entropy

IMPACT FACTOR 2.7

Indexed in: PubMed

CITESCORE 4.7

Article

Asymmetric Measurement-Device-Independent Quantum Key Distribution through Advantage Distillation

Kailu Zhang, Jingyang Liu, Huajian Ding, Xingyu Zhou, Chunhui Zhang and Qin Wang

Special Issue

Advances in Quantum Computing

Edited by

Dr. Brian R. La Cour and Dr. Giuliano Benenti

MDPI

https://doi.org/10.3390/e25081174

entropy

MDPI

Article

Asymmetric Measurement-Device-Independent Quantum Key Distribution through Advantage Distillation

Kailu Zhang [1,2,3,†], Jingyang Liu [1,2,3,†], Huajian Ding [1,2,3], Xingyu Zhou [1,2,3], Chunhui Zhang [1,2,3] and Qin Wang [1,2,3,*]

[1] Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China; 1221014031@njupt.edu.cn (K.Z.); 2020010107@njupt.edu.cn (J.L.); 2019010103@njupt.edu.cn (H.D.); xyz@njupt.edu.cn (X.Z.); chz@njupt.edu.cn (C.Z.)
[2] "Broadband Wireless Communication and Sensor Network Technology" Key Lab of Ministry of Education, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[3] "Telecommunication and Networks" National Engineering Research Center, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
* Correspondence: qinw@njupt.edu.cn
† These authors contributed equally to this work.

Abstract: Measurement-device-independent quantum key distribution (MDI-QKD) completely closes the security loopholes caused by the imperfection of devices at the detection terminal. Commonly, a symmetric MDI-QKD model is widely used in simulations and experiments. This scenario is far from a real quantum network, where the losses of channels connecting each user are quite different. To adapt such a feature, an asymmetric MDI-QKD model is proposed. How to improve the performance of asymmetric MDI-QKD also becomes an important research direction. In this work, an advantage distillation (AD) method is applied to further improve the performance of asymmetric MDI-QKD without changing the original system structure. Simulation results show that the AD method can improve the secret key rate and transmission distance, especially in the highly asymmetric cases. Therefore, this scheme will greatly promote the development of future MDI-QKD networks.

Keywords: quantum key distribution; asymmetric MDI-QKD; advantage distillation technology

Citation: Zhang, K.; Liu, J.; Ding, H.; Zhou, X.; Zhang, C.; Wang, Q. Asymmetric Measurement-Device-Independent Quantum Key Distribution through Advantage Distillation. *Entropy* **2023**, *25*, 1174. https://doi.org/10.3390/e25081174

Academic Editors: Giuliano Benenti and Brian R. La Cour

Received: 18 July 2023
Revised: 28 July 2023
Accepted: 3 August 2023
Published: 7 August 2023

1. Introduction

Quantum key distribution (QKD) can unconditionally ensure the theoretical security of information transmission between two or more distant users with quantum mechanics. In the process of development from theory to practice, there are many challenges to realizing remote and secure quantum key distribution in the practical applications. With various theoretical ideas and experimental schemes being put forward, many challenges have been overcome. The BB84 protocol [1] proposed by Bennett realizes two-point communication and the Ekert91 and BBM92 protocols have been proposed successively [2,3]. Although QKD has been proven to have unconditional security in theory, imperfect devices can lead to some security loopholes that hinder the development of QKD protocols in practical applications. In practical applications, we often use weak coherent sources (WCSs) with multi-photon components, and Eve can eavesdrop with photon-number splitting (PNS) attacks [4]. Fortunately, the decoy-state method proposed [5,6] can solve PNS attacks and obtain rapid development both theoretically and experimentally [7–9]. Considering the imperfection of the detector, Lo firstly proposed the MDI-QKD protocol [10] which thoroughly solves the security loopholes mainly at the detection terminal. With the advantages of the MDI-QKD protocol, the MDI-QKD protocol attracts extensive attention and has been greatly studied in theory and experiments [11–18].

In previous work, the MDI-QKD was mainly studied in symmetric scenarios for simplicity. With the development of theory and technology, researchers have paid more

attention to the asymmetric MDI-QKD protocol in recent years. To achieve good interference at the detection terminal, Lo proposed an asymmetric seven-intensity MDI-QKD [19], which can improve the performance of MDI-QKD in practical asymmetric structures based on the four-intensity MDI-QKD [11]. Consequently, asymmetric MDI-QKD is more suitable for the common QKD networks. However, due to its asymmetric nature, its performance is inferior to that of the original symmetric scheme. Improving the performance of asymmetric MDI-QKDs has become an urgent problem that needs to be addressed.

