Polarization alignment in measurement-device-independent quantum key distribution with intrinsic events

Jia-Xuan Li,[1,2,†] Guan-Jie Fan-Yuan,[1,2,†] Shuang Wang,[1,2,3,*] Ze-Hao Wang,[1,2] Feng-Yu Lu,[1,2] Zhen-Qiang Yin,[1,2,3] Wei Chen,[1,2,3] De-Yong He,[1,2,3] Guang-Can Guo,[1,2,3] and Zheng-Fu Han[1,2,3]

[1] *CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui 230026, China*

[2] *CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[3] *Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China*

(Received 17 May 2023; revised 5 July 2023; accepted 1 November 2023; published 20 November 2023)

Measurement-device-independent quantum key distribution (MDI QKD) is a crucial step for the quantum Internet, as it removes all detector side channels and enables secure QKD with untrusted nodes. However, MDI QKD faces a significant challenge from polarization alignment, since drift of the state of polarization affects the efficiency of key generation, especially when the quantum states are sent from remote locations. Conventional methods for polarization alignment either require additional resources, such as classical lasers or reference pulses, or interrupt the QKD process, which reduces the efficiency of the system. In this paper, an efficient polarization-alignment method in MDI QKD is proposed that leverages intrinsic events from MDI to directly calculate how to compensate for polarization drift. The proposed method does not require additional resources such as reference pulses, thereby eliminating bandwidth limitations, and it is fast, as it can directly calculate how to correct polarization with a small criterion fluctuation. We also introduce the polarization dimension in addition to the encoding dimension and establish a response-rate model for MDI QKD with additional polarization dimensions. Overall, the proposed method is a resource-efficient solution for polarization drift correction in MDI QKD, which can enhance the practicality and scalability of QKD networks.

DOI: 10.1103/PhysRevApplied.20.054041

I. INTRODUCTION

Quantum key distribution (QKD) can share private keys between Alice and Bob and its security relies on the principles of quantum physics and is independent of computational complexity [1,2]. For large-scale applications of QKD, networking is necessary and several trusted-node networks have been proposed [3–11]. But trusted-node QKD networks lack security, because the network may be paralyzed if a node is attacked and loses credibility. Therefore, it is necessary to build the untrusted-node-based networks using the protocol with untrusted nodes, as in measurement-device-independent QKD (MDI QKD) [12–14], twin-field QKD (TF QKD) [15–18], and device-independent QKD (DI QKD) [19–23]. Compared to other protocols, MDI QKD is the most mature and easiest solution to implement [24–27] and shows the capability of networking [28].

However, before large-scale commercial application, MDI QKD still faces many practical problems. For the most widely used quantum channel, fiber, its birefringence effect restricts the practical application of remote MDI systems. MDI QKD needs the photons sent by the two sides to be indistinguishable at the node but the standard single-mode fiber cannot preserve the state of polarization (SOP), so the birefringence effect will increase the quantum bit error rate (QBER) of MDI QKD, even it is not encoded by the polarization basis [25].

To align the polarization, there are two kinds of method, one of which requires direct measurement of the polarization [29–31,33,34,36,37], while the other does not [39–41]. For the direct-measurement methods, there are real-time [29–31,33,34] and interrupting methods [36,37]. For real-time methods, a reference signal is needed when using time-division multiplexing (TDM) [29–31] and wavelength-division multiplexing (WDM) [30,33,34]. But TDM reduces the effective bandwidth and prevents the increase in the clock rate [32] and WDM faces the problem that the wavelength dependence of the birefringence [35], and the leakage of the reference light into the quantum photon-transmitting procedures, will reduce the key rate. Interrupting methods may sacrifice the efficiency of the system and may suffer a potential security risk while

*wshuang@ustc.edu.cn

†These authors contributed equally to this work.

TABLE I. The existing polarization-alignment methods and their problems.

	Time overhead	Device loss	Potential security risk	Accuracy problems
TDM [29–31]	Yes [32]	No	No	No
WDM [30,33,34]	No	Yes	No	Yes [35]
Interrupting methods [36,37]	Yes	No	Yes [38]	No
QBER-based methods [39–41]	Yes	No	No	Yes [39,41]
Our method	No	No	No	No

switching the working modes of the system [38]. With regard to the methods that do not need direct measurement of the polarization, most of them are based on the QBER [39–41]. Reference [39] has provided a continuously working polarization-alignment method based on a gradient-searching and -control algorithm using feedback signals derived from single-photon-detection results. Reference [40] has proposed a method to compensate for the polarization random drift in optical fibers by mapping the estimated QBER onto the Poincaré sphere. But in order to estimate the QBER, we need to wait until Alice and Bob announce their qubit information, which is private. What is more, the larger the QBER is, the more qubits should be used for QBER estimation [39,41]; for example, compared with QBER = 1%, about 18.94 times as many qubits are needed to reach the same QBER estimation accuracy while the QBER is as high as 25%, which is the minimum QBER for the X basis of time-bin phase-coding MDI QKD. The problems with the previous polarization-alignment methods are summarized in Table I. To avoid the above problems, it is necessary to find a polarization-alignment method for MDI QKD that does not need direct measurement of the polarization and that does not use the QBER as the criterion; further, it should minimize the addition of hardware as much as possible.

In this paper, we develop a polarization-alignment method using the count number and the coincidence-count number as the criteria to directly calculate the operator needed to align the polarization. We calculate the effect of the SOP on the count number and find an efficient method to reverse the random drift of polarization through three iterations. Our method requires no reference light and theoretically uses the least number of devices, in that one of Alice and Bob needs an electronic polarization controller (EPC), which reduces the photon loss and improves the key rate. This method does not need to wait for the announcement of qubit information, uses criteria that are accurate when the QBER is about 25%, and uses very few iterations. These features allow us to deal with faster polarization changes, which improves the usability of the method and better aligns the polarization for MDI-QKD systems. Although our polarization-alignment method is developed for time-bin phase-coding MDI QKD as an example, it can also be generalized to other QKD systems, which need to measure the interference results at the untrusted node.

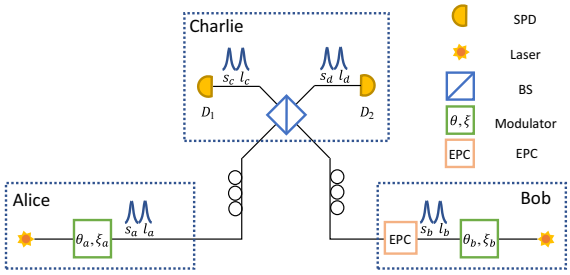

FIG. 1. The time-bin phase-coding MDI QKD that we use in this paper. SPD, single-photon detector; Laser, pulsed weak-coherent-state source; BS, beam splitter; Modulator, encoder; EPC, electronic polarization controller.

The remainder of the paper is structured as follows. In Sec. II, we establish a response-rate model for MDI QKD with an additional SOP dimension. In Section III, we present our polarization-alignment method. In Sec. IV, we discuss the precision of the method. Finally, Sec. V gives a simulation of our method and then Sec. VI discusses the main conclusions of this work.

II. POLARIZATION-RELATED TIME-BIN PHASE CODING MDI-QKD MODEL

In order to quantitatively calculate the polarization, we first need to obtain the relationship between the SOP and the gain of the detectors. This paper gives a method for time-bin phase-coding MDI QKD, the abridged general view of which is presented in Fig. 1, while the analytical method is inspired by Ref. [42]. In this system, the pulses from the lasers are coded at Alice and Bob into two time bins, $l_{a(b)}$ and $s_{a(b)}$, and all concrete coding devices on each side are abstracted into one modulator on each side. After the weak-coherent-state sources emit the weak-coherent-states $\left|e^{i\phi_a}\sqrt{\mu_a}\right\rangle_a$ and $\left|e^{i\phi_b}\sqrt{\mu_b}\right\rangle_b$ with phases ϕ_a and ϕ_b

TABLE II. The correspondence between the parameters and the codes in MDI QKD.

	Z		X	
	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
ξ_a	0	$\frac{\pi}{2}$	$\frac{\pi}{4}$	$\frac{\pi}{4}$
ξ_b	0	$\frac{\pi}{2}$	$\frac{\pi}{4}$	$\frac{\pi}{4}$
θ_a			0	π
θ_b			0	π

and average photon numbers μ_a and μ_b, the modulators encode them into

$$\begin{aligned}&\left|e^{i\phi_a}\cos(\xi_a)\sqrt{\mu_a}\right\rangle_{l_a}\left|e^{i(\phi_a+\theta_a)}\sin(\xi_a)\sqrt{\mu_a}\right\rangle_{s_a}\\&\left|e^{i\phi_b}\cos(\xi_b)\sqrt{\mu_b}\right\rangle_{l_b}\left|e^{i(\phi_b+\theta_b)}\sin(\xi_b)\sqrt{\mu_b}\right\rangle_{s_b},\end{aligned}\tag{1}$$

where θ_a and θ_b are the values of the relative phases encoded between the s modes $s_{a(b)}$ and the l modes $l_{a(b)}$, and ξ_a and ξ_b are the distribution of the light intensity between the l modes and the s modes, which determines whether to send the Z basis or X-Y basis and the codes of the Z basis. The correspondence between these variables and codes is shown in Table II. The coded pulses will then reach the untrusted node Charlie for measurement. After they interfere at the beam splitter (BS), there will be four modes, l_c, l_d, s_c, and s_d, that can be detected. For simplicity, we consider the events which are projected to the Bell state Ψ^- to generate key.

