R_{s/4} \cdot e^{i\phi},
\]

\[
P_2 : (I_b \cdot Q_R_{s/4} \cdot I_b) e^{i\phi} \cdot C : (s_a \cdot Q_R_{s/4} \cdot s_a) = e^{i\alpha} \cdot Q_R_{s/4} \cdot C : e^{i\beta} \cdot Q_R_{s/4} \cdot e^{i\phi},
\]

(3)

Considering that \( S_i, L_i, \) and \( C \) are unitary, interference output power can be expressed as:

\[
P_{out} = E_{out}^+ \cdot E_{out}
\]

\[
= E_{in}^+ \left[ \frac{1}{4} \left( e^{i(\alpha_a + \beta_b + \phi_a + \phi)} + e^{i(\alpha_b + \beta_a + \phi_a + \phi)} \right) Q_R_{s/4} \cdot C \cdot Q_R_{s/4} \right]^* \cdot \left[ \frac{1}{4} \left( e^{i(\alpha_a + \beta_b + \phi_a + \phi)} + e^{i(\alpha_b + \beta_a + \phi_a + \phi)} \right) Q_R_{s/4} \cdot C \cdot Q_R_{s/4} \right] E_{in}
\]

\[
= \frac{P_{in}}{8} [1 + \cos(\Delta \alpha + \Delta \beta + \Delta \phi)].
\]

(5)

where \( \Delta \alpha = \alpha_a - \alpha_b, \Delta \beta = \beta_a - \beta_b, \Delta \phi = \phi_a - \phi_b \). This means that the interference output \( P_{out} \) does not rely on any polarized perturbation in the whole QKD system. In an ideal case, \( \Delta \alpha \) and \( \Delta \beta \) are invariable, hence interference fringe is only modulated by PS. In the real case, the fluctuation of temperature or vibration will cause some drift in \( \Delta \alpha \) and \( \Delta \beta \), which can be solved by active compensation.

To prove the theory above, a time-bin phase encoding intrinsic-stabilization QKD experimental setup is built. The schematic and the real experimental setup are shown in Fig. 3. The system works in a way of decoy-state BB84 protocol including vacuum and weak decoy state.
Fig. 3. (a) Schematic diagram of Q-M based time-bin phase encoding intrinsic-stabilization QKD system. Q-Ms are shown in red dashed boxes. LD\textsubscript{1}-LD\textsubscript{4} are lasers, Cir\textsubscript{1} and Cir\textsubscript{2} are circulators, PMC\textsubscript{1} and PMC\textsubscript{2} are polarization maintaining couplers, BS\textsubscript{1}-BS\textsubscript{4} are beam splitters. (b) The real experimental setup in the lab, where the quantum channel is 50.4 km optical fiber.

The photons are generated by four strongly attenuated 1549.32 nm distributed-feedback pulsed laser diodes with a pulse width of 500 ps and 100 MHz repetition rate. The quantum fiber channel from Alice to Bob is 50.4 km (about 9.5 dB loss) in the lab. The ratio of signal, decoy and vacuum state numbers is 6:1:1, the intensity ratio of signal and decoy-state is 3:1, and the mean photon number is attenuated to 0.6. Four avalanche diode single detectors are used at Bob’s side with a gate width of 1ns.

We measured QBER and safe key rate to examine the performance of the system. As shown in Fig. 4, the averaged QBER and safe key rate are 0.83\(\pm\)0.23\% (a) and 7.34\(\pm\)0.72 kbps (b) during 2 hours over 50.4 km optical fiber, respectively. The experimental results indicate that the Q-M scheme can keep QKD system working stably.

A variable optical attenuator (ATT) is used at Alice’s side to simulate the loss of optical fiber. Assuming the optical fiber loss is 0.2 dB/km, the safe key rate can be
about 0.25 kbps over 100.0 km optical fiber (about 19.5 dB total channel loss) under lab condition.

In summary, we have proposed an unbalanced-arm Q-M interferometer based QKD scheme, which is free of polarization disturbances caused by quantum channel and optical devices in the system. Theoretical analysis has also been presented. An experimental verification is implemented by a Q-M based time-bin phase encoding QKD system. The experimental results show a long-term low QBER, and the safe key rates are about 7.34 kbps and 0.25 kbps over 50.4 km and equivalent 100.0 km optical fiber under lab condition.