Inspired by the advantage distillation (AD) method [20–23], we study the principle of the method and find that the AD method can be successfully applied to the asymmetric seven-intensity MDI-QKD protocol. Compared with the original protocol, the performance of the asymmetric protocol has been significantly improved, which provides another theoretical verification that the post-processing AD method can improve the performance of the QKD protocol. This method can divide the original key string into blocks of only a few bits to achieve a high key correlation and greatly improve the protocol's performance. The paper is organized as follows: In Section 2, we review the asymmetric seven-intensity MDI-QKD protocol and introduce the protocol with AD. The results of numerical simulations are shown in Section 3. Finally, summaries are given in Section 4.

2. Methods

2.1. Asymmetric MDI-QKD

Here, we mainly describe the process of the asymmetric seven-intensity MDI-QKD protocol, which develops from the four-intensity symmetric protocol, as follows:

(1). ***State preparation***. Alice (Bob) randomly prepares the signal state only in Z basis with s_A (s_B), and prepares the decoy states only in X basis with intensities of w_A,v_A (w_B,v_B), satisfying the formula $w_A < v_A$ ($w_B < v_B$). When preparing the vacuum state of intensity o, Alice (Bob) does not choose any base. The prepared states will be sent to Charlie to perform measurement;

(2). ***Measurement***. Charlie performs the Bell state measurement (BSM) after receiving the quantum states sent from Alice and Bob;

(3). ***Announcement***. After Alice and Bob repeat the above steps and enough counting events are recorded, Charlie publicly announces the BSM results. Subsequently, they announce the selected bases and intensities;

(4). ***Parameter estimation***. After finishing the quantum transmission phase, Alice and Bob can estimate the lower bound of single-photon yield $Y_{11}^{Z,L}$ and the upper bound of single-photon error rate (QBER) $e_{11}^{X,U}$ using the decoy-state technology;

(5). ***Post-processing***. Alice and Bob perform key reconciliation and privacy amplification on the raw key data to obtain the final secret key.

The decoupled bases are used in the asymmetric seven-intensity MDI-QKD protocol, thus the protocol can perform decoy states in the X basis only to estimate $Y_{11}^{X,L}$ and can use $Y_{11}^{Z,L} = Y_{11}^{X,L}$ to obtain the single-photon yield in Z basis [11]. Then, the secret key rate can be calculated by the following formula [10,11,19]:

$$R = P_{s_A} P_{s_B} \left\{ (s_A e^{-s_A})(s_B e^{-s_B}) Y_{11}^{Z,L} [1 - h(e_{11}^{X,U})] - f_e Q_{s_A s_B}^{Z} h(E_{s_A s_B}^{Z}) \right\}, \quad (1)$$

where P_{s_A} and P_{s_B} each correspond to the probability that Alice or Bob emits the signal states of s_A or s_B, respectively. $Q_{s_A s_B}^{Z}$ and $E_{s_A s_B}^{Z}$ are the gain and QBER in the Z basis, $Y_{11}^{X,L}(e_{11}^{X,U})$ is the lower (upper) bound of single-photon yield (QBER), which can be estimated from the decoy-state technology, $h(x)$ is the binary entropy function, and f_e is the error correction efficiency.

Based on the asymmetric seven-intensity MDI-QKD protocol above, the performance can be further improved by optimization techniques such as joint estimations and collective constraints [11]. Referring to the joint estimations method, the common part $\mathbb{H}$ is extracted from the following two parameters $Y_{11}^{X,L}$, $e_{11}^{X,U}$ to optimize the key rate. $e_{11}^{Z,U}$

is used in the following subsection. $Y_{11}^{X,L}$ is a piecewise function where $P_{v_A}^1 P_{w_A}^2 P_{w_B}^1 P_{v_B}^2 < P_{w_A}^1 P_{v_A}^2 P_{v_B}^1 P_{w_B}^2$ [19,24]. These parameters $Y_{11}^{X,L}$, $e_{11}^{X,U}$ and $e_{11}^{Z,U}$ can be estimated accurately by the decoy-state technology in the original MDI-QKD protocol [10,11]. The following formulas can estimate these parameters which lead to a much higher rate in distilling the secure final key:

