

Polarization Calibration Scheme for a Practical Handheld Free Space Quantum Key Distribution Link

Lai Zhou¹, David Lowndes², Vincent Lee¹, Indranil Mitra³, SaiGopal T³, John Rarity²,
Grahame Faulkner¹, Dominic O'Brien¹

¹Department of Engineering Science, University of Oxford, Oxford, UK

²Department of Electrical & Electronic Engineering, University of Bristol, Bristol, UK

³Cognizant Worldwide Limited, London, UK

Abstract—Free space Quantum Key Distribution (QKD) links between terminals that move relative to each other pose a number of challenges. The beam-steering components (typically mirrors) and the relative movement lead to variable birefringence, and for particular configuration there will also be fixed birefringence. The paper proposes a polarization calibration scheme suitable for real-time operation. Simulation and experiment are performed to verify the proposed scheme.

Index Terms—QKD, QBER, birefringence, polarization calibration, real-time.

I. INTRODUCTION

Wireless financial transactions using mobile devices and credit cards are rapidly growing in popularity. Conventional encryption methods such as RSA may ultimately be attacked by a quantum computer, so there is increasing interest in methods that are resistant to such approaches. Quantum Key Distribution (QKD) provides an unconditionally secure method of data transmission [1]–[3]. In order to encrypt financial transactions and protect the communication links, quantum random keys can be generated and distributed among two parties with QKD protocols, e.g., BB84 [4] and Reference-frame-independent (RFI) [5].

There have been a number of demonstrations of free space links, including between handheld platforms [6] and orbiting satellites [7]. Typically, the quantum information is encoded in the polarization of the transmitted photons. However, the birefringence due to optical fibre and optical components, and the dynamic relative motion of transmitter (TX) and receiver (RX), will lead to misalignment in the polarization reference frame of the system. This significantly affects the performance of the system and increases the corresponding Quantum Bit Error Rate (QBER).

Polarization calibration is required in most QKD systems [7]–[11]. Considering an optical fiber channel, [8] used piezoelectric actuators to compensate the change of polarization, and [9] proposed a polarization-basis tracking scheme using sifted key bits revealed in the error correction step. Real-time continuous control was demonstrated based on a wavelength-division multiplexing method in [10]. In free-space satellite-to-ground quantum communications, polarization basis tracking

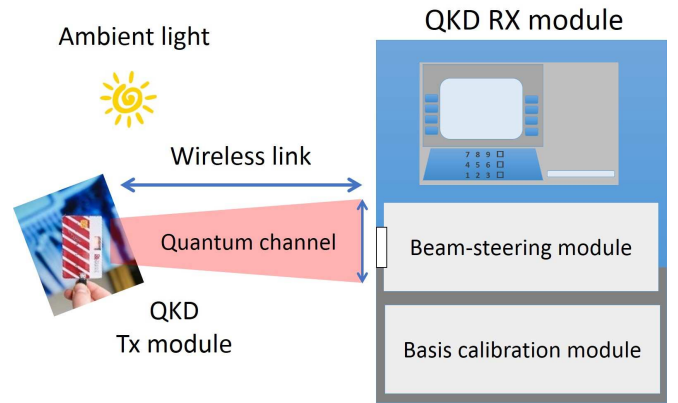


Fig. 1. Block diagram of the handheld QKD system.

schemes used a rotating half-wave plate to calibrate the relative movement [7], [11]. In addition, a RFI protocol was implemented in [6] for a handheld QKD system, where the qubits are encoded in a circular basis and are tolerant to relative rotation [12]. This required a relatively bulky TX capable of transmitting six polarization states, making this difficult to miniaturize. The system considered in this work aims to create a credit-card sized transmitter module [13], [14], so it is likely that there will be birefringence which will vary with position and orientation of the transmitter, and that it must be corrected at the receiver only.

In this paper we propose an efficient calibration scheme, and a method of real-time operation. The remainder of the paper is organized as follows: In Section II we introduce the system design, and Section III details the polarization calibration scheme. Section IV describes the real-time scheme. Verification and system implementation are presented in Section V. Finally, Section VI concludes the paper.

II. SYSTEM DESIGN

Fig. 1 shows a block diagram of the free-space, handheld and steerable QKD system prototype. The TX module is low cost and credit-card sized. The RX module mainly consists

of a beam-steering module that maintains the optical communication link and a basis calibration module to calibrate the polarization state. A wireless channel is used to share extra information for data processing, e.g., time synchronization [4].

