Practical asynchronous measurement-device-independent quantum key distribution with advantage distillation

Di Luo,[1] Xin Liu,[1] Kaibiao Qin,[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 January 2024; accepted 11 July 2024; published 6 August 2024)

The advantage distillation (AD) method has proven effective in improving the performance of quantum key distribution (QKD). In this paper we introduce the AD method into a recently proposed asynchronous measurement-device-independent (AMDI) QKD protocol, taking finite-key effects into account. Simulation results show that the AD method significantly enhances AMDI QKD, e.g., extending the transmission distance by 16 km with a total pulse count of $N = 7.24 \times 10^{13}$, and enables AMDI QKD, previously unable to generate keys, to generate keys with a misalignment error rate of 10%. As the AD method can be directly integrated into the current system through refined postprocessing, our results facilitate the practical implementation of AMDI QKD in various applications, particularly in scenarios with high channel losses and misalignment errors.

DOI: 10.1103/PhysRevA.110.022605

I. INTRODUCTION

Quantum key distribution (QKD) enables two legitimate users to share an unconditionally secure key, even in the presence of eavesdroppers with unlimited computational power and storage capacity. Since the proposal of the first QKD by Bennett and Brassard [1], through the extensive efforts of researchers, QKD has achieved significant milestones both theoretically and experimentally [2–11]. It is poised to become a crucial technology ensuring secure communication in the future.

However, due to the gap between the ideal model and practical devices, especially at the detector side [12,13], eavesdroppers can exploit these gaps to steal information [14–20]. Fortunately, measurement-device-independent (MDI) QKD was proposed [21,22], addressing detection loopholes by utilizing Bell state measurements. Currently, most MDI QKD systems [23–31] require strict coincidence detection for key generation, limiting the key rate and transmission distance of MDI QKD and preventing it from surpassing the repeaterless rate-transmittance bound [32,33].

The twin-field (TF) QKD [34], based on the single-photon interference concept, eliminates the need for coincidence detection, surpassing the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [33]. Various TF QKD protocol variants have been proposed [35–38], with experimental demonstrations reported [39–45]. However, TF QKD necessitates stringent phase and frequency locking techniques to stabilize the fluctuation between two coherent states, significantly increasing the system's cost and complexity.

To address these challenges, two recent works, namely, asynchronous MDI (AMDI) QKD [46] or mode-pairing (MP) QKD [47], were proposed almost simultaneously. Using an asynchronous coincidence method, both protocols can surpass the PLOB bound without requiring phase locking and phase tracking techniques. The practicality of these MDI-type QKD protocols has been demonstrated [48,49]. In particular, Zhou *et al.* [49] achieved a breakthrough in the transmission distance of MDI QKD, extending it from 404 km [23] to 508 km over fiber. Furthermore, theoretical developments have been reported [50–53]. Much effort has been put into further extending the distance [23,41,45,54], which is highly sought after in communication.

Advantage distillation (AD), proposed by Maurer [55], is a classical two-way communication protocol used to enhance the error tolerance [56–58]. The core step of the AD method involves dividing raw keys into a few blocks to extract highly correlated keys from weakly correlated keys, thereby increasing the correlation between the raw keys. The AD method has been applied to various QKD protocols [53,59–68] to extend the transmission distance and increase the maximum tolerance of background noise. Importantly, the AD method has been shown to improve performance when considering statistical fluctuations [61–63]. Recently, Liu *et al.* [53] demonstrated that the AD method can significantly enhance the performance of MP QKD. However, whether AD can improve the performance of AMDI QKD, especially when accounting for finite-key effects, remains unknown.

In this paper, building upon the work in Ref. [53], we incorporate the AD method into AMDI QKD [49]. Additionally, we analyze its performance while considering finite-key effects. Using typical experimental parameters of AMDI QKD, the simulation results demonstrate a significant improvement in the key rate and transmission distance and enhance

*Contact author: kjwei@gxu.edu.cn

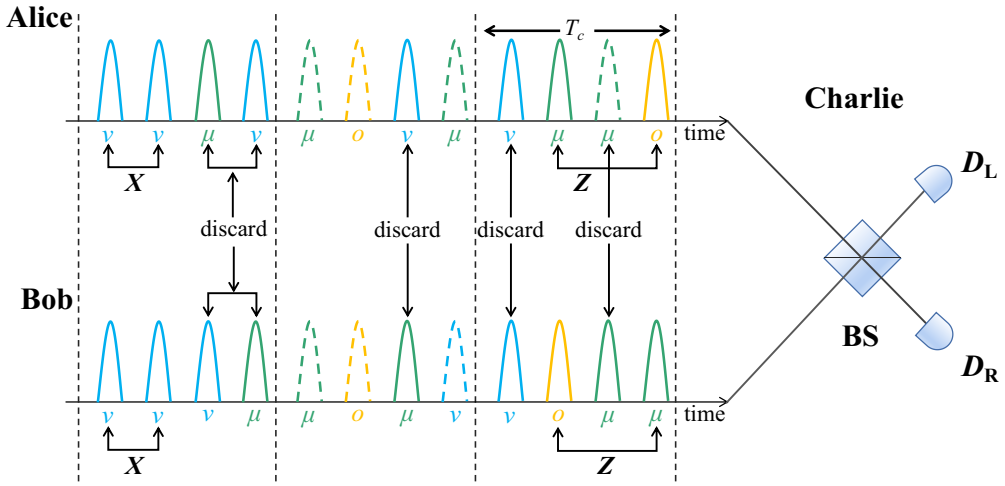

FIG. 1. Schematic diagram of the AMDI QKD protocol by using click filtering operation. Alice and Bob send the prepared state to Charlie for interference measurement. In the maximum pairing interval T_c, for any successful coincidence, if the total pairing intensity $\kappa^{\text{tot}}_{a\,(b)} = \mu$ as the Z basis, if the total pairing intensity $\kappa^{\text{tot}}_{a\,(b)} = 2\nu$ as the X basis, and if the total pairing intensity $\kappa^{\text{tot}}_{a\,(b)} \geqslant \mu + \nu$, then coincidence is discarded. If the click events are (ν_a, μ_b) or (μ_a, ν_b), these click events are discarded. If one of or both Alice and Bob do not click in the same time bin, the corresponding data are discarded. Here BS is the beam splitter and D_L (D_R) represents the left (right) detector.

tolerance to misalignment errors when accounting for finite-key effects.

The remainder of the article is structured as follows. In Sec. II we briefly introduce the original AMDI QKD protocol. In Sec. III we analyze the postprocessing step using the AD method. In Sec. IV we present simulation results for a more practical AMDI QKD model, comparing the performance of AMDI QKD with and without AD. We discuss and summarize our findings in Sec. V.

II. AMDI QKD PROTOCOL

Here we provide a brief overview of the AMDI QKD protocol [46,49], using a three-intensity decoy-state scheme as an example. The schematic diagram of the scheme is shown in Fig. 1 and the detailed process is as follows.

Step 1: Preparation and measurement. This step is repeated for N rounds to accumulate sufficient data. For each round or time bin $i \in \{1, 2, \ldots, N\}$, Alice randomly prepares a weak coherent state pulse $|e^{\mathrm{i}\theta^i_a}\sqrt{\kappa^i_a}\rangle$, with intensities $\kappa^i_a \in \{\mu_a, \nu_a, o_a\}$ $(\mu_a > \nu_a > o_a = 0)$ and the corresponding probabilities p_{μ_a}, p_{ν_a}, and $1 - p_{\mu_a} - p_{\nu_a}$. In this context, the random phase $\theta^i_a = 2\pi M^i_a/M$, with $M^i_a \in \{0, 1, \ldots, M-1\}$. Similarly, Bob prepares weak coherent pulses $|e^{\mathrm{i}\theta^i_b}\sqrt{\kappa^i_b}\rangle$, where $\kappa^i_b \in \{\mu_b, \nu_b, o_b\}$ using the same operation as Alice. Next, Alice and Bob send their prepared optical pulses to Charlie through the quantum channel. Charlie performs the interference measurement and then announces which detector (D_L or D_R) clicked and the corresponding time bin i.

Step 2: Click filtering. For each click, Alice and Bob announce whether they had sent a decoy-state pulse of intensity ν_a (ν_b). If the click event is $(\mu_a|\nu_b)$ and $(\nu_a|\mu_b)$, a click filtering operation is applied to discard this click event. All other click events are kept. Here we use $(\kappa_a|\kappa_b)$ to denote a successful click given that Alice and Bob sent pulse intensities of κ_a and κ_b.

Step 3: Coincidence pairing. For all kept clicks, Alice and Bob pair two adjacent clicks within the time interval T_c to form a successful coincidence. If the partner cannot be found within the maximum pairing interval T_c, Alice and Bob discard the corresponding lone click. For all successful pairing coincidences, Alice and Bob calculate the total intensity $[\kappa^e_a + \kappa^l_a = \kappa^{\text{tot}}_a, \kappa^e_b + \kappa^l_b = \kappa^{\text{tot}}_b]$ and the phase difference $\varphi_{a\,(b)} = \theta^l_{a\,(b)} - \theta^e_{a\,(b)}$ between two time bins, where the superscript e (l) denotes the early (late) time bin and κ^{tot}_a (κ^{tot}_b) denotes the total intensity of the pairing coincidence, and the notation $[\kappa^{\text{tot}}_a, \kappa^{\text{tot}}_b]$ denotes pairing coincidence where the total intensity in the two time bins of Alice (Bob) is κ^{tot}_a (κ^{tot}_b).

Step 4: Sifting. Alice and Bob publish the computational results of all successful coincidences and discard the events if $\kappa^{\text{tot}}_{a\,(b)} \geqslant \mu_{a\,(b)} + \nu_{a\,(b)}$. For $[\mu_a, \mu_b]$ coincidence, if Alice (Bob) sends intensity μ_a (o_b) in the early time bin and sends intensity o_a (μ_b) in the late time bin, they obtain Z basis bit 0; otherwise, bit 1 is obtained. For $[2\nu_a, 2\nu_b]$ coincidence, Alice and Bob calculate the relative phase difference $\varphi_{ab} = (\varphi_a - \varphi_b) \mathrm{mod} 2\pi$. If $\varphi_{ab} = 0$ or $\varphi_{ab} = \pi$, they extract X basis bit 0. As an extra step for the X basis, if $\varphi_{ab} = 0$ and both detectors are clicked or $\varphi_{ab} = \pi$ and the same detector clicked twice, Bob flips his bit value. The coincidence with other phase differences ($\varphi_{ab} \neq 0$ or π) is discarded.

