All-Fiber and Calibration-Free Intrinsically Stable Polarization-Modulated Units for Measurement-Device-Independent Quantum Key Distribution

Yongjie Chen, Naida Mo, Jindong Wang, Jianling Yin, Tianming Zhao, Zhengjun Wei, Yafei Yu, and Zhiming Zhang

***Abstract*—There are several groups have implemented polarization encoding measurement-device-independent quantum key distribution (MDI-QKD). However, these groups use manual polarization controller to achieve the initial polarization state for encoders, and some of the encoders cannot fully satisfy the two bases for polarization encoding quantum key distribution. Here, we apply an all-fiber and calibration-free intrinsically stable polarization-modulated unit (APMU), which can maintain stable encoding for several hours without any calibration. A proof-of-principle demonstration of MDI-QKD based on our APMU is implemented with the four-intensity decoy state protocol. The proposed APMU can realize stable MDI-QKD encoding and simplify the operation for Alice and Bob, which makes the polarization encoding MDI-QKD more practical.**

***Index Terms*—Quantum key distribution, Measurement-device-independent, Calibration-free, Intrinsic-stability.**

I. Introduction

QUANTUM cryptography is different from classical cryptography that guarantees security based on mathematical computational complexity, its security is unconditionally guaranteed by the basic physical principles of quantum mechanics [1]. Quantum Key Distribution (QKD) allows the two parties, commonly known as Alice and Bob, to share a string of secret keys remotely. Combined with one time pad, eavesdroppers can't obtain any information from it even with unlimited computing power [2]. Unfortunately, in the practical QKD implement, due to the great gap between the practical devices and the theoretical assumptions of QKDs, there will still be loopholes for eavesdropper to carry out security attacks [3], [4], [5], [6], [7], [8], [9], [10], such as the faked state attack [7], [10], time-shift attack [6], [8], phase-remapping attack [4], [9] and detector blinding attack [3], [5], [11] etc. However, device-independent quantum key distribution (DI-QKD) can close these loopholes [12], it does not require detailed knowledge of how the QKD device works, and it can prove security based on the violation of Bell's inequality, but DI-QKD is impractical with current technology and has an extremely low secure key rate [13]. In contrast, the proposed measurement-device-independent quantum key distribution (MDI-QKD) based on partial Bell state measurements (BSMs) is practical with current technology, which allow eavesdropper to fully control the measurement devices without any information leakage [14]. MDI-QKD makes all known attacks against the detection side invalid.

As the most secure QKD protocol at present, MDI-QKD has been implemented in many experiments. MDI-QKD experiments based on polarization are generally employed [15], [16], [17], [18] as well as those based on phase encoding or time-bin encoding [19], [20], [21]. Polarization encoding QKD has potential advantages, since there is only one time slide, The stability of polarization encoding can be achieved by an encoder with intrinsically stability. The random birefringence effect of polarization encoding MDI-QKD in fiber channel can be compensated by polarization compensation equipment [18]. While the depolarization of MDI-QKD in free-space channel is negligible because of the isotropic tendency of free space [22], [23], and the polarization states have extremely stable transmission characteristics in free space channel.

In the previous polarization encoding MDI-QKD experiments, the performance of polarization encoder will directly determine the stability of MDI-QKD system, that is, the increasing of quantum bit error rate (QBER). Researchers encode polarization qubits into polarization states by using electronic

Manuscript received 23 July 2023; revised 12 September 2023; accepted 14 September 2023. Date of publication 19 September 2023; date of current version 3 October 2023. This work was supported in part by the National Nature Science Foundation of China under Grants 62071186 and 61771205 and in part by Guangdong Provincial Key Laboratory under Grant 2020B1212060066. *(Corresponding author: Jindong Wang.)*

Yongjie Chen, Naida Mo, Jindong Wang, Zhengjun Wei, and Zhiming Zhang are with the Institute of Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials, School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou 510006, China (e-mail: jaye9859@163.com; 571473961@qq.com; wangjd@scnu.edu.cn; weizhengjun@m.scnu.edu.cn; zhangzhiming@m.scnu.edu.cn).

Tianming Zhao and Yafei Yu are with the Institute of Guangdong Provincial Key Laboratory of Nanophotonic Functional Materials and Devices, School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou 510006, China (e-mail: zhaotm@scnu.edu.cn; yuyafei@m.scnu.edu.cn).

Jianling Yin is with the Institute of Shijiazhuang Campus, Army Engineering University of PLA, Shijiazhuang 050003, China (e-mail: yinjianling2002@163.com).

Digital Object Identifier 10.1109/JPHOT.2023.3316771

polarization controller [16], [18], which will increase the complexity of the system and the consumption of resources, or prepare polarization qubits by polarization modulation module [24], which will make circular polarization states affected by birefringence of a small section of fiber [17].

Our group have proposed intrinsically stable polarization-modulated unit (PMU)[25] and applied them in MDI-QKD system to achieve stability of polarization state preparation [15]. However, every time before experiment getting start, we still need manual polarization controller (PC) to adjust the initial polarization state into the polarization with equal amplitudes of the two polarization components. Still, we cannot guarantee the long-term stable operation of the system in real-time in an environment with external disturbances, manual calibration may be required during system operation. This is a common problem for polarization encoders [26], [27], [28]. Although there is a previous work to achieve the initial state of the encoder through spatial coupling [29], in practical applications, this solution will cause the optical signal to couple in and out multiple times between the fiber and space, which will increase the complexity of the overall device. Therefore, it is very important to design an all-fiber encoder that automatically matches the input polarization to a polarization with equal amplitudes of the two polarization components.