Quantum information is encoded with four polarization states from four polarized micro light-emitting diodes (LEDs) in the TX module, i.e., horizontal and vertical (H, V) basis and diagonal and anti-diagonal (D, A) basis. This BB84 (H, V, D, A) reference frame forms a plane in the Poincare sphere. However, light from these sources is coupled into a single mode fibre in the TX, which will distort the polarization states. The relationship between the initial and final polarization states is expressed as,

$$\mathbf{S} = \mathbf{R} \cdot \mathbf{S}_0, \quad (1)$$

where \mathbf{R} represents the rotation operator caused by birefringence and hand movement. $\mathbf{S}_0(\mathbf{H}_0, \mathbf{V}_0, \mathbf{D}_0, \mathbf{A}_0)$ is the Stokes vector of aligned polarization basis and \mathbf{S} is the distorted vector.

A general method to eliminate birefringence is to use two quarter wave plates (QWPs) and a half wave plate (HWP) to rotate any polarization state from one to another. Fig. 2 depicts a receiver box with three detection bases and a calibration module consisting of three motorized wave plates (2 QWP followed by a HWP). In addition to decoding the four linear polarization states with HV and DA bases, we use an extra basis, i.e., the right and left circular (R, L) polarization basis, to fully characterize the birefringence and reference frame rotation resulted from hand movement. Accordingly, the normalized Stokes vectors of the polarization state after misalignment can be obtained as [15],

$$\mathbf{S} = \begin{bmatrix} 1 \\ Q_S \\ U_S \\ V_S \end{bmatrix} = \begin{bmatrix} 1 \\ (S_H - S_V)/(S_H + S_V) \\ (S_D - S_A)/(S_D + S_A) \\ (S_R - S_L)/(S_R + S_L) \end{bmatrix}, \quad (2)$$

where $S_H, S_V, S_D, S_A, S_R, S_L$ are the detected counts in the H, V, D, A, R, L channels, respectively. In the calibration period, the TX sends a large number of photons with specific polarization states to obtain the corresponding Stokes vector. Then the polarization states can be recovered using three motorized wave plates configured as described in the following scenario.

III. POLARIZATION CALIBRATION SCHEME

The polarization calibration scheme is implemented with the rotation of the corresponding wave plates in three steps, so that the final polarization state is $\mathbf{R}^{-1} \cdot \mathbf{S} = \mathbf{R}^{-1} \cdot \mathbf{R} \mathbf{S}_0 = \mathbf{S}_0$. The transformation operator is expressed as,

$$\mathbf{R}^{-1}(\theta_1, \theta_2, \theta_3) = \mathbf{M}_{\lambda/2}(\theta_3) \cdot \mathbf{M}_{\lambda/4}(\theta_2) \cdot \mathbf{M}_{\lambda/4}(\theta_1), \quad (3)$$

where $\mathbf{M}_{\lambda/4}$ and $\mathbf{M}_{\lambda/2}$ denote the Mueller matrix of QWP and HWP, respectively. θ_i is the rotation angle of i^{th} wave plate. Usually, we use two non-orthogonal polarization states, e.g., H and D.

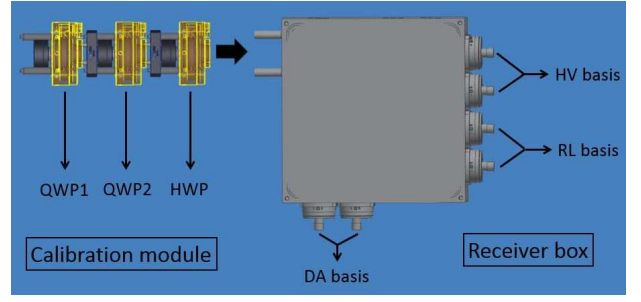


Fig. 2. The calibration module in the QKD system.