Step 5: Postprocessing. Alice and Bob assign their data to different data sets $S_{[\kappa^{\text{tot}}_a, \kappa^{\text{tot}}_b]}$ and count the corresponding amount $n_{[\kappa^{\text{tot}}_a, \kappa^{\text{tot}}_b]}$. Then they respectively generate raw keys $\mathcal{Z}$ by using data $n_{[\mu_a,\mu_b]}$ from $S_{[\mu_a,\mu_b]}$. The secret keys are obtained through error correction and privacy amplification with a security bound ε_{sec}.

After the above steps, the final key rate of AMDI QKD with considering finite-key effects can be expressed as

$$R = \frac{1}{N}\left(\underline{s}^z_0 + \underline{s}^z_{11}\left[1 - H\left(\overline{\phi}^z_{11}\right)\right] - \lambda_{\text{EC}} - \log_2\frac{2}{\varepsilon_{\text{cor}}} - 2\log_2\frac{2}{\varepsilon'\hat{\varepsilon}} - 2\log_2\frac{1}{2\varepsilon_{\text{PA}}}\right), \quad (1)$$

where N is the total number of pulses, $\underline{s}_0^z$ is the lower bound of the estimated number of vacuum events, s_{11}^z is event number of single-photon pair, and ϕ_{11}^z is phase error rate of a single-photon pair in the Z basis. The underline and overline of the parameters denote the lower and upper bounds, respectively. Here $\lambda_{\mathrm{EC}} = n_{[\mu_a,\mu_b]} f H(E_z)$ represents the maximum amount of information stolen by Eve during the error correction step; f is the correction efficiency, E_z is the quantum bit error rate (QBER), and $n_{[\mu_a,\mu_b]}$ is the total successful pairing number in the Z basis. In addition, $\varepsilon_{\mathrm{cor}}$ implies the failure probability in the error correction, $\varepsilon_{\mathrm{PA}}$ denotes the failure probability in the privacy amplification, and ε' and $\hat{\varepsilon}$ are coefficients after using smooth entropies. The specific calculation of the parameters is in Appendix A.

III. AMDI QKD WITH ADVANTAGE DISTILLATION

As a postprocessing method, AD only changes the step of the data processing to improve the performance. Thus AMDI QKD with AD is different from the original AMDI QKD only in step 5. The new step 5 is as follows.

New step 5. After obtaining the raw key, Alice and Bob divide their raw key into b-bit blocks $\{x_1, x_2, \ldots, x_b\}$ and $\{y_1, y_2, \ldots, y_b\}$. Alice chooses a local random bit $c \in \{0, 1\}$ and sends 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. Alice and Bob only keep the block if Bob calculates the results of $\{m_1 \oplus y_1, m_2 \oplus y_2, \ldots, m_b \oplus y_b\} = \{0, 0, \ldots, 0\}$ or $\{1, 1, \ldots, 1\}$ and then retain the first bits x_1 and y_1 as the raw key. It is noteworthy that if the block size b is 1, it means that the AD step has not been executed. Finally, the final keys are obtained through error correction and privacy amplification.

To gain deeper insights into the enhanced key rate achieved through the AD method, we employ the information security theoretical analysis method to reassess the key rate of AMDI QKD. The detailed analysis is provided in Appendix B. The key rate of AMDI QKD is reformulated as

$$R \geqslant \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} \frac{1}{N} n_z \left\{ \frac{\underline{s}_0^z}{n_z} + \frac{\underline{s}_{11}^z}{n_z} \left[1 - (\lambda_1+\lambda_2) H\left(\frac{\lambda_1}{\lambda_1+\lambda_2}\right) - (\lambda_3+\lambda_4) H\left(\frac{\lambda_3}{\lambda_3+\lambda_4}\right) \right] - f H(E_z) - \frac{1}{n_z}\left(\log_2 \frac{2}{\varepsilon_{\mathrm{cor}}} + 2\log_2 \frac{2}{\varepsilon'\hat{\varepsilon}} + 2\log_2 \frac{1}{2\varepsilon_{\mathrm{PA}}} \right) \right\}, \tag{2}$$

where $\sum_{i=1}^4 \lambda_i = 1$ and the λ_i $(i = 1, 2, 3, 4)$ satisfy the following relationships with the error rates: $\underline{\phi}_{11}^z \leqslant \lambda_2 + \lambda_4 \leqslant \overline{\phi}_{11}^z$ and $\underline{e}_{11}^z \leqslant \lambda_3 + \lambda_4 \leqslant \overline{e}_{11}^z$. After postprocessing using the AD method (new step 5), the key rate of AMDI QKD can be rewritten as (details can be found in Appendix C)

$$\tilde{R} \geqslant \max_b \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} \frac{1}{N}\frac{n_z}{b} q_{\mathrm{succ}} \left\{ \left(\frac{\underline{s}_0^z}{n_z}\right)^b + \left(\frac{\underline{s}_{11}^z}{n_z}\right)^b \left[1 - (\tilde{\lambda}_1+\tilde{\lambda}_2) H\left(\frac{\tilde{\lambda}_1}{\tilde{\lambda}_1+\tilde{\lambda}_2}\right) - (\tilde{\lambda}_3+\tilde{\lambda}_4) H\left(\frac{\tilde{\lambda}_3}{\tilde{\lambda}_4+\tilde{\lambda}_4}\right) \right] - f H(\tilde{E}_z) - \frac{b}{n_z q_{\mathrm{succ}}}\left(\log_2 \frac{2}{\varepsilon_{\mathrm{cor}}} + 2\log_2 \frac{2}{\varepsilon'\hat{\varepsilon}} + 2\log_2 \frac{1}{2\varepsilon_{\mathrm{PA}}} \right) \right\}, \tag{3}$$

subject to

$$\begin{aligned} \underline{\phi}_{11}^z &\leqslant \lambda_2 + \lambda_4 \leqslant \overline{\phi}_{11}^z, \\ \underline{e}_{11}^z &\leqslant \lambda_3 + \lambda_4 \leqslant \overline{e}_{11}^z, \\ q_{\mathrm{succ}} &= (E_z)^b + (1-E_z)^b, \\ \tilde{E}_z &= \frac{(E_z)^b}{(E_z)^b + (1-E_z)^b}, \end{aligned} \tag{4}$$

and

$$\begin{aligned} \tilde{\lambda}_1 &= \frac{(\lambda_1+\lambda_2)^b + (\lambda_1-\lambda_2)^b}{2p_{\mathrm{succ}}}, \\ \tilde{\lambda}_2 &= \frac{(\lambda_1+\lambda_2)^b - (\lambda_1-\lambda_2)^b}{2p_{\mathrm{succ}}}, \\ \tilde{\lambda}_3 &= \frac{(\lambda_3+\lambda_4)^b + (\lambda_3-\lambda_4)^b}{2p_{\mathrm{succ}}}, \\ \tilde{\lambda}_4 &= \frac{(\lambda_3+\lambda_4)^b - (\lambda_3-\lambda_4)^b}{2p_{\mathrm{succ}}}, \end{aligned} \tag{5}$$

where $\underline{\phi}_{11}^z$ $(\underline{e}_{11}^z)$ and $\overline{\phi}_{11}^z$ $(\overline{e}_{11}^z)$ denote the lower and upper bounds of the error rates of ϕ_{11}^z (e_{11}^z) [49,52], which can be estimated by the decoy state; $p_{\mathrm{succ}} = (\lambda_1+\lambda_2)^b + (\lambda_3+\lambda_4)^b$; and q_{succ} and $\tilde{E}_z$ represent the successful probability to perform the AD method and the total error rate after AD postprocessing in the Z basis, respectively.

Equation (3) can be understood from two perspectives. First, the quantum channel is manipulated by Eve, who can select the optimal parameter λ_i $(i = 1, 2, 3, 4)$ to diminish the key rate. Second, the AD method is governed by Alice and Bob, affording them the capability to choose the optimal value of b to increase the key rate. Furthermore, Alice and Bob can optimize the value of b in order to enhance the successful probability q_{succ}. Consequently, the error rate in the Z basis can be changed from E_z to $\tilde{E}_z = \frac{(E_z)^b}{q_{\mathrm{succ}}}$ and the number of raw keys and single-photon bits retained by Alice and Bob are $n_z q_{\mathrm{succ}}/b$ and $(\underline{s}_{11}^z/n_z)^b n_z q_{\mathrm{succ}}/b$, respectively.

IV. SIMULATION

In this section we present simulation results that detail the performance of the proposed scheme, taking into account finite-key effects. The simulations use a standard symmetric quantum channel model and include practical experimental parameters. The specific numerical values for the simulations

TABLE I. Numerical simulation parameters: $\eta_d^{D_L}$ ($\eta_d^{D_R}$) and $p_d^{D_L}$ ($p_d^{D_R}$) denote the detection efficiency and dark count rate, respectively; D_L (D_R) is left (right) detector; α (dB/km) and f are the loss coefficient of the fiber and the error-correction efficiency, respectively; ϵ is the failure probability; and the insert loss is 1.50 dB on Charlie's side.

$\eta_d^{D_L}$	$\eta_d^{D_R}$	$p_d^{D_L}$	$p_d^{D_R}$	α	ϵ	f
78.1%	77%	3.03×10^{-9}	3.81×10^{-9}	0.16	10^{-10}	1.1

are outlined in Table I, taken from the experimental data in Ref. [49]. For each distance, we optimize implementation parameters using a numerical simulation tool. This includes the intensities of the signal and decoy states, as well as the probabilities of sending them. The optimization routine resembles that in Ref. [69]. Furthermore, the variable b is restricted to the interval [1,4].

First, we evaluate the performance of AMDI QKD with and without the AD method under the given parameters $e_d^z = 0.5\%$, $E_{\text{Hom}} = 4\%$, and a total pulse count of $N = 7.24 \times 10^{13}$. As shown in Fig. 2(a), at a transmission distance exceeding 608 km, the key rate of AMDI QKD with AD surpasses that of AMDI QKD without AD, resulting in a maximum distance increase of 16 km.