Here, we propose an All-fiber and calibration-free intrinsically stable polarization-modulated unit (APMU). Using a customized polarization maintaining beam splitter (PMBS) to replace the manual polarization calibration structure of PC and circulator (CIR) in current encoders, solve the problem that the encoder cannot operate stably for a long time and requires manual calibration in the experiment, and achieve long-term calibration-free self-stabilizing polarization encoding. And a particular back and forth identical modulation method to achieve intrinsic stability within the encoder is used. The four polarization states of the diagonal and circular basis can be prepared by loading voltage V_0, $V_{\pi/2}$, V_π and $V_{3\pi/2}$ to phase modulator without any calibration. Our proposal realizes the stability of APMUs for a long time without any calibration, that is, the QBER of the system can be kept at a low level for a long time. In the following sections, we firstly theoretically prove the system stability of our proposed encoder and conduct experimental QBER tests. Then we apply four-intensity decoy states [30] to MDI-QKD experiments based on the encoder to avoid side channel attacks caused by imperfect sources.

II. Performance Of The APMU

In this section, we first describe the structure of APMU and prove its intrinsic-stability, and then perform QBER tests on the APMU-based BB84-QKD system.

A. Configuration of APMU

The configuration of APMU is depicted in Fig. 1. A linearly polarized laser pulse enters the polarization beam splitter (PBS-1) and exits aligned with slow axis of polarization maintaining fiber (PMF). The PMBS is a customized component which is essentially a beam splitter (BS). The port 1 of PMBS is aligned

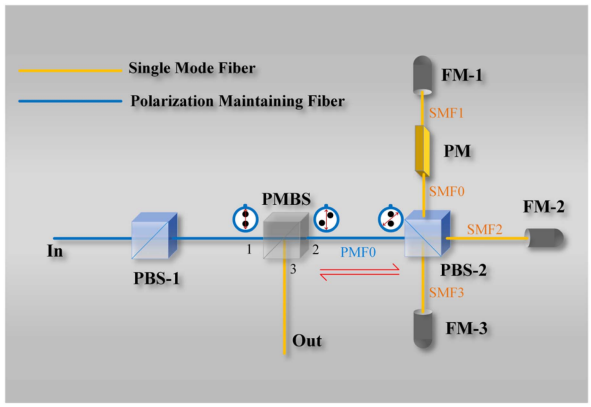

Fig. 1. Configuration of the APMU. PBS: Polarization beam splitter, PMBS: Polarization maintaining beam splitter, FM: Faraday mirror, PM: Phase modulator.

with slow axis of PMF, the slow axis of the port 2 is 45° relative to the slow axis of the port 1, and the port 3 is a single mode fiber (SMF). Which means the linearly polarized light incident along the slow axis of the port 1 will exit at 45° along the slow axis of the port 2. Therefore, taking the slow axis of port 2 of PMBS as X axis of the reference frame, the polarization state exits from port 2 transform to

$$\boldsymbol{J_{in}} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}. \tag{1}$$

Polarization maintaining fiber PMF0 in Fig. 1 can be described as a Jones matrix [27]

$$\overrightarrow{PMF} = \begin{pmatrix}1 & \\ & e^{i\delta_{PMF}}\end{pmatrix} = \overleftarrow{PMF}. \tag{2}$$

where $\delta_{PMF}$is the phase shift between TE mode and TM mode of the PMF0. The direction of the arrow above the matrix indicates the propagation direction of the laser pulse, PMF0 is the slow axis aligned with PBS-2, so the laser pulse becomes

$$\begin{aligned}\boldsymbol{J_0} &= \overrightarrow{PMF}\cdot\boldsymbol{J_{in}} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\e^{i\delta_{PMF}}\end{pmatrix}\\ &= \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}0\\e^{i\delta_{PMF}}\end{pmatrix} = \boldsymbol{J_{0H}} + \boldsymbol{J_{0V}},\\ \boldsymbol{J_{0H}} &= \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix},\ \boldsymbol{J_{0V}} = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\e^{i\delta_{PMF}}\end{pmatrix}.\end{aligned} \tag{3}$$

The reflection and transmission matrices of Polarization Beam Splitter PBS-2 can be written as

$$R = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}, T = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}. \tag{4}$$

After beam splitting by PBS-2, the TE mode $\boldsymbol{J_{0H}}$ is transmitted into SMF2, and the TM mode $\boldsymbol{J_{0V}}$ is reflected into SMF3. Firstly, taking single-mode fibers (SMF) as the arbitrary birefringent components with phase φ_k and azimuth θ_k, then the matrix for a single-mode fiber given by [24], [31]

