Mode-pairing quantum key distribution with advantage distillation

Xin Liu,[1] Di Luo,[1] Zhenrong Zhang,[2] and Kejin Wei[1,*]

[1]*Guangxi Key Laboratory for Relativistic Astrophysics, School of Physical Science and Technology, Guangxi University, Nanning 530004, China*

[2]*Guangxi Key Laboratory of Multimedia Communications and Network Technology, School of Computer Electronics and Information, Guangxi University, Nanning 530004, China*

(Received 9 April 2023; accepted 5 June 2023; published 29 June 2023)

Mode-pairing quantum key distribution (MP-QKD) is an easy-to-implement scheme that transcends the Pirandola-Laurenza-Ottaviani-Banchi bound without using quantum repeaters. In this paper, we present an improvement of the performance of MP-QKD using an advantage distillation method. The simulation results demonstrate that the proposed scheme extends the transmission distance significantly with a channel loss exceeding 7.6 dB. Moreover, the scheme tolerates a maximum quantum bit error rate of 8.9%, which is nearly twice that of the original MP-QKD. In particular, as the system misalignment error increases, the expandable distance of the proposed scheme also increases. The proposed system is expected to promote the practical implementation of MP-QKD in a wide range of applications, particularly in scenarios involving high channel losses and system errors.

DOI: 10.1103/PhysRevA.107.062613

I. INTRODUCTION

With the development of quantum computers, classical encryption methods based on algorithm complexity [1,2] have demonstrated to be insufficient in guaranteeing communication security. Thus, quantum key distribution (QKD) [3], which operates by distributing information-theoretic secure keys, has garnered significant attention in research. Specifically, chip-based QKD has garnered considerable attention in recent years due to its advantages involving small size and cost efficiency [4,5]. However, there is a significant gap between the ideal QKD model and realistic models, resulting in security vulnerabilities in realistic QKD systems [6].

The improvement of the practical security of QKD systems has been researched for decades. To this end, one approach involves the construction of more realistic models to analyze the security of QKD systems [7–13]. However, characterizing all devices in real-world systems is challenging. In contrast, device-independent QKD has been proposed to address all security loopholes induced by device imperfections [14]. However, this protocol exhibits a low key rate and is difficult to implement because of the strict requirement on the detection efficiency of single-photon detectors. Fortunately, measurement-device-independent QKD (MDI-QKD) [15], which closes all loopholes in detection devices, is relatively simple to implement with excellent performance. Significant experimental progress has been made with regard to this method [16–22].

Currently, most MDI-QKD methods are called two-mode MDI-QKD because they encode single-sided key information in the relative phases of the coherent states of two orthogonal optical modes. A successful two-photon interference measurement is required to correlate the information encoded in the photons by Alice or Bob in a two-mode scheme. If the photon emitted by Alice or Bob is lost during transmission, coincidence detection cannot be performed for successful interference, rendering the restoration of the raw key information impossible. Thus, the requirement of coincidence detection of MDI-QKD is a critical factor limiting its transmission distance.

In recent years, the performance of MDI-QKD has been improved from multiple perspectives, e.g., increasing the secret key rate and the transmission distance [23–28]. Twin-field QKD (TF-QKD) [29], which encodes information in a single optical mode, is the most representative improvement. In particular, TF-QKD transcends the repeaterless secret key capacity bound [30], and more tightly, the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [31]. Subsequently, variants of the TF-QKD protocol have been proposed, such as phase-matching QKD, in which key information is encoded in phase with the coherent states [32]; sending-or-not-sending TF-QKD, in which information is encoded in intensity [33,34]; and so on [35–41]. However, TF-QKD requires locking the frequency and phase of the coherent state and stabilizing the global phase, which inevitably complicates the implementation setup with peripheral hardware [42–49]. This makes experimentation challenging and hinders the use of single-mode schemes in real-life applications.

Recently, a new variant of MDI-type QKD, called mode-pairing QKD (MP-QKD), was proposed [50]. Similar to TF-QKD, MP-QKD transcends the PLOB bound, but it does not require the use of phase-locking technology. This feature enables MP-QKD to be implemented using a simpler setup than TF-QKD. More recently, the tight finite-key effect [51] and experimental demonstrations using off-the-shelf optical devices for MP-QKD were reported [52].

*Corresponding author: kjwei@gxu.edu.cn

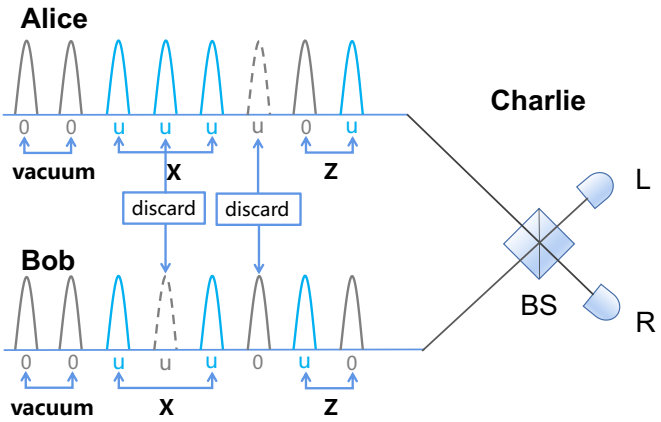

FIG. 1. Diagram of the MP-QKD scheme. Alice and Bob transmit the prepared coherent pulses to Charlie and they utilize the Z pairs to generate the key after postprocessing. For time bins k and l, one intensity is 0 and the other is nonzero as the Z basis, the intensities are given by (μ, μ) as the X basis, and they are $(0, 0)$ in the vacuum state. If one or both of Alice and Bob lose data at the same time bin, they both discard the corresponding data and start searching for the following time bin. L/R: detector; BS: beam splitter.

In this study, we further improve the performance of MP-QKD by using the advantage distillation (AD) method. The proposed scheme modifies the postprocessing step without changing the hardware of a realistic MP-QKD system. Hence, it can be directly applied to current systems. Its fundamental underlying concept is to divide the original key into blocks of a few bits each, enabling highly correlated keys to be distinguished from weakly correlated bits. The typical experimental parameters of MP-QKD are used for simulations. The simulation results demonstrate that the proposed scheme extends the transmission distance significantly. Moreover, the maximum tolerable quantum bit error rate (QBER) of the proposed system is 8.9%, which is nearly twice that of the original MP-QKD. In particular, in some specific cases, the proposed scheme exhibits a longer expandable distance, paving the way for the widespread real-world application of MP-QKD.

The remainder of this paper is organized as follows. In Sec. II, we briefly summarize the steps involved in MP-QKD. In Sec. III, we introduce the protocol steps of the proposed scheme and present its security analysis in detail. Subsequently, in Sec. IV, we present the numerical simulation results, comparing the performances of the proposed scheme and the original MP-QKD. The results demonstrate the impact of the misalignment error e_d on the performance of the proposed scheme. Finally, we present further discussion and our conclusions in Sec. V.

II. ORIGINAL MP-QKD

In this section, we briefly review the original MP-QKD method proposed in [50]. A schematic of this scheme is presented in Fig. 1 and its specific steps are summarized as follows.

Step 1. Preparation. Alice (Bob) prepares n weak coherent state pulses $|e^{i\theta_A^k}\sqrt{\lambda_A^k}\rangle(|e^{i\theta_B^k}\sqrt{\lambda_B^k}\rangle)$ with intensities $\lambda_A^k(\lambda_B^k) \in \{\mu, 0\}$, where each time bin satisfies $k \in \{1, 2, \ldots, n\}$, and the phase satisfies $\theta_A^k(\theta_B^k) \in [0, 2\pi)$.

Step 2. Measurement and announcement. Alice and Bob transmit weak coherent light pulses to Charlie. For each time bin k, Charlie performs an interference measurement on the two received pulses and records the responses of detectors L and/or R. Subsequently, Charlie publicly announces whether a detection event is acquired and the detector that clicks.

Step 3. Mode pairing. Alice and Bob repeat the two aforementioned steps N times. Corresponding to each round with successful detection, only one detector click (L or R) round is retained. Alice and Bob group the two clicked rounds into pairs to determine the bases. The phases and intensities encoded in these two rounds form a data pair. The paired bases are then compared: they are retained if they satisfy the sifting conditions; otherwise, they are discarded.