To further explain the essential reasons for the AD method increasing the key rate over long distances, we present Fig. 2(b). At 0–372 km, the influence of noise on the correlation between Alice and Bob is minimal. The AD method cannot significantly increase s_{11}^z and reduce the QBER. At 372–608 km, the QBER begins to increase significantly. If the AD method is applied and the raw key is divided into $b = 2$ blocks at 500 km, the QBER is reduced, but the finite-key effect leads to a significant reduction in s_{11}^z. The impact of the reduction in s_{11}^z is greater and the key rate is lower, Therefore, AD is not effective at those distances. At 608–628 km, noise significantly disrupts the correlation of the raw keys between Alice and Bob and the QBER is already close to the maximum error tolerated by the original protocol. The QBER using the AD method will be changed from E_z to $(E_z)^2/[(E_z)^2 + (1 - E_z)^2]$ and the reduction in QBER will contribute more to the key rate than the finite-key effect, so the use of the AD method can obtain a higher key rate.

Now we delve into the finite-key effects and scrutinize the distinct impact of the AD method on AMDI QKD for varying pulse counts $N = 10^{12}$, 10^{13}, and 10^{15} and in the asymptotic case. In Fig. 3 it is evident that when the pulse count is 10^{15}, the AD method extends the maximum transmission distance of AMDI QKD by 28 km. Nevertheless, with a reduced pulse count of 10^{13}, the maximum transmission distance improvement for AMDI QKD with AD is limited to 8 km. Further reducing the pulse count to 10^{12}, the optimal value of b is all 1, which means that the AD step is not executed. These results suggest that AD becomes sensitive to pulse reduction when subjected to a finite-key analysis.

Furthermore, we investigate the impact of the misalignment error rate on the performance of AMDI QKD with AD, and the results are illustrated in Fig. 4. For a relatively small misalignment error rate of $e_d^z = E_{\text{Hom}} = 1\%$ (5%), the optimal value of b exceeds 1 at 604 km (408 km), leading to a substantial increase in the maximum transmission distance of AMDI QKD with AD by 20 km (96 km). However, with a further increase in the misalignment error rate to 10%, AMDI QKD without AD is unable to generate a key, whereas AMDI QKD with AD exhibits a substantial key rate and transmission distance of up to 504 km.

Finally, we assess the performance for arbitrary combinations of misalignment error rates e_d^z and E_{Hom}. We fix the misalignment error rate within the range [0, 20%] and set

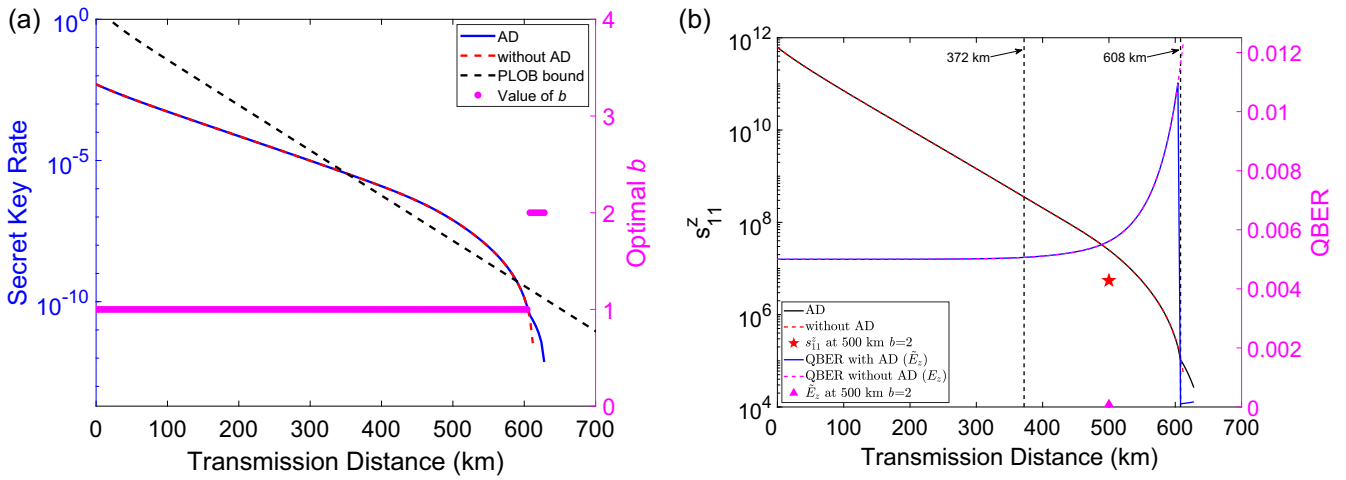

FIG. 2. Comparison of AMDI QKD performance with and without AD. (a) Relationship between secret key rate and transmission distance, and the corresponding optimal value of b. The blue solid line and red dotted line represent the secret key rate of AMDI QKD with AD and without AD, respectively. The black dashed line is the PLOB bound and the pink scatter represents the optimal b value. (b) Relationship between s_{11}^z and transmission distance, and the corresponding QBER. The black solid and red dotted lines represent the s_{11}^z of AMDI QKD with AD and without AD, respectively. The blue solid and pink dotted lines represent the QBER of AMDI QKD with AD and without AD, respectively. The red five-pointed star and pink triangles are s_{11}^z and QBER at 500 km and $b = 2$, respectively. Here we set $N = 7.24 \times 10^{13}$, $e_d^z = 0.5\%$, and $E_{\text{Hom}} = 4\%$.

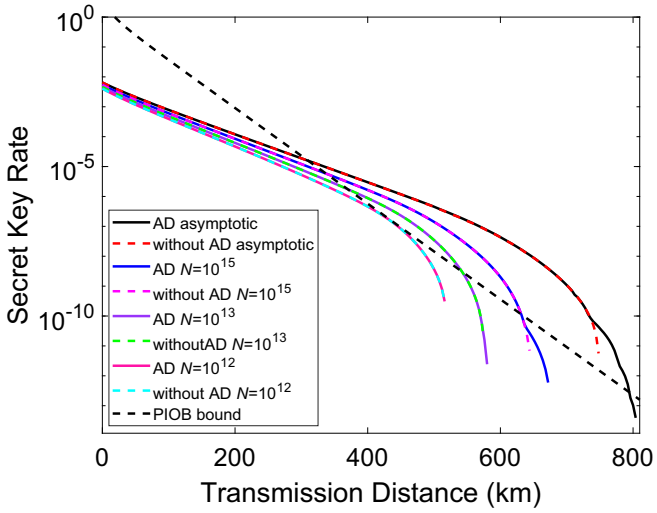

FIG. 3. Performance comparison between AMDI QKD with AD and without AD under different pulses. We simply fix the numbers of pulses 10^{12}, 10^{13}, and 10^{15} and in the asymptotic case, the misalignment error rates are $E_{\mathrm{Hom}} = 4\%$ and $e_d^z = 0.05\%$. The solid and dotted colored curves represent the results of AMDI QKD with and without AD, respectively. The optimal value of b of the overlapping part by the solid line and the dotted line is 1 and the remaining solid line part is $b > 1$.

$L = 500\,\mathrm{km}$ and $N = 7.24 \times 10^{13}$. The simulation results are shown in Fig. 5. The comparison reveals that AMDI QKD with AD exhibits a higher tolerance for misalignment error rates in the Z basis used for key generation compared to AMDI QKD without AD. For instance, at $e_d^z = 6\%$ and $E_{\mathrm{Hom}} = 6\%$, AMDI QKD with AD can generate a key rate of 1.35×10^{-9} bits/pulse, while AMDI QKD without AD is unable to generate a key. Objectively, AMDI QKD with AD outperforms AMDI QKD without AD, particularly at high misalignment error rates.

V. CONCLUSION

We have explored the performance of AMDI QKD with AD, considering a finite-key effect. Simulation results demonstrated the feasibility and significant impact of the AD method in enhancing the secure key rate and transmission distance of AMDI QKD. Meanwhile, with a misalignment error rate of 10%, AMDI QKD without AD failed to generate the key at 0 km, whereas AMDI QKD with AD could still generate secure bits.

In future research it would be interesting to further analyze the performance of AMDI QKD with AD for a limited number of modulated phases [70].

ACKNOWLEDGMENTS

This study was supported by the National Natural Science Foundation of China (Grants No. 62171144 and No. 11905065), Guangxi Science Foundation (Grants No. 2021GXNSFAA220011 and No. 2021AC19384), and Innovation Project of Guangxi Graduate Education (Grant No. YCSW2022040).

APPENDIX A: SECRET KEY RATE CALCULATION

1. Secrecy analysis

The secrecy analysis follows the idea of Refs. [4,71]. If the protocol successfully passes the error correction step, then it is $\varepsilon_{\mathrm{cor}}$-correct. If the extracted key length of the protocol does not surpass a certain length, then it is $\varepsilon_{\mathrm{sec}}$-secret. Specifically, if the protocol fulfills both conditions $\varepsilon_{\mathrm{cor}}$-correct and $\varepsilon_{\mathrm{sec}}$-secret, and $\varepsilon_{\mathrm{tol}} = \varepsilon_{\mathrm{cor}} + \varepsilon_{\mathrm{sec}}$, it is $\varepsilon_{\mathrm{tol}}$-secure.