A. Setting QWP1

As depicted in Fig. 3(a) and Fig. 3(b), the first step is to use QWP1 to make the initial polarization plane cut the poles of the Poincare sphere. Based on the detection counts from six channels, the Stokes vectors of horizontal and diagonal polarizations in the RX are expressed as,

$$\mathbf{H} = [1, Q_H, U_H, V_H]^T, \quad (4)$$

$$\mathbf{D} = [1, Q_D, U_D, V_D]^T. \quad (5)$$

The Mueller matrix of a QWP with angle θ_1 is expressed as,

$$\mathbf{M}_{\lambda/4}(\theta_1) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos^2(2\theta_1) & \frac{\sin(4\theta_1)}{2} & -\sin(2\theta_1) \\ 0 & \frac{\sin(4\theta_1)}{2} & \sin^2(2\theta_1) & \cos(2\theta_1) \\ 0 & \sin(2\theta_1) & -\cos(2\theta_1) & 0 \end{bmatrix}. \quad (6)$$

After the adjustment of first QWP, the Stokes vectors of the two polarizations are expressed as,

$$\begin{aligned} \mathbf{H}_1 &= \mathbf{M}_{\lambda/4}(\theta_1) \cdot \mathbf{H} \\ &= [1, Q_{H_1}, U_{H_1}, V_{H_1}]^T \\ &= \begin{bmatrix} 1 \\ Q_H \cos^2(2\theta_1) + U_H \sin(4\theta_1)/2 - V_H \sin(2\theta_1) \\ Q_H \sin(4\theta_1)/2 + U_H \sin^2(2\theta_1) + V_H \cos(2\theta_1) \\ Q_H \sin(2\theta_1) - U_H \cos(2\theta_1) \end{bmatrix}, \end{aligned} \quad (7)$$

$$\begin{aligned} \mathbf{D}_1 &= \mathbf{M}_{\lambda/4}(\theta_1) \cdot \mathbf{D} \\ &= [1, Q_{D_1}, U_{D_1}, V_{D_1}]^T \\ &= \begin{bmatrix} 1 \\ Q_D \cos^2(2\theta_1) + U_D \sin(4\theta_1)/2 - V_D \sin(2\theta_1) \\ Q_D \sin(4\theta_1)/2 + U_D \sin^2(2\theta_1) + V_D \cos(2\theta_1) \\ Q_D \sin(2\theta_1) - U_D \cos(2\theta_1) \end{bmatrix}. \end{aligned} \quad (8)$$

$\hat{\mathbf{H}}_1$ and $\hat{\mathbf{D}}_1$ are defined as $\hat{\mathbf{H}}_1 = [Q_{H_1}, U_{H_1}, V_{H_1}]^T$, $\hat{\mathbf{D}}_1 = [Q_{D_1}, U_{D_1}, V_{D_1}]^T$. The cross product of the two vectors is $\hat{\mathbf{H}}_1 \times \hat{\mathbf{D}}_1 = [U_{H_1}V_{D_1} - V_{H_1}U_{D_1}, V_{H_1}Q_{D_1} - Q_{H_1}V_{D_1}, Q_{H_1}U_{D_1} - U_{H_1}Q_{D_1}]^T$. In order to make the HVDA plane perpendicular to the equator of Poincare sphere, the last element should be zero, and

$$Q_{H_1}U_{D_1} = U_{H_1}Q_{D_1}. \quad (9)$$

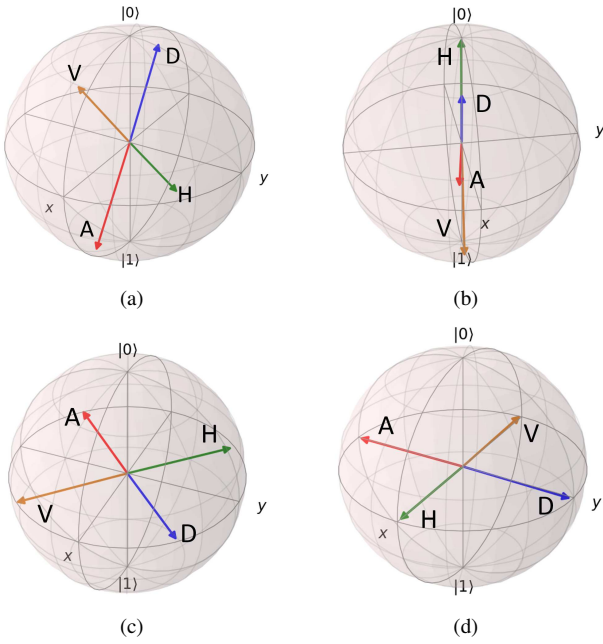


Fig. 3. A simulation example with polarization calibration steps (a. initial state; b. state after first step; c. state after second step; d. state after third step.)