After the pulses are transmitted through the fiber channels to Charlie, the weakly coherent pulses from Alice and Bob are attenuated by η_a and η_b, respectively, and their SOPs evolve into $\alpha_a|H\rangle+\beta_a|V\rangle$ and $\alpha_b|H\rangle+\beta_b|V\rangle$. Then, the gain D_i of a mode for a single detector can be calculated as

$$D_i=\frac{1}{4\pi^2}\int_{-\pi}^{\pi}\int_{-\pi}^{\pi}1-(1-P_d)\exp\left(-\eta_d|\Psi_i|^2\right)\mathrm{d}\phi_a\mathrm{d}\phi_b,\tag{2}$$

where subscript $i=1,2,3,4$ corresponds to the gains of l_c, l_d, s_c, and s_d, respectively, P_d is the dark-count rate, η_d is the detection efficiency of the detectors, and $|\Psi_i|^2$ is the intensity in mode i after the interference of the pulses from Alice and Bob. The coincident gains Q_{ij} of two detectors can be calculated as

$$\begin{aligned}Q_{ij}&=\frac{1}{4\pi^2}\int_{-\pi}^{\pi}\int_{-\pi}^{\pi}[1-(1-P_d)\exp\left(-\eta_d|\Psi_i|^2\right)][1-(1-P_d)\exp\left(-\eta_d|\Psi_j|^2\right)]\mathrm{d}\phi_a\mathrm{d}\phi_b\\&=D_i+D_j-1+\frac{1}{4\pi^2}\int_{-\pi}^{\pi}\int_{-\pi}^{\pi}(1-P_d)^2\exp\left[-\eta_d(|\Psi_i|^2+|\Psi_j|^2)\right]\mathrm{d}\phi_a\mathrm{d}\phi_b,\end{aligned}\tag{3}$$

where subscript ij denotes the coincident gains $ll, ls, \ldots$, which are short for $l_cl_d, l_cs_d, \ldots$. Then, the $|\Psi_i|^2$ values mentioned above are

$$\begin{aligned}|\Psi_1|^2&=A'^2\cos(\xi_a)^2+B'^2\cos(\xi_b)^2+2A'B'\cos(\xi_a)\cos(\xi_b)\times[\kappa_1\sin(\phi_a-\phi_b)+\kappa_2\cos(\phi_a-\phi_b)],\\|\Psi_2|^2&=A'^2\cos(\xi_a)^2+B'^2\cos(\xi_b)^2-2A'B'\cos(\xi_a)\cos(\xi_b)[\kappa_1\sin(\phi_a-\phi_b)+\kappa_2\cos(\phi_a-\phi_b)],\\|\Psi_3|^2&=A'^2\sin(\xi_a)^2+B'^2\sin(\xi_b)^2+2A'B'\sin(\xi_a)\sin(\xi_b)[\kappa_1\sin(\phi_a-\phi_b+\theta_a-\theta_b)+\kappa_2\cos(\phi_a-\phi_b+\theta_a-\theta_b)],\\|\Psi_4|^2&=A'^2\sin(\xi_a)^2+B'^2\sin(\xi_b)^2-2A'B'\sin(\xi_a)\sin(\xi_b)[\kappa_1\sin(\phi_a-\phi_b+\theta_a-\theta_b)+\kappa_2\cos(\phi_a-\phi_b+\theta_a-\theta_b)],\end{aligned}\tag{4}$$

where $A'=\sqrt{\mu_a\eta_a/2}$ and $B'=\sqrt{\mu_b\eta_b/2}$, μ_a and μ_b are the average photon numbers of the weak-coherent-states of Alice and Bob, η_a and η_b are the attenuations of the fibers, $\xi_{a(b)}$ and $\theta_{a(b)}$ are the coding parameters shown in Table II, $\phi_{a(b)}$ is the phase of the photon, $\varepsilon_1=\arg(\alpha_a)-\arg(\alpha_b)$, $\varepsilon_2=\arg(\beta_a)-\arg(\beta_b)$, $\kappa_1=|\alpha_a||\alpha_b|\cos\varepsilon_1+|\beta_a||\beta_b|\cos\varepsilon_2$, and $\kappa_2=|\alpha_a||\alpha_b|\sin\varepsilon_1+|\beta_a||\beta_b|\sin\varepsilon_2$. The detailed calculations of the above are shown in Appendix A.

For example, we can calculate the gain of the detector that detects the l model on routes c and d:

$$\begin{aligned}D_{1(2)}&=\frac{1}{4\pi^2}\int_{-\pi}^{\pi}\int_{-\pi}^{\pi}1-(1-P_d)\\&\quad\exp\left(-\eta_d|\Psi_{1(2)}|^2\right)\mathrm{d}\phi_a\mathrm{d}\phi_b\\&=1-(1-P_d)\mathrm{e}^{-A^2\cos(\xi_a)^2-B^2\cos(\xi_b)^2}\mathrm{I}_0\\&\quad\times(2AB\cos(\xi_a)\cos(\xi_b)\sqrt{\kappa_1^2+\kappa_2^2}),\end{aligned}\tag{5}$$

where $\mathrm{I}_0(x)$ is the modified Bessel function of the first kind of zeroth order, $A=\sqrt{\mu_a\eta_a\eta_d/2}$, and $B=\sqrt{\mu_b\eta_b\eta_d/2}$.

For the coincident gains of the detectors on routes c and d that detect the l models, we have

$$\begin{aligned}Q_{12}&=D_1+D_2-1+\frac{1}{4\pi^2}\int_{-\pi}^{\pi}\int_{-\pi}^{\pi}(1-P_d)^2\\&\quad\times\exp\left[-\eta_d(|\Psi_1|^2+|\Psi_2|^2)\right]\mathrm{d}\phi_a\mathrm{d}\phi_b\end{aligned}$$

$$= 1 + [(1 - P_d)e^{-A^2\cos(\xi_a)^2 - B^2\cos(\xi_b)^2}]^2 - 2(1 - P_d)e^{-A^2\cos(\xi_a)^2 - B^2\cos(\xi_b)^2} \times I_0(2AB\cos(\xi_a)\cos(\xi_b)\sqrt{\kappa_1^2 + \kappa_2^2}). \quad (6)$$

In the same way, we can obtain other gains and coincident gains with formats similar to Eqs. (5) and (6). We can clearly note that the SOP only affects the gains and coincident-gains rate in one term, $\kappa_1^2 + \kappa_2^2$. Furthermore, $I_0(x)$ is monotone for $x > 0$, which proves that one $\kappa_1^2 + \kappa_2^2$ only corresponds to one gain or coincident gain.

By the definitions of κ_1, κ_2, ε_1, and ε_2, we have

$$\begin{aligned}\kappa_1^2 + \kappa_2^2 &= |\alpha_a|^2|\alpha_b|^2 + |\beta_a|^2|\beta_b|^2 \\ &\quad + 2|\alpha_a||\alpha_b||\beta_a||\beta_b|\cos(\varepsilon_1 - \varepsilon_2) \\ &= \left|\begin{pmatrix}\alpha_a^* & \beta_a^*\end{pmatrix}\begin{pmatrix}\alpha_b \\ \beta_b\end{pmatrix}\right|^2 \\ &= |p_a^\dagger p_b|^2, \end{aligned} \quad (7)$$

where $p_{a(b)} = (\alpha_{a(b)}\ \beta_{a(b)})^T$ is the Jones matrix for the SOP $\alpha_{a(b)}|H\rangle + \beta_{a(b)}|V\rangle$. This is the only term in which the SOP affects the gains and coincident gains. Just to simplify, we define $\delta = \kappa_1^2 + \kappa_2^2$ and substitute δ for $\kappa_1^2 + \kappa_2^2$ in the following passage.

III. POLARIZATION-ALIGNMENT METHOD

As we are treating the SOP in terms of the Jones matrix, the conversion of the SOP can be treated as a 2×2 unitary matrix U and the SOP can be written as a 2×1 column vector. The influence of fiber on both sides can be written as U_{Alice} and U_{Bob} and our active operation of the SOP can be denoted as U_b, for we only need one of Alice and Bob to run our polarization-alignment method—we might let Bob run it. δ can be written as

$$\delta = \left|p_a^\dagger U_{\text{Alice}}^\dagger U_{\text{Bob}} U_b p_b\right|^2, \quad (8)$$

where p_a and $U_b p_b$ are the SOPs of the pulses that have just been emitted from Alice and Bob, while $U_{\text{Alice}} p_a$ and $U_{\text{Bob}} U_b p_b$ are the SOPs of the same pulses when they reach Charlie. Our polarization-alignment method will determine a proper U_b that makes $\delta = 1$, which means that the SOPs of the pulses from Alice and Bob are the same as those from Charlie.

The polarization on the coding side is stable and controllable, so we can assume that $p_a = p_b = (1\,0)^T$ and that δ can be written as

$$\delta = \left|(U_{\text{channel}} U_{\text{COR}} U_i)_{(1,1)}\right|^2, \quad (9)$$

where the subscript $(1, 1)$ refers to the value of the first column in the first row of the matrix, $U_{\text{channel}} = U_{\text{Alice}}^\dagger U_{\text{Bob}}$, $U_{\text{COR}} U_i = U_b$, and the division of U_b into U_{COR} and U_i is intended to distinguish a repeated operation U_i and corrective operation U_{COR} in each round for easier description in subsequent analyses.