Using a random $\mathtt{universal_2\ hash}$ function [72], the communication parties can extract an $\varepsilon_{\mathrm{sec}}$ -secret key of length ℓ from the raw key $\mathcal{Z}$ [73],

$$\varepsilon_{\mathrm{sec}} = 2\varepsilon + \frac{1}{2}\sqrt{2^{\ell - H_{\min}^{\varepsilon}(\mathcal{Z}|E')}}, \tag{A1}$$

where E' denotes all information of Eve learned from the raw key after error correction and $H_{\min}^{\varepsilon}(\mathcal{Z}|E')$ denotes the smooth minimum entropy, which quantifies the average probability that Eve guesses $\mathcal{Z}$ correctly using the optimal strategy with access to E'. According to a chain-rule inequality for smooth entropies [59], we obtain

$$H_{\min}^{\varepsilon}(\mathcal{Z}|E') \geqslant H_{\min}^{\varepsilon}(\mathcal{Z}|E) - \lambda_{\mathrm{EC}} - \log_2(2/\varepsilon_{\mathrm{cor}}), \tag{A2}$$

where E denotes the information of Eve before error correction and $\lambda_{\mathrm{EC}} + \log_2(2/\varepsilon_{\mathrm{cor}})$ is the amount of bit information that is leaked during the error correction step. The bits of $\mathcal{Z}$ can be distributed among three different strings $\mathcal{Z}_0$, $\mathcal{Z}_{11}$, and $\mathcal{Z}_{\mathrm{rest}}$, where $\mathcal{Z}_0$ is the bits where Alice sent a vacuum state, $\mathcal{Z}_{11}$ is the bits where both Alice and Bob sent a single photon, and $\mathcal{Z}_{\mathrm{rest}}$ is the rest of the bits. Using a generalized chain rule for smooth entropies [74], we have

$$\begin{aligned} H_{\min}^{\varepsilon}(\mathcal{Z}|E) &\geqslant H_{\min}^{\varepsilon'+2\varepsilon_e+(\hat{\varepsilon}+2\hat{\varepsilon}'+\hat{\varepsilon}'')}(\mathcal{Z}_0\mathcal{Z}_{11}\mathcal{Z}_{\mathrm{rest}}|E) \\ &\geqslant H_{\min}^{\hat{\varepsilon}''}(\mathcal{Z}_0|E) + H_{\min}^{\varepsilon_e}(\mathcal{Z}_{11}|\mathcal{Z}_0\mathcal{Z}_{\mathrm{rest}}E) \\ &\quad + H_{\min}^{\hat{\varepsilon}'}(\mathcal{Z}_{\mathrm{rest}}|\mathcal{Z}_0E) - 2\log_2\frac{2}{\varepsilon'\hat{\varepsilon}} \\ &\geqslant s_0^z + H_{\min}^{\varepsilon_e}(\mathcal{Z}_{11}|\mathcal{Z}_0\mathcal{Z}_{\mathrm{rest}}E) - 2\log_2\frac{2}{\varepsilon'\hat{\varepsilon}}, \end{aligned} \tag{A3}$$

where $\varepsilon = \varepsilon' + 2\varepsilon_e + (\hat{\varepsilon} + 2\hat{\varepsilon}' + \hat{\varepsilon}'')$ and we have used the fact that $H_{\min}^{\hat{\varepsilon}'}(\mathcal{Z}_{\mathrm{rest}}|\mathcal{Z}_0E) \geqslant 0$, since all multiphoton events are considered insecure due to the risk of photon-number-splitting attacks, $H_{\min}^{\hat{\varepsilon}''}(\mathcal{Z}_0|E) \geqslant H_{\min}(\mathcal{Z}_0) = \log_2 2^{s_0^z} = s_0^z$. Here we consider that the bit values of the vacuum states are uniformly distributed and contain no information.

In addition, we use $|01\rangle$ and $|10\rangle$ for the Z basis and $\frac{1}{\sqrt{2}}(|10\rangle \pm e^{\mathrm{i}\varphi}|10\rangle)$ for the X basis. We let Alice and Bob use χ_{11} and χ_{11}' of length s_{11}^z instead of the raw keys $\mathcal{Z}_{11}$ and $\mathcal{Z}_{11}'$ if they had measured on the X basis. According to the uncertainty relation of smooth minimum entropy and maximum entropy, we can get a lower bound for $H_{\min}^{\varepsilon_e}(\mathcal{Z}_{11}|\mathcal{Z}_0\mathcal{Z}_{\mathrm{rest}}E)$ as

$$\begin{aligned} H_{\min}^{\varepsilon_e}(\mathcal{Z}_{11}|\mathcal{Z}_0\mathcal{Z}_{\mathrm{rest}}E) &\geqslant s_{11}^z - H_{\max}^{\varepsilon_e}(\chi_{11}|\chi_{11}') \\ &\geqslant s_{11}^z\left[1 - H\left(\phi_{11}^z\right)\right], \end{aligned} \tag{A4}$$

where the first inequality is derived from the uncertainty relation in Ref. [75], the second inequality utilizes Lemma 3 from Ref. [73], $H(\phi_{11}^z)$ quantifies the number of bits Bob needs to reconstruct χ_{11} using bit string χ_{11}', and ϕ_{11}^z is the phase error

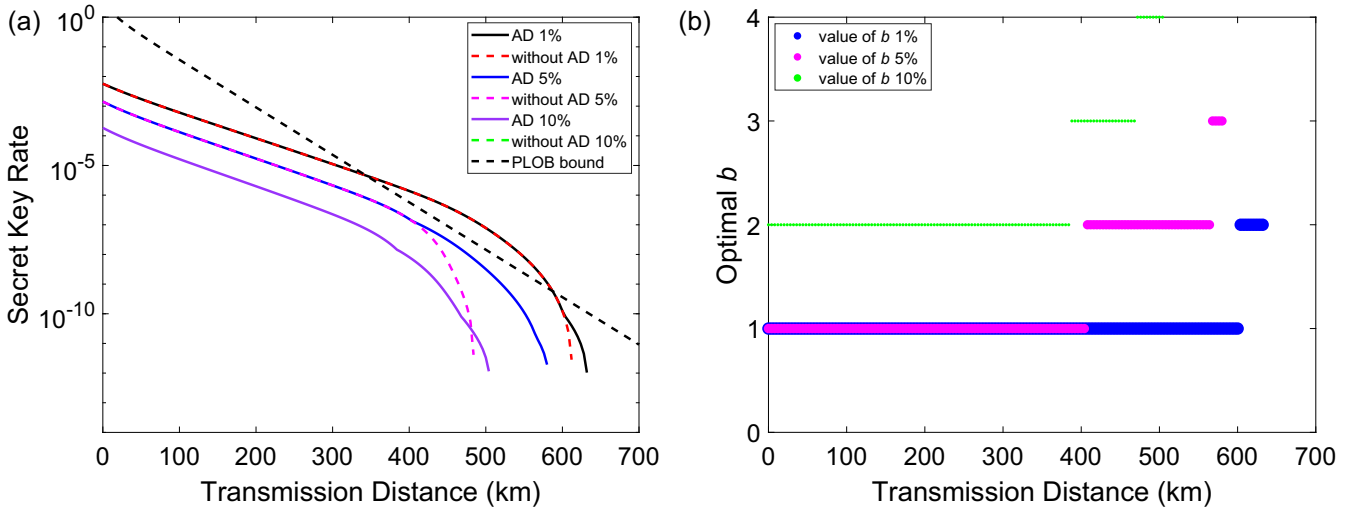

FIG. 4. Performance of AMDI QKD with AD under different misalignment error rates. Here we assume $e_d^z = E_{\mathrm{Hom}} = 1\%$, 5%, and 10% and $N = 7.24 \times 10^{13}$. (a) Relationship between key rate and distance under different misalignment error rates e_d^z and E_{Hom}. The solid line indicates AMDI QKD with AD and the dashed line indicates AMDI QKD without AD. (b) Relationship between the optimal b value and transmission distance.

of a single photon in the Z basis. Combined with Eq. (A1), we obtain the expression for the key length ℓ as

$$\ell = H_{\min}^{\varepsilon}(\mathcal{Z}|E') - 2\log_2\frac{1}{2\varepsilon_{\mathrm{PA}}}, \tag{A5}$$

and combining Eqs. (A2)–(A5), the specific expression for ℓ is

$$\begin{aligned}\ell \geqslant\ & s_0^z + s_{11}^z\left[1 - H\left(\phi_{11}^z\right)\right] - \lambda_{\mathrm{EC}} \\ & - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}} - 2\log_2\frac{2}{\varepsilon'\hat{\varepsilon}} - 2\log_2\frac{1}{2\varepsilon_{\mathrm{PA}}},\end{aligned} \tag{A6}$$

where $\varepsilon_{\mathrm{sec}} = 2(\varepsilon' + 2\varepsilon_e + \hat{\varepsilon} + 2\hat{\varepsilon}' + \hat{\varepsilon}'') + \varepsilon_{\mathrm{PA}}$, we assume $\hat{\varepsilon}' = \hat{\varepsilon}'' = 0$ without compromising security, and $\varepsilon_{\mathrm{PA}} = \frac{1}{2}\sqrt{2^{\ell - H_{\min}^{\varepsilon}(\mathcal{Z}|E')}}$ is a security parameter that involves privacy amplification. Finally, the parameters s_0^z, s_{11}^z, and e_{11}^x are estimated by using the failure probabilities ε_0, ε_1, and ε_β, respectively; we have $\varepsilon_{\mathrm{sec}} = 2(\varepsilon' + 2\varepsilon_e + \hat{\varepsilon}) + \varepsilon_0 + \varepsilon_1 + \varepsilon_\beta + \varepsilon_{\mathrm{PA}}$.

2. Parameter estimation

By using decoy-state estimation, the key rate can be written as [49]

$$\begin{aligned}R = \frac{1}{N}\Bigg(& \underline{s}_0^z + \underline{s}_{11}^z\left[1 - H\left(\overline{\phi}_{11}^z\right)\right] - \lambda_{\mathrm{EC}} \\ & - \log_2\frac{2}{\varepsilon_{\mathrm{cor}}} - 2\log_2\frac{2}{\varepsilon'\hat{\varepsilon}} - 2\log_2\frac{1}{2\varepsilon_{\mathrm{PA}}}\Bigg).\end{aligned} \tag{A7}$$