$\overrightarrow{SMF_k} =$

$$\begin{pmatrix} e^{i\varphi_k/2}\cos^2\theta_k + e^{-i\varphi_k/2}\sin^2\theta_k & i\sin 2\theta_k \sin\varphi_k/2 \\ i\sin 2\theta_k \sin\varphi_k/2 & e^{-i\varphi_k/2}\cos^2\theta_k + e^{i\varphi_k/2}\sin^2\theta_k \end{pmatrix} = \begin{pmatrix} A_k & B_k \\ B_k & D_k \end{pmatrix},$$

$$\overleftarrow{SMF_k} = \begin{pmatrix} A_k & -B_k \\ -B_k & D_k \end{pmatrix}, \tag{5}$$

where $k = 0, 1, 2, 3$ for SMFk in Fig. 1, $A_k D_k - B_k^2 = 1$. The Faraday rotators (FM) always convert the incident polarization state into its perpendicular polarization as output, we can write the function of FM as [27]

$$FM_l = \begin{pmatrix} & -1 \\ -1 & \end{pmatrix}, \tag{6}$$

where$l = 1, 2, 3$ for FMl in Fig. 1. When the phase modulator (PM) is not driven, we can describe PM as

$$\overrightarrow{PM_0} = \begin{pmatrix} 1 & \\ & e^{i\phi} \end{pmatrix} = \overleftarrow{PM_0}, \tag{7}$$

when the PM is driven

$$\overrightarrow{PM} = \begin{pmatrix} e^{i\varphi_o} & 0 \\ 0 & e^{i(\varphi_e+\phi)} \end{pmatrix} = \overleftarrow{PM}, \tag{8}$$

where φ_o and φ_e respectively represent the phase shift applied to TE and TM mode by the PM when there is an electric pulse drive, and ϕ represents the phase shift between the two modes of the PM waveguide itself when there is no electric pulse drive. During the encoding process, the same modulation is performed twice on $\boldsymbol{J_{0H}}$ by PM when $\boldsymbol{J_{0H}}$ is back and forth propagation. So, the evolution of $\boldsymbol{J_{0H}}$ is

$$\begin{aligned} \boldsymbol{J}_1 &= R \cdot \overleftarrow{SMF_3} \cdot FM_3 \cdot \overrightarrow{SMF_3} \cdot T \cdot \overleftarrow{SMF_0} \cdot \overleftarrow{PM} \cdot \overleftarrow{SMF_1} \cdot FM_1 \\ &\cdot \overrightarrow{SMF_1} \cdot \overrightarrow{PM} \cdot \overrightarrow{SMF_0} \cdot R \cdot \overleftarrow{SMF_2} \cdot FM_2 \cdot \overrightarrow{SMF_2} \cdot \boldsymbol{J}_{0\boldsymbol{H}} \\ &= R \cdot \overleftarrow{SMF_3} \cdot FM_3 \cdot \overrightarrow{SMF_3} \cdot T \cdot \overleftarrow{SMF_0} \cdot \overleftarrow{PM} \cdot \overleftarrow{SMF_1} \cdot FM_1 \\ &\cdot \overrightarrow{SMF_1} \cdot \overrightarrow{PM} \cdot \overrightarrow{SMF_0} \cdot R \cdot \frac{1}{\sqrt{2}} e^{i\pi} \begin{pmatrix} A_2B_2 - A_2B_2 \\ -B_2^2 + A_2D_2 \end{pmatrix} \\ &= R \cdot \overleftarrow{SMF_3} \cdot FM_3 \cdot \overrightarrow{SMF_3} \cdot T \cdot \overleftarrow{SMF_0} \cdot \overleftarrow{PM} \\ &\cdot \overleftarrow{SMF_1} \cdot FM_1 \cdot \overrightarrow{SMF_1} \cdot \overrightarrow{PM} \cdot \overrightarrow{SMF_0} \cdot R \cdot \frac{1}{\sqrt{2}} e^{i\varphi_{SMF2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} e^{i(\varphi_{SMF0}+\varphi_{SMF1}+\varphi_{SMF2}+\varphi_{SMF3}+\pi)} \begin{pmatrix} 0 \\ e^{i(\varphi_o+\varphi_e+\phi)} \end{pmatrix}, \end{aligned} \tag{9}$$

where φ_{SMFk} $(k = 0, 1, 2, 3)$ is the global phase of the SMFk. Similarly, the evolution of component $\boldsymbol{J_{0V}}$ is

$$\begin{aligned} \boldsymbol{J_2} &= T \cdot \overleftarrow{SMF_2} \cdot FM_2 \cdot \overrightarrow{SMF_2} \cdot R \cdot \overleftarrow{SMF_0} \cdot \overleftarrow{PM_0} \\ &\cdot \overleftarrow{SMF_1} \cdot FM_1 \\ &\cdot \overrightarrow{SMF_1} \cdot \overrightarrow{PM_0} \cdot \overrightarrow{SMF_0} \cdot T \cdot \overleftarrow{SMF_3} \cdot FM_3 \cdot \overrightarrow{SMF_3} \cdot \boldsymbol{J}_{0\boldsymbol{V}} \\ &= \frac{1}{\sqrt{2}} e^{i(\varphi_{SMF0}+\varphi_{SMF1}+\varphi_{SMF2}+\varphi_{SMF3}+2\pi)} \begin{pmatrix} e^{i(\phi+\delta_{PMF})} \\ 0 \end{pmatrix}. \end{aligned} \tag{10}$$

After $\boldsymbol{J}_1$ and $\boldsymbol{J}_2$ combine at PBS-2, the polarization of laser pulse becomes

$$\boldsymbol{J}_3 = \boldsymbol{J}_1 + \boldsymbol{J}_2 = \frac{1}{\sqrt{2}} e^{i(\varphi_{SMF0}+\varphi_{SMF1}+\varphi_{SMF2}+\varphi_{SMF3}+\pi)} \begin{pmatrix} e^{i(\phi+\delta_{PMF}+\pi)} \\ e^{i(\varphi_o+\varphi_e+\phi)} \end{pmatrix}. \tag{11}$$