As is known, a unitary matrix can be written as

$$U_{\text{channel}} = e^{i\varpi}\begin{pmatrix}1 & 0 \\ 0 & e^{i\psi}\end{pmatrix}\begin{pmatrix}\cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta)\end{pmatrix}\begin{pmatrix}1 & 0 \\ 0 & e^{i\varphi}\end{pmatrix}. \quad (10)$$

Therefore, of the four degrees of freedom ϖ, ψ, θ, and φ in U_{channel}, we only need to know θ and φ to compute U_{COR}, which meets $\left|(U_{\text{channel}} U_{\text{COR}} U_i)_{(1,1)}\right|^2 = 1$ when $U_i = I$. Then, if we can calculate δ from each measurement result, we can obtain the value of θ and φ by changing U_i to obtain the equations. Moreover, we define an observable quantity

$$V_{ij} = \frac{Q_{ij}}{D_i D_j} = N \cdot \frac{N_{ij}}{N_i N_j}, \quad (11)$$

where N is the total number of pulses sent by Alice and Bob, N_i is the count number of model i, N_{ij} is the coincidence-count number of the models i and j, and subscript $i, j = 1, 2, 3, 4$ corresponds to the model lc, ld, sc, sd. Then, given the relation between V_{ij} and δ, we can calculate the SOP with the observable quantities N_{ij}, N_i, and N_j. In this paper, we use the relation between V_{12} and δ. With Eqs. (5) and (6), if we only choose the X basis, according to the discussion in Appendix C, we have

$$V_{12} = \frac{1 - 2CI_0(AB\sqrt{\delta}) + C^2}{1 - 2CI_0(AB\sqrt{\delta}) + [CI_0(AB\sqrt{\delta})]^2}, \quad (12)$$

where $A = \sqrt{\mu_a \eta_a \eta_d/2}$, $B = \sqrt{\mu_b \eta_b \eta_d/2}$, and $C = (1 - P_d)e^{-A^2+B^2/2}$. Therefore, if we know the value of V_{12}, we can calculate the value of δ and then determine the value of U_{COR} to make $\delta = 1$ by changing several of the U_i.

According to the discussion in Appendix B, we see that the basis-choosing-probability P_X has no significant effect on the shape of the SOP-V_{12} curve but does affect its position. Thus, we analyze the case of all Alice and Bob choosing the X basis, and the analysis is similar for other P_X. Also, we do not ask which qubits they have chosen. We use δ_i to tag the result calculated by the ith measurement. Below, we will give the specific method.

Before describing the steps, two proper U_i values are given as

$$U_1 = \frac{\sqrt{2}}{2}\begin{pmatrix}1 & -1 \\ 1 & 1\end{pmatrix}, \quad U_2 = \frac{\sqrt{2}}{2}\begin{pmatrix}1 & i \\ i & 1\end{pmatrix}. \quad (13)$$

The three steps are as follows:

1. Keep $U_b = U'_{\mathrm{COR}}$, where U'_{COR} is the U_{COR} that is calculated in step 3 in the result of the last round of our polarization-alignment method, and the initial value of U_{COR} can be chosen as I. Continuously monitor the value of V_{12} until it exceeds the threshold V_{th}. Then calculate the value of δ_1 and carry out the next step, where $\delta_1 = \cos(\theta)^2$ with $\theta \in [0, \pi/2]$. The purpose of this step is to monitor the system and it requires no action.

2. Change U_i from I to U_1 and then measure the value of V to calculate the value of δ_2, where $\delta_2 = (1 + 2\cos(\theta)\sin(\theta)\cos(\varphi))/2$. For $\varphi \in [0, 2\pi]$, it is necessary to calculate $\sin(\varphi)$ to figure out φ.

3. Change U_i from U_1 to U_2 and then measure the value of V to calculate the value of δ_3, where $\delta_3 = (1 - 2\cos(\theta)\sin(\theta)\sin(\varphi))/2$. We can state that

$$U_{\mathrm{COR}} = U'_{\mathrm{COR}} \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{-\mathrm{i}\varphi} \end{pmatrix} \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}, \quad (14)$$

where

$$\theta = \arccos\left(\sqrt{\delta_1}\right), \qquad \theta \in \left[0, \frac{\pi}{2}\right], \quad (15)$$

and

$$\varphi = \begin{cases} \arcsin\left(\frac{1-2\delta_3}{2\sqrt{\delta_1}\sqrt{1-\delta_1}}\right), & |1-2\delta_3| < 2\delta_2 - 1, \\ \arccos\left(\frac{2\delta_2-1}{2\sqrt{\delta_1}\sqrt{1-\delta_1}}\right), & |2\delta_2 - 1| < 1 - 2\delta_3, \\ \pi - \arcsin\left(\frac{1-2\delta_3}{2\sqrt{\delta_1}\sqrt{1-\delta_1}}\right), & |1-2\delta_3| < 1 - 2\delta_2, \\ 2\pi - \arccos\left(\frac{2\delta_2-1}{2\sqrt{\delta_1}\sqrt{1-\delta_1}}\right), & |2\delta_2 - 1| < 2\delta_3 - 1. \end{cases} \quad (16)$$

Then change U_i into I, which means that $U_b = U_{\mathrm{COR}}$. This makes $\left|(U_{\mathrm{channel}} U_{\mathrm{COR}} U_i)_{1,1}\right|^2 = 1$, which means that the polarization of Alice and Bob changes in the same direction. Then go back into step 1.

For the choice of threshold V_{th}, as we know that $2E = V$ in Appendix C, if we need a threshold of the QBER called E_{th}, then $V_{th} = 2E_{th}$.

IV. PRECISION OF THE METHOD

If the number of pulses used in each step is infinite, we can calculate the polarization exactly. However, there are deviations between the measured and true values due to the nonasymptotic case.

To calculate the relation between the accuracy of the method and the finite length of the number of pulses, first, we should calculate the relationship between the accuracy of U_{COR} and the length of the number of pulses, where U_{COR} is the unitary matrix that the EPC should perform to align the SOP mentioned in Sec. III. Then, as we have calculated the relationship between the QBER and the SOP in Appendix C, by combining with Eqs. (9) and (14), we can calculate how the length of the number of pulses affects the accuracy of the method, which is shown as the accuracy of the QBER after our polarization-alignment method. The specific calculation process is shown in Appendix D, and, finally, we can calculate that the polarization-alignment method makes the accuracy $\sigma_{E_{\mathrm{fin}}}$ of the corrected QBER meet

$$\sigma^2_{E_{\mathrm{fin}}} < \frac{(1-\beta)^2}{16\alpha^2}\left(\frac{(3+\sqrt{2}\alpha)^2}{1-\sqrt{2}\alpha}\frac{1}{N_{12}^{2(3)}} + \frac{(1-2\beta)^2(2-\beta)^2}{\alpha^2\beta}\frac{1}{N_{12}^{1}}\right), \quad (17)$$

where $\beta = 2 - 4E_{th}$, $\alpha = \sqrt{(4E_{th}-1)(2-4E_{th})}$, E_{th} is the threshold of the QBER set by how much we need, E_{fin} is the QBER after the polarization-alignment method, N_{12}^{i} is the coincidence-count number of step i of our method.

For step 1 of our method, we do not change the system—it can run for as long as possible. We use $n = N_{12}^{1}/N_{12}^{2(3)}$ to quantify how much longer step 1 can run than step 2 (step 3). In order to prolong the execution time of QKD, n should be as large as possible. This is because the first step is a monitoring step, which does not affect the system or consume the key. The relationship between $N_{12}^{2(3)}$ and $\sigma_{E_{\mathrm{fin}}}$ is shown in Fig. 2.

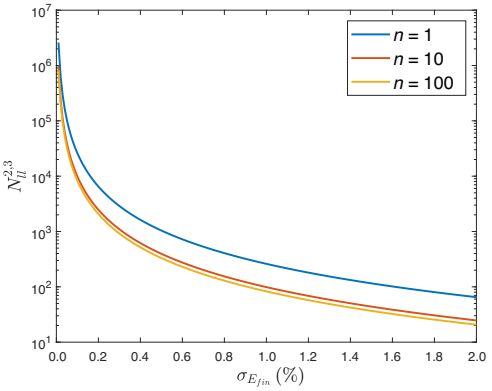

FIG. 2. The relationship between $N_{12}^{2(3)}$ and $\sigma_{E_{\mathrm{fin}}}$, with different n chosen. E_{fin}, the QBER after the polarization-alignment method; $\sigma_{E_{\mathrm{fin}}}$, the precision of E_{fin}; $N_{12}^{2(3)}$, the coincidence-count number of step 2 (step 3) of our method; n, the ratio of the count of the monitoring step to the count of the modulation step.

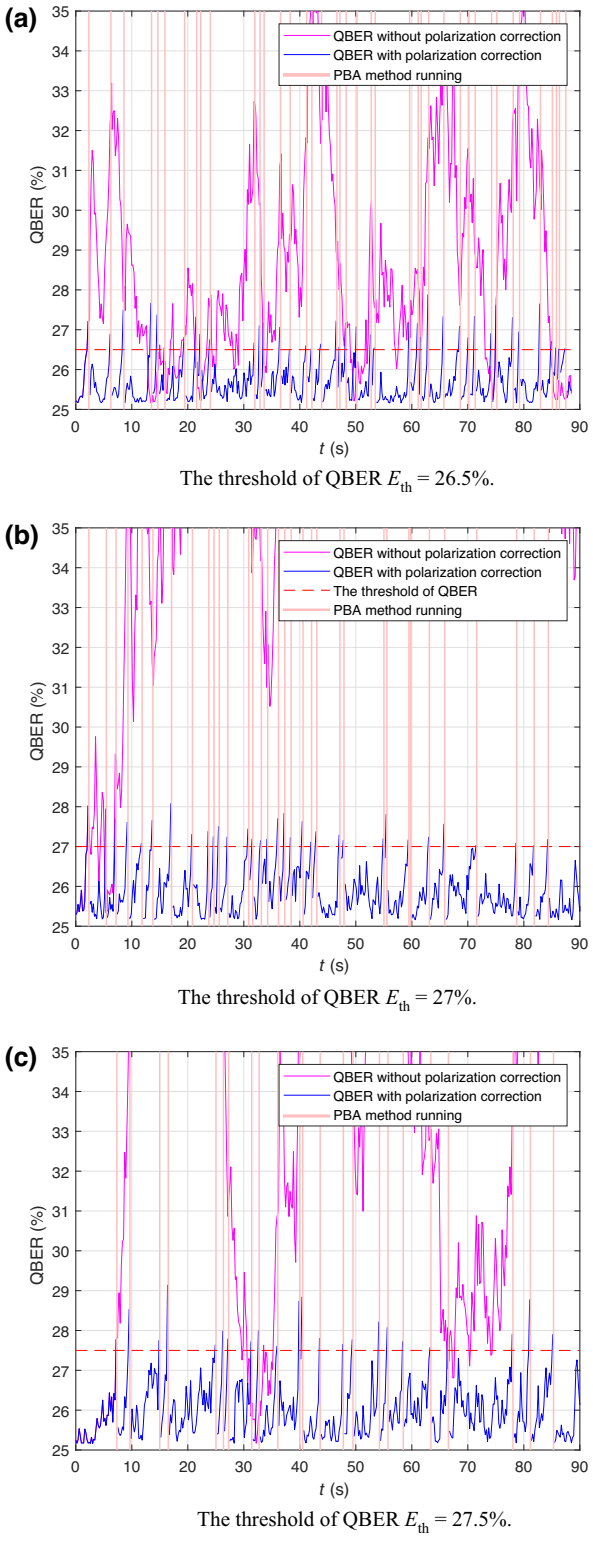

FIG. 3. Examples of our polarization-alignment method, with the polarization linewidth $\Delta_p = 3 \times 10^{-2}$. The threshold of the QBER, E_{th}, is as follows: (a) 26.5%, (b) 27%, and (c) 27.5%.