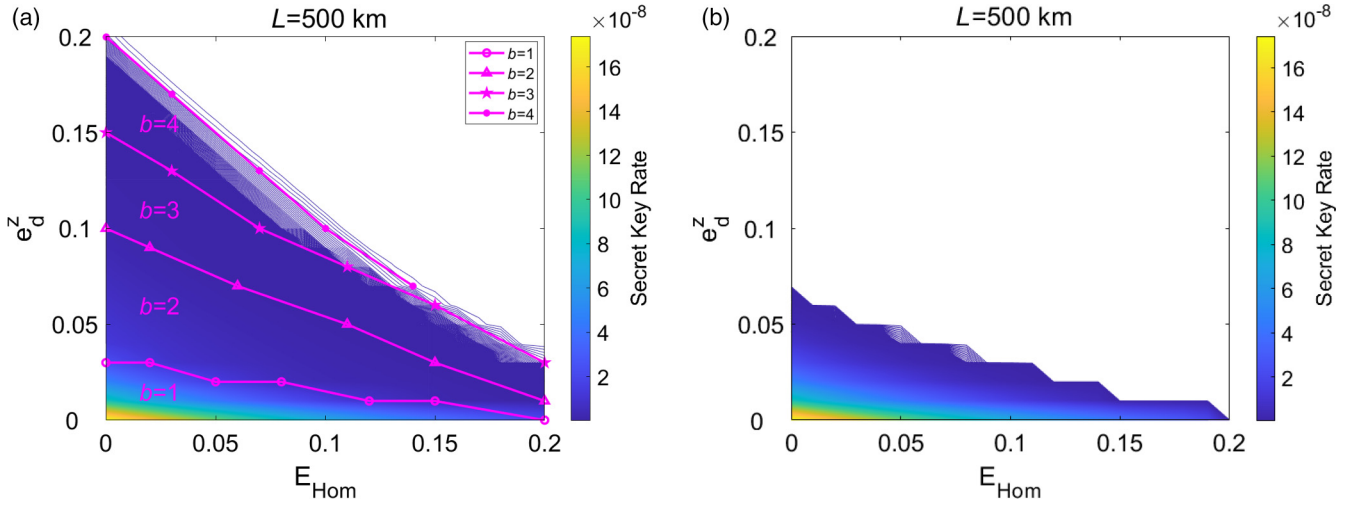

FIG. 5. Relationship between arbitrary e_d^z and E_{Hom} combinations and key rates. (a) Results of AMDI QKD with AD, with the open circle for $b = 1$, the triangle for $b = 2$, the five-pointed star for $b = 3$, and the closed circle for $b = 4$. (b) Results of AMDI QKD without AD. We assume $L = 500$ km, $N = 7.24 \times 10^{13}$, and the misalignment error rate is in the range [0, 20%]. The color depth represents the distribution of key rates.

We assume failure parameters $\varepsilon_{\rm cor}$, ε', $\hat{\varepsilon}$, and $\varepsilon_{\rm PA}$ to be equal to ϵ. As described in the protocol, Alice and Bob publish information about the decoy states when the click filtering operation is used, so only $[\mu_a, \mu_b]$ can be used to generate the key. The amount of data consumed during error correction is

$$\lambda_{\rm EC} = n_{[\mu_a,\mu_b]} f H(E_z), \tag{A8}$$

where $E_z = \frac{m_{[\mu_a,\mu_b]}}{n_{[\mu_a,\mu_b]}}$ is the QBER in the Z basis. The total error pairing numbers $m'_{[\mu_a,\mu_b]}$ do not consider e_d^z in the Z basis, which include two click events with $(\mu_a|\mu_b)$ and $(o_a|o_b)$ to pair.

When we take e_d^z into account [50], the count of error detection can be given as

$$m_{[\mu_a,\mu_b]} = e_d^z\left(n_{[\mu_a,\mu_b]} - m'_{[\mu_a,\mu_b]}\right) + \left(1 - e_d^z\right) m'_{[\mu_a,\mu_b]}. \tag{A9}$$

The lower bound of single-photon pair events in the Z basis estimated by the decoy-state method can be written as

$$\underline{s}_{11}^{z*} \geqslant \frac{e^{-\mu_a-\mu_b} p_{[\mu_a,\mu_b]}}{\nu_a \nu_b (\mu' - \nu')}(S_1 - S_2), \tag{A10}$$

where

$$\begin{aligned} S_1 &= \mu_a \mu_b \mu' \left(e^{\nu_a+\nu_b} \frac{\underline{n}^*_{[\nu_a,\nu_b]}}{p_{[\nu_a,\nu_b]}} - e^{\nu_b} \frac{\overline{n}^*_{[o_a,\nu_b]}}{p_{[o_a,\nu_b]}} - e^{\nu_a} \frac{\overline{n}^*_{[\nu_a,o_b]}}{p_{[\nu_a,o_b]}} + \frac{\underline{n}^*_{[o_a,o_b]}}{p_{[o_a o_b]}} \right), \\ S_2 &= \nu_a \nu_b \nu' \left(e^{\mu_a+\mu_b} \frac{\overline{n}^*_{[\mu_a,\mu_b]}}{p_{[\mu_a,\mu_b]}} - e^{\mu_b} \frac{\underline{n}^*_{[o_a,\mu_b]}}{p_{[o_a \mu_b]}} - e^{\mu_a} \frac{\underline{n}^*_{[\mu_a,o_b]}}{p_{[\mu_a,o_b]}} + \frac{\underline{n}^*_{[o_a,o_b]}}{p_{[o_a o_b]}} \right), \end{aligned} \tag{A11}$$

and

$$p_{[\kappa_a^{\rm tot},\kappa_b^{\rm tot}]} = \sum_{\kappa_a^e+\kappa_a^l=\kappa_a^{tot}} \sum_{\kappa_b^e+\kappa_b^l=\kappa_b^{tot}} \frac{p_{\kappa_a^e} p_{\kappa_b^e}}{p_s} \frac{p_{\kappa_a^l} p_{\kappa_b^l}}{p_s}, \tag{A12}$$

where $p_{[\kappa_a^{\rm tot},\kappa_b^{\rm tot}]}$ is the coincidence pairing $[\kappa_a^{\rm tot}, \kappa_b^{\rm tot}]$ successful probability, $p_s = 1 - p_{\mu_a} p_{\nu_b} - p_{\nu_a} p_{\mu_b}$ by using click filtering, e (l) denotes the early (late) time bin. We set $o_a = o_b = 0$, $\mu_a = \mu_b = \mu'$, and $\nu_a = \nu_b = \nu'$ with symmetric channels. The lower bound of the vacuum number is given by

$$\underline{s}_0^{z*} = \frac{e^{-\mu_a} p_{[\mu_a,\mu_b]}}{p_{[o_a,\mu_b]}} \underline{n}^*_{[o_a,\mu_b]}. \tag{A13}$$

The upper bound on the number of errors of single-photon pairs in the X basis is given by

$$\overline{t}_{11}^x \leqslant m_{[2\nu_a,2\nu_b]} - \underline{m}^0_{[2\nu_a,2\nu_b]}, \tag{A14}$$

where $m_{[2\nu_a,2\nu_b]}$ is the observed error pairing number in the X basis and $\underline{m}^0_{[2\nu_a,2\nu_b]}$ is the lower bound of error pairing numbers when there is at least one sending vacuum state between communication parties in the X basis,

$$\begin{aligned} \underline{m}^{0*}_{[2\nu_a,2\nu_b]} = {} & e^{-2\nu_a} \frac{p_{[2\nu_a,2\nu_b]} \underline{n}^*_{[o_a,2\nu_b]}}{2 p_{[o_a,2\nu_b]}} + e^{-2\nu_b} \frac{p_{[2\nu_a,2\nu_b]} \underline{n}^*_{[2\nu_a,o_b]}}{2 p_{[2\nu_a,o_b]}} \\ & - e^{-2\nu_a-2\nu_b} \frac{p_{[2\nu_a,2\nu_b]} \overline{n}^*_{[o_a,o_b]}}{2 p_{[o_a,o_b]}}, \end{aligned} \tag{A15}$$

where $p_{[2\nu_a,2\nu_b]} = \frac{2}{M} \frac{p_{\nu_a}^2 p_{\nu_b}^2}{p_s^2}$ denotes the probability of coincidence $[2\nu_a, 2\nu_b]$ in the X basis. The single-photon pairing error numbers in the X basis is

$$\overline{e}_{11}^x = \frac{\overline{t}_{11}^x}{\underline{s}_{11}^x}, \tag{A16}$$

where $\underline{s}_{11}^x$ is the number of single-photon pairing in the X basis, whose lower bound is estimated by the decoy state, expressed as

$$\underline{s}_{11}^{x*} \leqslant \frac{e^{-2\nu_a-2\nu_b} 4 p_{[2\nu_a,2\nu_b]}}{\mu_a \mu_b (\mu' - \nu')}(S_1 - S_2). \tag{A17}$$

The upper bound on the phase error rate of a single-photon pair in the Z basis is

$$\overline{\phi}_{11}^z \leqslant \overline{e}_{11}^x + \gamma\left(\underline{s}_{11}^z, \underline{s}_{11}^x, \overline{e}_{11}^x, \varepsilon_e\right). \tag{A18}$$

3. Simulation formula

We assume that Alice and Bob send pulses of intensity κ_a and κ_b, respectively, with phase difference θ. The gain of only one detector response can be given

$$\begin{aligned} q^{\theta,D_L}_{(\kappa_a|\kappa_b)} = {} & y^{D_R}_{(\kappa_a|\kappa_b)} e^{\eta_d^{D_R} \sqrt{\eta_a \kappa_a \eta_b \kappa_b} cos\theta} \\ & \times \left(1 - y^{D_L}_{(\kappa_a|\kappa_b)} e^{-\eta_d^{D_L} \sqrt{\eta_a \kappa_a \eta_b \kappa_b} cos\theta}\right) \end{aligned} \tag{A19}$$

and

$$\begin{aligned} q^{\theta,D_R}_{(\kappa_a|\kappa_b)} = {} & y^{D_L}_{(\kappa_a|\kappa_b)} e^{-\eta_d^{D_L} \sqrt{\eta_a \kappa_a \eta_b \kappa_b} cos\theta} \\ & \times \left(1 - y^{D_R}_{(\kappa_a|\kappa_b)} e^{\eta_d^{D_R} \sqrt{\eta_a \kappa_a \eta_b \kappa_b} cos\theta}\right), \end{aligned} \tag{A20}$$

where $y^{D_L(D_R)}_{(\kappa_a|\kappa_b)} = (1 - p_d^{D_L(D_R)}) e^{-\eta_d^{D_L(D_R)} \frac{(\eta_a \kappa_a + \eta_b \kappa_b)}{2}}$, D_L (D_R) is left (right) detector, and $\eta_{a\,(b)} = 10^{-\alpha L_{a\,(b)}/10}$. By calculating the phase θ from 0 to 2π, the total gain of Alice sending κ_a and Bob sending κ_b can be given as