Substituting (7)(8) into (9) gives the desired result for θ_1 ,

$$\theta_1 = \frac{1}{2} \arctan(-a/b), \quad (10)$$

where $a = Q_H V_D - V_H Q_D$ and $b = U_H V_D - V_H U_D$. If a and b both approach 0, θ_1 can be an arbitrary angle.

B. Setting QWP2

As depicted in Fig. 3(c), the second step is to use QWP2 to make the HVDA plane rotate back to the equator of the Poincaré sphere. After the adjustment of second QWP with angle θ_2 , the Stokes vectors of horizontal and diagonal polarization are expressed as,

$$\begin{aligned} \mathbf{H}_2 &= \mathbf{M}_{\lambda/4}(\theta_2) \cdot \mathbf{H}_1 \\ &= [1, Q_{H_2}, U_{H_2}, V_{H_2}]^T \\ &= \begin{bmatrix} 1 \\ Q_{H_1} \cos^2(2\theta_2) + U_{H_1} \sin(4\theta_2)/2 - V_{H_1} \sin(2\theta_2) \\ Q_{H_1} \sin(4\theta_2)/2 + U_{H_1} \sin^2(2\theta_2) + V_{H_1} \cos(2\theta_2) \\ Q_{H_1} \sin(2\theta_2) - U_{H_1} \cos(2\theta_2) \end{bmatrix}, \end{aligned} \quad (11)$$

$$\begin{aligned} \mathbf{D}_2 &= \mathbf{M}_{\lambda/4}(\theta_2) \cdot \mathbf{D}_1 \\ &= [1, Q_{D_2}, U_{D_2}, V_{D_2}]^T \\ &= \begin{bmatrix} 1 \\ Q_{D_1} \cos^2(2\theta_2) + U_{D_1} \sin(4\theta_2)/2 - V_{D_1} \sin(2\theta_2) \\ Q_{D_1} \sin(4\theta_2)/2 + U_{D_1} \sin^2(2\theta_2) + V_{D_1} \cos(2\theta_2) \\ Q_{D_1} \sin(2\theta_2) - U_{D_1} \cos(2\theta_2) \end{bmatrix}. \end{aligned} \quad (12)$$

The angle θ_2 can be obtained by setting V_{H_2} and V_{D_2} equal to zero, and

$$Q_{H_1} \sin(2\theta_2) = U_{H_1} \cos(2\theta_2), \quad (13)$$

$$Q_{D_1} \sin(2\theta_2) = U_{D_1} \cos(2\theta_2). \quad (14)$$

Considering the special case of Q_{H_1} and U_{H_1} both approaching zero, the expression of θ_2 is given as,

$$\theta_2 = \begin{cases} \frac{1}{2} \arctan\left(\frac{U_{D_1}}{Q_{D_1}}\right), & |U_{H_1}| < \varepsilon \text{ and } |U_{Q_1}| < \varepsilon \\ \frac{1}{2} \arctan\left(\frac{U_{H_1}}{Q_{H_1}}\right), & \text{other conditions,} \end{cases} \quad (15)$$

where ε is the threshold taken to be zero, i.e., $1e^{-5}$. The required solution $\theta_2 = \theta_2 + 90$ satisfies the condition when $Q_{H_2} U_{D_2} - U_{H_2} Q_{D_2} > 0$.

C. Setting HWP

As depicted in Fig. 3(d), the third step is to use the last HWP to align each polarization basis (H, V, D, A). The Mueller matrix of HWP with angle θ_3 is expressed as,

$$\mathbf{M}_{\lambda/2}(\theta_3) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(4\theta_3) & \sin(4\theta_3) & 0 \\ 0 & \sin(4\theta_3) & -\cos(4\theta_3) & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}. \quad (16)$$

After the adjustment of HWP, the Stokes vector of horizontal polarization is expressed as,

$$\begin{aligned} \mathbf{H}_3 &= \mathbf{M}_{\lambda/2}(\theta_3) \cdot \mathbf{H}_2 \\ &= [1, Q_{H_3}, U_{H_3}, 0]^T \\ &= \begin{bmatrix} 1 \\ Q_{H_2} \cos(4\theta_3) + U_{H_2} \sin(4\theta_3) \\ Q_{H_2} \sin(4\theta_3) - U_{H_2} \cos(4\theta_3) \\ 0 \end{bmatrix} \\ &= \mathbf{H}_0. \end{aligned} \quad (17)$$