Step 4. Basis sifting. For time bins k and l, if one of the intensities is 0 and the other is nonzero, the data are retained and recorded as the Z basis, if the intensities are (μ, μ) in terms of the X basis, or if the intensities are $(0, 0)$ as in a vacuum state, then the rest of the data are discarded. Subsequently, Alice and Bob announce the bases and the sum of the intensities corresponding to the time bins k and l. If the announced bases are identical and no "discard" is present, the bases are recorded and the data are retained.

Step 5. Key mapping. For each Z pair at time bins k and l, Alice sets her key to $\kappa_A = 0$ if the intensity pair is $(\lambda_A^k, \lambda_A^l) = (\mu, 0)$. Alternatively, Alice sets her key to $\kappa_A = 1$ if the intensity pair is $(\lambda_A^k, \lambda_A^l) = (0, \mu)$. For each X pair at time bins k and l, the key is extracted from the relative phase $(\theta_A^l - \theta_A^k) = \phi_A + \pi\kappa_A$, where the raw key bit is given by $\kappa_A = \{[(\theta_A^l - \theta_A^k)/\pi] \bmod 2\}$, and the alignment angle is given by $\phi_A := (\theta_A^l - \theta_A^k) \bmod \pi$. Similarly, Bob assigns a raw key bit κ_B and determines ϕ_B. For each X pair, Alice and Bob announce the alignment angles ϕ_A and ϕ_B. If $\phi_A = \phi_B$, the data pairs are retained; otherwise, they are discarded.

Step 6. Parameter estimation. Alice and Bob use the Z pairs to generate a key. All the raw data obtained can be used to estimate the bit error rate $E_{(\mu,\mu)}^{ZZ}$ of the raw key in Z pairs with overall intensities of $(\lambda_A^{k,l}, \lambda_B^{k,l}) = (\mu, \mu)$. When Alice and Bob both transmit a single photon each at time bins k and l, they can estimate the fraction of clicked signals, $\bar{q}_{11}$, using the data of Z pairs with different intensities and can estimate the single-photon phase error rate $e_{(1,1)}^{XX}$ using the data of the X pairs.

Step 7. Postprocessing. Alice and Bob perform error correction and privacy amplification on the raw key data to obtain the final secret key.

Based on the security proof presented in [50], the final key rate of MP-QKD can be estimated as follows:

$$R = r_p(p, \delta) r_s \left\{ \bar{q}_{11} \left[1 - h\left(e_{(1,1)}^{XX}\right) \right] - f h\left(E_{(\mu,\mu)}^{ZZ}\right) \right\}, \quad (1)$$

where $r_p(p, \delta)$ denotes the expected pair rate contributed during each round, δ denotes the maximum pairing interval, and p denotes the probability of the kth emitted pulse results in each successful click. r_s denotes the probability that a generated pair is a Z pair, $e_{(1,1)}^{XX}$ denotes the single-photon phase error rate, $\bar{q}_{11}$ denotes the expected single-photon pair ratio in all Z pairs, f denotes the error correction efficiency, $h(x) =$

$-x\log_2(x)-(1-x)\log_2(1-x)$ denotes the binary Shannon entropy function, and $E^{ZZ}_{(\mu,\mu)}$ denotes the bit error rate of the Z pairs. The detailed calculation process for obtaining these parameters is described in Appendix A.

III. MP-QKD WITH AD METHOD

Next, we discuss the specific steps involved in applying the AD method to MP-QKD. The AD method [53–59] only changes the postprocessing steps. Thus, steps 1 to 6 of the proposed scheme are identical to those of the original MP-QKD. The only change is in the postprocessing procedure of the original MP-QKD. The specific details are presented below.

New step 7. Alice and Bob divide their raw key into b blocks each, i.e., $\{x_1, x_2, \ldots, x_b\}$ and $\{y_1, y_2, \ldots, y_b\}$. Alice randomly selects a bit $c \in \{0, 1\}$ and transmits the messages $m = \{m_1, m_2, \ldots, m_b\} = \{x_1 \oplus c, x_2 \oplus c, \ldots, x_b \oplus c\}$ to Bob via an authenticated classical channel. Alice and Bob accept the block only if Bob announces that the result of $\{m_1 \oplus y_1, m_2 \oplus y_2, \ldots, m_b \oplus y_b\}$ is $\{0, 0, \ldots, 0\}$ or $\{1, 1, \ldots, 1\}$. Then, they retain the first bits, x_1 and y_1, as raw keys. Finally, Alice and Bob perform error correction and privacy amplification on the raw key data to obtain the secret keys.

To obtain further insights into the improvement of the achieved key rate using the AD method, we first reanalyze the key rate of MP-QKD using quantum information theory. We rewrite the key rate formulas as follows:

$$R \geqslant \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} r_p(p,\delta) r_s \left\{ \bar{q}_{11} \left[1-(\lambda_0+\lambda_1) h\left(\frac{\lambda_0}{\lambda_0+\lambda_1}\right) -(\lambda_2+\lambda_3) h\left(\frac{\lambda_2}{\lambda_2+\lambda_3}\right) \right] - f h\left(E^{ZZ}_{(\mu,\mu)}\right) \right\}, \tag{2}$$

where $\sum_{j=0}^{3}\lambda_j = 1$ and $\lambda_j (j = \{0, 1, 2, 3\})$ denote factors of the characterizing quantum channel. The single-photon error rates in the X basis and Z basis are constrained by $\lambda_1 + \lambda_3 = e^{XX}_{(1,1)}$ and $\lambda_2 + \lambda_3 = e^{ZZ}_{(1,1)}$, respectively. A detailed analysis of Eq. (2) is presented in Appendix B.

After postprocessing using the AD method (new step 7), highly correlated bits can be separated from weakly correlated information and the key rate of the MP-QKD protocol can be modified as follows (the detailed formulas following AD postprocessing are presented in Appendix C):

$$\tilde{R} \geqslant \max_{b} \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{1}{b} q_s r_p(p,\delta) r_s \times \left\{ (\bar{q}_{11})^b \left[1-(\tilde{\lambda}_0+\tilde{\lambda}_1) h\left(\frac{\tilde{\lambda}_0}{\tilde{\lambda}_0+\tilde{\lambda}_1}\right) -(\tilde{\lambda}_2+\tilde{\lambda}_3) h\left(\frac{\tilde{\lambda}_2}{\tilde{\lambda}_2+\tilde{\lambda}_3}\right) \right] - f h\left(\tilde{E}^{ZZ}_{(\mu,\mu)}\right) \right\}, \tag{3}$$

subject to

$$\begin{aligned} e^{XX}_{(1,1)} &= \lambda_1+\lambda_3, \\ e^{ZZ}_{(1,1)} &= \lambda_2+\lambda_3, \\ q_s &= \left(E^{ZZ}_{(\mu,\mu)}\right)^b + \left(1-E^{ZZ}_{(\mu,\mu)}\right)^b, \\ \tilde{E}^{ZZ}_{(\mu,\mu)} &= \frac{\left(E^{ZZ}_{(\mu,\mu)}\right)^b}{\left(E^{ZZ}_{(\mu,\mu)}\right)^b + \left(1-E^{ZZ}_{(\mu,\mu)}\right)^b}, \end{aligned} \tag{4}$$

and

$$\begin{aligned} \tilde{\lambda}_0 &= \frac{(\lambda_0+\lambda_1)^b + (\lambda_0-\lambda_1)^b}{2[(\lambda_0+\lambda_1)^b + (\lambda_2+\lambda_3)^b]}, \\ \tilde{\lambda}_1 &= \frac{(\lambda_0+\lambda_1)^b - (\lambda_0-\lambda_1)^b}{2[(\lambda_0+\lambda_1)^b + (\lambda_2+\lambda_3)^b]}, \\ \tilde{\lambda}_2 &= \frac{(\lambda_2+\lambda_3)^b + (\lambda_2-\lambda_3)^b}{2[(\lambda_0+\lambda_1)^b + (\lambda_2+\lambda_3)^b]}, \\ \tilde{\lambda}_3 &= \frac{(\lambda_2+\lambda_3)^b - (\lambda_2-\lambda_3)^b}{2[(\lambda_0+\lambda_1)^b + (\lambda_2+\lambda_3)^b]}, \end{aligned} \tag{5}$$

where q_s represents the probability of a successful advantage distillation on a block of length b and $\tilde{E}^{ZZ}_{(\mu,\mu)}$ represents the overall error rate after the AD postprocessing step.