$$Y_{11}^{X,L} = Y_{11}^{X,e} = \frac{P_{v_A}^1 P_{v_B}^2 Q_{w_A w_B} + P_{w_A}^1 P_{w_B}^2 P_{v_A}^0 Q_{o w_B} + P_{w_A}^1 P_{w_B}^2 P_{v_B}^0 Q_{v_A o}}{P_{w_A}^1 P_{v_A}^1 (P_{w_B}^1 P_{v_B}^2 - P_{w_B}^2 P_{v_B}^1)} - \frac{P_{w_A}^1 P_{w_B}^2 Q_{v_A v_B} + P_{w_A}^1 P_{w_B}^2 P_{v_A}^0 P_{v_B}^0 Q_{oo}}{P_{w_A}^1 P_{v_A}^1 (P_{w_B}^1 P_{v_B}^2 - P_{w_B}^2 P_{v_B}^1)} - \frac{P_{v_A}^1 P_{v_B}^2 \mathbb{H}}{P_{w_A}^1 P_{v_A}^1 (P_{w_B}^1 P_{v_B}^2 - P_{w_B}^2 P_{v_B}^1)}, \tag{2}$$

$$Y_{11}^{X,L} = Y_{11}^{X,f} = \frac{P_{v_B}^1 P_{v_A}^2 Q_{w_A w_B} + P_{w_B}^1 P_{w_A}^2 P_{v_A}^0 Q_{o w_B} + P_{w_B}^1 P_{w_A}^2 P_{v_B}^0 Q_{v_A o}}{P_{w_B}^1 P_{v_B}^1 (P_{w_A}^1 P_{v_A}^2 - P_{w_A}^2 P_{v_A}^1)} - \frac{P_{w_B}^1 P_{w_A}^2 Q_{v_A v_B} + P_{w_B}^1 P_{w_A}^2 P_{v_A}^0 P_{v_B}^0 Q_{oo}}{P_{w_B}^1 P_{v_B}^1 (P_{w_A}^1 P_{v_A}^2 - P_{w_A}^2 P_{v_A}^1)} - \frac{P_{v_B}^1 P_{v_A}^2 \mathbb{H}}{P_{w_B}^1 P_{v_B}^1 (P_{w_A}^1 P_{v_A}^2 - P_{w_A}^2 P_{v_A}^1)}, \tag{3}$$

$$e_{11}^{X,U} = \frac{T_{w_A w_B}(1 + \gamma\sqrt{1/(N_{x w_A w_B} T_{w_A w_B})}) - \mathbb{H}/2}{P_{w_A}^1 P_{w_B}^1 Y_{11}^{X,L}}, \tag{4}$$

$$e_{11}^{Z,U} = \frac{T_{s_A s_B} + P_{s_A}^0 P_{s_B}^0 T_{oo} - [P_{s_A}^0 T_{o s_B} + P_{s_B}^0 T_{s_A o}]}{P_{s_A}^1 P_{s_B}^1 Y_{11}^{Z,L}}, \tag{5}$$

$$\mathbb{H} = P_{w_A}^0 Q_{o w_B} + P_{w_B}^0 Q_{w_A o} - P_{w_A}^0 P_{w_B}^0 Q_{oo}, \tag{6}$$

where $P_{l_A}^n (P_{l_B}^m)$ denotes the photon-number distribution of the source at Alice's (Bob's) side, $Q_{l_A l_B}$ and $T_{l_A l_B}$ are the gain and the total quantum bit errors [25], and $\mathbb{H}$ is the combination of the gain of the decoy state and the vacuum state. γ is the standard error, and its value is set to 5.3 here. The expression for $Y_{11}^{X,L}$ is equal to $Y_{11}^{X,e}$ when $P_{v_A}^1 P_{w_A}^2 P_{w_B}^1 P_{v_B}^2 < P_{w_A}^1 P_{v_A}^2 P_{v_B}^1 P_{w_B}^2$, otherwise the expression equals $Y_{11}^{X,f}$ [19,24]. Considering the effect of statistical fluctuations on multiple observations, the method of collective constraints can provide tighter constraint conditions between different sources$(s_A, w_A, v_A, s_B, w_B, v_B, o)$ than independent bounds. Thus, these parameters $Y_{11}^{X,L}, e_{11}^{Z,U}, \mathbb{H}$ can be further optimized to achieve a higher key rate by the joint constraints method [8].

By the above formulas, we can calculate the final secret key rate of the asymmetric seven-intensity MDI-QKD protocol.