$$\begin{aligned} q_{(\kappa_a|\kappa_b)} = {} & \frac{1}{2\pi} \int_0^{2\pi} \left(q^{\theta,D_L}_{(\kappa_a|\kappa_b)} + q^{\theta,D_R}_{(\kappa_a|\kappa_b)}\right) d\theta \\ = {} & y^{D_L}_{(\kappa_a|\kappa_b)} I_0\left(\eta_d^{D_L} \sqrt{\eta_a \kappa_a \eta_b \kappa_b}\right) \\ & + y^{D_R}_{(\kappa_a|\kappa_b)} I_0\left(\eta_d^{D_R} \sqrt{\eta_a \kappa_a \eta_b \kappa_b}\right) \\ & - 2 y^{D_L}_{(\kappa_a|\kappa_b)} y^{D_R}_{(\kappa_a|\kappa_b)} I_0\left[\left(\eta_d^{D_L} - \eta_d^{D_R}\right) \sqrt{\eta_a \kappa_a \eta_b \kappa_b}\right], \end{aligned} \tag{A21}$$

where $I_0(x) \approx 1 + \frac{x^2}{4}$ represents the first kind of zeroth-order modified Bessel function and $q^{\theta}_{(\kappa_a|\kappa_b)} = q^{\theta,D_L}_{(\kappa_a|\kappa_b)} + q^{\theta,D_R}_{(\kappa_a|\kappa_b)}$. The

total number of valid successful pairings is $n_{\rm tot} = \frac{Nq_{\rm tot}}{1+1/q_{T_c}}$, where $q_{T_c} = 1-(1-q_{tot})^{N_{T_c}}$ is the probability of having at least a click in the time interval T_c if the detector has a click in a time bin. Thus, an average of $1+1/q_{T_c}$ valid events is required to form a valid pairing. The average time it takes to form a valid pairing is $T_{\rm mean} = \frac{1-N_{T_c}q_{\rm tot}(1/q_{T_c}-1)}{Fq_{\rm tot}}$, where $F = 1\,\text{GHz}$ is the system's repetition rate and $N_{T_c} = FT_c$ is the total number of time bins in the interval T_c.

When we use the three-intensity decoy-state protocol, there are nine independent and random events, which are $(\mu_a|\mu_b)$, $(\mu_a|\nu_b)$, $(\mu_a|o_b)$, $(\nu_a|\nu_b)$, $(\nu_a|\mu_b)$, $(\nu_a|o_b)$, $(o_a|o_b)$, $(o_a|\mu_b)$, and $(o_a|\nu_b)$. By using click filtering, $(\mu_a|\nu_b)$ and $(\nu_a|\mu_b)$ are discarded. The probability of having the click event is $q_{\rm tot} = \sum_{\kappa_a,\kappa_b} p_{\kappa_a}p_{\kappa_b}q_{(\kappa_a|\kappa_b)} - p_{\mu_a}p_{\nu_b}q_{(\mu_a|\nu_b)} - p_{\nu_a}p_{\mu_b}q_{(\nu_a|\mu_b)}$. In addition, the number of successful pairings $S_{[\kappa_a^{\rm tot},\kappa_b^{\rm tot}]}$ (except the set $S_{[2\nu_a,2\nu_b]}$) is counted as

$$n_{[\kappa_a^{\rm tot},\kappa_b^{\rm tot}]} = n_{\rm tot}\sum_{\kappa_a^e+\kappa_a^l=\kappa_a^{\rm tot}}\sum_{\kappa_b^e+\kappa_b^l=\kappa_b^{\rm tot}}\left(\frac{p_{\kappa_a^e}p_{\kappa_b^e}q_{(\kappa_a^e|\kappa_b^e)}}{q_{\rm tot}}\,\frac{p_{\kappa_a^l}p_{\kappa_b^l}q_{(\kappa_a^l|\kappa_b^l)}}{q_{\rm tot}}\right). \tag{A22}$$

The set $S_{[2\nu_a,2\nu_b]}$ which we need to take into account the phase difference is counted as

$$n_{[2\nu_a,2\nu_b]} = \frac{n_{\rm tot}}{M\pi}\int_0^{2\pi}\left(\frac{p_{\nu_a}p_{\nu_b}q^{\theta}_{(\nu_a|\nu_b)}}{q_{\rm tot}}\,\frac{p_{\nu_a}p_{\nu_b}q^{\theta}_{(\nu_a|\nu_b)}}{q_{\rm tot}}\right)d\theta. \tag{A23}$$

In the experiment, we encode the quantum states by randomly selecting the phase $\{0, (2\pi/M), (4\pi/M), \ldots, [2\pi(M-1)]/M\}$ $(M = 16)$ to fulfill the phase randomization requirement. The total number of errors in the X basis can be given as

$$m_{[2\nu_a,2\nu_b]} = \frac{n_{\rm tot}}{M\pi}\int_0^{2\pi}\left((1-E_{\rm Hom})\frac{p_{\nu_a}^2p_{\nu_b}^2\left[q^{\theta,D_L}_{(\nu_a|\nu_b)}q^{\theta+\delta,D_R}_{(\nu_a|\nu_b)}+q^{\theta,D_R}_{(\nu_a|\nu_b)}q^{\theta+\delta,D_L}_{(\nu_a|\nu_b)}\right]}{q_{\rm tot}^2}+E_{\rm Hom}\frac{p_{\nu_a}^2p_{\nu_b}^2\left[q^{\theta,D_L}_{(\nu_a|\nu_b)}q^{\theta+\delta,D_L}_{(\nu_a|\nu_b)}+q^{\theta,D_R}_{(\nu_a|\nu_b)}q^{\theta+\delta,D_R}_{(\nu_a|\nu_b)}\right]}{q_{\rm tot}^2}\right)d\theta, \tag{A24}$$

where $E_{\rm Hom}$ is the interference misalignment error rate, $\delta = T_{\rm mean}(2\pi\Delta\nu+\omega_{\rm fib})$ is the light pulse phase drift cause by the laser frequency difference $\Delta\nu = 10\,\text{Hz}$, and the fiber drift rate $\omega_{\rm fib} = 5900\,\text{rad/s}$.

4. Statistical fluctuation

We use the Chernoff bound [76] to calculate statistical fluctuation. Assuming a failure probability ϵ and expectation value x^*, we can estimate the upper and lower bounds of the observed value x by the Chernoff bound

$$\overline{x} = x^* + \frac{\beta}{2} + \sqrt{2\beta x^* + \frac{\beta^2}{4}} \tag{A25}$$

and

$$\underline{x} = x^* - \sqrt{2\beta x^*}, \tag{A26}$$

where $\beta = \ln\epsilon^{-1}$. Similarly, the variant of the Chernoff bound can be used to estimate the upper and lower bounds of the expected value x^* from the observed value x:

$$\overline{x}^* = x + \beta + \sqrt{2\beta x + \beta^2} \tag{A27}$$

and

$$\underline{x}^* = \max\left\{x - \frac{\beta}{2} - \sqrt{2\beta x + \frac{\beta^2}{4}}, 0\right\}. \tag{A28}$$

The upper bound of the phase error rate in the Z basis is estimated by a random sampling theorem, whose specific expression is [76]

$$\overline{\chi} \leqslant \lambda + \gamma^U(n,k,\lambda,\epsilon), \tag{A29}$$

where

$$\gamma^U(n,k,\lambda,\epsilon) = \frac{\frac{(1-2\lambda)AG}{n+k} + \sqrt{\frac{A^2G^2}{(n+k)^2}+4\lambda(1-\lambda)G}}{2+2\frac{A^2G}{(n+k)^2}},$$
$$A = \max\{n,k\}, \quad G = \frac{n+k}{nk}\ln\frac{n+k}{2\pi nk\lambda(1-\lambda)\epsilon^2}. \tag{A30}$$

APPENDIX B: SECURITY OF AMDI QKD BASED ON QUANTUM INFORMATION THEORY

Now we present a brief description of the security of AMDI QKD based on quantum information theory; a more detailed analysis can be found in [45,49,59]. The key rate based on quantum information theory is [59]

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

where Γ represents the set of all density operators σ_{AB} within the Hilbert space $\mathcal{H}_A\otimes\mathcal{H}_B$ that satisfy the requirements; $S(X|E)$ represents the uncertainty of the eavesdropper's auxiliary state E for Alice's measurement outcome X, quantified by von Neumann entropy; and $H(X|Y)$ represents the uncertainty of Bob's measurement outcome Y to Alice's measurement outcome X, quantified by classical Shannon entropy.

In a security analysis similar to the entanglement purification protocol, Alice and Bob randomly prepare the quantum states $|1,0\rangle^{i,j}$ and $|0,1\rangle^{i,j}$ as the Z basis and $(|1,0\rangle^{i,j}\pm|0,1\rangle^{i,j})\sqrt{2}$ as the X basis and send to Charlie for Bell state measurement. The $|1,0\rangle^{i,j}$ indicates $|1\rangle^i\otimes|0\rangle^j$ and is the tensor product of time bins i and j, with quantum states $|1\rangle$ and $|0\rangle$ indicating single-photon and vacuum states, respectively.

Before the communication parties' measurement, the whole system consisting of Alice, Bob, and Eve can be described by the quantum state as

$$|\Phi\rangle_{ABE} := \sum_{i=1}^{4} \sqrt{\lambda_i}|\varphi_i\rangle_{AB} \otimes |\upsilon_i\rangle_E, \tag{B2}$$

where

$$\begin{aligned}
|\varphi_1\rangle &= \frac{1}{\sqrt{2}}\left(|1,0\rangle_A^{i,j}|1,0\rangle_B^{i,j} + |0,1\rangle_A^{i,j}|0,1\rangle_B^{i,j}\right),\\
|\varphi_2\rangle &= \frac{1}{\sqrt{2}}\left(|1,0\rangle_A^{i,j}|1,0\rangle_B^{i,j} - |0,1\rangle_A^{i,j}|0,1\rangle_B^{i,j}\right),\\
|\varphi_3\rangle &= \frac{1}{\sqrt{2}}\left(|1,0\rangle_A^{i,j}|0,1\rangle_B^{i,j} + |0,1\rangle_A^{i,j}|1,0\rangle_B^{i,j}\right),\\
|\varphi_4\rangle &= \frac{1}{\sqrt{2}}\left(|1,0\rangle_A^{i,j}|0,1\rangle_B^{i,j} - |0,1\rangle_A^{i,j}|1,0\rangle_B^{i,j}\right),
\end{aligned} \tag{B3}$$

and $\sum_{i=1}^{4}\lambda_i = 1$. The single-photon error rate satisfies the equations $\lambda_2 + \lambda_4 = \phi_{11}^z$ and $\lambda_3 + \lambda_4 = e_{11}^z$. The subscripts A and B represent Alice and Bob, respectively, and $|\upsilon_i\rangle_E$ denotes the orthonormal basis in a Hilbert space $\mathcal{H}_E$.