IV. SIMULATION

In this section, we report the simulation of the asymptotic performance of the proposed scheme using a typical symmetric quantum channel model and practical experimental parameters. The parameters for all numerical simulations described below are listed in Table I. The parameters are adopted from [50]. The value of b is restricted to the interval [1, 3].

First, we specify the misalignment error e_d for MP-QKD to be 4% and compare the asymptotic secret key rate performance of the proposed scheme with that of the original MP-QKD. Figure 2 reveals that the performance of the proposed scheme is comparable to that of the original MP-QKD scheme corresponding to distances between 0 and 482 km. As the transmission distance increases, the secret key rate of the original MP-QKD decreases rapidly owing to the introduction of more noise, and the correlation of the original key deteriorates. When the distance exceeds 482 km, the proposed scheme represents an improvement over the original MP-QKD and the maximum transmission distance increases by 40 km.

To estimate the QBER tolerance of the proposed scheme, the relationship between the secret key rate and the QBER is simulated. The results are depicted in Fig. 3. The simulation results indicate that QBER increases rapidly to 4.6%, and the original MP-QKD becomes incapable of generating a secret key rate. In contrast, the proposed scheme remains capable of generating a secret key rate with a magnitude of 10^{-9}. Thus, the proposed scheme tolerates a maximum QBER of 8.9%, which is nearly twice that of the original MP-QKD.

Finally, we investigate the effect of the misalignment error e_d on the performance of the proposed scheme and the optimal b values, with the results depicted in Fig. 4. When $e_d = 1\%$ ($e_d = 10\%$, $e_d = 20\%$), the optimal b value is greater

TABLE I. List of parameters used for numerical simulations. η_d denotes the detection efficiency, α denotes the loss coefficient of the fiber, p_d denotes detector dark count rate, f denotes the error correction, and δ denotes the maximum pairing interval.

η_d	α	p_d	f	δ
20%	0.2 dB/km	1.2×10^{-8}	1.15	10^6

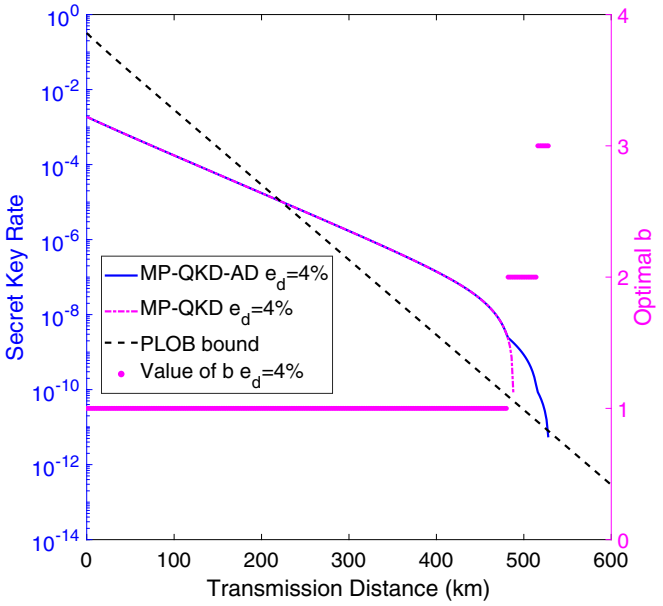

FIG. 2. Performance comparison between the proposed scheme (MP-QKD-AD) and the original MP-QKD scheme and the relationship between the optimal b values and the transmission distance assuming $e_d = 4\%$. The blue solid line represents the secret key rate of the proposed scheme, the pink dotted line represents the secret key rate of the original MP-QKD scheme, the black dotted line represents PLOB bound, and the pink scattered points represent the optimized b values of the proposed scheme.

than 1 at a distance of 490 km (466 km, 434 km), and the transmission distance of the proposed scheme increases by 38 km (46 km, 56 km). This observation implies that, as the system misalignment error increases, the distance extension of the scheme also increases.

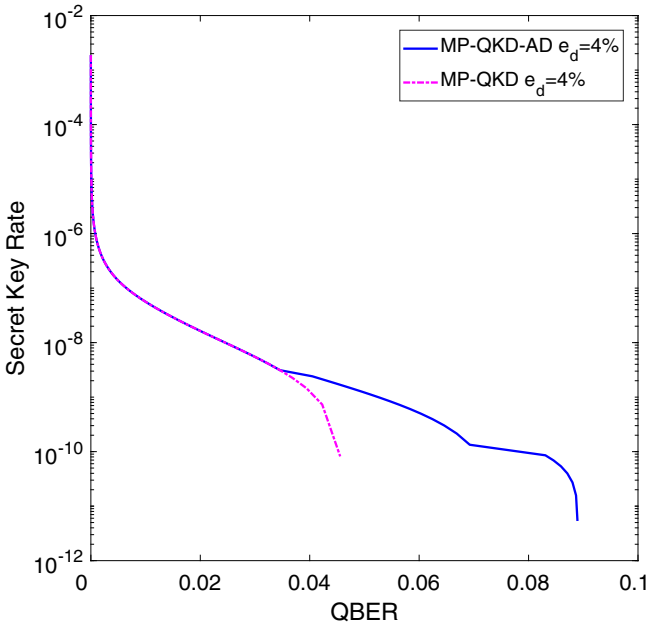

FIG. 3. Comparison of the maximal tolerated quantum bit error rates (QBER) of the proposed scheme and the original MP-QKD assuming $e_d = 4\%$. The blue solid line and pink dotted line represent the relationships between the secret key rate and the QBER of the proposed scheme and original MP-QKD, respectively.

V. DISCUSSION AND CONCLUSION

In summary, this paper proposes a scheme to improve the performance of MP-QKD using the AD method and simulates its performance for an asymptotic case. The simulation results reveal that, compared to the original MP-QKD, the proposed scheme can tolerate a higher QBER and exhibits a significantly increased transmission distance. When the QBER reaches 4.6%, the original MP-QKD becomes incapable of generating the secret key rate. In contrast, the proposed scheme remains capable of generating a secret key rate with a magnitude of 10^{-9}. The maximum QBER tolerated by the proposed scheme is nearly twice that of the original MP-QKD. Moreover, the expandable distance of high misalignment error systems in the proposed scheme is higher than that of low misalignment error systems. Overall, the proposed scheme outperforms the original MP-QKD in scenarios with high channel loss and system errors.

The proposed scheme does not require any alterations to the original hardware devices, it only requires modification of the classical postprocessing process. Thus, it can be applied to existing MP-QKD systems easily to improve their performance [52].

In future research we can investigate the performance of the MP-QKD protocol with an AD method in a more realistic model by combining it with a tight finite-key analysis [51]. In addition, the possibility of improving the performance of MP-QKD further using random postselection should be investigated as it has been shown to outperform the AD method in device-independent QKD [60]. Moreover, the application of the AD method to asynchronous MDI-QKD protocol [61], which is a similar single-mode MDI-type QKD, should be investigated.

ACKNOWLEDGMENTS

This study was supported by the National Natural Science Foundation of China (Grants No. 62171144, No. 62031024, and No. 11865004), Guangxi Science Foundation (Grants No. 2021GXNSFAA220011 and No. 2021AC19384), and the Open Fund of IPOC (BUPT) (Grant No. IPOC2021A02).

APPENDIX A: SIMULATION MODEL OF MP-QKD

According to Supplemental Material 4 in [50], we can summarize the model of the mode-pairing QKD scheme as follows.

In the asymptotic case, we assume that the probability of Alice and Bob choosing a random emission intensity of $\{0, \mu\}$ is close to $1/2$, and the probability of decoy intensity ν is negligible. We express the coherent pulse transmitted by Alice in the kth round as $|\sqrt{\xi_A^k \mu} e^{\mathbf{i}\theta_A^k}\rangle$, where ξ_A^k represents the random variable of intensity and θ_A^k is the random phase. Similarly, Bob transmits $|\sqrt{\xi_B^k \mu} e^{\mathbf{i}\theta_B^k}\rangle$ in the kth round. The intensity setting for round k is represented by the two-bit vector $\xi^k := [\xi_A^k, \xi_B^k]$.