The last angle θ_3 can be derived by setting U_{H_3} equal to zero. Considering the difference in Q_{H_2} , the adjustment is implemented as,

$$\theta_3 = \begin{cases} \frac{1}{4} [\arctan(\frac{U_{H_2}}{Q_{H_2}}) + 180], & Q_{H_2} < 0 \\ \frac{1}{4} \arctan(\frac{U_{H_2}}{Q_{H_2}}), & Q_{H_2} \geq 0. \end{cases} \quad (18)$$

IV. REAL-TIME SCHEME

Fig. 4 shows the sequence of calibration and transmission in a time multiplexing scheme. At the beginning, the initial angles of motorized wave plates are zero. The calibration module in the RX firstly performs an initial calibration for different TXs or users when setting up the quantum link. Then the data transmission is performed to generate a secure key. The calibration operation is expressed as,

$$\mathbf{R}^{-1}(\theta_1(t), \theta_2(t), \theta_3(t)) \cdot \mathbf{R}(t) \mathbf{S}_0(t) = \mathbf{S}_0(t), \quad (19)$$

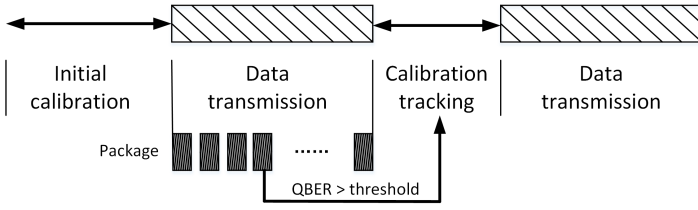


Fig. 4. The real-time calibration scheme.

where t is the start time of data transmission. In order to eliminate the influence of hand movement or varying birefringence, the fidelity of the polarization state is maintained by a calibration tracking step. Data transmission will be undertaken using packets, and if the QBER of the packet is more than a threshold, the system will perform a calibration tracking step immediately, otherwise, the data transmission is maintained until the end time $t + \Delta t$.

Considering the rotated wave plates, the detected Stokes vectors obtained from (2) is expressed as,

$$\mathbf{S}(t + \Delta t) = \mathbf{R}^{-1}(t) \cdot \mathbf{R}(t + \Delta t) \mathbf{S}_0(t + \Delta t), \quad (20)$$

where $\mathbf{R}^{-1}(t)$ denotes the transformation operator caused by three rotated wave plates at time t , and $\mathbf{R}(t + \Delta t)$ denotes the operator caused by new birefringence at time $t + \Delta t$. According to (3)(20), the Stokes vector used in the calibration tracking step is adjusted as,

$$\begin{aligned} \mathbf{S}'(t + \Delta t) &= \mathbf{R}(t + \Delta t) \mathbf{S}_0(t + \Delta t) \\ &= \mathbf{R}(\theta_1(t), \theta_2(t), \theta_3(t)) \cdot \mathbf{S}(t + \Delta t) \\ &= [\mathbf{M}_{\lambda/2}(\theta_3(t)) \mathbf{M}_{\lambda/4}(\theta_2(t)) \mathbf{M}_{\lambda/4}(\theta_1(t))]^{-1} \mathbf{S}(t + \Delta t). \end{aligned} \quad (21)$$

That is to say, the quantum channel characterization can be undertaken with current detection and prior information. It is not necessary to reset the system and the wave plates can be rotated based on the previous angle, which decreases the operation time. In addition, although the quantum signal should be single photons or weak coherent light [16], [17], we can increase the TX light intensity in the calibration step to obtain enough counts to calculate the accurate Stokes vector.

V. SCHEME VERIFICATION AND SYSTEM IMPLEMENTATION

Assuming that $\mathbf{H}_c, \mathbf{V}_c, \mathbf{D}_c, \mathbf{A}_c$ are the Stokes vectors of the polarization states before or after the calibration, the QBER can be defined as,

$$QBER = (\mathbf{H}_0 \mathbf{V}_c + \mathbf{V}_0 \mathbf{H}_c + \mathbf{D}_0 \mathbf{A}_c + \mathbf{A}_0 \mathbf{D}_c) / 8. \quad (22)$$