Because Eve controls the channel, if the measurement outcomes of communication parties are $xy \in \{00, 11, 01, 10\}$, the quantum states that Eve obtains include

$$\begin{aligned}
|\phi\rangle^{0,0} &= \frac{1}{\sqrt{2}}(\sqrt{\lambda_1}|\upsilon_1\rangle + \sqrt{\lambda_2}|\upsilon_2\rangle),\\
|\phi\rangle^{1,1} &= \frac{1}{\sqrt{2}}(\sqrt{\lambda_1}|\upsilon_1\rangle - \sqrt{\lambda_2}|\upsilon_2\rangle),\\
|\phi\rangle^{0,1} &= \frac{1}{\sqrt{2}}(\sqrt{\lambda_3}|\upsilon_3\rangle + \sqrt{\lambda_4}|\upsilon_4\rangle),\\
|\phi\rangle^{1,0} &= \frac{1}{\sqrt{2}}(\sqrt{\lambda_3}|\upsilon_3\rangle - \sqrt{\lambda_4}|\upsilon_4\rangle).
\end{aligned} \tag{B4}$$

After disturbance from Eve on the quantum channel, Alice and Bob gain the density operators for the whole system as

$$\sigma_{XYE} = \sum_{xy} |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes |\phi^{xy}\rangle\langle\phi^{xy}|. \tag{B5}$$

Taking all of the above analysis into account, we can get

$$\begin{aligned}
S(\sigma_{XE}) &= 1 + H(\lambda_1 + \lambda_2),\\
S(\sigma_E) &= H(\lambda_1 + \lambda_2) + (\lambda_1 + \lambda_2)H\left(\frac{\lambda_1}{\lambda_1 + \lambda_2}\right)\\
&\quad + (\lambda_3 + \lambda_4)H\left(\frac{\lambda_3}{\lambda_3 + \lambda_4}\right),\\
H(X|Y) &= H(\lambda_1 + \lambda_2).
\end{aligned} \tag{B6}$$

Finally, we obtain the final key rate in the asymptotic case as

$$\begin{aligned}
R &\geqslant \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} S(X|E) - H(X|Y)\\
&= \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} H(\sigma_{XE}) - H(\sigma_E) - H(X|Y)\\
&= \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} 1 - (\lambda_1 + \lambda_2)H\left(\frac{\lambda_1}{\lambda_1 + \lambda_2}\right)\\
&\quad - (\lambda_3 + \lambda_4)H\left(\frac{\lambda_3}{\lambda_3 + \lambda_4}\right) - H(\lambda_1 + \lambda_2).
\end{aligned} \tag{B7}$$

Suppose that the single-photon bit error rate and phase error rate are e_{11}^z and ϕ_{11}^z, respectively. We then have

$$\begin{aligned}
\lambda_2 + \lambda_4 &= \phi_{11}^z,\\
\lambda_3 + \lambda_4 &= e_{11}^z,\\
\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 &= 1.
\end{aligned} \tag{B8}$$

By simplifying the above formula, we can get

$$\begin{aligned}
\lambda_1 &= 1 - e_{11}^z - \phi_{11}^z - \lambda_4,\\
\lambda_2 &= \phi_{11}^z - \lambda_4,\\
\lambda_3 &= e_{11}^z - \lambda_4.
\end{aligned} \tag{B9}$$

By combining Eqs. (B9) and (B7), we obtain a new key rate formula

$$\begin{aligned}
R &\geqslant \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} 1 - (1 - e_{11}^z)H\left(\frac{1 - \phi_{11}^z - e_{11}^z + \lambda_4}{1 - e_{11}^z}\right)\\
&\quad - e_{11}^z H\left(\frac{e_{11}^z - \lambda_4}{e_{11}^z}\right) - H\left(1 - e_{11}^z\right).
\end{aligned} \tag{B10}$$

With the minimum value of the above key rate formula, by computing the partial derivative with respect to Eq. (B10), we can obtain the satisfying condition $\lambda_4 = e_{11}^z\phi_{11}^z$. In order to find the minimum value of Eq. (B10), λ_1, λ_2, λ_3, and λ_4 should satisfy the conditions

$$\begin{aligned}
\lambda_1 &= 1 - e_{11}^z - \phi_{11}^z - \lambda_4,\\
\lambda_2 &= \phi_{11}^z - \lambda_4,\\
\lambda_3 &= e_{11}^z - \lambda_4,\\
\lambda_4 &= e_{11}^z\phi_{11}^z.
\end{aligned} \tag{B11}$$

In the practical AMDI QKD protocol [49], we utilize discrete phase random modulation to fulfill the phase randomization requirements and the Chernoff bound to calculate statistical fluctuations. After obtaining the raw key generated in the Z basis, Alice and Bob perform error correction on the raw key. So the uncertainty between Alice and Bob $H(X|Y) \leqslant fH(E_z)$, where $H(E_z)$ is the maximum amount of information leaked during error correction. The key rate formula of AMDI QKD is

$$\begin{aligned}
R &\geqslant \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} \frac{1}{N} n_z \left\{ \frac{s_0^z}{n_z} + \frac{s_{11}^z}{n_z}\left[1 - (\lambda_1 + \lambda_2)H\left(\frac{\lambda_1}{\lambda_1 + \lambda_2}\right)\right.\right.\\
&\quad \left.\left. - (\lambda_3 + \lambda_4)H\left(\frac{\lambda_3}{\lambda_3 + \lambda_4}\right)\right] - fH(E_z) - \frac{1}{n_z}\right.\\
&\quad \left.\times\left(\log_2\frac{2}{\varepsilon_{\mathrm{cor}}} + 2\log_2\frac{2}{\varepsilon'\hat{\varepsilon}} + 2\log_2\frac{1}{2\varepsilon_{\mathrm{PA}}}\right)\right\},
\end{aligned} \tag{B12}$$

where N is the total number of pulses sent by Alice, n_z is the total number of bits in the Z basis, $\underline{s}_0^z$ is the lower bound of the vacuum state, $\underline{s}_{11}^z$ represents the single-photon pair successful coincidence number, and E_z is the QBER in the Z basis.

APPENDIX C: SECURITY OF AMDI QKD WITH AD

Next we analyze the security of AMDI with AD, similarly to the analysis in [53,64,68]. In AMDI QKD, Alice and Bob divide the raw keys that they get into blocks of size b, that is, $\{x_1, x_2, \ldots, x_b\}$ and $\{y_1, y_2, \ldots, y_b\}$, respectively. Then Alice randomly selects a privately generated bit $c \in \{0, 1\}$ and sends 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 through a public authenticated classical channel. Alice and Bob acquire blocks when Bob calculates the results $\{m_1 \oplus y_1, m_2 \oplus y_2, \ldots, m_b \oplus y_b\} = \{0, 0, \ldots, 0\}$ or $\{1, 1, \ldots, 1\}$; they retain x_1 and y_1 as raw keys. Moreover, if Eve knows arbitrary measurement results m_i $(1 \leqslant i \leqslant b)$, she has the ability to know all the b measurement results. Thus, only when all the b pulses are single-photon states can they be employed for key generation. The successful probability of advantage distillation can be calculated as

$$q_{\text{succ}} = (E_z)^b + (1 - E_z)^b. \tag{C1}$$

When performing the AD step, the quantum state of the whole system composed of Alice, Bob, and Eve can be described as [59,68]

$$|\tilde{\Phi}\rangle_{ABE} := \sum_{i=1}^{4} \sqrt{\tilde{\lambda}_i} |\varphi_i\rangle_{AB} \otimes |\upsilon_i\rangle_E, \tag{C2}$$

where

$$\begin{aligned}
\tilde{\lambda}_1 &= \frac{(\lambda_1 + \lambda_2)^b + (\lambda_1 - \lambda_2)^b}{2p_{\text{succ}}}, \\
\tilde{\lambda}_2 &= \frac{(\lambda_1 + \lambda_2)^b - (\lambda_1 - \lambda_2)^b}{2p_{\text{succ}}}, \\
\tilde{\lambda}_3 &= \frac{(\lambda_3 + \lambda_4)^b + (\lambda_3 - \lambda_4)^b}{2p_{\text{succ}}}, \\
\tilde{\lambda}_4 &= \frac{(\lambda_3 + \lambda_4)^b - (\lambda_3 - \lambda_4)^b}{2p_{\text{succ}}},
\end{aligned} \tag{C3}$$

and $p_{\text{succ}} = (\lambda_1 + \lambda_2)^b + (\lambda_3 + \lambda_4)^b$. Based on quantum state $|\tilde{\Phi}\rangle_{ABE}$ and the optimal value of b, Eq. (B7) is amended as

$$\tilde{R} \geqslant \max_b \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} \frac{1}{b} q_{\text{succ}} \left[1 - (\tilde{\lambda}_1 + \tilde{\lambda}_2) H\left(\frac{\tilde{\lambda}_1}{\tilde{\lambda}_1 + \tilde{\lambda}_2} \right) - (\tilde{\lambda}_3 + \tilde{\lambda}_4) H\left(\frac{\tilde{\lambda}_3}{\tilde{\lambda}_3 + \tilde{\lambda}_4} \right) - H(\tilde{\lambda}_1 + \tilde{\lambda}_2) \right]. \tag{C4}$$

When considering the practical model [49], Alice and Bob divide the raw keys n_z into blocks of size b. After the AD step is successfully completed, the number of raw keys they retain is $n_z q_{\text{succ}}/b$, the number of single-photon bits is $(\underline{s}_{11}^z/n_z)^b n_z q_{\text{succ}}/b$, and the QBER in the Z basis can be changed from E_z to $(E_z)^b/q_{\text{succ}}$. Therefore, after executing the AD step, Eq. (B12) is amended as

$$\begin{aligned}
\tilde{R} \geqslant \max_b \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} \frac{1}{N} \frac{n_z}{b} q_{\text{succ}} \Bigg\{ & \left(\frac{\underline{s}_0^z}{n_z} \right)^b + \left(\frac{\underline{s}_{11}^z}{n_z} \right)^b \left[1 - (\tilde{\lambda}_1 + \tilde{\lambda}_2) H\left(\frac{\tilde{\lambda}_1}{\tilde{\lambda}_1 + \tilde{\lambda}_2} \right) - (\tilde{\lambda}_3 + \tilde{\lambda}_4) H\left(\frac{\tilde{\lambda}_3}{\tilde{\lambda}_4 + \tilde{\lambda}_4} \right) \right] \\
& - f H(\tilde{E}_z) - \frac{b}{n_z q_{\text{succ}}} \left(\log_2 \frac{2}{\varepsilon_{\text{cor}}} + 2\log_2 \frac{2}{\varepsilon' \hat{\varepsilon}} + 2\log_2 \frac{1}{2\varepsilon_{\text{PA}}} \right) \Bigg\},
\end{aligned} \tag{C5}$$

subject to

$$\begin{aligned}
\underline{\phi}_{11}^z \leqslant \lambda_2 + \lambda_4 \leqslant \overline{\phi}_{11}^z, \\
\underline{e}_{11}^z \leqslant \lambda_3 + \lambda_4 \leqslant \overline{e}_{11}^z, \\
\tilde{E}_z = \frac{(E_z)^b}{(E_z)^b + (1 - E_z)^b},
\end{aligned} \tag{C6}$$

where $\tilde{E}_z$ represents total error rate after AD postprocessing in the Z basis.