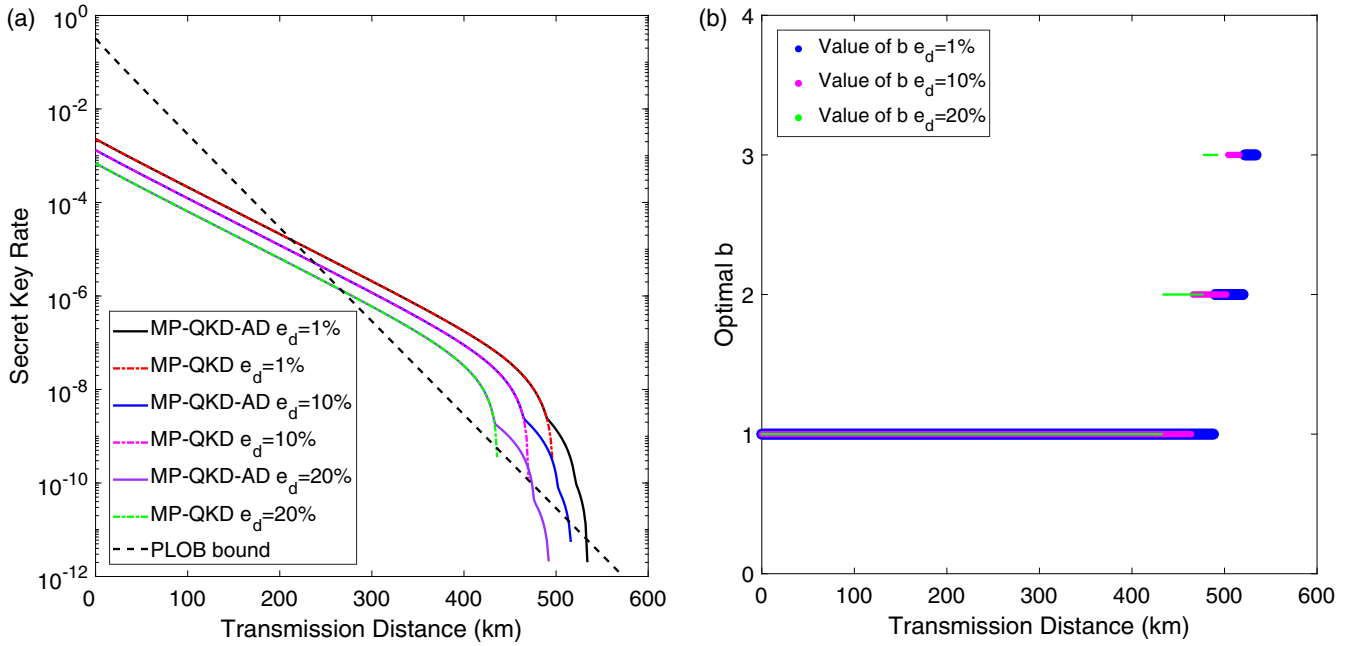

FIG. 4. The performance of the proposed scheme corresponding to different e_d. (a) Relationship between the secret key rate and the total transmission distance corresponding to different e_d. The solid lines and dotted lines of different colors represent the performances of the proposed scheme and the original MP-QKD corresponding to different e_d, respectively. (b) Relationship between the optimal value of b and the total transmission distance corresponding to different e_d. The blue, pink, and green scattered points represent the optimal value b with respect to different distances corresponding to $e_d = 1\%$, 10%, and 20%, respectively.

Alice and Bob are assumed to transmit weak coherent light pulses to Charlie through a typical symmetric-attenuation channel, the channel is i.i.d. for each round. Alice and Bob then pair the clicked pulses and determine their bases. For the (k, l)th pulses to be paired, let $\tau^{k,l} = [\tau_A^{k,l}, \tau_B^{k,l}] := [\xi_A^k \oplus \xi_A^l, \xi_B^k \oplus \xi_B^l]$, where $\oplus$ is the bit-wise addition modulo 2. When $\tau^{k,l} = [1, 1]$ the (k, l) pair is set to be a Z pair.

In the kth round, we adopt two variables (L^k, R^k) to represent the click events of the L and R detectors in the kth round. The successful click variable is $C^k = L^k \oplus R^k$. A successful click will occur only when $C^k = 1$. The detection probability $\Pr(C^k = 1|\xi^k)$ can be expressed as

$$\Pr(C^k = 1|\xi^k) \approx 1 - (1 - 2p_d)\exp\left[-\eta_s \mu\left(\xi_A^k + \xi_B^k\right)\right]. \tag{A1}$$

The phase-randomized coherent states transmitted by the kth round can be regarded as a mixture of photon number states. $\Pr(C^k = 1|n^k)$ represents the detection probability when Alice and Bob each transmit photon number states $|n_A^k\rangle$ and $|n_B^k\rangle$, respectively, and is expressed as

$$\Pr(C^k = 1|n^k) \approx 1 - (1 - 2p_d)(1 - \eta_s)^{(n_A^k + n_B^k)}. \tag{A2}$$

Next, we are going to consider the calculation of r_s. Without loss of generality, we regard the kth and lth rounds as a pair. For a general round, the probability of an intensity setting ξ causing a click is given by

$$\Pr(\xi|C = 1) = \frac{\Pr(\xi, C = 1)}{\Pr(C = 1)} = \frac{\Pr(C = 1|\xi)}{\sum_{\xi'} \Pr(C = 1|\xi')}. \tag{A3}$$

Note that the subscripts are omitted because all rounds of detection are identical and independently distributed in our simulation.

In the mode-pairing QKD scheme, a successful click occurs when $\tau^{k,l} = [1, 1]$. Therefore, four possible configurations of ξ^k and ξ^l (which generate Z pairs) are

$$[\xi^k, \xi^l] \in \{[00, 11], [01, 10], [10, 01], [11, 00]\}, \tag{A4}$$

of these, $\mathcal{E} := \{[00, 11], [11, 00]\}$ are the two configurations that cause bit error. To simplify the notation, we introduce several events:

$$\begin{aligned}
\Pr(C) &= \Pr(\text{Pair Clicked}) := \Pr(C^k = C^l = 1) = p^2, \\
\Pr(E) &= \Pr(\text{Pair Effective}) := \Pr(\xi^k \oplus \xi^l = 11), \\
\Pr(\mathcal{E}) &= \Pr(\text{Pair Erroneous}) := \Pr([\xi^k, \xi^l] \in \mathcal{E}), \\
\Pr(S) &= \Pr(\text{Single-Photon Pair}) := \Pr(n^k \oplus n^l = 11).
\end{aligned} \tag{A5}$$

Below, we will list the possible situations of ξ^k and ξ^l:

$$\begin{aligned}
\xi^k &:= \left[\xi_A^k, \xi_B^k\right] = [0, 1], [1, 0], [0, 0], [1, 1], \\
\xi^l &:= \left[\xi_A^l, \xi_B^l\right] = [0, 1], [1, 0], [0, 0], [1, 1],
\end{aligned} \tag{A6}$$

of these, the conditions conforming to $\xi^k \oplus \xi^l = 11$ are

$$\begin{aligned}
&(1)\ \xi^k := \left[\xi_A^k, \xi_B^k\right] = [1, 0]\ \ \xi^l := \left[\xi_A^l, \xi_B^l\right] = [0, 1], \\
&(2)\ \xi^k := \left[\xi_A^k, \xi_B^k\right] = [0, 1]\ \ \xi^l := \left[\xi_A^l, \xi_B^l\right] = [1, 0], \\
&(3)\ \xi^k := \left[\xi_A^k, \xi_B^k\right] = [0, 0]\ \ \xi^l := \left[\xi_A^l, \xi_B^l\right] = [1, 1], \\
&(4)\ \xi^k := \left[\xi_A^k, \xi_B^k\right] = [1, 1]\ \ \xi^l := \left[\xi_A^l, \xi_B^l\right] = [0, 0].
\end{aligned} \tag{A7}$$