Thus, we can see that for a proper $\sigma_{E_{\text{fin}}}$, such as 0.5%, we only need $N_{12}^{2(3)} = 500$, which is a small cost in megahertz-gigahertz MDI-QKD systems.

V. SIMULATION OF OUR METHOD

We perform a numerical simulation, to simulate how our method affects the system. We assume that our MDI system runs at 100 MHz, the length of the channel $l =$ 100 km, the fiber-attenuation coefficient $\alpha = 0.2$ dB/km, the average number of photons per pulse of source $\mu =$ 0.6, the detection efficiency $\eta_d = 40\%$, and the dark-count rate $P_d = 3 \times 10^{-6}$ [43]. We also use the polarization line width, Δ_p, to quantify the speed of the polarization drift [44]. In our simulation, we give $\Delta_p = 3 \times 10^{-2}$, because the duration of the key distribution procedure is about 3 s for buried fibers that run between cities [45].

For our method, we choose the threshold values $V_{th} =$ 0.53, 0.54, and 0.55, which means that we can keep the QBER of the X basis of the system lower than 26.5%, 27%, and 27.5%. For steps 2 and 3, we use $N_{12}^{2(3)} =$ 500, which means that we will use 500 coincident gains in these steps. We use 0.2 s as the period in which to accumulate data to monitor V, which is also the data size that we use in step 1.

Thus, Fig. 3 shows examples of our polarization-alignment method, where Figs. 3(a)–3(c) are selected for the different thresholds of the QBER mentioned above. The pink areas are the times for which our polarization-alignment method runs: although our method does not stop key distribution, the running of polarization alignment will cause a random rise in the QBER. Although it only has a small impact on the average QBER, we will discard it in the interest of better system performance. As we can see, the QBER is kept in the set threshold if our method runs, and if we do not run the method, most times the QBER will be larger than the set threshold. For the time during which the method is in use, in the example shown in Fig. 3(b), which chooses $E_{th} = 27\%$, the system runs for 90 s and our method uses 5.7 s in total to correct the polarization, which means that we only use about 6.3% of the total MDI-protocol running time to correct the polarization, with the length of the channel being $l = 100$ km and the polarization line width being $\Delta_p = 3 \times 10^{-2}$. Then, if we increase or decrease the threshold, the time taken by the method will also increase or decrease, because the lower the threshold, the more times the polarization alignment method will work per unit time. This can be seen in Figs. 3(a) and 3(c), where thresholds of 26.5% and 27.5%, respectively, are chosen, which makes the percentages of the occupied times 7.7% and 4.3%.

VI. DISCUSSION AND CONCLUSIONS

We have proposed a polarization-alignment method that eliminates the effect of birefringence on time-bin phase-coding MDI QKD in fiber. The method uses the count number and the coincidence-count number as the criteria and directly calculates the Jones matrix that the EPC should execute. We have shown that by selecting the

criteria mentioned in this paper, an accurate polarization-alignment operation can be found after three iterations. Moreover, the accuracy of the method can be guaranteed. We have calculated the amount of data required for the method to achieve the predicted accuracy and found that the method is still efficient for the X basis of MDI QKD. Compared with the previous methods, our method is more adaptable when the QBER is high and more efficient because it is fast, does not consume qubit data, and does not introduce any additional photon loss. With these advantages, our method can more effectively eliminate the birefringence effect on the MDI-QKD systems. Furthermore, although we have used time-bin phase-coding MDI QKD as an example in this paper, with similar analysis and construction methods, this method can be extended to other protocols that need to measure the interference results at the untrusted node.

MDI QKD is an ideal candidate for the untrusted-node-based network. With our method, MDI-QKD systems can work without barriers due to the birefringence effect between cities, which means that the construction of MDI-QKD networks should become more feasible. Our high-efficiency polarization-alignment method hopefully paves the way for large-scale and field applications of MDI-QKD networks.

ACKNOWLEDGMENTS

This work was supported by the Fundamental Research Funds for the Central Universities, the National Natural Science Foundation of China (Grant No. 62105318, 62271463, 62171424, 62301524), the China Postdoctoral Science Foundation (Grant No. 2021M693098, 2022M723064), and the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300700).

APPENDIX A: CALCULATION OF GAINS AND COINCIDENT GAINS OF DETECTORS WITH THE SOP

Here, we employ the method to calculate the response rate that is proposed in Ref. [42]. As is known, for a coherent state with polarization $\alpha\,|H\rangle + \beta\,|V\rangle$, it can be written as

$$\left|\alpha\sqrt{\mu}\right\rangle_H \left|\beta\sqrt{\mu}\right\rangle_V, \tag{A1}$$

where μ is the average number of photons of the coherent state and α and β are the coefficients of the SOP, with $|\alpha|^2 + |\beta|^2 = 1$.

The time-bin phase-coding MDI QKD is shown in Fig. 1. To analyze the system, we must mark four checkpoints, which are shown in Fig. 4:

1. *Checkpoint 1*. It is considered that both pulses on both sides have been attenuated and phase randomized and that the SOPs of Alice and Bob are in the H direction. In order to make the analysis clear, we first analyze the pure states with different random phases and then integrate them. And for the attenuation of the pulses, although in reality we attenuate the pulse before it enters the quantum channel, for simplicity, we do it first in our discussion. These operations will not affect the result. Therefore, we analyze in the pure state

$$\left|\mathrm{e}^{\mathrm{i}\phi_a}\sqrt{\mu_a}\right\rangle_{a^H} \left|\mathrm{e}^{\mathrm{i}\phi_b}\sqrt{\mu_b}\right\rangle_{b^H}. \tag{A2}$$

2. *Checkpoint 2*. After the modulation device, the quantum state becomes

$$\begin{aligned}&\left|e^{i\phi_a}\cos(\xi_a)\sqrt{\mu_a}\right\rangle_{a_l^H} \left|e^{i(\phi_a+\theta_a)}\sin(\xi_a)\sqrt{\mu_a}\right\rangle_{a_s^H},\\ &\left|e^{i\phi_b}\cos(\xi_b)\sqrt{\mu_b}\right\rangle_{b_l^H} \left|e^{i(\phi_b+\theta_b)}\sin(\xi_b)\sqrt{\mu_b}\right\rangle_{b_s^H},\end{aligned} \tag{A3}$$

where subscript a_l^H refers to the l mode with H polarization, which belongs to Alice, and the other subscripts are similar, θ_a and θ_b are the values of the additional phase encoded on the short arm, and ξ_a and ξ_b are the distribution of the light intensity between the long and short arms, which determines whether to send Z basis or X-Y basis and codes of the Z basis. The correspondence between these variables and codes is shown in Table II.

3. *Checkpoint 3*. After transmission through the fiber channel, there are two effects: the first is the attenuation of the fiber, denoted as η_a, η_b; the second is the change of the SOP. Under the representation of H and V, the SOPs of two paths of coherent states are transformed into $\alpha_a\,|H\rangle + \beta_a\,|V\rangle$ and $\alpha_b\,|H\rangle + \beta_b\,|V\rangle$. The quantum state can then be written as

$$\begin{aligned}&\left|\alpha_a e^{i\phi_a}\cos(\xi_a)\sqrt{\mu_a\eta_a}\right\rangle_{a_l^H} \left|\alpha_a e^{i(\phi_a+\theta_a)}\sin(\xi_a)\sqrt{\mu_a\eta_a}\right\rangle_{a_s^H}\\ &\left|\alpha_b e^{i\phi_b}\cos(\xi_b)\sqrt{\mu_b\eta_b}\right\rangle_{b_l^H} \left|\alpha_b e^{i(\phi_b+\theta_b)}\sin(\xi_b)\sqrt{\mu_b\eta_b}\right\rangle_{b_s^H}\\ &\left|\beta_a e^{i\phi_a}\cos(\xi_a)\sqrt{\mu_a\eta_a}\right\rangle_{a_l^V} \left|\beta_a e^{i(\phi_a+\theta_a)}\sin(\xi_a)\sqrt{\mu_a\eta_a}\right\rangle_{a_s^V}\\ &\left|\beta_b e^{i\phi_b}\cos(\xi_b)\sqrt{\mu_b\eta_b}\right\rangle_{b_l^V} \left|\beta_b e^{i(\phi_b+\theta_b)}\sin(\xi_b)\sqrt{\mu_b\eta_b}\right\rangle_{b_s^V}.\end{aligned} \tag{A4}$$

It is worth noting that there is no loss due to the EPC, because the EPC is in the trusted channel on the Bob (Alice) side and any loss can be compensated. In other words, the EPC only coforms the above-mentioned channel with the untrusted channel from Bob (Alice) to Charlie but the loss caused by it can be ignored.