In order to verify the proposed calibration scheme, the influences of birefringence and hand rotation are simulated by a QWP and a HWP, respectively. The distorted polarization state is expressed as $\mathbf{S} = \mathbf{M}_{\lambda/2}(\phi_1) \mathbf{M}_{\lambda/4}(\phi_2) \cdot \mathbf{S}_0$, where ϕ_1 and ϕ_2 are the rotated angles from 0 to 180 degrees, to generate an arbitrary polarized state to test the robustness of calibration

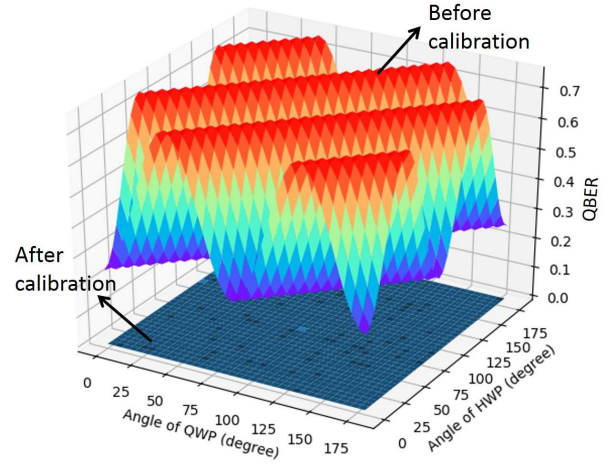


Fig. 5. A comparison of QBER before and after calibration (simulation results).

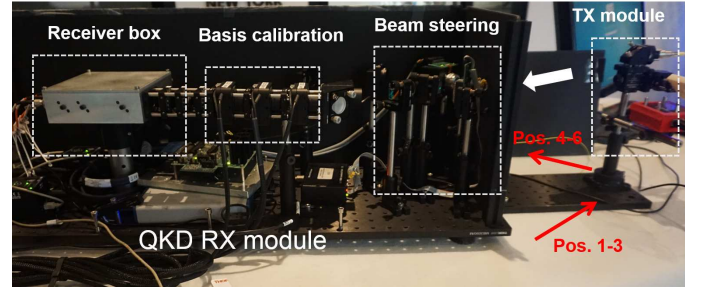


Fig. 6. Handheld QKD demonstration system.

scheme. Fig. 5 depicts a comparison of QBER before and after calibration. This shows that calibration significantly improves the QKD system performance, and the QBER after calibration is approximately zero.

Fig. 6 depicts a handheld QKD demonstration based on a polarization-encoding BB84 protocol. The TX module generates continuous wave (CW) light at 633 nm with different polarization states. The calibration method was implemented for a fixed TX position. Fig. 7 depicts the polarization state of the experimental result in the Poincare sphere. In this case, the QBER decreases from 34.6% before compensation to 7.9% after compensation. Once this has been performed the TX unit is moved to different positions as shown with the red arrows in Fig. 6. In each case calibration uses the previous rotated angle as a starting position, as set out in section IV. Fig. 8 shows the wave plate angles with different positions, showing the limited impact that position change has. Since the calibration tracking step is realized with previous rotated angle, the experiment validates that the real-time scheme can operate correctly.

Based on simulation and experiment, we find that the QBER in the practical demonstration is high compared to the theoretical analysis. The reason why the polarization state in Poincare sphere after calibration is degraded (as shown in Fig. 7) is the source, i.e., the polarization state generated from the TX is not perfectly polarized [18]. Therefore, more

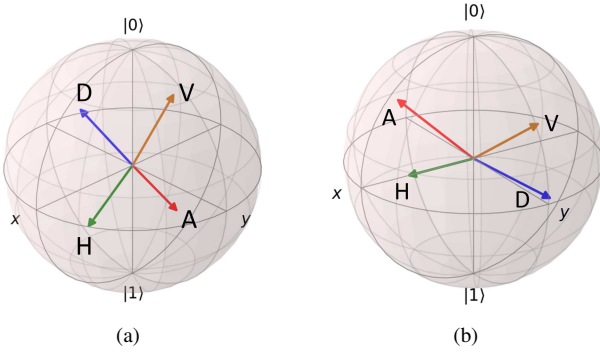


Fig. 7. Stokes vectors before and after calibration (experimental results).