Ignoring the global phase that does not contribute to the polarization state in the (11), we could write $\boldsymbol{J}_3$ as

$$\boldsymbol{J}_3 = \frac{1}{\sqrt{2}} \begin{pmatrix} -e^{i\delta_{PMF}} \\ e^{i(\varphi_0+\varphi_e)} \end{pmatrix}. \tag{12}$$

Finally, PMBS can output the encoded polarization state

$$\boldsymbol{J_{Out}} = \overleftarrow{PMF} \cdot \boldsymbol{J}_3 = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ e^{i(\varphi_0+\varphi_e)} \end{pmatrix} \tag{13}$$

to the quantum channel through port 3. Set different voltages of PM to satisfy $\varphi_o + \varphi_e = \pi, 0$ then we have $\pm 45°$ (Diagonal(D) and Antidiagonal(A)) linear polarization for diagonal basis Z. Set voltages of PM to satisfy $\varphi_o + \varphi_e = 3\pi/2, \pi/2$ then we have Right-hand circular polarization(R) and Left-hand circular polarization(L) for circular basis X. So far, we have theoretically proved the self-stability of the APMU, and the prepared polarization state depends entirely on the voltage loaded on the PM.

It is worth mentioning that in our proving derivation, the polarization-dependent loss is not considered. Because the laser pulse is always transmitted back and forth in the components, the polarization-dependent loss will be converted into the total loss of the laser pulse, and does not contribute to the polarization encoding.

B. QBERs of the APMU-based BB84-QKD System

In order to demonstrate the stability of the APMU experimentally, we conducted a QBER test on the APMU-based BB84-QKD system, show as Fig. 2. Considering that this article is for implementing the APMU-based MDI-QKD system. We use a continuous wave frequency-locked laser (CW Laser, Clarity-NLL-1550-LP) and an intensity modulator (IM) to realize the generation of laser pulse, and the relevant parameter settings are also considered based on the MDI-QKD system described later. Such a QBER test of the BB84-QKD system can not only illustrate the experimental stability of the APMU, but also directly reflect the performance of the APMU applied in the MDI-QKD system.

With the modulation of the modulator bias controller (MBC, MX10A) and the pulse width modulator (PWM, EPG-210B-0100-S-P-T-A), the IM will convert the continuous wave laser into a weak coherent pulse with a frequency of 50 MHz and a full width at half maxima (FWHM) of 200 ps. By controlling the fiber length difference between SMF2 and SMF3 to be 36 cm in Fig. 2, there is a delay difference of 3.6 ± 0.02 ns when the horizontal(H) and vertical(V) polarization components reach the PM. The waveguide of the PM is 7 cm long, so it takes 350 ps for the pulse to pass through the PM. We set the length from PM to FM1 to be 300 cm, then the total round-trip delay from

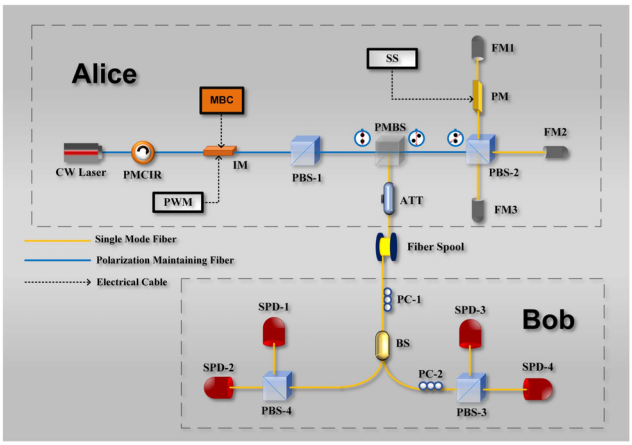

Fig. 2. Experimental setup for the APMU-based BB84-QKD system. CW Laser: Continuous wave laser, PMCIR: Polarization maintaining circulator, IM: Intensity modulator, PWM: Pulse width modulator, MBC: Modulator bias controller, SS: Signal source, ATT: Attenuator, PC: Manual polarization controller, BS: Beam splitter, PBS: Polarization beam splitter, SPD: Single photon detector, PWM: Pulse width modulator, SS: Signal source, MBC: Modulator bias controller.

PM to FM1 is 30 $\pm$ 0.4 ns. During the encoding process, a voltage-variable square wave pulse with a frequency of 100 MHz and a pulse width of 3.3 ns is provided by signal source (SS) to the PM to realize twice modulation for the H component and avoid crosstalk between H and V in different modulation directions. The specific encoding process for one qubit between PM and FM1 is shown in Fig. 3. Before the pulse enter the fiber spool, we attenuate the average photon number per pulse to 0.1 with an attenuator (ATT).

We conducted a total of 14.6 hours of QBERs test on the APMU-based BB84-QKD system without any calibration, using the FPGA to collect the QBER once per second and average every 60 collections as a point in Fig. 4. In order to illustrate the self-stability and calibration-free characteristics of the APMU, a short-distance of 3 m fiber channel was used in this experiment. During the experiment, the QBERs of the polarization states are always lower than 0.8%, and the average QBERs of the Z basis is 0.34%, and the average QBERs of the X basis is 0.36%, which shows that our APMU can stably prepare four polarization states for QKD for a long time without any calibration.