For case (1):

$$\begin{aligned}\Pr(C^k=1|\xi^k)&\approx 1-(1-2p_d)\exp\left[-\eta_s u\left(\xi_A^k+\xi_B^k\right)\right]\\&=1-(1-2p_d)\exp(-\eta_s u),\\\Pr(C^l=1|\xi^l)&\approx 1-(1-2p_d)\exp\left[-\eta_s u\left(\xi_A^l+\xi_B^l\right)\right]\\&=1-(1-2p_d)\exp(-\eta_s u),\end{aligned}\tag{A8}$$

$$\begin{aligned}\Pr(C^k=1|n^k=\xi^k)&\approx 1-(1-2p_d)(1-\eta_s)^{n_A^k+n_B^k}\\&=1-(1-2p_d)(1-\eta_s),\\\Pr(C^l=1|n^l=\xi^l)&\approx 1-(1-2p_d)(1-\eta_s)^{n_A^l+n_B^l}\\&=1-(1-2p_d)(1-\eta_s).\end{aligned}\tag{A9}$$

For case (2):

$$\begin{aligned}\Pr(C^k=1|\xi^k)&\approx 1-(1-2p_d)\exp(-\eta_s u),\\\Pr(C^l=1|\xi^l)&\approx 1-(1-2p_d)\exp(-\eta_s u),\end{aligned}\tag{A10}$$

$$\begin{aligned}\Pr(C^k=1|n^k=\xi^k)&\approx 1-(1-2p_d)(1-\eta_s),\\\Pr(C^l=1|n^l=\xi^l)&\approx 1-(1-2p_d)(1-\eta_s).\end{aligned}\tag{A11}$$

For case (3):

$$\begin{aligned}\Pr(C^k=1|\xi^k)&\approx 1-(1-2p_d)=2p_d,\\\Pr(C^l=1|\xi^l)&\approx 1-(1-2p_d)\exp(-2\eta_s u),\end{aligned}\tag{A12}$$

$$\begin{aligned}\Pr(C^k=1|n^k=\xi^k)&\approx 2p_d,\\\Pr(C^l=1|n^l=\xi^l)&\approx 1-(1-2p_d)(1-\eta_s)^2.\end{aligned}\tag{A13}$$

For case (4):

$$\begin{aligned}\Pr(C^k=1|\xi^k)&\approx 1-(1-2p_d)\exp(-2\eta_s u),\\\Pr(C^l=1|\xi^l)&\approx 2p_d,\end{aligned}\tag{A14}$$

$$\begin{aligned}\Pr(C^k=1|n^k=\xi^k)&\approx 1-(1-2p_d)(1-\eta_s)^2,\\\Pr(C^l=1|n^l=\xi^l)&\approx 2p_d.\end{aligned}\tag{A15}$$

The expected pair rate contributed during each round is

$$r_p(p,\delta)=\left[\frac{1}{p[1-(1-p)^\delta]}+\frac{1}{p}\right]^{-1}.\tag{A16}$$

The expected successful click probability, i.e., the total transmittance of each round, is

$$\begin{aligned}p:=\Pr(C^k=1)&=\sum_{\xi^k}\Pr(C^k=1|\xi^k)\Pr(\xi^k)\\&=\frac{1}{4}\sum_{\xi^k}\Pr(C^k=1|\xi^k)\\&=\frac{1}{4}\{2[1-(1-2p_d)e^{-\eta_s\mu}]\\&\quad+2p_d+[1-(1-2p_d)e^{-2\eta_s\mu}]\}\\&\approx\eta_s\mu.\end{aligned}\tag{A17}$$

The Z-pair ratio r_s is expressed as

$$\begin{aligned}r_s=\Pr(E|C)&=\Pr(\xi^k\oplus\xi^l=11|C^k=1,C^l=1)\\&=\sum_{\xi^k\oplus\xi^l=11}\Pr(\xi^k|C^k=1)\Pr(\xi^l|C^l=1)\\&=\sum_{\xi^k\oplus\xi^l=11}\frac{\Pr(C^k=1|\xi^k)\Pr(\xi^k)}{\Pr(C^k=1)}\frac{\Pr(C^l=1|\xi^l)\Pr(\xi^l)}{\Pr(C^l=1)}\\&=\frac{1}{16}\frac{1}{p^2}\sum_{\xi^k\oplus\xi^l=11}\Pr(C^k=1|\xi^k)\Pr(C^l=1|\xi^l)\\&=\frac{1}{8}\frac{1}{p^2}[1-(1-2p_d)\exp(-\eta_s\mu)]^2.\end{aligned}\tag{A18}$$

The expected quantum bit error rate $E_{(\mu,\mu)}^{ZZ}$ of the (k,l) pair is

$$\begin{aligned}E_{(\mu,\mu)}^{ZZ}&=\Pr(\mathcal{E}|E,C)\\&=\frac{\Pr(\mathcal{E},E|C)}{\Pr(E|C)}=\frac{\Pr(\mathcal{E}\,|C)}{\Pr(E|C)}\\&=r_s^{-1}\Pr(\mathcal{E}\,|C).\end{aligned}\tag{A19}$$

The erroneous pair event is included in the valid pair event. Therefore, the erroneous probability can be written as

$$\begin{aligned}\Pr(\mathcal{E}|C)&=\Pr([\xi^k,\xi^l]\in\mathcal{E}\,|C^k=C^l=1)\\&=\sum_{[\xi^k,\xi^l]\in\mathcal{E}}\Pr(\xi^k|C^k=1)\Pr(\xi^l|C^l=1)\\&=\sum_{[\xi^k,\xi^l]\in\mathcal{E}}\frac{\Pr(C^k=1|\xi^k)\Pr(\xi^k)}{\Pr(C^k=1)}\\&\quad\times\frac{\Pr(C^l=1|\xi^l)\Pr(\xi^l)}{\Pr(C^l=1)}\\&=\frac{1}{16}\frac{1}{p^2}\sum_{[\xi^k,\xi^l]\in\mathcal{E}}\Pr(C^k=1|\xi^k)\Pr(C^l=1|\xi^l).\end{aligned}\tag{A20}$$

With the above Eqs. (A19) and (A20), we can obtain

$$\begin{aligned}E_{(\mu,\mu)}^{ZZ}&=\frac{1}{16}\frac{1}{r_s p^2}\sum_{[\xi^k,\xi^l]\in\mathcal{E}}\Pr(C^k=1|\xi^k)\Pr(C^l=1|\xi^l)\\&=\frac{1}{4}\frac{1}{r_s p^2}p_d[1-(1-2p_d)\exp(-2\eta_s\mu)].\end{aligned}\tag{A21}$$

Then, we calculate the expected single-photon pair ratio $\bar{q}_{11}$ in the effective Z pairs as follows:

$$\begin{aligned}\bar{q}_{11}=\Pr(S|E,C)&=\frac{\Pr(S,E,C)}{\Pr(E,C)}=\frac{1}{r_s p^2}\Pr(S,E,C)\\&=\frac{1}{r_s p^2}\sum_{\xi^k,\xi^l}\Pr(S,E,C|\xi^k,\xi^l)\Pr(\xi^k,\xi^l)\\&=\frac{1}{16}\frac{1}{r_s p^2}\sum_{\xi^k\oplus\xi^l=11}\Pr(S,C|\xi^k,\xi^l)\\&=\frac{1}{16}\frac{1}{r_s p^2}\sum_{\xi^k\oplus\xi^l=11}\Pr(C|S,\xi^k,\xi^l)\Pr(S|\xi^k,\xi^l)\end{aligned}$$

$$= \frac{1}{16}\frac{P_\mu(1)^2}{r_s p^2} \sum_{\xi^k \oplus \xi^l = 11} \Pr(C^k = 1 | n^k = \xi^k) \times \Pr(C^l = 1 | n^l = \xi^l)$$
$$= \frac{1}{8}\frac{P_\mu(1)^2}{r_s p^2}[1 - (1 - 2p_d)(1 - \eta_s)]^2, \tag{A22}$$

where $P_\mu(k) = \exp(-\mu)\frac{\mu^k}{k!}$ is the Poisson distribution, $\eta_s = \eta_A = \eta_B$, $\eta_A(\eta_B)$ is the transmittance from Alice (Bob) to Charlie.