2.2. Asymmetric MDI-QKD with AD

Many previous works have demonstrated that the AD method can further improve the performance of QKD [20–23]. In this section, we improve the secure key rate and transmission distance of the asymmetric seven-intensity MDI-QKD protocol with the AD method. An additional AD method is performed between parameter estimation and post-processing step, and highly correlated bit pairs are discriminated from weakly correlated information. The security of AD method will be analyzed in an entanglement-based scheme. Alice prepares the quantum state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and sends the second particle to Bob through the quantum channel. Since Eve controls the quantum channel by certain value λ_i(i = 0, 1, 2, 3), the quantum state shared between Alice and Bob after transmission can be expressed by the following formula:

$$\sigma_{AB} = \lambda_0 |\phi_0\rangle\langle\phi_0| + \lambda_1 |\phi_1\rangle\langle\phi_1| + \lambda_2 |\phi_2\rangle\langle\phi_2| + \lambda_3 |\phi_3\rangle\langle\phi_3|, \tag{7}$$

$$
\begin{aligned}
|\phi_0\rangle &= \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle),\\
|\phi_1\rangle &= \frac{1}{\sqrt{2}}(|00\rangle-|11\rangle),\\
|\phi_2\rangle &= \frac{1}{\sqrt{2}}(|01\rangle+|10\rangle),\\
|\phi_3\rangle &= \frac{1}{\sqrt{2}}(|01\rangle-|10\rangle),
\end{aligned}
\tag{8}
$$

and $\lambda_0+\lambda_1+\lambda_2+\lambda_3=1$. For the quantum state σ_{AB}, the bit error rate of Alice and Bob's measurements on different bases can be expressed as $\lambda_1+\lambda_3=e_1^x$ (four-state or six-state protocol), $\lambda_2+\lambda_3=e_1^z$ (four-state or six-state protocol), and $\lambda_1+\lambda_2=e_1^y$ (six-state protocol). Eve can steal information and reduce the key rate by choosing the certain value λ_i and the secret key rate can be given by [20]:

$$
\begin{aligned}
R &\geq min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3}[H(X|E)-H(X|Y)]\\
&= min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3}[1-(\lambda_0+\lambda_1)h(\frac{\lambda_0}{\lambda_0+\lambda_1})-(\lambda_2+\lambda_3)h(\frac{\lambda_2}{\lambda_2+\lambda_3})-h(\lambda_0+\lambda_1)].
\end{aligned}
\tag{9}
$$

In the AD method, Alice and Bob divide their own raw bits into blocks $(x_1,\ldots,x_b)$ and $(y_1,\ldots,y_b)$ of size b. Then, choosing a random binary value c, Alice sends $(x_1\oplus c,\ldots,x_1\oplus c)$ to Bob. Bob compares this bitstring with their bitstring $(y_1,\ldots,y_b)$ and accepts the security of information only if the results are either all zeros or all ones in the block. In the two cases accepted, Alice (Bob) saves the first bit x_1 (y_1) of the initial string as the raw key. Thus, AD can discern highly correlated bitstring from weakly correlated information as the final raw key. Obviously, the successful probability of the AD method on a certain block of size b can be calculated by:

$$
P_{succ}=(\lambda_0+\lambda_1)^b+(\lambda_2+\lambda_3)^b. \tag{10}
$$

After performing the AD step, the practical QBER value $\lambda_2+\lambda_3$ in the Z basis can be replaced by $\frac{(\lambda_2+\lambda_3)}{P_{succ}}$, and the practical QBER in the X basis also can be recalculated. The quantum state shared between Alice and Bob can be replaced by:

$$
\sigma_{AB}=\overline{\lambda}_0|\phi_0\rangle\langle\phi_0|+\overline{\lambda}_1|\phi_1\rangle\langle\phi_1|+\overline{\lambda}_2|\phi_2\rangle\langle\phi_2|+\overline{\lambda}_3|\phi_3\rangle\langle\phi_3|, \tag{11}
$$

$$
\begin{aligned}
\overline{\lambda}_0 &= \frac{(\lambda_0+\lambda_1)^b+(\lambda_0-\lambda_1)^b}{2P_{succ}},\\
\overline{\lambda}_1 &= \frac{(\lambda_0+\lambda_1)^b-(\lambda_0-\lambda_1)^b}{2P_{succ}},\\
\overline{\lambda}_2 &= \frac{(\lambda_2+\lambda_3)^b+(\lambda_2-\lambda_3)^b}{2P_{succ}},\\
\overline{\lambda}_3 &= \frac{(\lambda_2+\lambda_3)^b-(\lambda_2-\lambda_3)^b}{2P_{succ}}.
\end{aligned}
\tag{12}
$$