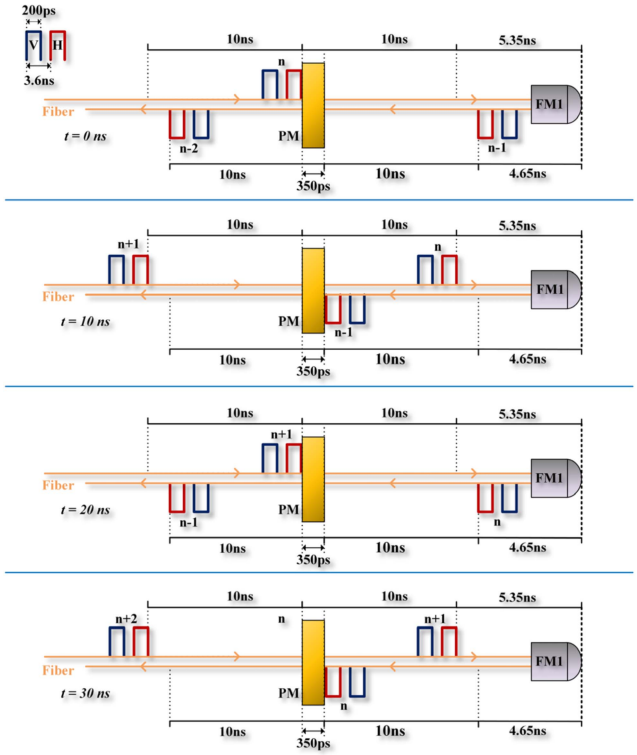

Fig. 3. Encoding process for nth pulse pair between PM and FM1. Fiber length is described by time scale. H: Horizontal polarization component, V: Vertical polarization component. Here, we assume that the nth pulse pair exactly arrives at PM when $t = 0$ ns. In actual encoding, the two polarization components are not H and V in PM, H and V are only defined according to the two path states after PBS-2 beam splitting.

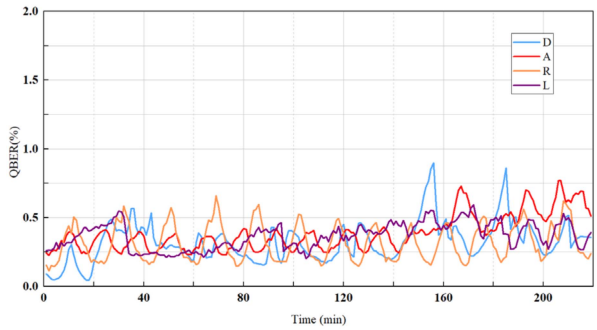

Fig. 4. The record of QBERs of the APMU-based BB84-QKD system over time.

III. System Configuration of MDI-QKD Setup

Fig. 5 schematically shows our experimental setup for MDI-QKD base on APMU, the two identical legitimate users Alice and Bob both use a CW Laser (Clarity-NLL-1550-LP) as laser source, which can achieve a dip visibility up to 48.1%. The following optical apparatus is a fast axis blocked and slow axis free-pass polarization maintaining circulator (PMCIR), which is also used as an optical isolator with a return loss greater than 60 dB. Before the modulation of the optical intensity modulator (IM), we use the MBC (MX10A and MBC-DG-BT-PD) to automatically find the appropriate DC bias voltage to achieve the lowest IM output laser intensity. Then we use PWM (EPG-210B-0100-S-P-T-A) to generate an electrical signal with $V_{PP} = 6$ V, frequency of 50 MHz and FWHM of 200 ps for IM to generate 50 MHz, 200 ps optical pulse, and the extinction ratio of IM can reach 29 dB. The voltage-variable, 100 MHz, 3.3 ns electrical signal generated by the SS is used to realize the polarization qubits encoding of the Z basis and X basis when the optical pulse enters the APMU (same as Fig. 1).

Electrical optic attenuators (EATT) attenuate the polarization qubits to the single-photon level and perform a total length of 85 kilometers of equivalent fiber loss(0.2 dB/km) between

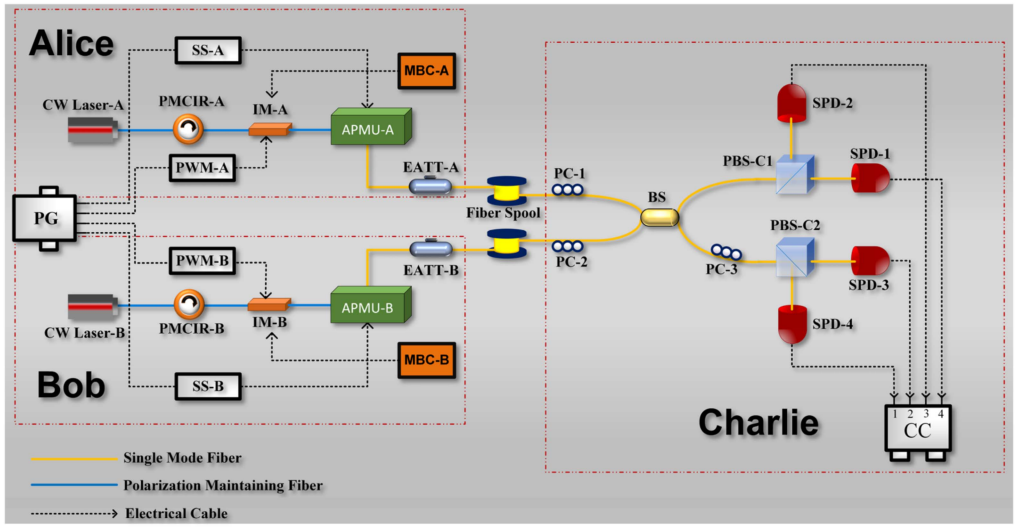

Fig. 5. Experimental setup for the APMU-based MDI-QKD system. CW Laser: Continuous wave laser, PMCIR: Polarization maintaining circulator, IM: Intensity modulator, EATT: Electrical attenuator, PC: Manual polarization controller, BS: Beam splitter, PBS: Polarization beam splitter, SPD: Single photon detector, PG: Pulse generator, PWM: Pulse width modulator, SS: Signal source, MBC: Modulator bias controller, CC: Coincidence counter.

