CHIN. PHYS. LETT. Vol. 33, No. 12 (2016) 120301

Time-Bin Phase-Encoding Measurement-Device-Independent Quantum Key Distribution with Four Single-Photon Detectors *

Guang-Zhao Tang(唐光召)[1], Shi-Hai Sun(孙仕海)[1**], Huan Chen(陈欢)[1],
Chun-Yan Li(李春燕)[1], Lin-Mei Liang(梁林梅)[2**]

[1]*College of Science, National University of Defense Technology, Changsha 410073*
[2]*State Key Laboratory of High Performance Computing, National University of Defense Technology, Changsha 410073*

(Received 12 August 2016)

Measurement-device-independent quantum key distribution (MDI-QKD) eliminates all loopholes on detection. Previous experiments of time-bin phase-encoding MDI-QKD allow a factor of $\frac{3}{4}$ loss in the final key for the incapability of identifying two successive detection events by a single photon detector. Here we propose a new scheme to realize the time-bin phase-encoding MDI-QKD. The polarization states are used to generate the time bins and the phase-encoding states. The factor of loss in the final key is eliminated by using four single photon detectors at the measurement site. We show the feasibility of our scheme with a proof-of-principle experimental demonstration. The phase reference frame is rotated extremely slowly with only passive stabilization measures. The quantum bit error rate can reach 0.8% in the Z-basis and 26.2% in the X-basis.

PACS: 03.67.Dd, 03.67.Hk, 89.70.Cf DOI: 10.1088/0256-307X/33/12/120301

Based on the principle of quantum mechanics, quantum key distribution (QKD)[1,2] satisfies the requirement of secure communication for legitimate parties. The feasibility of QKD has been demonstrated by tremendous experiments.[3–7] However, the practical system suffers from all kinds of loopholes originating from the gap between theory and practice.[8–11] In general, three approaches have been developed to bridge the gap. The first one is the security patch.[12,13] However, it does not work on the potential and unnoticed loopholes. The second one is the device-independent QKD (DI-QKD).[14,15] However, it is impractical to carry out the DI-QKD with the current technology, since it requires almost perfect single photon detectors (SPDs). The third approach is the measurement-device-independent quantum key distribution (MDI-QKD),[16] which removes all measurement-related security loopholes. Such loopholes are considered to be the main source of attacks.

MDI-QKD has attracted extensive efforts of experimental demonstration. Achievements have been made in both the laboratory and the field.[17–21] Most of them apply the time-bin phase-encoding scheme,[22] and utilize two SPDs to conduct the BSM.[17,18,20,21] Due to the incapability of identifying two successive detection events within an interval of no more than 30 ns by one single photon detector (SPD), a factor of $\frac{3}{4}$ loss in the final key is allowed in these experiments (the arm difference of AMZI in Ref. [18] is 6 m, in Ref. [21] is 4.9 m; in Ref. [20], the time bins are separated by a 6.5 ns time delay). In addition, most of these demonstrations apply the feed-back temporal control units[18–21] to precisely calibrate the arrival time of signals, which makes the operation of MDI-QKD complex.

Here we propose a new scheme to realize the time-bin phase-encoding MDI-QKD. At the encoding site, the polarization states are used to generate the time bin (0 or 1) of the Z-basis and the relative phase (0 or π) of the X-basis. At the measurement site, two polarizing beam splitters (PBSs) and two polarization-maintaining beam splitters (BSs), together with four commercial SPDs are employed to realize an efficient BSM. A proof-of-principle experiment is made to show the feasibility of our scheme. The temperature control units are applied to a pair of homemade signal laser sources to match the spectral mode. A passive temporal calibration method is used to guarantee the precise overlap of optical pulses from Alice and Bob. By taking passive phase stabilization measures, the phase reference is rotated at an extremely low speed. Finally, we obtain a quantum bit error rate (QBER) of 0.8% for the Z-basis, and 26.2% for the X-basis over the 36 km standard optical fiber.

In MDI-QKD, Alice and Bob prepare their encoding states and send them to Charlie independently. Charlie measures the signals received with the Bell state measurement (BSM). After Charlie reveals the Bell states obtained, Alice and Bob broadcast the intensity and basis settings to sift the raw key and estimate the parameters. With the parameters estimated, Alice and Bob can generate the final secure key through error correction and privacy amplification. In the traditional time-bin phase encoding MDI-QKD

*Supported by the National Natural Science Foundation of China under Grant Nos 11304391, 11674397 and 61671455, and the Program for New Century Excellent Talents in University of China.
**Corresponding author. Email: shsun@nudt.edu.cn; nmliang@nudt.edu.cn
© 2016 Chinese Physical Society and IOP Publishing Ltd

scheme, the time bins are generated by an asymmetric Mach–Zehnder interferometer (AMZI) with a time delay of no more than 30 ns. The detection windows of two SPDs are fixed at alternative time bins. Thus only 25% of the BSM results are detected.