4. *Checkpoint 4*. After passing through the beam splitter, the state can be written as

$$\begin{aligned}&|\Psi_{11}\rangle_{c_l^H}\,|\Psi_{21}\rangle_{d_l^H}\,|\Psi_{31}\rangle_{c_s^H}\,|\Psi_{41}\rangle_{d_s^H}\\ &|\Psi_{12}\rangle_{c_l^V}\,|\Psi_{22}\rangle_{d_l^V}\,|\Psi_{32}\rangle_{c_s^V}\,|\Psi_{42}\rangle_{d_s^V},\end{aligned} \tag{A5}$$

$$
\begin{aligned}
|\Psi_{11}\rangle_{c_l^H} &= \left|\alpha_a e^{i\phi_a}\cos(\xi_a)\sqrt{\frac{\mu_a\eta_a}{2}} + i\alpha_b e^{i\phi_b}\cos(\xi_b)\sqrt{\frac{\mu_b\eta_b}{2}}\right\rangle_{c_l^H},\\
|\Psi_{21}\rangle_{d_l^H} &= \left|i\alpha_a e^{i\phi_a}\cos(\xi_a)\sqrt{\frac{\mu_a\eta_a}{2}} + \alpha_b e^{i\phi_b}\cos(\xi_b)\sqrt{\frac{\mu_b\eta_b}{2}}\right\rangle_{d_l^H},\\
|\Psi_{31}\rangle_{c_s^H} &= \left|\alpha_a e^{i(\phi_a+\theta_a)}\sin(\xi_a)\sqrt{\frac{\mu_a\eta_a}{2}} + i\alpha_b e^{i(\phi_b+\theta_b)}\sin(\xi_b)\sqrt{\frac{\mu_b\eta_b}{2}}\right\rangle_{c_s^H},\\
|\Psi_{41}\rangle_{d_s^H} &= \left|i\alpha_a e^{i(\phi_a+\theta_a)}\sin(\xi_a)\sqrt{\frac{\mu_a\eta_a}{2}} + \alpha_b e^{i(\phi_b+\theta_b)}\sin(\xi_b)\sqrt{\frac{\mu_b\eta_b}{2}}\right\rangle_{d_s^H},\\
|\Psi_{12}\rangle_{c_l^V} &= \left|\beta_a e^{i\phi_a}\cos(\xi_a)\sqrt{\frac{\mu_a\eta_a}{2}} + i\beta_b e^{i\phi_b}\cos(\xi_b)\sqrt{\frac{\mu_b\eta_b}{2}}\right\rangle_{c_l^V},\\
|\Psi_{22}\rangle_{d_l^V} &= \left|i\beta_a e^{i\phi_a}\cos(\xi_a)\sqrt{\frac{\mu_a\eta_a}{2}} + \beta_b e^{i\phi_b}\cos(\xi_b)\sqrt{\frac{\mu_b\eta_b}{2}}\right\rangle_{d_l^V},\\
|\Psi_{32}\rangle_{c_s^V} &= \left|\beta_a e^{i(\phi_a+\theta_a)}\sin(\xi_a)\sqrt{\frac{\mu_a\eta_a}{2}} + i\beta_b e^{i(\phi_b+\theta_b)}\sin(\xi_b)\sqrt{\frac{\mu_b\eta_b}{2}}\right\rangle_{c_s^V},\\
|\Psi_{42}\rangle_{d_s^V} &= \left|i\beta_a e^{i(\phi_a+\theta_a)}\sin(\xi_a)\sqrt{\frac{\mu_a\eta_a}{2}} + \beta_b e^{i(\phi_b+\theta_b)}\sin(\xi_b)\sqrt{\frac{\mu_b\eta_b}{2}}\right\rangle_{d_s^V}.
\end{aligned}
\tag{A6}
$$

Because the detector cannot resolve the SOP, the state changes into

$$
|\Psi_1\rangle_{lc}\,|\Psi_2\rangle_{ld}\,|\Psi_3\rangle_{sc}\,|\Psi_4\rangle_{sd}\,, \tag{A7}
$$

where $|\Psi_i\rangle = |\Psi_{i1}\rangle\,|\Psi_{i2}\rangle$ and

$$
|\Psi_i|^2 = |\Psi_{i1}|^2 + |\Psi_{i2}|^2, \tag{A8}
$$

and the $|\Psi_i|^2$ are the light intensities of the different modes.

Then, for convenience, defining $A' = \sqrt{\mu_a\eta_a/2}$, $B' = \sqrt{\mu_b\eta_b/2}$, $\varepsilon_1 = \arg(\alpha_a) - \arg(\alpha_b)$, $\varepsilon_2 = \arg(\beta_a) - \arg(\beta_b)$, $\kappa_1 = |\alpha_a||\alpha_b|\cos\varepsilon_1 + |\beta_a||\beta_b|\cos\varepsilon_2$, and $\kappa_2 = |\alpha_a||\alpha_b|\sin\varepsilon_1 + |\beta_a||\beta_b|\sin\varepsilon_2$, we can calculate that

$$
\begin{aligned}
|\Psi_1|^2 &= A'^2\cos(\xi_a)^2 + B'^2\cos(\xi_b)^2 + 2A'B'\cos(\xi_a)\cos(\xi_b)\\
&\quad\times[\kappa_1\sin(\phi_a-\phi_b) + \kappa_2\cos(\phi_a-\phi_b)],\\
|\Psi_2|^2 &= A'^2\cos(\xi_a)^2 + B'^2\cos(\xi_b)^2 - 2A'B'\cos(\xi_a)\cos(\xi_b)\\
&\quad\times[\kappa_1\sin(\phi_a-\phi_b) + \kappa_2\cos(\phi_a-\phi_b)],\\
|\Psi_3|^2 &= A'^2\sin(\xi_a)^2 + B'^2\sin(\xi_b)^2 + 2A'B'\sin(\xi_a)\sin(\xi_b)\\
&\quad\times[\kappa_1\sin(\phi_a-\phi_b+\theta_a-\theta_b)\\
&\quad+\kappa_2\cos(\phi_a-\phi_b+\theta_a-\theta_b)],\\
|\Psi_4|^2 &= A'^2\sin(\xi_a)^2 + B'^2\sin(\xi_b)^2 - 2A'B'\sin(\xi_a)\sin(\xi_b)\\
&\quad\times[\kappa_1\sin(\phi_a-\phi_b+\theta_a-\theta_b)\\
&\quad+\kappa_2\cos(\phi_a-\phi_b+\theta_a-\theta_b)].
\end{aligned}
\tag{A9}
$$

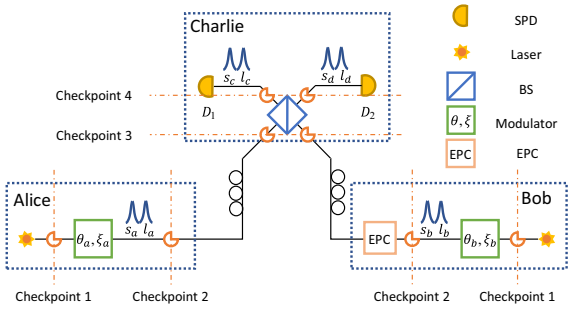

FIG. 4. The time-bin phase coding MDI-QKD system that we use in this paper, with four checkpoints marked.

As is known, the detector response rate is [46]

$$
p = 1 - (1 - P_d)\exp\left(-\eta_d|\Psi|^2\right), \tag{A10}
$$

where P_d is dark-count rate and η_d is the detection efficiency of the detectors; hence we can calculate the gain of each detector.

Finally, the gain of a mode for a single detector can be calculated as

$$
D_i = \frac{1}{4\pi^2}\int_{-\pi}^{\pi}\int_{-\pi}^{\pi} 1 - (1 - P_d)\exp\left(-\eta_d|\Psi_i|^2\right)d\phi_a d\phi_b, \tag{A11}
$$

where the subscript $i = 1, 2, 3, 4$ corresponds to the gains of l_c, l_d, s_c, and s_d, and the coincident gains of two detectors can be calculated as

$$\begin{aligned} Q_{ij} &= \frac{1}{4\pi^2}\int_{-\pi}^{\pi}\int_{-\pi}^{\pi}[1-(1-P_d)\exp\left(-\eta_d|\Psi_i|^2\right)] \\ &\quad [1-(1-P_d)\exp\left(-\eta_d|\Psi_j|^2\right)]\mathrm{d}\phi_a\mathrm{d}\phi_b \\ &= D_i + D_j - 1 + \frac{1}{4\pi^2}\int_{-\pi}^{\pi}\int_{-\pi}^{\pi}(1-P_d)^2 \\ &\quad \times \exp\left[-\eta_d(|\Psi_i|^2+|\Psi_j|^2)\right]\mathrm{d}\phi_a\mathrm{d}\phi_b, \end{aligned} \tag{A12}$$

where subscript $i,j = 1, 2, 3, 4$ corresponds to the coincident gains of l_c, l_d, s_c, and s_d, which can be written as $ll, ls, \ldots$.

APPENDIX B: THE RELATIONSHIP BETWEEN BASIS-CHOOSING-PROBABILITY P_X AND V_{12}

In this appendix, we will calculate the relationship between the SOP and V_{12} and the relationship between basis-choosing-probability P_X and V_{12}. As we have calculated in Sec. II, we have obtained Eqs. (5)–(7) and in view of Table II, this problem will be discussed in the following cases.