Alice and Bob. It is necessary to use manual polarization controllers (PC) to align Alice's and Bob's polarization qubits to Charlie's reference frame since we did not apply a real-time polarization compensation. Charlie performs partial Bell state measurements and records the contributing events that two of the single-photon detectors (SPD, gate windows ~1 ns, gate frequency ~50 MHz, detection efficiency ~16.6%, dark count probability per gate $\sim 3 \times 10^{-6}$) click simultaneous[14], [18] by coincidence counter (CC) with resolution of 5 ps. It's worth noting that all active devices are synchronized by a multi-channel clock pulse generator (PG).

We applied the four-intensity decoy state MDI-QKD protocol [30] to our MDI-QKD system to estimate the low bound of the final secure key rate. According to the optimal parameters for MDI-QKD protocol in [30], Alice and Bob choose with probability 0.423 to send a signal state with an average photon numbers of $\mu_Z = 0.252$ in the Z basis, and choose with probability 0.398, 0.138, 0.041 to send decoy states with average photon numbers of $\mu_x = 0.078$, $\mu_y = 0.241$, $\mu_0 = 0$ respectively. The contributing events cause by pulse pairs from Z basis are used to distill the key bits only, while the contributing events cause by pulse pairs from X basis will be used to estimate the yield and the phase-flip error rate of the single-photon pulse pairs [30].

TABLE I
THE EXPERIMENTAL VALUE OF YIELD $Q_Z^{\mu_Z,\mu_Z}$ AND QBER $E_Z^{\mu_Z,\mu_Z}$ IN Z BASIS. ERRORS SHOWN REPRESENT 5 STANDARD DEVIATIONS

$Q_Z^{\mu_Z,\mu_Z}$	$E_Z^{\mu_Z,\mu_Z}$
$(1.24 \pm 0.0036) \times 10^{-5}$	0.0228±0.0004

TABLE II
THE EXPERIMENTAL VALUES OF YIELDS $Q_X^{I_A,I_B}$ AND QBERS $E_X^{I_A,I_B}$ WITH AVERAGE PHOTON NUMBERS I_A AND I_B ($I_A, I_B \in \{\mu_x, \mu_y, \mu_0\}$) IN X BASIS

I_A	I_B	$Q_X^{I_A,I_B}$	$E_X^{I_A,I_B}$
μ_x	μ_x	$(2.45 \pm 0.016) \times 10^{-6}$	0.2925±0.0035
μ_x	μ_y	$(9.1 \pm 0.0308) \times 10^{-6}$	0.3672±0.0021
μ_x	μ_0	$(6.01 \pm 0.0891) \times 10^{-7}$	0.5004±0.0093
μ_y	μ_x	$(8.95 \pm 0.0305) \times 10^{-6}$	0.3623±0.0021
μ_y	μ_y	$(2.24 \pm 0.0048) \times 10^{-5}$	0.2849±0.0012
μ_y	μ_0	$(5.50 \pm 0.0239) \times 10^{-6}$	0.4952±0.0031
μ_0	μ_x	$(5.97 \pm 0.0789) \times 10^{-7}$	0.5065±0.0094
μ_0	μ_y	$(5.59 \pm 0.0214) \times 10^{-6}$	0.4987±0.0065
μ_0	μ_0	$(1.17 \pm 1.104) \times 10^{-10}$	0.5001±0.0167

Errors shown represent 5 standard deviations.

IV. RESULTS AND DISCUSSION

Alice and Bob have sent out a total number of 2.4×10^{12} pulse pairs for Charlie to measure. After key sifting, we performed the measurement of yields and QBERs with different combination intensity in both bases from sifted key. With a failure probability of 5.73×10^{-7} in $n_a = 5$ [32], the yields and QBERs of Z basis and X basis are listed in Tables I and II respectively.

In the implementation of MDI-QKD, both Alice and Bob send out weak coherent pulses, and Charlie's Bell state measurements are taken in Z basis, cause the asymmetric QBERs of the Z basis and X basis. The QBER of Z basis is caused by dark counts of the detectors and the polarization misalignment between users and Charlie. In an ideal case, if there is no polarization misalignment and dark counts, the $E_Z^{\mu_Z,\mu_Z} = 0$. The lower $E_Z^{\mu_Z,\mu_Z}$ is expected while the polarization aligned properly. However, due to the existence of multi-photon pulse in the weak coherent pulses, the QBERs in X basis will be much higher than the QBER in Z basis. This is because the case that one of Alice and Bob sends a vacuum pulse and the other sends a two-photon pulse could occur, then Charlie's successful Bell state measurement

TABLE III
PARAMETERS TO ESTIMATE THE SECURE KEY RATE

p_{ZA}, p_{ZB}	$p_Z^{1,1}$	$Y_Z^{1,1}$	$E_X^{1,1}$	f	$Q_Z^{\mu_Z,\mu_Z}$	$E_Z^{\mu_Z,\mu_Z}$
0.423	0.1959	1.707×10^{-4}	0.1767	1.16	1.23×10^{-5}	0.0228

may generate bit that irrelevant, resulting in a bit error. Since this case happens with the same probability as if Alice and Bob both sent single-photon pulses, there would be a QBER of 25% in the X basis even without polarization misalignment and dark counts [18]. In our MDI-QKD experiments, the QBERs of the Z basis and X basis are a bit larger compared to the previous works [17], [18] due to the $\pm 0.6\%$ difference in detection efficiency between the single-photon detectors.