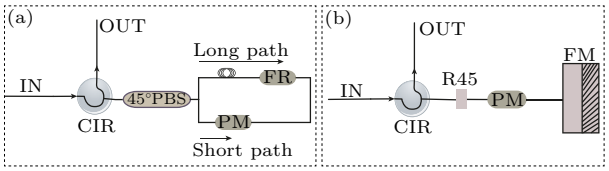

Fig. 1. (a) Schematic diagram of polarization modulator. CIR, circulator; FR, 90°Faraday rotator; PM, phase modulator; 45° PBS, polarizing beam splitter with 45° rotation from the optical axis. (b) The two-way polarization modulator mentioned in Ref. [23]. FM, Faraday mirror; R_{45}, the slow axis of polarization maintaining fiber (PMF) is rotated 45° with respect to the optical axis of the modulator waveguide.

To realize an efficient time-bin phase-encoding MDI-QKD, we utilize a polarization modulator (Pol-M),[23] together with an AMZI, which is composed of two polarizing beam splitters (PBSs) to generate the encoding states. The schematic diagram of the Pol-M is shown in Fig. 1(a). It consists of an optical circulator (CIR), a PBS with 45° rotation from the optical axis (45°PBS), a phase modulator (PM), and a Faraday rotator. The function of this setting is equal to that of the two-way polarization modulator in Fig. 1(b). By modulating the relative phase between the long path and the short path, we can obtain different polarization states at the output port of CIR. Here we only modulate the optical signals of the long-path. The function of the polarization modulator is expressed with the Jones matrix[23]

$$J_{\text{out}} = e^{-i\psi}e^{-i\phi/2} \cdot \begin{pmatrix} \cos(\phi/2) & -ie^{i\varphi}\sin(\phi/2) \\ -ie^{-i\varphi}\sin(\phi/2) & \cos(\phi/2) \end{pmatrix} J_{\text{in}}^{\perp}, \quad (1)$$

where $J_{\text{out(in)}}$ is the polarization state of output (input) signals, $J^{\perp}$ represents the orthogonal state of J, ψ is the overall phase introduced by the modulator, φ is the phase caused by the polarization maintaining fiber (PMF) located ahead of the 45°PBS, and ϕ is the phase modulated by us. Thus for an input signal of horizontal polarization, we find

$$J_{\text{out}} = e^{-i\psi}e^{-i\phi/2} \begin{pmatrix} ie^{i\varphi}\sin(\phi/2) \\ -\cos(\phi/2) \end{pmatrix}. \quad (2)$$

Here we can see that the modulation of ϕ to 0 (π, $\pi/2$, $3\pi/2$) results in an output polarization state of $V(H, H + e^{i(\pi/2-\varphi)}V, H - e^{i(\pi/2-\varphi)}V)$.

We can use two PBSs to compose an AMZI. Therefore, the polarization states of V and H are transformed to the time bins of 0 and 1 in the Z-basis. The polarization states of $H+e^{i(\pi/2-\varphi)}V$ and $H-e^{i(\pi/2-\varphi)}V$ correspond to the relative phases of 0 and π in the X-basis.

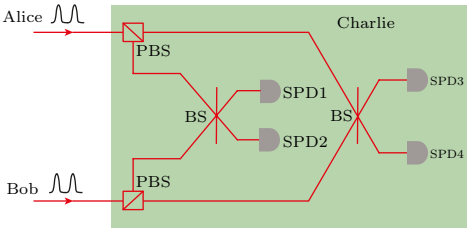

Fig. 2. Experimental setup of the measurement. Two PBSs, two BSs, and together with four SPDs are utilized to realize the partial BSM.