[1] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 1984* (IEEE, New York, 1984), pp. 175–179.

[2] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[3] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[4] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, Phys. Rev. A **89**, 022307 (2014).

[5] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Secure quantum key distribution over 421 km of optical fiber, Phys. Rev. Lett. **121**, 190502 (2018).

[6] J. Dynes, A. Wonfor, W.-S. Tam, A. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. Yuan, A. Dixon, J. Cho *et al.*, Cambridge quantum network, npj Quantum Inf. **5**, 101 (2019).

[7] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, Performance and security of 5 GHz repetition rate polarization-based quantum key distribution, Appl. Phys. Lett **117**, 144003 (2020).

[8] D. Ma, X. Liu, C. Huang, H. Chen, H. Lin, and K. Wei, Simple quantum key distribution using a stable transmitter-receiver scheme, Opt. Lett. **46**, 2152 (2021).

[9] D. Scalcon, C. Agnesi, M. Avesani, L. Calderaro, G. Foletto, A. Stanco, G. Vallone, and P. Villoresi, Cross-encoded quantum key distribution exploiting time-bin and polarization states with qubit-based synchronization, Adv. Quantum Technol. **5**, 2200051 (2022).

[10] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan *et al.*, High-rate quantum key distribution exceeding 110 Mbs^{-1}, Nat. Photon. **17**, 416 (2023).

[11] K. Wei, X. Hu, Y. Du, X. Hua, Z. Zhao, Y. Chen, C. Huang, and X. Xiao, Resource-efficient quantum key distribution with integrated silicon photonics, Photon. Res. **11**, 1364 (2023).

[12] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photon. **8**, 595 (2014).

[13] 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).

[14] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photon. **4**, 686 (2010).

[15] K. Wei, W. Zhang, Y.-L. Tang, L. You, and F. Xu, Implementation security of quantum key distribution due to polarization-dependent efficiency mismatch, Phys. Rev. A **100**, 022325 (2019).

[16] M. Ye, J.-H. Li, Y. Wang, P. Gao, X.-X. Lu, and Y.-J. Qian, Quantum key distribution system against the probabilistic faint after-gate attack, Commun. Theor. Phys. **72**, 115102 (2020).

[17] P. Acheva, K. Zaitsev, V. Zavodilenko, A. Losev, A. Huang, and V. Makarov, Automated verification of countermeasure against detector-control attack in quantum key distribution, EPJ Quantum Technol. **10**, 22 (2023).

[18] 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).

[19] A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, V. Egorov, V. Makarov, and A. Huang, Protecting fiber-optic quantum key distribution sources against light-injection attacks, PRX Quantum **3**, 040307 (2022).

[20] 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).

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

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

[23] 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).

[24] H. Liu, J. Wang, H. Ma, and S. Sun, Polarization-multiplexing-based measurement-device-independent quantum key distribution without phase reference calibration, Optica **5**, 902 (2018).

[25] 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).

[26] 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).

[27] 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).

[28] 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).

[29] F.-Y. Lu, Z.-H. Wang, Z.-Q. Yin, S. Wang, R. Wang, G.-J. Fan-Yuan, X.-J. Huang, D.-Y. He, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Unbalanced-basis-misalignment-tolerant measurement-device-independent quantum key distribution, Optica **9**, 886 (2022).

[30] 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).

[31] J.-Y. Liu, X. Ma, H.-J. Ding, C.-H. Zhang, X.-Y. Zhou, and Q. Wang, Experimental demonstration of five-intensity measurement-device-independent quantum key distribution over 442 km, Phys. Rev. A **108**, 022605 (2023).

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

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

[34] 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).

[35] X. Ma, P. Zeng, and H. Zhou, Phase-matching quantum key distribution, Phys. Rev. X **8**, 031043 (2018).

[36] 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).

[37] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, npj Quantum Inf. **5**, 64 (2019).

[38] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system, Phys. Rev. X **9**, 021046 (2019).

[39] 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. Photon. **14**, 422 (2020).
[40] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, and A. J. Shields, 600-km repeater-like quantum communications with dual-band stabilization, Nat. Photon. **15**, 530 (2021).
[41] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution over 830-km fibre, Nat. Photon. **16**, 154 (2022).
[42] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, D.-F. Zhao, W.-J. Zhang, F.-X. Chen, H. Li, L.-X. You, Z. Wang, Y. Chen, X.-B. Wang, Q. Zhang, and J.-W. Pan, Quantum key distribution over 658 km fiber with distributed vibration sensing, Phys. Rev. Lett. **128**, 180502 (2022).
[43] L. Zhou, J. Lin, Y. Jing, and Z. Yuan, Twin-field quantum key distribution without optical frequency dissemination, Nat. Commun. **14**, 928 (2023).
[44] W. Li, L. Zhang, Y. Lu, Z.-P. Li, C. Jiang, Y. Liu, J. Huang, H. Li, Z. Wang, X.-B. Wang, Q. Zhang, L. You, F. Xu, and J.-W. Pan, Twin-field quantum key distribution without phase locking, Phys. Rev. Lett. **130**, 250802 (2023).
[45] 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).
[46] 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).
[47] P. Zeng, H. Zhou, W. Wu, and X. Ma, Mode-pairing quantum key distribution, Nat. Commun. **13**, 3903 (2022).
[48] 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).
[49] L. Zhou, J. Lin, Y.-M. Xie, Y.-S. Lu, Y. Jing, H.-L. Yin, and Z. Yuan, Experimental quantum communication overcomes the rate-loss limit without global phase tracking, Phys. Rev. Lett. **130**, 250801 (2023).
[50] Z.-H. Wang, R. Wang, Z.-Q. Yin, S. 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, Commun. Phys. **6**, 265 (2023).
[51] J.-L. Bai, Y.-M. Xie, F. Yao, H.-L. Yin, and Z.-B. Chen, Asynchronous measurement-device-independent quantum key distribution with hybrid source, Opt. Lett. **48**, 3551 (2023).
[52] Y.-M. Xie, J.-L. Bai, Y.-S. Lu, C.-X. Weng, H.-L. Yin, and Z.-B. Chen, Advantages of asynchronous measurement-device-independent quantum key distribution in intercity networks, Phys. Rev. Appl. **19**, 054070 (2023).
[53] X. Liu, D. Luo, Z. Zhang, and K. Wei, Mode-pairing quantum key distribution with advantage distillation, Phys. Rev. A **107**, 062613 (2023).
[54] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen *et al.*, An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature (London) **589**, 214 (2021).
[55] U. Maurer, Secret key agreement by public discussion from common information, IEEE Trans. Inf. Theory **39**, 733 (1993).
[56] D. Gottesman and H.-K. Lo, Proof of security of quantum key distribution with two-way classical communications, IEEE Trans. Inf. Theory **49**, 457 (2003).
[57] X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo, Decoy-state quantum key distribution with two-way classical postprocessing, Phys. Rev. A **74**, 032330 (2006).
[58] S. Khatri and N. Lütkenhaus, Numerical evidence for bound secrecy from two-way postprocessing in quantum key distribution, Phys. Rev. A **95**, 042320 (2017).
[59] R. Renner, Security of quantum key distribution, Int. J. Quantum Inf. **06**, 1 (2008).
[60] 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).
[61] 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).
[62] 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).
[63] 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).
[64] 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).
[65] 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, Quantum **7**, 1201 (2023).
[66] 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).
[67] K. Zhang, J. Liu, H. Ding, X. Zhou, C. Zhang, and Q. Wang, Asymmetric measurement-device-independent quantum key distribution through advantage distillation, Entropy **25**, 1174 (2023).
[68] Y. Zhou, R.-Q. Wang, C.-M. Zhang, Z.-Q. Yin, Z.-H. Wang, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Sending-or-not-sending twin-field quantum key distribution with advantage distillation, Phys. Rev. Appl. **21**, 014036 (2024).
[69] Z. Li and K. Wei, Improving parameter optimization in decoy-state quantum key distribution, Quantum Eng. **2022**, 9717591 (2022).
[70] C.-M. Zhang, Z. Wang, Y.-D. Wu, J.-R. Zhu, R. Wang, and H.-W. Li, Discrete-phase-randomized twin-field quantum key distribution with advantage distillation, Phys. Rev. A **109**, 052432 (2024).
[71] 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).
[72] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, Leftover hashing against quantum side information, IEEE Trans. Inf. Theory **57**, 5524 (2011).

[73] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 634 (2012).

[74] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner, Chain rules for smooth min- and max-entropies, IEEE Trans. Inf. Theory **59**, 2603 (2013).

[75] M. Tomamichel and R. Renner, Uncertainty relation for smooth entropies, Phys. Rev. Lett. **106**, 110506 (2011).

[76] H.-L. Yin, M.-G. Zhou, J. Gu, Y.-M. Xie, Y.-S. Lu, and Z.-B. Chen, Tight security bounds for decoy-state quantum key distribution, Sci. Rep. **10**, 14312 (2020).