In the mode-pairing QKD scheme, if the decoy-state estimation is perfect, then the gain and error rate of X basis can be directly estimated by using the formula as follows [62]:

$$Y_{(1,1)} = (1 - p_d)^2\left[\frac{\eta_A\eta_B}{2} + (2\eta_A + 2\eta_B - 3\eta_A\eta_B)p_d + 4(1 - \eta_A)(1 - \eta_B)p_d^2\right],$$
$$e^{XX}_{(1,1)} = \frac{\left[e_0 Y_{(1,1)} - (e_0 - e_d)(1 - p_d)^2\frac{\eta_A\eta_B}{2}\right]}{Y_{(1,1)}}. \tag{A23}$$

APPENDIX B: SECURITY OF MP-QKD BASED ON QUANTUM INFORMATION THEORY

The formula of the key rate based on information theory is [63,64]

$$R = \min_{\sigma_{AB}\in\Gamma} S(X|E) - H(X|Y), \tag{B1}$$

where Γ is the ensemble of all density operators σ_{AB} on the 2×2-dimensional Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, $S(X|E)$ is the von Neumann entropy, indicating the uncertainty of the eavesdropper's (Eve's) auxiliary state E for the Alice's measurement result X, and $H(X|Y)$ is the Shannon entropy, indicating the uncertainty of the receiver Bob's measurement result Y to Alice's measurement result X.

Similar to the security analysis based on the entanglement purification protocol, Alice and Bob prepare quantum states, $|1,0\rangle^{k,l}$ and $|0,1\rangle^{k,l}$ are the eigenstates in the Z basis, $|+\rangle = (|1,0\rangle^{k,l} + |0,1\rangle^{k,l})/\sqrt{2}$ and $|-\rangle = (|1,0\rangle^{k,l} - |0,1\rangle^{k,l})/\sqrt{2}$ arethe eigenstates in the X basis, who then send them to Charlie for the Bell-state measurement, where $|1,0\rangle^{k,l} = |1\rangle^k|0\rangle^l$ indicates that there is one photon in time-bin k and zero photons in time-bin l. Before Alice and Bob measure the quantum states, the entire system can be described by the following quantum state:

$$|\Psi\rangle_{ABE} := \sum_{j=0}^{3}\sqrt{\lambda_j}|\Phi_j\rangle_{AB} \otimes |e_j\rangle_E, \tag{B2}$$

where

$$|\Phi_0\rangle = \frac{1}{\sqrt{2}}\left(|1,0\rangle_A^{k,l}|1,0\rangle_B^{k,l} + |0,1\rangle_A^{k,l}|0,1\rangle_B^{k,l}\right),$$
$$|\Phi_1\rangle = \frac{1}{\sqrt{2}}\left(|1,0\rangle_A^{k,l}|1,0\rangle_B^{k,l} - |0,1\rangle_A^{k,l}|0,1\rangle_B^{k,l}\right),$$
$$|\Phi_2\rangle = \frac{1}{\sqrt{2}}\left(|1,0\rangle_A^{k,l}|0,1\rangle_B^{k,l} + |0,1\rangle_A^{k,l}|1,0\rangle_B^{k,l}\right),$$
$$|\Phi_3\rangle = \frac{1}{\sqrt{2}}\left(|1,0\rangle_A^{k,l}|0,1\rangle_B^{k,l} - |0,1\rangle_A^{k,l}|1,0\rangle_B^{k,l}\right), \tag{B3}$$

and $\sum_{j=0}^{3}\lambda_j = 1$, $\lambda_j (j = \{0,1,2,3\})$ characterize quantum channel and the single-photon error rates in the X basis and Z basis are constrained by $\lambda_1 + \lambda_3 = e_x$ and $\lambda_2 + \lambda_3 = e_z$, respectively. The subscript A denotes mode "Alice" and B denotes mode "Bob". $|e_j\rangle_E$ is an orthonormal basis of a four-dimensional Hilbert space $\mathcal{H}_E$.

Since the quantum channel is controlled by Eve, when the measurement results of Alice and Bob are 00, 11, 01, 10, respectively, the quantum states that Eve can obtain are

$$|\varphi_{0,0}\rangle = \frac{1}{\sqrt{2}}(\sqrt{\lambda_0}|e_0\rangle + \sqrt{\lambda_1}|e_1\rangle),$$
$$|\varphi_{1,1}\rangle = \frac{1}{\sqrt{2}}(\sqrt{\lambda_0}|e_0\rangle - \sqrt{\lambda_1}|e_1\rangle),$$
$$|\varphi_{0,1}\rangle = \frac{1}{\sqrt{2}}(\sqrt{\lambda_2}|e_2\rangle + \sqrt{\lambda_3}|e_3\rangle),$$
$$|\varphi_{1,0}\rangle = \frac{1}{\sqrt{2}}(\sqrt{\lambda_2}|e_2\rangle - \sqrt{\lambda_3}|e_3\rangle). \tag{B4}$$

Note that Eve can choose the optimal parameter $\lambda_j (j = \{0,1,2,3\})$ to reduce the security key rate, but λ_j is constrained by the quantum bit error rate of two different bases.

After the interference of Eve in the quantum channel, Alice and Bob obtain the density operators σ_{XYE} of the entire system by the orthonormal measurement of $\mathcal{H}_A$ and $\mathcal{H}_B$

$$\sigma_{XYE} = \sum_{x,y}|x\rangle\langle x| \otimes |y\rangle\langle y| \otimes |\varphi_{x,y}\rangle\langle\varphi_{x,y}|. \tag{B5}$$

Based on the above analysis, we can easily obtain

$$H(\sigma_{XE}) = 1 + h(\lambda_0 + \lambda_1),$$
$$H(\sigma_E) = h(\lambda_0 + \lambda_1) + (\lambda_0 + \lambda_1)h\left(\frac{\lambda_0}{\lambda_0 + \lambda_1}\right) + (\lambda_2 + \lambda_3)h\left(\frac{\lambda_2}{\lambda_2 + \lambda_3}\right),$$
$$H(X|Y) = h(\lambda_0 + \lambda_1). \tag{B6}$$

Therefore, the final formula of key rate is

$$R \geqslant \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} S(X|E) - H(X|Y)$$
$$= \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} H(\sigma_{XE}) - H(\sigma_E) - H(X|Y)$$
$$= \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} 1 - (\lambda_0 + \lambda_1)h\left(\frac{\lambda_0}{\lambda_0 + \lambda_1}\right) - (\lambda_2 + \lambda_3)h\left(\frac{\lambda_2}{\lambda_2 + \lambda_3}\right) - h(\lambda_0 + \lambda_1), \tag{B7}$$

where $h(x) = -x\log_2(x) - (1 - x)\log_2(1 - x)$ is the binary Shannon entropy function.

Ideally, assuming $e_x = e_z = Q$, we can obtain

$$\lambda_1 + \lambda_3 = Q,$$
$$\lambda_2 + \lambda_3 = Q,$$
$$\lambda_0 + \lambda_1 + \lambda_2 + \lambda_3 = 1, \tag{B8}$$

which can be rewritten as

$$\begin{aligned}\lambda_0 &= 1-2Q+\lambda_3,\\ \lambda_1 &= Q-\lambda_3,\\ \lambda_2 &= Q-\lambda_3,\end{aligned} \tag{B9}$$

where Q denotes the bit error rate.

By substituting Eq. (B9) into Eq. (B7), the formula of the key rate is given by

$$\begin{aligned}R \geqslant \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} & 1-(1-Q)h\left(\frac{1-2Q+\lambda_3}{1-Q}\right)\\ & -Qh\left(\frac{Q-\lambda_3}{Q}\right)-h(Q).\end{aligned} \tag{B10}$$

There is a minimum value in the Eq. (B10), i.e., $\frac{\partial R}{\partial Q}=0$ is satisfied, which requires that $\lambda_3 = Q^2$.