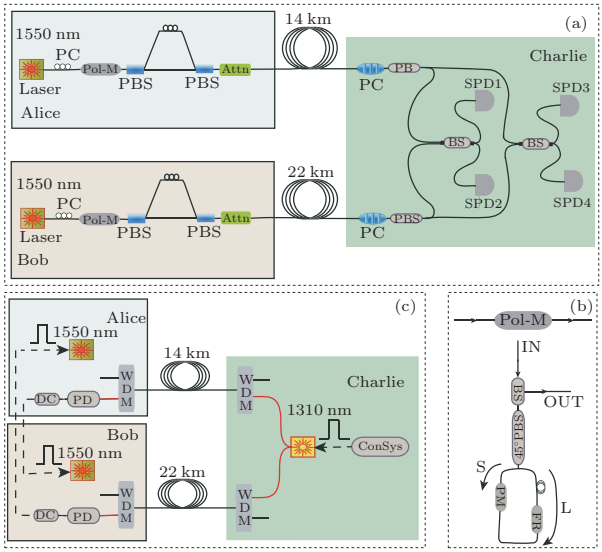

Fig. 3. (a) Experimental setup of MDI-QKD with four SPDs. The signal laser pulses of Alice (Bob) are modulated by the Pol-M. An AMZI which is composed of two PBSs is followed to convert the polarization states to the encoding states of MDI-QKD. Charlie's setup consists of a polarization controller (PC) and a BSM system. The BSM system is composed of two PBSs, two interference BS, and four SPDs. SPD1 and SPD2: id201 of id Quantique. SPD3 and SPD4: Gated SPD of Quantum Communication Technology Co. Ltd. Anhui. (b) Polarization modulator. In the experiment, we use a BS to replace the CIR to improve the polarization extinction ratio. (c) Schematic diagram of the time calibration system. A SynLs (1310 nm) is adopted here. The control system (ConSys) supplies the 1 MHz clock. The SynL pulses pass through the fiber link to Alice (Bob). Alice (Bob) utilizes a photoelectric detector (PD) to detect them and outputs the system clock of Bob (Alice). WDM: wavelength division multiplexer, Attn: attenuator, and DC: delay chip.

At the measurement site, we can use the setting shown in Fig. 2 to realize the efficient BSM. Since the time bins are attached with the orthogonal polarization states (H and V), we can use the PBS to separate them easily. Two BSs are used to realize the interference. An SPD is placed at each output port of the BSs. Therefore, all results of BSM are effectively detected.

We make a proof-of-principle experiment shown in Fig. 3(a) to show the feasibility of our MDI-QKD

scheme. The signal laser sources (1550 nm) of Alice and Bob are internally modulated into a pulse train with a width of 2 ns and a repetition rate of 1 MHz. Then, the signal pulses are modulated into one of the four encoding states by Pol-M and AMZI. The AMZI used here is composed of two PBSs and with a time delay of 5 ns. At the detection site, Charlie takes advantage of two PBSs, two BSs, and four SPDs to conduct the BSM. We use the asymmetric setting in the experiment. The quantum channels from Alice and Bob to Charlie are 14 km and 22 km standard optical fibers.

The qubits of Alice are sent to Charlie to interfere with the ones sent by Bob. The perfect interference indicates a successful BSM, and results in a coincidence at alternative time bins, namely a click in SPD1 and SPD3, or in SPD2 and SPD4, corresponding to a projection into the Bell state $|\psi^+\rangle$, a click in SPD1 and SPD4, or in SPD2 and SPD3, corresponding to a projection into the Bell state $|\psi^-\rangle$. The crucial aspect in the experiment is the indistinguishability of signal pulses from Alice and Bob, mainly in three dimensions: spectrum, polarization, and arrival time. For the spectral mode, the temperature control units are applied to a pair of signal lasers. By adjusting the temperature precisely, we obtain a high-quality interference between two independent signal laser sources. The Hong–Ou–Mandel (HOM) interference is measured at an average photon number of 0.1 per pulse, and the measured HOM dip is 0.55.

The polarization states are calibrated by adjusting the polarization controllers at each fiber link. For the temporal mode shown in Fig. 3(c), a synchronization laser (SynL,1310 nm) is utilized to send the SynL pulses from Charlie to Alice and Bob. A photoelectric detector is used by Alice (Bob) to detect the SynL pulses and output a 1 MHz system clock. Then, Alice (Bob) sends the system clock to Bob (Alice) to drive the signal laser source of Bob (Alice). Therefore, the arrival time difference is a constant which can be compensated for by adjusting the relative time delay between two delay chips. In our experiment, the temporal mode mismatch is about 10 ps, which is much smaller than the width of the signal pulse.