First, we consider both Alice and Bob choosing the X basis. From Table II, we know that $\xi_a = \xi_b = \pi/4$. Then, we can calculate

$$\begin{aligned} D_{1(2)}^{XX} &= 1-(1-P_d)\mathrm{e}^{-\frac{A^2}{2}-\frac{B^2}{2}}\mathrm{I}_0(AB|p_a^\dagger p_b|), \\ Q_{12}^{XX} &= 1+\left[(1-P_d)\mathrm{e}^{-\frac{A^2}{2}-\frac{B^2}{2}}\right]^2 \\ &\quad -2(1-P_d)\mathrm{e}^{-\frac{A^2}{2}-\frac{B^2}{2}}\mathrm{I}_0(AB|p_a^\dagger p_b|), \end{aligned} \tag{B1}$$

where the superscript X means choosing the X basis.

Then, we consider Alice and Bob choosing different bases; for example, Alice chooses X and Bob chooses Z. There are two cases:

1. Bob chooses bit 0. Then, we can calculate

$$\begin{aligned} D_{1(2)}^{XZ_0} &= 1-(1-P_d)\mathrm{e}^{-\frac{A^2}{2}-B^2}\mathrm{I}_0(\sqrt{2}AB|p_a^\dagger p_b|), \\ Q_{12}^{XZ_0} &= 1+\left[(1-P_d)\mathrm{e}^{-\frac{A^2}{2}-B^2}\right]^2 \\ &\quad -2(1-P_d)\mathrm{e}^{-\frac{A^2}{2}-B^2}\mathrm{I}_0(\sqrt{2}AB|p_a^\dagger p_b|), \end{aligned} \tag{B2}$$

where the superscript Z_i means choosing bit i of the Z basis.

2. Bob chooses bit 1. Then, we can calculate

$$\begin{aligned} D_{1(2)}^{XZ_1} &= 1-(1-P_d)\mathrm{e}^{-\frac{A^2}{2}}, \\ Q_{12}^{XZ_1} &= 1+[(1-P_d)\mathrm{e}^{-\frac{A^2}{2}}]^2-2(1-P_d)\mathrm{e}^{-\frac{A^2}{2}}. \end{aligned} \tag{B3}$$

Finally, we consider both Alice and Bob choosing the Z basis and there are four cases:

1. Both Alice and Bob choose bit 0:

$$\begin{aligned} D_{1(2)}^{Z_0Z_0} &= 1-(1-P_d)\mathrm{e}^{-A^2-B^2}\mathrm{I}_0(2AB|p_a^\dagger p_b|), \\ Q_{12}^{Z_0Z_0} &= 1+\left[(1-P_d)\mathrm{e}^{-A^2-B^2}\right]^2 \\ &\quad -2(1-P_d)\mathrm{e}^{-A^2-B^2}\mathrm{I}_0(2AB|p_a^\dagger p_b|). \end{aligned} \tag{B4}$$

2. Alice chooses bit 0 and Bob chooses bit 1:

$$\begin{aligned} D_{1(2)}^{Z_0Z_1} &= 1-(1-P_d)\mathrm{e}^{-A^2}, \\ Q_{12}^{Z_0Z_1} &= 1+[(1-P_d)\mathrm{e}^{-A^2}]^2-2(1-P_d)\mathrm{e}^{-A^2}. \end{aligned} \tag{B5}$$

3. Alice chooses bit 1 and Bob chooses bit 0:

$$\begin{aligned} D_{1(2)}^{Z_0Z_1} &= 1-(1-P_d)\mathrm{e}^{-B^2}, \\ Q_{12}^{Z_0Z_1} &= 1+[(1-P_d)\mathrm{e}^{-B^2}]^2-2(1-P_d)\mathrm{e}^{-B^2}. \end{aligned} \tag{B6}$$

4. Both Alice and Bob choose bit 1:

$$\begin{aligned} D_{1(2)}^{Z_0Z_1} &= 1-(1-P_d), \\ Q_{12}^{Z_0Z_1} &= 1+[(1-P_d)]^2-2(1-P_d). \end{aligned} \tag{B7}$$

After the above calculations, according to Eq. (12), under the condition that the probability of choosing the X basis is P_X, we obtain

$$V_{12} = \frac{Q_{12}}{D_1 D_2}, \tag{B8}$$

where

$$\begin{aligned} Q_{12} &= (P_X)^2 Q_{12}^{XX} + 2P_X(1-P_X)\frac{\sum_{i=0,1}Q_{12}^{XZ_i}}{2} \\ &\quad + (1-P_X)^2\frac{\sum_{i,j=0,1}Q_{12}^{Z_iZ_j}}{4} \end{aligned} \tag{B9}$$

and

$$\begin{aligned} D_{1(2)} &= (P_X)^2 D_{1(2)}^{XX} + 2P_X(1-P_X)\frac{\sum_{i=0,1}D_{1(2)}^{XZ_i}}{2} \\ &\quad + (1-P_X)^2\frac{\sum_{i,j=0,1}D_{1(2)}^{Z_iZ_j}}{4}, \end{aligned} \tag{B10}$$

and this is the relationship between P_X, the SOP, and V_{12}.

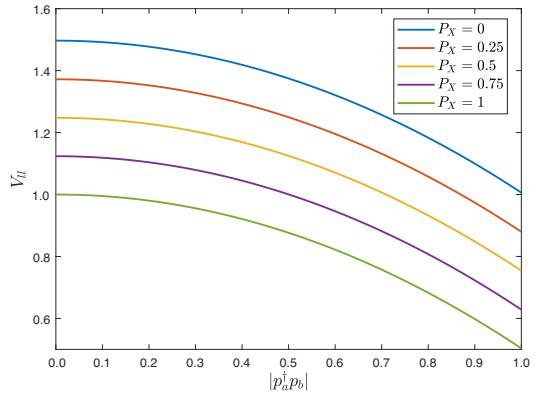

FIG. 5. The relationship between the basis-choosing-probability P_X and V_{12}. Simulation parameters: length of channel $l = 100$ km; fiber-attenuation coefficient $\alpha = 0.2$ dB/km; average number of photons per pulse of source $\mu = 0.6$; detection efficiency $\eta_d = 40\%$; and dark-count rate $P_d = 3 \times 10^{-6}$.

We can see how P_X influences V_{12} in Fig. 5. What we can see is that P_X has no significant effect on the shape of the SOP-V_{12} curve but does affect its position. Thus, we may as well treat all P_X as $P_X = 1$ throughout the whole paper.

APPENDIX C: EFFECT OF POLARIZATION ON THE QBER IN THE X BASIS AND THE RELATIONSHIP BETWEEN IT AND V_{12}

After calculating Eqs. (A9)–(A12), it is possible for us to calculate all gains and coincident gains of all detectors, which means that we can calculate how much the polarization affects the QBER in the X basis. We know that the QBER is [42]

$$E = \frac{Q_{23}|_{\theta_a=\theta_b}}{Q_{23}|_{\theta_a=\theta_b} + Q_{23}|_{\theta_a\neq\theta_b}} \tag{C1}$$

and we have

$$V_{12} = \frac{Q_{12}}{D_1 D_2}. \tag{C2}$$

Given that in view of Table II, in the X basis, $\xi_{a,b} = \pi/4$ and $\theta_{a,b} = 0$ or π, we can calculate that

$$\begin{aligned} D_{1,2,3,4} &= 1 - (1 - P_d)\mathrm{e}^{-\frac{A^2+B^2}{2}}\mathrm{I}_0(AB|p_a^\dagger p_b|), \\ Q_{23}|_{\theta_a=\theta_b} &= 1 - 2(1 - P_d)\mathrm{e}^{-\frac{A^2+B^2}{2}}\mathrm{I}_0(AB|p_a^\dagger p_b|) \\ &\quad + \left[(1 - P_d)\mathrm{e}^{-\frac{A^2+B^2}{2}}\right]^2, \end{aligned}$$

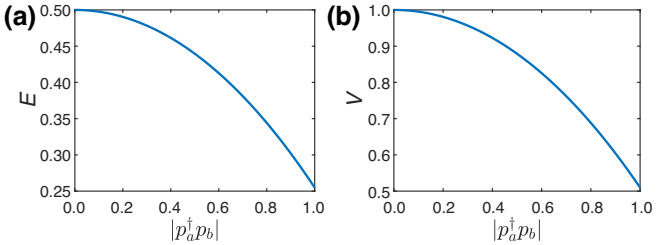

FIG. 6. The effect of the polarization on (a) the QBER and (b) V. Simulation parameters: length of channel $l = 100$ km; fiber-attenuation coefficient $\alpha = 0.2$ dB/km; average number of photons per pulse of source $\mu = 0.6$; detection efficiency $\eta_d = 40\%$; and dark-count rate $P_d = 3 \times 10^{-6}$.

$$\begin{aligned} Q_{23}|_{\theta_a\neq\theta_b} &= 1 - 2(1 - P_d)\mathrm{e}^{-\frac{A^2+B^2}{2}}\mathrm{I}_0(AB|p_a^\dagger p_b|) \\ &\quad + \left[(1 - P_d)\mathrm{e}^{-\frac{A^2+B^2}{2}}\right]^2 \mathrm{I}_0(2AB|p_a^\dagger p_b|), \\ Q_{12} &= Q_{23}|_{\theta_a=\theta_b}; \end{aligned} \tag{C3}$$

thus we can calculate the effects of the polarization on the QBER and V, which are

$$\begin{aligned} E &= \frac{1 - 2C\mathrm{I}_0(AB|p_a^\dagger p_b|) + C^2}{2 - 4C\mathrm{I}_0(AB|p_a^\dagger p_b|) + C^2[1 + \mathrm{I}_0(2AB|p_a^\dagger p_b|)]}, \\ V_{12} &= \frac{1 - 2C\mathrm{I}_0(AB|p_a^\dagger p_b|) + C^2}{1 - 2C\mathrm{I}_0(AB|p_a^\dagger p_b|) + [C\mathrm{I}_0(AB|p_a^\dagger p_b|)]^2}, \end{aligned} \tag{C4}$$

where $A = \sqrt{\mu_a \eta_a \eta_d/2}$, $B = \sqrt{\mu_b \eta_b \eta_d/2}$, and $C = (1 - P_d)\mathrm{e}^{-A^2+B^2/2}$. And if we consider the case where Alice and Bob are symmetric, which means that $\eta_a = \eta_a = \eta$ and $\mu_a = \mu = \mu$, then under the condition that the length of the unilateral channel $l = 50$ km and the fiber-attenuation coefficient $\alpha = 0.2$ dB/km, we have $\eta = 10^{-\alpha l/10} = 0.1$, $\mu = 0.6$, $\eta_d = 40\%$, and $P_d = 3 \times 10^{-6}$, and then we are able to calculate the effect of the polarization on the QBER in the X basis and V in Fig. 6.