A lower bound of the secure key rate is given by [14]

$$R \geqslant p_{ZA}p_{ZB}\{p_Z^{1,1}Y_Z^{1,1}[1-H(E_X^{1,1})]-fQ_Z^{\mu_Z,\mu_Z}H(E_Z^{\mu_Z,\mu_Z})\}, \tag{14}$$

where p_{ZA}, p_{ZB} is the probability for Alice and Bob both send out signal pulses in Z basis, $p_Z^{1,1}$ is the probability that the signal pulses sent by Alice and Bob contains only one photon. The yield $Q_Z^{\mu_Z,\mu_Z}$ and QBER $E_Z^{\mu_Z,\mu_Z}$ of the Z basis can be obtained directly from the experimental values as listed in Table I. $f = 1.16$ is the inefficiency of error correction and $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function [14]. $Y_Z^{1,1}$ is the lower bound of the yield when both Alice and Bob send single-photon pulses in Z basis, $E_X^{1,1}$ is the upper bound of the QBER for single-photon pulse pair in X basis, and both $Y_Z^{1,1}$ and $E_X^{1,1}$ are estimated from the decoy-state experimental values of the X basis in Table II. Take the finite key effect into account when estimating $Y_Z^{1,1}$ and $E_X^{1,1}$, all parameters used to estimate the lower bound of the secure key rate are listed in Table III. Finally, we have a secure key rate of 3.88×10^{-8} bits per pulse.

Limited by the performance of experimental equipment, the repetition frequency of our optical pulse can only reach 50 MHz, that is, 1.95 bits of security keys can be obtained per second. More secure key bits be obtained if we can apply a higher pulse repetition rate and SPDs with higher gate frequency and detection efficiency. As mentioned above, the detection efficiency of the SPDs we use are mismatch, resulting in higher QBERs and a lower secure key rate. The secure key rate of our system can also be improved when the detection efficiency of the SPDs can be more matched.

V. CONCLUSION

We proposed an all-fiber and calibration-free intrinsically stable polarization-modulated units and theoretically proved its self-stability that the encoded polarization states are completely dependent on the loading voltage for the PM. Without any calibration, a total of 14.6 hours of QBER tests were performed on the APMU-based BB84-QKD system, resulting in average QBERs of 0.34% and 0.35% for Z basis and X basis, respectively. We also demonstration of polarization encoding MDI-QKD based on APMUs, obtained the Z basis QBER of 2.28% and the secure key rate of 3.88×10^{-8} bits per pulse. The secure key rate can be improved by increasing the detection efficiency and making the detection efficiency more matched. Overall, our work proposed a portable and extremely stable encoder, not only providing an easy-to-operate and well-performance encoding unit for future practical polarization encoding applications such as MDI-QKD networks or conventional QKD systems, but also providing an all-fiber and calibration-free solution for all current encoder that use phase modulator to achieve polarization encoding. It will upgrade the stability of polarization encoding practical application. Combining the advantages of free-space polarization encoding communication, our work is one step closer to the practicality of free-space polarization encoding QKD.

REFERENCES

[1] N. Gisin, G. G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002, doi: 10.1103/RevModPhys.74.145.

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Sep. 2009, doi: 10.1103/RevModPhys.81.1301.

[3] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, "Controlling an actively-quenched single photon detector with bright light," *Opt. Exp.*, vol. 19, no. 23, pp. 23590–23600, Nov. 2011, doi: 10.1364/OE.19.023590.

[4] F. H. Xu, B. Qi, and H. K. Lo, "Experimental demonstration of phase-remapping attack in a practical quantum key distribution system," *New J. Phys.*, vol. 12, no. 11, Nov. 2010, Art. no. 113026, doi: 10.1088/1367-2630/12/11/113026.

[5] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Thermal blinding of gated detectors in quantum cryptography," *Opt. Exp.*, vol. 18, no. 26, pp. 27938–27954, Dec. 2010, doi: 10.1364/OE.18.027938.

[6] Y. Zhao, C. H. F. Fung, B. Qi, C. Chen, and H. K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A*, vol. 78, no. 4, Oct. 2008, Art. no. 042333, doi: 10.1103/PhysRevA.78.042333.

[7] V. Makarov and J. Skaar, "Fakes states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols," *Quantum Inf. Comput.*, vol. 8, no. 6, pp. 622–635, Jul. 2008, doi: 10.5555/2016976.2016980.

[8] B. Qi, C. H. F. Fung, H. K. Lo, and X. F. Ma, "Time-shift attack in practical quantum cryptosystems," *Quantum Inf. Comput.*, vol. 7, no. 1, pp. 73–82, Jan. 2007, doi: 10.1117/12.717206.

[9] C. H. F. Fung, B. Qi, K. Tamaki, and H. K. Lo, "Phase-remapping attack in practical quantum-key-distribution systems," *Phys. Rev. A*, vol. 75, no. 3, Mar. 2007, Art. no. 032314, doi: 10.1103/PhysRevA.75.032314.