In our proof-of-principle demonstration, the phase-reference-frame is not calibrated. We only take the passive measures to stabilize the phase reference frame. Thus the coincidence between two SPDs ($|\psi^+\rangle$ or $|\psi^-\rangle$) is changed periodically [an inevitable problem for the asymmetric Mach–Zehnder interferometers is the phase drift; the phase drift is affected by the environment; the passive measures (strict thermal and mechanical isolation) can slow down the phase drift; in MDI-QKD, the key bit in the X-basis is encoded into the relative phase (0 or π) of two time-bin pulses; the encoded pulses of the X-basis from Alice and Bob interference at the BSs of Charlie; we denote the relative phase of Alice (Bob) with θ_a (θ_b); here $\theta_a - \theta_b = \pi$ indicates a projection into $|\psi^-\rangle$; however, in real cases, $\theta_a - \theta_b = \pi + \Delta\theta(t)$, and $\Delta\theta(t) \in [0\pi]$ is caused by the phase drift]. We firstly demonstrate the feasibility of our scheme without the transmission fiber. The Bell state ($|\psi^-\rangle$) is post-selected with two SPDs (id201). The results are shown in Fig. 4. The high coincidence indicates the phase difference is π in the interference. While the low coincidence indicates that the phase difference is 0. We can see that the phase reference frame is rotated extremely slowly. It shows great potential for us to realize a high-quality active phase-tracking.

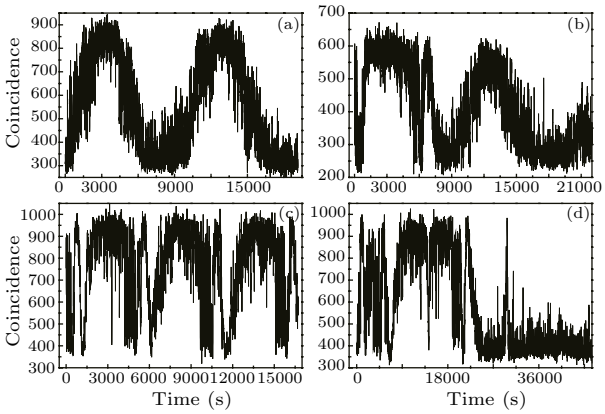

Fig. 4. Coincidences between two SPDs corresponding to $|\psi^-\rangle$. The coincidence is measured without the transmission fiber. Two SPDs (id201), with an efficiency of 10% and a gate width of 2.5 ns, are utilized in the measurement. The dead time is 10 μs with a dark count rate of 6×10^{-6} per gate. (a) The coincidence is collected every 2 s with an optical intensity of $\mu = 0.5$. (b) The coincidence is collected every 3 s with an optical intensity of $\mu = 0.4$. (c) The coincidence is collected every 5 s with an optical intensity of $\mu = 0.4$. (d) The coincidence is collected every 15 s with an optical intensity of $\mu = 0.2$.

Lastly, the quantum bit error rates (QBERs) of the Z-basis and the X-basis are measured over the asymmetric channel setting with an optical intensity of $\mu = 0.5$. We obtain a QBER of 0.8% for the Z-basis. The QBER of the X-basis can reach 26.2%. The QBERs of the Z-basis are due to the polarization extinction ratio of Pol-M and the detectors' dark counts. In the ideal case, the QBERs of the Z-basis should be 0. While in the X-basis, the vacuum and multiphoton components of weak coherent states cause accidental coincidences, which introduce a typical error rate of 25%.[19] Thus the QBERs of our experiment are small enough to verify the feasibility of our MDI-QKD scheme.

We remark that the passive timing calibration method can be directly implemented in quantum networks, since the fiber link always exists between Alice and Bob. We can use the setup as shown in Fig. 5 to calibrate the arrival time of signals.

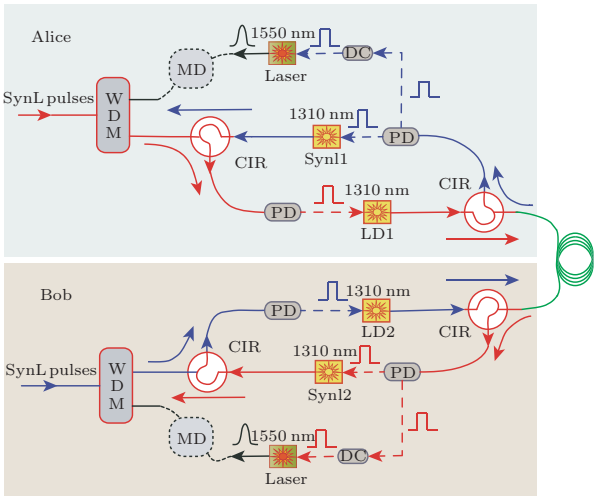

Fig. 5. Schematic diagram of the passive time calibration system in quantum networks. Alice (Bob) detects the SynL pulses with a PD and regenerates the synchronization optical pulses with LD1 (LD2). The optical pulses of LD1 (LD2) pass through the fiber link between Alice and Bob, and are detected by another PD to recover the system clock of Bob (Alice). The system clocks are utilized to drive the signal laser (1550 nm) and another synchronization laser (Synl2 and Synl1). The Synls are used to provide the detection clock for SPDs of Charlie. MD: modulation device.