Considering the relationship between the QBER and V, we can discover that

$$\frac{1}{E} - \frac{2}{V} = \frac{C^2[1 + \mathrm{I}_0(2AB|p_a^\dagger p_b|) - 2(\mathrm{I}_0(AB|p_a^\dagger p_b|))^2]}{1 - 2C\mathrm{I}_0(AB|p_a^\dagger p_b|) + C^2} \tag{C5}$$

and we know that $\lim_{x\to 0} I_0(x) = 1$, so, for $AB = \mu\eta\eta_d/2$, when the MDI-QKD protocol is working, it is obvious that $AB \to 0$, so we have

$$2E \approx V \tag{C6}$$

and this is the approximation of the relationship between the QBER and V.

APPENDIX D: CALCULATION OF THE RELATIONSHIP BETWEEN THE ACCURACY OF THE METHOD AND THE FINITE LENGTH OF THE NUMBER OF PULSES

First, we analyze the influence of the finite length on the polarization-correction criterion V_{ij}, which is defined in Eq. (12). We know that, for two random variables A and B, we have

$$\begin{aligned}\mathrm{Var}\left(\frac{A}{B}\right) &\approx E^2\left(\frac{A}{B}\right)\left[\frac{\mathrm{Var}(A)}{E^2(A)}+\frac{\mathrm{Var}(B)}{E^2(B)}-2\frac{\mathrm{Cov}(A,B)}{E(A)E(B)}\right],\\ \mathrm{Var}(AB) &\approx E^2(AB)\left[\frac{\mathrm{Var}(A)}{E^2(A)}+\frac{\mathrm{Var}(B)}{E^2(B)}+2\frac{\mathrm{Cov}(A,B)}{E(A)E(B)}\right],\end{aligned} \tag{D1}$$

from Ref. [47], where "Var" and "Cov" represent the variance and covariance and E represents the expectation. Further, we know that N_i, N_j, and N_{ij} all satisfy the binomial distribution and that $N_{ij} = N_i \bigcap N_j$; thus we can calculate

$$\begin{aligned}\mathrm{Var}(N_{12}) &= NQ_{12}(1-Q_{12}),\\ \mathrm{Var}(N_1) &= ND_1(1-D_1),\\ \mathrm{Var}(N_2) &= ND_2(1-D_2),\\ E(N_1N_2) &= N(N-1)D_1D_2+NQ_{12},\\ \mathrm{Cov}(N_1,N_2) &= N(Q_{12}-D_1D_2),\\ \mathrm{Cov}(N_{12},N_1N_2) &= N(N-1)(D_1+D_2-2D_1D_2)Q_{12}\\ &\quad +N(1-Q_{12})Q_{12}\end{aligned} \tag{D2}$$

and then we can calculate the influence of the finite length on the polarization-correction criterion V_{ij}:

$$\begin{aligned}\sigma_{V_{12}} &= \sqrt{\mathrm{Var}(N\frac{N_{12}}{N_1N_2})} \approx \sqrt{V_{12}^2[\frac{\mathrm{Var}(N_{12})}{N_{12}^2}+\frac{\mathrm{Var}(N_1)}{N_1^2}+\frac{\mathrm{Var}(N_2)}{N_2^2}+2\frac{\mathrm{Cov}(N_1,N_2)}{N_1N_2}-2\frac{\mathrm{Cov}(N_{12},N_1N_2)}{N_{12}E(N_1N_2)}]}\\ &= V_{12}\sqrt{\frac{1}{N}[\frac{1}{Q_{12}}+\frac{1}{D_1}+\frac{1}{D_2}+2V_{12}+1-\frac{(N-1)(D_1+D_2)+(1+Q_{12})}{(N-1)(D_1D_2)+Q_{12}}]}.\end{aligned} \tag{D3}$$

If $N \gg 1$ and $Q_{12} \ll 1$, we have

$$\sigma_{V_{12}} \approx V_{12}\sqrt{\frac{1}{NQ_{12}}} = V_{12}\sqrt{\frac{1}{N_{12}}}. \tag{D4}$$

According to Eqs. (5), (6), and (12), we can calculate that for the ith measurement,

$$\sigma_{V_{12}i}^2 = [F(\delta_i)]^2\sigma_{\delta_i}^2, \tag{D5}$$

where

$$\begin{aligned}F(\delta_i) &= 2(1-P_d)\mathrm{e}^{-A^2\cos(\xi_a)^2-B^2\cos(\xi_b)^2}\\ &\quad\times\left(\frac{V_{12}}{Q_{12}}-\frac{V_{12}}{P_l}\right)AB\cos(\xi_a)\cos(\xi_b)\\ &\quad\times \mathrm{I}_1(2AB\cos(\xi_a)\cos(\xi_b)\sqrt{\delta_i}),\end{aligned} \tag{D6}$$

in which $f(x) = \mathrm{I}_1(x)$ is the modified Bessel function of the first kind of first order, which is monotone increasing. For step 1, we know that $\delta_1 = \cos(\theta)^2$. And for steps 2 and 3, it is clear that $\delta_{2(3)} > 1-\sqrt{2}\sin(\theta)\cos(\theta)/2$ in view of Eq. (16). Therefore, we have

$$\begin{aligned}{\sigma_{\delta_1}}^2 &= \frac{\sigma_{V_{12}}^2}{[F(\cos(\theta)^2)]^2},\\ {\sigma_{\delta_{2,3}}}^2 &< \frac{\sigma_{V_{12}}^2}{\left[F\left(\frac{1-\sqrt{2}\sin(\theta)\cos(\theta)}{2}\right)\right]^2}.\end{aligned} \tag{D7}$$

For the MDI system, $A, B \to 0$, so $F(\delta_i) \approx \sqrt{\delta_i}$. What is more, in view of Eq. (12), we have $V_{12} \approx 1-\frac{1}{2}|p_a^\dagger p_b|^2 = 1-\frac{1}{2}\delta$. Then, using Eq. (D4) we can see that

$$\begin{aligned}\sigma_{V_{12}1} &= \left(1-\frac{\cos(\theta)^2}{2}\right)\sqrt{\frac{1}{N_{12}1}},\\ \sigma_{V_{12}2,3} &< \left(1-\frac{1-\sqrt{2}\sin(\theta)\cos(\theta)}{4}\right)\sqrt{\frac{1}{N_{12}^{2(3)}}},\\ {\sigma_{\delta_1}}^2 &= \frac{\sigma_{V_{12}}^2}{\cos(\theta)^2},\\ {\sigma_{\delta_{2(3)}}}^2 &< \frac{2\sigma_{V_{12}}^2}{1-\sqrt{2}\sin(\theta)\cos(\theta)}.\end{aligned} \tag{D8}$$

Combined with the above discussion and Eq. (16), we can calculate that

$$\sigma_\varphi^2 = \begin{cases} \frac{\cos(\varphi)^2}{\sin(\varphi)^2}\frac{1}{\cos(\theta)^2\sin(\theta)^2}\left(\frac{1}{\cos(\varphi)^2}\sigma_{\delta_2}^2 + \frac{(1-2\cos(\theta)^2)^2}{\cos(\theta)^2\sin(\theta)^2}\sigma_{\delta_1}^2\right), & |1-2\delta_3| < |2\delta_2 - 1|, \\ \frac{\sin(\varphi)^2}{\cos(\varphi)^2}\frac{1}{\cos(\theta)^2\sin(\theta)^2}\left(\frac{1}{\sin(\varphi)^2}\sigma_{\delta_3}^2 + \frac{(1-2\cos(\theta)^2)^2}{\cos(\theta)^2\sin(\theta)^2}\sigma_{\delta_1}^2\right), & |2\delta_2 - 1| < |1-2\delta_3|, \end{cases} \tag{D9}$$

in which it is clear that $\cos(\varphi)^2/\sin(\varphi)^2 < 1$ and $1/\sin(\varphi)^2 < 2$ when $|1-2\delta_3| < |2\delta_2 - 1|$ and $\sin(\varphi)^2/\cos(\varphi)^2 < 1$ and $1/\cos(\varphi)^2 < 2$ when $|2\delta_2 - 1| < |1-2\delta_3|$. For each step, we repeatedly measure N_i pulses, and in combination with Eq. (D8), we have

$$\sigma_\varphi^2 < \frac{1}{4\alpha^2}\left(\frac{(3+\sqrt{2}\alpha)^2}{1-\sqrt{2}\alpha}\frac{1}{N_{12}^{2(3)}} + \frac{(1-2\beta)^2(2-\beta)^2}{\alpha^2\beta}\frac{1}{N_{12}^1}\right), \tag{D10}$$

in which $\alpha = \sin\theta'\cos\theta' = \sqrt{(1-\beta)\beta}$, $\beta = \cos\theta'^2$, and θ' satisfies $|p_a^\dagger p_b| = \cos(\theta')$, where

$$E = \frac{1 - 2C\mathrm{I}_0(AB|p_a^\dagger p_b|) + C^2}{2 - 4C\mathrm{I}_0(AB|p_a^\dagger p_b|) + C^2[1 + \mathrm{I}_0(2AB|p_a^\dagger p_b|)]}, \tag{D11}$$

when $E = E_{th}$, where $A = \sqrt{\mu_a\eta_a\eta_d/2}$, $B = \sqrt{\mu_b\eta_b\eta_d/2}$, and $C = (1-P_d)\mathrm{e}^{-(A^2+B^2)/2}$. Hence Eq. (D11) is the relation between the QBER E and the SOP $|p_a^\dagger p_b|$, which is calculated in Appendix C.