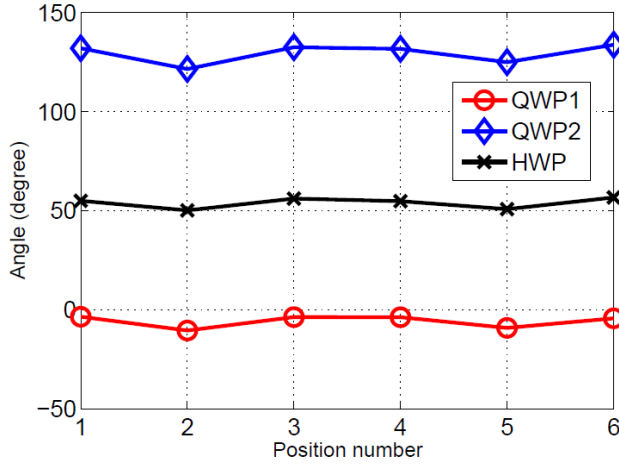


Fig. 8. The rotation angles of three wave plates in different TX position.

investigations should be undertaken to optimize the TX and thus decrease the overall QBER in the practical system.

VI. CONCLUSIONS

Considering the induced birefringence from TX and the hand movement, this paper proposes an efficient polarization calibration scheme for handheld QKD system. Based on the detected photons of six channels in the calibration step, the angle of three motorized wave plates can be calculated directly without exhaustive searching. A real-time scheme to speed up the calibration tracking step and decrease the system latency is also proposed. We have demonstrated the proposed method with simulation and measurement, and also validated that the real-time scheme can be implemented efficiently in a practical system.

REFERENCES

- [1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145-195, Mar. 2002.
- [2] O. Elmagbrok, M. Razavi, "Wireless quantum key distribution in indoor environments," *JOSA B*, vol. 35, no. 2, pp. 197-207, 2018.
- [3] G. Mlen, et al., "Integrated quantum key distribution sender unit for daily-life implementations," in *Advances in Photonics of Quantum Computing, Memory, and Communication IX*, 2016, vol. 9762, p. 97620A.
- [4] C. H. Bennett, G. Brassard, "Quantum cryptography: public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, no. 12, pp. 7-11, 2014.

- [5] A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, "Reference-frame-independent quantum key distribution," *Physical Review A*, vol. 82, no. 1, p. 012304, 2010.
- [6] H. Chun, et al., "Handheld free space quantum key distribution with dynamic motion compensation," *Optics Express*, vol. 25, no. 6, pp. 6784-6795, 2017.
- [7] M. Toyoshima, et al., "Polarization-Basis Tracking Scheme in Satellite Quantum Key Distribution," *International Journal of Optics*, pp. 1-8, 2011.
- [8] J. Chen, G. Wu, Y. Li, et al., "Active polarization stabilization in optical fibers suitable for quantum key distribution," *Optics express*, vol. 15, no. 26, pp. 17928-17936, 2007.
- [9] Y.-Y. Ding et al., "Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits," *Optics letters*, vol. 42, no. 6, pp. 1023-1026, 2017.
- [10] G. B. Xavier, et al., "Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation," *New Journal of Physics*, vol. 11, no. 4, p. 045015, 2009.
- [11] M. Zhang, L. Zhang, J. Wu, et al., "Detection and compensation of basis deviation in satellite-to-ground quantum communications," *Optics express*, vol. 22, no. 8, pp. 9871-9886, 2014.
- [12] J. Wabnig, D. Bitauld, H. W. Li, A. Laing, J. L. O'Brien, and A. O. Niskanen, "Demonstration of free-space reference frame independent quantum key distribution," *New J. Phys.*, vol. 15, no. 7, p. 073001, 2013.
- [13] G. Vest, et al., "Design and Evaluation of a Handheld Quantum Key Distribution Sender module," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 131-137, May 2015.
- [14] D. Lowndes, S. Frick, B. Harrington, and J. Rarity, "Low cost, short range quantum key distribution," in *2017 Conference on Lasers and Electro-Optics Europe European Quantum Electronics Conference (CLEO/Europe-EQEC)*, 2017.
- [15] H. G. Berry, G. Gabrielse, A. E. Livingston, "Measurement of the Stokes parameters of light," *Applied optics*, vol. 16, no. 12, pp. 3200-3205, 1997.
- [16] X. Ma, "Unconditional security at a low cost," *Physical Review A*, vol. 74, no. 5, p. 052325, 2006.
- [17] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security," *J Cryptology*, vol. 18, no. 2, pp. 133-165, Apr. 2005.
- [18] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quant. Inf. Comput.*, vol. 5, pp. 325-360, 2004.