MDI-QKD is immune to all measurement-related loopholes. As to source-related loopholes, we should take other measures to defend them. For example, the decoy-state method is always used to defend the photon-number-splitting (PNS) attack. Compared with the traditional time-bin phase-encoding scheme, our scheme can efficiently record the results of BSM, while it does not introduce any additional security loopholes. Also, the operation complexity is not increased. A complete MDI-QKD system can be realized by applying the reference-frame-independent QKD protocol.[21]

In conclusion, we have proposed a new scheme to realize the time-bin phase-encoding MDI-QKD with four SPDs. A proof-of-principle experiment is made to show the feasibility of our scheme. The polarization modulator, together with an AMZI, which is composed of two PBSs, are used to generate the encoding states of MDI-QKD, namely, the polarization states of V and H correspond to the time bins of 0 and 1 in the Z-basis, and the polarization states of $H+e^{i(\pi/2-\varphi)}V$, $H-e^{i(\pi/2-\varphi)}V$ correspond to the relative phase of 0 and π in the X-basis. At the detection site, Charlie makes use of two PBSs, two BSs, and four SPDs to conduct the BSM. We use a passive temporal calibration method to guarantee the overlap of signal pulses. The phase reference shows an outstanding character of stabilization only with the passive stabilization measures. Lastly, we obtain a QBER of 0.8% for the Z-basis. The QBER of the X-basis can reach 26.2%.

References

[1] Bennett C H and Brassard G 1984 *Int. Conf. Comput. Syst. Signal Process* (Bangalore India) (New York: IEEE) p 175
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Huang Y X, Hu H P, Liang R S, Lu Y Q, Wang J D and Lu W 2008 *Chin. Phys. Lett.* **25** 2485
[4] Yin Z Q, Han Z F, Chen W, Xu F X, Wu Q L and Guo G C 2008 *Chin. Phys. Lett.* **25** 3547
[5] Yuan Z L, Dixon A R, Dynes J F, Sharpe A W and Shields A J 2008 *Appl. Phys. Lett.* **92** 201104
[6] Han J J, Sun S H and Liang L M 2011 *Chin. Phys. Lett.* **28** 040303
[7] Wang S, Chen W, Guo J F, Yin Z Q, Li H W, Zhou Z, Guo G C and Han Z F 2012 *Opt. Lett.* **37** 1008
[8] Zhao Y, Fung C H F, Qi B, Chen C and Lo H K 2008 *Phys. Rev.* A **78** 042333
[9] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 686
[10] Sun S H, Jiang M S and Liang L M 2011 *Phys. Rev.* A **83** 062331
[11] Jain N, Wittmann C, Lydersen L, Wiechers C et al 2011 *Phys. Rev. Lett.* **107** 110501
[12] Yuan Z L, Dynes J F and Shields A J 2010 *Nat. Photon.* **4** 800
[13] Sun S H, Xu F H, Jiang M S, Ma X C, Lo H K and Liang L M 2015 *Phys. Rev.* A **92** 022304
[14] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[15] Gisin N, Pironio S and Sangouard N 2010 *Phys. Rev. Lett.* **105** 070501
[16] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[17] Rubenok A, Slater J A, Chan P, Lucio-Martinez I and Tittel W 2013 *Phys. Rev. Lett.* **111** 130501
[18] Liu Y, Chen T Y, Wang L J et al 2013 *Phys. Rev. Lett.* **111** 130502
[19] Tang Z Y, Liao Z F, Xu F H, Qi B, Qian L and Lo H K 2014 *Phys. Rev. Lett.* **112** 190503
[20] Tang Y L, Hua H L, Chen S J et al 2014 *Phys. Rev. Lett.* **113** 190501
[21] Wang C, Song X T, Yin Z Q, Wang S, Chen W, Zhang C M, Guo G C and Han Z F 2015 *Phys. Rev. Lett.* **115** 160502
[22] Ma X, Razavi M 2012 *Phys. Rev.* A **86** 062319
[23] Lucio-Martinez I, Chan P, Mo X, Hosier S and Tittel W 2009 *New J. Phys.* **11** 095001