In view of Eq. (9) and (14), we can calculate that

$$\sigma_{\delta_{\mathrm{fin}}}^2 = \sin(\theta)^4\sigma_\varphi^2, \tag{D12}$$

where δ_{fin} is the term through which the polarization affects the system after correction.

Further, from Appendix C, we know that $2E \approx V$, and in view of Eq. (D5), we have

$$\sigma_{E_{\mathrm{fin}}}^2 = \frac{[F(1)]^2}{4}\sigma_{\delta_{\mathrm{fin}}}^2, \tag{D13}$$

where $\sigma_{E_{\mathrm{fin}}}$ is the precision of the QBER after polarization correction. Then,

$$\sigma_{E_{\mathrm{fin}}}^2 < \frac{(1-\beta)^2}{16\alpha^2}\left(\frac{(3+\sqrt{2}\alpha)^2}{1-\sqrt{2}\alpha}\frac{1}{N_{12}^{2(3)}}\right. \tag{D14}$$

$$\left. + \frac{(1-2\beta)^2(2-\beta)^2}{\alpha^2\beta}\frac{1}{N_{12}^1}\right). \tag{D15}$$

Given Eq. (D11), and for the MDI system, $A, B \to 0$, so that $E \approx \frac{1}{2} - \frac{1}{4}|p_a^\dagger p_b|^2$, we can know that $\beta = 2 - 4E_{th}$, $\alpha = \sqrt{(4E_{th}-1)(2-4E_{th})}$.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[3] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, in *Quantum Information and Computation III*, Vol. 5815, edited by E. J. Donkor, A. R. Pirich, and H. E. Brandt, International Society for Optics and Photonics (SPIE, 2005), p. 138..

[4] M. Peev, *et al.*, The SECOQC quantum key distribution network in Vienna, New J. Phys. **11**, 075001 (2009).

[5] W. Chen, Z.-F. Han, T. Zhang, H. Wen, Z.-Q. Yin, F.-X. Xu, Q.-L. Wu, Y. Liu, Y. Zhang, X.-F. Mo, Y.-Z. Gui, G. Wei, and G.-C. Guo, Field experiment on a "star type" metropolitan quantum key distribution network, IEEE Photonics Technol. Lett. **21**, 575 (2009).

[6] S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, D.-J. Huang, L.-J. Zhang, F.-Y. Li, D. Liu, Y.-G. Wang, G.-C. Guo, and Z.-F. Han, Field test of wavelength-saving quantum key distribution network, Opt. Lett. **35**, 2454 (2010).

[7] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, L.-K. Chen, L.-J. Wang, Y. Gao, K. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, Metropolitan all-pass and inter-city quantum communication network, Opt. Express **18**, 27217 (2010).

[8] D. Stucki, *et al.*, Long-term performance of the swissquantum quantum key distribution network in a field environment, New J. Phys. **13**, 123001 (2011).

[9] M. Sasaki, *et al.*, Field test of quantum key distribution in the Tokyo QKD network, Opt. Express **19**, 10387 (2011).

[10] S. Wang, *et al.*, Field and long-term demonstration of a wide area quantum key distribution network, Opt. Express **22**, 21739 (2014).

[11] Y.-A. Chen, *et al.*, An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature **589**, 214 (2021).

[12] S. L. Braunstein and S. Pirandola, Side-channel-free quantum key distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[13] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[14] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nat. Commun. **5**, 3732 (2014).

[15] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate-distance limit of quantum key

distribution without quantum repeaters, Nature **557**, 400 (2018).
[16] X. Ma, P. Zeng, and H. Zhou, Phase-matching quantum key distribution, Phys. Rev. X **8**, 031043 (2018).
[17] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A **98**, 062323 (2018).
[18] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution without phase postselection, Phys. Rev. Appl. **11**, 034053 (2019).
[19] D. Mayers and A. Yao, in *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)* (Palo Alto, CA, USA, 1998), p. 503.
[20] L. Masanes, S. Pironio, and A. Acín, Secure device-ind ependent quantum key distribution with causally independent measurement devices, Nat. Commun. **2**, 238 (2011).
[21] B. W. Reichardt, F. Unger, and U. Vazirani, Classical command of quantum systems, Nature **496**, 456 (2013).
[22] U. Vazirani and T. Vidick, Fully device-independent quantum key distribution, Phys. Rev. Lett. **113**, 140501 (2014).
[23] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Practical device-independent quantum cryptography via entropy accumulation, Nat. Commun. **9**, 459 (2018).
[24] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, Quantum key distribution without detector vulnerabilities using optically seeded lasers, Nat. Photonics **10**, 312 (2016).
[25] C. Wang, X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, and Z.-F. Han, Phase-reference-free experiment of measurement-device-independent quantum key distribution, Phys. Rev. Lett. **115**, 160502 (2015).
[26] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Measurement-device-independent quantum key distribution over a 404 km optical fiber, Phys. Rev. Lett. **117**, 190501 (2016).
[27] X.-Y. Zhou, H.-J. Ding, C.-H. Zhang, J. Li, C.-M. Zhang, and Q. Wang, Experimental three-state measurement-device-independent quantum key distribution with uncharacterized sources, Opt. Lett. **45**, 4176 (2020).
[28] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, Measurement-device-independent quantum key distribution over untrustful metropolitan network, Phys. Rev. X **6**, 011024 (2016).
[29] G. B. Xavier, N. Walenta, G. V. de Faria, G. P. Temporão, N. Gisin, H. Zbinden, and J. P. von der Weid, Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation, New J. Phys. **11**, 045015 (2009).
[30] N. J. Muga, M. F. S. Ferreira, and A. N. Pinto, QBER estimation in QKD systems with polarization encoding, J. Lightwave Technol. **29**, 355 (2011).
[31] J. Chen, G. Wu, L. Xu, X. Gu, E. Wu, and H. Zeng, Stable quantum key distribution with active polarization control based on time-division multiplexing, New J. Phys. **11**, 065004 (2009).
[32] N. J. Muga, Á. J. Almeida, M. F. Ferreira, and A. N. Pinto, in *International Conference on Applications of Optics and Photonics*, Vol. 8001, edited by M. F. Costa, International Society for Optics and Photonics (SPIE, 2011), p. 80013N.
[33] G. B. Xavier, G. V. de Faria, G. P. T. ao, and J. P. von der Weid, Full polarization control for fiber optical quantum communication systems using polarization encoding, Opt. Express **16**, 1867 (2008).
[34] D.-D. Li, S. Gao, G.-C. Li, L. Xue, L.-W. Wang, C.-B. Lu, Y. Xiang, Z.-Y. Zhao, L.-C. Yan, Z.-Y. Chen, G. Yu, and J.-H. Liu, Field implementation of long-distance quantum key distribution over aerial fiber with fast polarization feedback, Opt. Express **26**, 22793 (2018).
[35] W. Eickhoff, Y. Yen, and R. Ulrich, Wavelength dependence of birefringence in single-mode fiber, Appl. Opt. **20**, 3428 (1981).
[36] J. Chen, G. Wu, Y. Li, E. Wu, and H. Zeng, Active polarization stabilization in optical fibers suitable for quantum key distribution, Opt. Express **15**, 17928 (2007).
[37] A. Treiber, A. Poppe, M. Hentschel, D. Ferrini, T. Lorünser, E. Querasser, T. Matyus, H. Hübel, and A. Zeilinger, A fully automated entanglement-based quantum cryptography system for telecom fiber networks, New J. Phys. **11**, 045013 (2009).
[38] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Device calibration impacts security of quantum key distribution, Phys. Rev. Lett. **107**, 110501 (2011).
[39] Y.-Y. Ding, W. Chen, H. Chen, C. Wang, Y.-P. li, S. Wang, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits, Opt. Lett. **42**, 1023 (2017).
[40] M. F. Ramos, N. A. Silva, N. J. Muga, and A. N. Pinto, Reversal operator to compensate polarization random drifts in quantum communications, Opt. Express **28**, 5035 (2020).
[41] Á. J. Almeida, N. J. Muga, N. A. Silva, J. M. Prata, P. S. André, and A. N. Pinto, Continuous control of random polarization rotations for quantum communications, J. Lightwave Technol. **34**, 3914 (2016).
[42] G.-J. Fan-Yuan, F.-Y. Lu, S. Wang, Z.-Q. Yin, D.-Y. He, Z. Zhou, J. Teng, W. Chen, G.-C. Guo, and Z.-F. Han, Measurement-device-independent quantum key distribution for nonstandalone networks, Photon. Res. **9**, 1881 (2021).
[43] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, Higher key rate of measurement-device-independent quantum key distribution through joint data processing, Phys. Rev. A **103**, 012402 (2021).
[44] C. B. Czegledi, M. Karlsson, E. Agrell, and P. Johannisson, Polarization drift channel model for coherent fibre-optic systems, Sci. Rep. **6**, 21217 (2016).
[45] Y.-Y. Ding, H. Chen, S. Wang, D.-Y. He, Z.-Q. Yin, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Polarization variations in installed fibers and their influence on quantum key distribution systems, Opt. Express **25**, 27923 (2017).
[46] G.-J. Fan-Yuan, C. Wang, S. Wang, Z.-Q. Yin, H. Liu, W. Chen, D.-Y. He, Z.-F. Han, and G.-C. Guo, Afterpulse analysis for quantum key distribution, Phys. Rev. Appl. **10**, 064032 (2018).
[47] R. C. Elandt-Johnson and N. L. Johnson, *Survival Models and Data Analysis* (Wiley, Hoboken, New Jersey, USA, 1980), p. 22.