This work was funded by the National Natural Science Foundation of China under grants 61705202 and the Innovation Funds of China Academy of Electronics and Information Technology.

Reference

[1] H.-K. Lo and H. F. Chau, “Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances,” *Science*, vol. 283, no. 5410, pp. 2050–2056, Mar. 1999.

[2] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Proc IEEE Int Conf Comput Syst Signal Process India*, pp. 175–179, 1984.

[3] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug. 1991.

[4] C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without Bell’s theorem,” *Phys. Rev. Lett.*, vol. 68, no. 5, pp. 557–559, Feb. 1992.

[5] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, “Quantum cryptography protocols
robust against photon number splitting attacks for weak laser pulses implementations,” Nov. 2002.

[6] H.-K. Lo, X. Ma, and K. Chen, “Decoy State Quantum Key Distribution,” Oct. 2004.

[7] C.-Z. Peng et al., “Experimental Long-Distance Decoy-State Quantum Key Distribution Based On Polarization Encoding,” Phys. Rev. Lett., vol. 98, no. 1, Jan. 2007.

[8] X.-F. Mo, B. Zhu, Z.-F. Han, Y.-Z. Gui, and G.-C. Guo, “Faraday-Michelson system for quantum cryptography,” Opt. Lett., vol. 30, no. 19, pp. 2632–2634, Oct. 2005.

[9] A. Tomita et al., “High speed quantum key distribution system,” Opt. Fiber Technol., vol. 16, pp. 55–62, Jan. 2010.

[10] B. Kraus, N. Gisin, and R. Renner, “Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication,” Phys. Rev. Lett., vol. 95, no. 8, p. 080501, Aug. 2005.

[11] Z. Yuan and A. Shields, “Continuous operation of a one-way quantum key distribution system over installed telecom fibre,” Opt. Express, vol. 13, no. 2, pp. 660–665, Jan. 2005.

[12] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, “‘Plug and play’ systems for quantum cryptography,” Nov. 1996.

[13] C. Zhou, G. Wu, X. Chen, and H. Zeng, “‘Plug and play’ quantum key distribution system with differential phase shift,” Appl. Phys. Lett., vol. 83, no. 9, pp. 1692–1694, Aug. 2003.

[14] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, “Quantum Key Distribution over 67 km with a plug & play system,” Mar. 2002.

[15] X. Tang et al., “1310 nm Differential Phase Shift QKD System Using Superconducting Single Photon Detectors | NIST,” New J. Phys., vol. 11, Apr. 2009.

[16] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, “Quantum cryptography with entangled photons,” Phys. Rev. Lett., vol. 84, no. 20, pp. 4729–4732, May 2000.

[17] F. Grosshans and P. Grangier, “Continuous variable quantum cryptography using coherent states,” Sep. 2001.

[18] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, “Quantum key distribution using gaussian-modulated coherent states,” Dec. 2003.

[19] C. Gobby, Z. L. Yuan, and A. J. Shields, “Quantum key distribution over 122 km of standard telecom fiber,” Dec. 2004.

[20] S. Wang et al., “2-GHz clock quantum key distribution over 260 km of standard telecom fiber,” Opt. Lett., vol. 37, no. 6, p. 1008, Mar. 2012.

[21] W. T. Buttler et al., “Free-space quantum-key distribution,” Phys. Rev. A, vol. 57, pp. 2379–2382, Apr. 1998.

[22] C.-Z. Peng et al., “Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication,” Phys.
[23] T. Schmitt-Manderbach et al., “Experimental demonstration of free-space decoy-state quantum key distribution over 144 km,” Phys. Rev. Lett., vol. 98, no. 1, p. 010504, Jan. 2007.

[24] Z.-F. Han, X.-F. Mo, Y.-Z. Gui, and G.-C. Guo, “Stability of phase-modulated quantum key distribution systems,” Appl. Phys. Lett., vol. 86, p. 221103, May 2005.

[25] M. Yoshida-Dierolf, “Operator algebra for birefringence and mirror reflection,” Opt. Commun., vol. 203, pp. 79–85, Mar. 2002.