Therefore, to find the minimum value of the Eq. (B7), the following conditions must be satisfied for λ_0, λ_1, λ_2, and λ_3, respectively:

$$\begin{aligned}\lambda_0 &= 1-2Q+\lambda_3,\\ \lambda_1 &= Q-\lambda_3,\\ \lambda_2 &= Q-\lambda_3,\\ \lambda_3 &= Q^2.\end{aligned} \tag{B11}$$

In practical MP-QKD systems, phase-randomized weakly coherent sources are widely used to prepare quantum states. According to the specific protocol steps in Sec. II, Alice and Bob only use the successfully paired Z basis to generate a key and they use the decoy state method to resist photon number splitting attacks. In total, all errors are corrected by Alice and Bob so that in the Eq. (B6) $H(X|Y)\leqslant fh(E^{ZZ}_{(\mu,\mu)})$. $h(E^{ZZ}_{(\mu,\mu)})$ is the maximum information that Eve steals during the error correction step. Therefore, the secret key rate of the MP-QKD protocol can be given by

$$\begin{aligned}R \geqslant \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} & r_p(p,\delta)r_s\left\{\bar{q}_{11}\left[1-(\lambda_0+\lambda_1)h\left(\frac{\lambda_0}{\lambda_0+\lambda_1}\right)\right.\right.\\ & \left.\left.-(\lambda_2+\lambda_3)h\left(\frac{\lambda_2}{\lambda_2+\lambda_3}\right)\right]-fh\left(E^{ZZ}_{(\mu,\mu)}\right)\right\},\end{aligned} \tag{B12}$$

where $r_p(p,\delta)$ is the expected pair rate contributed during each round, r_s is the probability that a generated pair is a Z pair, and $\bar{q}_{11}$ is the expected single-photon pair ratio in all Z pairs. f is the error-correction efficiency, $E^{ZZ}_{(\mu,\mu)}$ is the bit-error rate of the Z pairs.

APPENDIX C: SECURITY OF MP-QKD WITH AD

In this section, we calculate the parameters in Eq. (3) to estimate the secret key rate. In our protocol, Alice and Bob divide their raw key into blocks of b size $\{x_1, x_2, \ldots, x_b\}$ and $\{y_1, y_2, \ldots, y_b\}$. Alice depends on a randomly chosen bit $c\in\{0,1\}$ and sends the message $m=\{m_1,m_2,\ldots,m_b\}=\{x_1\oplus c, x_2\oplus c,\ldots,x_b\oplus c\}$ to Bob through an authenticated classical channel. They accept the block if and only if Bob announces the result of $\{m_1\oplus y_1, m_2\oplus y_2,\ldots,m_b\oplus y_b\}$ is either $\{0,0,\ldots,0\}$ or $\{1,1,\ldots,1\}$. By a straightforward calculation, the probability of a successful advantage distillation on a block of length b is

$$q_s = \left(E^{ZZ}_{(\mu,\mu)}\right)^b + \left(1-E^{ZZ}_{(\mu,\mu)}\right)^b. \tag{C1}$$

For the message $m=\{m_1,m_2,\ldots,m_b\}$, once Eve gets any one of the measurements in $\{m_1,m_2,\ldots,m_b\}$, she (he) can obtain all b measurements. Therefore, it can only be used to generate the secret key if all the b pulses used for pairing are the single-photon state and the probability is $(\bar{q}_{11})^b$.

With these, Eq. (B12) can be modified as

$$\begin{aligned}\tilde{R} \geqslant \max_b \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} & \frac{1}{b}q_s\, r_p(p,\delta)r_s\\ & \times\left\{(\bar{q}_{11})^b\left[1-(\tilde{\lambda}_0+\tilde{\lambda}_1)h\left(\frac{\tilde{\lambda}_0}{\tilde{\lambda}_0+\tilde{\lambda}_1}\right)\right.\right.\\ & \left.\left.-(\tilde{\lambda}_2+\tilde{\lambda}_3)h\left(\frac{\tilde{\lambda}_2}{\tilde{\lambda}_2+\tilde{\lambda}_3}\right)\right]-fh\left(\tilde{E}^{ZZ}_{(\mu,\mu)}\right)\right\},\end{aligned} \tag{C2}$$

subject to

$$\begin{aligned}e^{XX}_{(1,1)} &= \lambda_1+\lambda_3,\\ e^{ZZ}_{(1,1)} &= \lambda_2+\lambda_3,\end{aligned} \tag{C3}$$

$$q_s = \left(E^{ZZ}_{(\mu,\mu)}\right)^b + \left(1-E^{ZZ}_{(\mu,\mu)}\right)^b,$$

$$\tilde{E}^{ZZ}_{(\mu,\mu)} = \frac{\left(E^{ZZ}_{(\mu,\mu)}\right)^b}{\left(E^{ZZ}_{(\mu,\mu)}\right)^b + \left(1-E^{ZZ}_{(\mu,\mu)}\right)^b}, \tag{C4}$$

and

$$\begin{aligned}\tilde{\lambda}_0 &= \frac{(\lambda_0+\lambda_1)^b+(\lambda_0-\lambda_1)^b}{2[(\lambda_0+\lambda_1)^b+(\lambda_2+\lambda_3)^b]},\\ \tilde{\lambda}_1 &= \frac{(\lambda_0+\lambda_1)^b-(\lambda_0-\lambda_1)^b}{2[(\lambda_0+\lambda_1)^b+(\lambda_2+\lambda_3)^b]},\\ \tilde{\lambda}_2 &= \frac{(\lambda_2+\lambda_3)^b+(\lambda_2-\lambda_3)^b}{2[(\lambda_0+\lambda_1)^b+(\lambda_2+\lambda_3)^b]},\\ \tilde{\lambda}_3 &= \frac{(\lambda_2+\lambda_3)^b-(\lambda_2-\lambda_3)^b}{2[(\lambda_0+\lambda_1)^b+(\lambda_2+\lambda_3)^b]},\end{aligned} \tag{C5}$$

where $\tilde{E}^{ZZ}_{(\mu,\mu)}$ represents the overall error rate after the AD method step.

[1] P. Shor, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA* (IEEE, Piscataway, NJ, 1994), pp. 124–134.

[2] L. K. Grover, in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, Pennsylvania, USA* (ACM, New York, 1996), pp. 212–219.

[3] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

[4] L.-C. Kwek, L. Cao, W. Luo, Y. Wang, S. Sun, X. Wang, and A. Q. Liu, Chip-based quantum key distribution, AAPPS Bull. **31**, 15 (2021).

[5] Q. Liu, Y. Huang, Y. Du, Z. Zhao, M. Geng, Z. Zhang, and K. Wei, Advances in chip-based quantum key distribution, Entropy **24**, 1334 (2022).

[6] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[7] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Quantum Inf. Comput. **4**, 325 (2004).

[8] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Loss-tolerant quantum cryptography with imperfect sources, Phys. Rev. A **90**, 052314 (2014).

[9] Y.-J. Qian, D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Hacking the Quantum Key Distribution System by Exploiting the Avalanche-Transition Region of Single-Photon Detectors, Phys. Rev. Appl. **10**, 064062 (2018).

[10] S. Sun and F. Xu, Security of quantum key distribution with source and detection imperfections, New J. Phys. **23**, 023011 (2021).

[11] C. Huang, Y. Chen, L. Jin, M. Geng, J. Wang, Z. Zhang, and K. Wei, Experimental secure quantum key distribution in the presence of polarization-dependent loss, Phys. Rev. A **105**, 012421 (2022).

[12] A. Huang, A. Mizutani, H.-K. Lo, V. Makarov, and K. Tamaki, Characterization of State-Preparation Uncertainty in Quantum Key Distribution, Phys. Rev. Appl. **19**, 014048 (2023).

[13] Y. Chen, C. Huang, Z. Chen, W. He, C. Zhang, S. Sun, and K. Wei, Experimental study of secure quantum key distribution with source and detection imperfections, Phys. Rev. A **106**, 022614 (2022).

[14] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (2007).

[15] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[16] L. Cao, W. Luo, Y. X. Wang, J. Zou, R. D. Yan, H. Cai, Y. Zhang, X. L. Hu, C. Jiang, W. J. Fan *et al.*, Chip-Based Measurement-Device-Independent Quantum Key Distribution Using Integrated Silicon Photonic Systems, Phys. Rev. Appl. **14**, 011001(R) (2020).

[17] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, and J.-W. Pan, High-Speed Measurement-Device-Independent Quantum Key Distribution with Integrated Silicon Photonics, Phys. Rev. X **10**, 031030 (2020).

[18] R. I. Woodward, Y. Lo, M. Pittaluga, M. Minder, T. Paraïso, M. Lucamarini, Z. Yuan, and A. Shields, Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers, npj Quantum Inf. **7**, 58 (2021).