[10] A. Acin, S. Massar, and S. Pironio, "Efficient quantum key distribution secure against no-signalling eavesdroppers," *New J. Phys.*, vol. 8, no. 2, Aug. 2006, Art. no. 126, doi: 10.1088/1367-2630/8/8/126.

[11] V. Makarov, "Controlling passively quenched single photon detectors by bright light," *New J. Phys.*, vol. 11, no. 6, Jun. 2009, Art. no. 065003, doi: 10.1088/1367-2630/11/6/065003.

[12] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 98, no. 23, Jun. 2007, Art. no. 23050, doi: 10.1103/PhysRevLett.98.230501.

[13] N. Gisin, S. Pironio, and N. Sangouard, "Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier," *Phys. Rev. Lett.*, vol. 105, no. 7, Aug. 2010, Art. no. 070501, doi: 10.1103/PhysRevLett.105.070501.

[14] H. K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, Mar. 2012, Art. no. 130503, doi: 10.1103/PhysRevLett.108.130503.

[15] Y. P. Yuan et al., "Proof-of-principle demonstration of measurement-device-independent quantum key distribution based on intrinsically stable polarization-modulated units," *Opt. Exp.*, vol. 28, no. 8, pp. 10772–10782, Apr. 2020, doi: 10.1364/OE.387968.

[16] L. C. Comandar et al., "Quantum key distribution without detector vulnerabilities using optically seeded lasers," *Nature Photon.*, vol. 10, no. 5, pp. 312–316, May 2016, doi: 10.1038/Nphoton.2016.50.

[17] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H. K. Lo, "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 112, no. 19, May 2014, Art. no. 190503, doi: 10.1103/PhysRevLett.112.190503.

[18] T. F. da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Tempor~ao, and J. P. von der Weid, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits," *Phys. Rev. A*, vol. 88, no. 5, Nov. 2013, Art. no. 052303, doi: 10.1103/PhysRevA.88.052303.

[19] Y. Cao et al., "Long-distance free-space measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 125, no. 26, Dec. 2020, Art. no. 260503, doi: 10.1103/PhysRevLett.125.260503.

[20] Y. L. Tang et al., "Measurement-device-independent quantum key distribution over 200 km," *Phys. Rev. Lett.*, vol. 113, no. 19, Nov. 2014, Art. no. 190501, doi: 10.1103/PhysRevLett.113.190501.

[21] Y. Liu et al., "Experimental measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 111, no. 13, Sep. 2013, Art. no. 130502, doi: 10.1103/PhysRevLett.111.130502.

[22] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical freespace quantum key distribution over 10 km in daylight and at night," *New J. Phys.*, vol. 4, no. 1, Jul. 2002, Art. no. 43, doi: 10.1088/1367-2630/4/1/343.

[23] S. K. Liao et al., "Long-distance free-space quantum key distribution in daylight towards 16 inter-satellite communication," *Nature Photon.*, vol. 11, no. 8, pp. 509–514, Aug. 2017, doi: 10.1038/Nphoton.2017.116.

[24] I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel, "Proof-of-concept of real-world quantum key distribution with quantum frames," *New J. Phys.*, vol. 11, no. 9, pp. 095001–095026, Sep. 2009, doi: 10.1088/1367-2630/11/9/095001.

[25] J. Wang et al., "Experimental demonstration of polarization encoding quantum key distribution system based on intrinsically stable polarization-modulated units," *Opt. Exp.*, vol. 24, no. 8, pp. 8302–8309, Apr. 2016, doi: 10.1364/OE.24.008302.

[26] C. Agnesi et al., "Simple quantum key distribution with qubit based synchronization and a self-compensating polarization encoder," *Optica*, vol. 7, no. 4, pp. 284–290, Apr. 2020, doi: 10.1364/Optica.381013.

[27] X. B. Liu, C. J. Liao, J. L. Mi, J. D. Wang, and S. H. Liu, "Intrinsically stable phase-modulated polarization encoding system for quantum key distribution," *Phys. Lett. A*, vol. 373, no. 1, pp. 54–57, Dec. 2008, doi: 10.1016/j.physleta.2008.10.081.

[28] X. B. Liu, Z. L. Tang, C. J. Liao, Y. Q. Lu, F. Zhao, and S. H. Liu, "Polarization states encoded by phase modulation for high bit rate quantum key distribution," *Phys. Lett. A*, vol. 358, no. 5-6, pp. 386–389, Oct. 2006, doi: 10.1016/j.physleta.2006.05.068.

[29] M. Avesani et al., "Resource-effective quantum key distribution: A field trial in Padua city center," *Opt. Lett.*, vol. 46, no. 12, pp. 2848–2851, Jun. 2021, doi: 10.1364/OL.422890.

[30] Y. H. Zhou, Z. W. Yu, and X. B. Wang, "Making the decoy state measurement-device-independent quantum key distribution practically useful," *Phys. Rev. A*, vol. 93, no. 4, Apr. 2016, Art. no. 042324, doi: 10.1103/PhysRevA.93.042324.

[31] M. Martinelli, "A universal compensator for polarization changes induced by birefringence on a retracing beam," *Opt. Commun.*, vol. 72, no. 6, pp. 341–344, Aug. 1989, doi: 10.1016/0030-4018(89)90436-7.

[32] X. F. Ma, C. H. F. Fung, and M. Razavi, "Statistical fluctuation analysis for measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 86, no. 5, Nov. 2016, Art. no. 052305, doi: 10.1103/PhysRevA.86.052305.