[19] X.-Y. Zhou, H.-J. Ding, M.-S. Sun, S.-H. Zhang, J.-Y. Liu, C.-H. Zhang, J. Li, and Q. Wang, Reference-Frame-Independent Measurement-Device-Independent Quantum Key Distribution Over 200 km of Optical Fiber, Phys. Rev. Appl. **15**, 064016 (2021).

[20] 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).

[21] G.-Z. Tang, C.-Y. Li, and M. Wang, Polarization discriminated time-bin phase-encoding measurement-device-independent quantum key distribution, Quantum Eng. **3**, e79 (2021).

[22] J. Gu, X.-Y. Cao, Y. Fu, Z.-W. He, Z.-J. Yin, H.-L. Yin, and Z.-B. Chen, Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources, Sci. Bull. **67**, 2167 (2022).

[23] C.-H. Zhang, C.-M. Zhang, and Q. Wang, Efficient passive measurement-device-independent quantum key distribution, Phys. Rev. A **99**, 052325 (2019).

[24] W. Wang, F. Xu, and H.-K. Lo, Asymmetric Protocols for Scalable High-Rate Measurement-Device-Independent Quantum Key Distribution Networks, Phys. Rev. X **9**, 041012 (2019).

[25] F.-Y. Lu, Z.-Q. Yin, G.-J. Fan-Yuan, R. Wang, H. Liu, S. Wang, W. Chen, D.-Y. He, W. Huang, B.-J. Xu, G.-C. Guo, and Z.-F. Han, Efficient decoy states for the reference-frame-independent measurement-device-independent quantum key distribution, Phys. Rev. A **101**, 052318 (2020).

[26] 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).

[27] X.-F. Wang, X.-J. Sun, Y.-X. Liu, W. Wang, B.-X. Kan, P. Dong, and L.-L. Zhao, Transmission of photonic polarization states from geosynchronous earth orbit satellite to the ground, Quantum Eng. **3**, e73 (2021).

[28] C. Jiang, X.-L. Hu, Z.-W. Yu, and X.-B. Wang, Measurement-device-independent quantum key distribution protocol with phase post-selection, Photon. Res. **10**, 1703 (2022).

[29] 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 (London) **557**, 400 (2018).

[30] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, Nat. Commun. **5**, 5235 (2014).

[31] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[32] X. Ma, P. Zeng, and H. Zhou, Phase-Matching Quantum Key Distribution, Phys. Rev. X **8**, 031043 (2018).

[33] 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).

[34] Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu, and X.-B. Wang, Sending-or-not-sending twin-field quantum key distribution in practice, Sci. Rep. **9**, 3080 (2019).

[35] 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).

[36] V. Chistiakov, A. Kozubov, A. Gaidash, A. Gleim, and G. Miroshnichenko, Feasibility of twin-field quantum key distri-

bution based on multi-mode coherent phase-coded states, Opt. Express **27**, 36551 (2019).
[37] F. Grasselli, Álvaro Navarrete, and M. Curty, Asymmetric twin-field quantum key distribution, New J. Phys. **21**, 113032 (2019).
[38] C.-M. Zhang, Y.-W. Xu, R. Wang, and Q. Wang, Twin-Field Quantum Key Distribution with Discrete-Phase-Randomized Sources, Phys. Rev. Appl. **14**, 064070 (2020).
[39] W. Wang and H.-K. Lo, Simple method for asymmetric twin-field quantum key distribution, New J. Phys. **22**, 013020 (2020).
[40] B.-H. Li, Y.-M. Xie, Z. Li, C.-X. Weng, C.-L. Li, H.-L. Yin, and Z.-B. Chen, Long-distance twin-field quantum key distribution with entangled sources, Opt. Lett. **46**, 5529 (2021).
[41] L. Zhou, J. Lin, Y. Jing, and Z. Yuan, Twin-field quantum key distribution without optical frequency dissemination, Nat. Commun. **14**, 928 (2023).
[42] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. J. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, Nat. Photonics **13**, 334 (2019).
[43] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending, Phys. Rev. Lett. **123**, 100505 (2019).
[44] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution, Phys. Rev. Lett. **123**, 100506 (2019).
[45] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li *et al.*, Implementation of quantum key distribution surpassing the linear rate-transmittance bound, Nat. Photonics **14**, 422 (2020).
[46] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu *et al.*, Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas, Nat. Photonics **15**, 570 (2021).
[47] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Zhu *et al.*, Twin-field quantum key distribution over 830-km fibre, Nat. Photonics **16**, 154 (2022).
[48] C. Clivati, A. Meda, S. Donadello, S. Virzì, M. Genovese, F. Levi, A. Mura, M. Pittaluga, Z. Yuan, A. J. Shields *et al.*, Coherent phase transfer for real-world twin-field quantum key distribution, Nat. Commun. **13**, 157 (2022).
[49] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental Twin-Field Quantum key Distribution Over 1000 km Fiber Distance, Phys. Rev. Lett. **130**, 210801 (2023).
[50] P. Zeng, H. Zhou, W. Wu, and X. Ma, Mode-pairing quantum key distribution, Nat. Commun. **13**, 3903 (2022).
[51] Z.-H. Wang, Z.-Q. Yin, S. Wang, R. Wang, F.-Y. Lu, W. Chen, D.-Y. He, G.-C. Guo, and Z.-F. Han, Tight finite-key analysis for mode-pairing quantum key distribution, arXiv:2302.13481.
[52] H.-T. Zhu, Y. Huang, H. Liu, P. Zeng, M. Zou, Y. Dai, S. Tang, H. Li, L. You, Z. Wang, Y.-A. Chen, X. Ma, T.-Y. Chen, and J.-W. Pan, Experimental Mode-Pairing Measurement-Device-Independent Quantum Key Distribution without Global Phase Locking, Phys. Rev. Lett. **130**, 030801 (2023).
[53] E. Y.-Z. Tan, C. C.-W. Lim, and R. Renner, Advantage Distillation for Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **124**, 020502 (2020).
[54] H.-W. Li, C.-M. Zhang, M.-S. Jiang, and Q.-Y. Cai, Improving the performance of practical decoy-state quantum key distribution with advantage distillation technology, Commun. Phys. **5**, 53 (2022).
[55] H.-W. Li, R.-Q. Wang, C.-M. Zhang, and Q.-Y. Cai, Improving the performance of twin-field quantum key distribution with advantage distillation technology, arXiv:2202.10059.
[56] R.-Q. Wang, C.-M. Zhang, Z.-Q. Yin, H.-W. Li, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phase-matching quantum key distribution with advantage distillation, New J. Phys. **24**, 073049 (2022).
[57] J.-R. Zhu, C.-M. Zhang, R. Wang, and H.-W. Li, Reference-frame-independent quantum key distribution with advantage distillation, Opt. Lett. **48**, 542 (2023).
[58] X.-L. Jiang, Y. Wang, J.-J. Li, Y.-F. Lu, C.-P. Hao, C. Zhou, and W.-S. Bao, Improving the performance of reference-frame-independent quantum key distribution with advantage distillation technology, Opt. Express **31**, 9196 (2023).
[59] L.-W. Hu, C.-M. Zhang, and H.-W. Li, Practical measurement-device-independent quantum key distribution with advantage distillation, Quantum Inf. Process. **22**, 77 (2023).
[60] F. Xu, Y.-Z. Zhang, Q. Zhang, and J.-W. Pan, Device-Independent Quantum Key Distribution with Random Postselection, Phys. Rev. Lett. **128**, 110506 (2022).
[61] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference, PRX Quantum **3**, 020315 (2022).
[62] X. Maand M. Razavi, Alternative schemes for measurement-device-independent quantum key distribution, Phys. Rev. A **86**, 062319 (2012).
[63] R. Renner, Security of quantum key distribution, Int. J. Quantum Inform. **06**, 1 (2008).
[64] H.-W. Li, W. Chen, J.-Z. Huang, Y. Yao, D. Liu, F.-Y. Li, S. Wang, Z.-Q. Yin, D.-Y. He, Z. Zhou, Y.-H. Li, N.-H. Yu, and Z.-F. Han, Security of quantum key distribution, Sci. Sin.-Phys. Mech. Astron. **42**, 1237 (2012).