The QKD protocol enhanced by the AD method can achieve the secret key at rate [20]:

$$
\begin{aligned}
R \geq max_b\ &\frac{1}{b}P_{succ}min_{\overline{\lambda}_0,\overline{\lambda}_1,\overline{\lambda}_2,\overline{\lambda}_3}[1-(\overline{\lambda}_0+\overline{\lambda}_1)h(\frac{\overline{\lambda}_0}{\overline{\lambda}_0+\overline{\lambda}_1})-(\overline{\lambda}_2+\overline{\lambda}_3)h(\frac{\overline{\lambda}_2}{\overline{\lambda}_2+\overline{\lambda}_3})\\
&-h(\overline{\lambda}_0+\overline{\lambda}_1)].
\end{aligned}
\tag{13}
$$

Based on the previous analysis, the AD method can be combined with the QKD protocol. It has been widely used in other protocols in previous works. Similarly, the

AD method can be applied to further optimize the properties of quantum channels in the asymmetric MDI-QKD. When the AD method is combined with the asymmetric seven-intensity MDI-QKD protocol, the secret key rate can be estimated by the following formula:

$$R \geq P_{s_A} P_{s_B} \frac{1}{b} q_{succ} Q^Z_{s_A s_B} \{ (\frac{P_{11} Y^{Z,L}_{11}}{Q^Z_{s_A s_B}})^b [1 - (\overline{\lambda}_0 + \overline{\lambda}_1) h(\frac{\overline{\lambda}_0}{\overline{\lambda}_0 + \overline{\lambda}_1}) - (\overline{\lambda}_2 + \overline{\lambda}_3) h(\frac{\overline{\lambda}_2}{\overline{\lambda}_2 + \overline{\lambda}_3})] - f_e h(\overline{E}^Z_{s_A s_B}) \}, \tag{14}$$

$$P_{11} = s_A e^{-s_A} s_B e^{-s_B}, \tag{15}$$

$$q_{succ} = (E^Z_{s_A s_B})^b + (1 - E^Z_{s_A s_B})^b, \tag{16}$$

$$\overline{E}^Z_{s_A s_B} = \frac{(E^Z_{s_A s_B})^b}{(E^Z_{s_A s_B})^b + (1 - (E^Z_{s_A s_B}))^b}, \tag{17}$$

where P_{11} is the probability of both Alice and Bob's signal states emitting single-photon events, q_{succ} is the successful probability of the AD method, $\overline{E}^Z_{s_A s_B}$ is the error rate value after the AD method, and e^x_{11} and e^z_{11} are the single-photon error rate in the X and Z bases, respectively. Note that $Y^{X,L}_{11}$, e^x_{11}, and e^z_{11} can be estimated with the decoy-state method.

3. Results

In this work, we explore the combination of a QKD and a post-processing method. We adopt the asymmetric seven-intensity MDI-QKD protocol and the AD method, which can improve the performance of asymmetric MDI-QKD protocol greatly. In this section, numerical simulations of the asymmetric seven-intensity MDI-QKD protocol with AD method are given and the simulation parameters are shown in Table 1. After analyzing the simulation results, we obtained the following significant research results.

Table 1. The basic system parameters used in our numerical simulations. η_D and Y_0 are the efficiency and dark count rate of detectors at Charlie's side; e_d: the misalignment error of the QKD system; f_e: the error correction efficiency; N: the number of pulse pairs Alice and Bob send.

e_d	η_D	Y_0	f_e	N
0.5%	65%	8×10^{-7}	1.16	10^{11}

We analyze the secret key rate of the asymmetric MDI-QKD protocol with and without the AD method, and the corresponding comparison results are shown in Figure 1 under different conditions L_{asy} = 0 dB, 12 dB, 24 dB. The figure shows that the key rate with and without AD are consistent within a short distance. However, for example, the red line with L_{asy} = 12 dB, the AD method has a clear advantage at a transmission loss of about 33 dB, and a final transmission loss reaching 39 dB as well as the secret key rate showing a clear improvement. For a more obvious exploration of the reason, we present Figure 2 with respect to b. We can observe that, in the above example, the value of b at about 33 dB has changed from 1 to 2, indicating that the AD method begins to work. With the increase of transmission loss, the AD method requires a larger b value to obtain a tight correlation from weak correlation. Furthermore, the results of the above case are similar to the other two cases (L_{asy} = 0 dB, L_{asy} = 24 dB). Therefore, the AD method can improve the key generation rate of asymmetric MDI-QKD over a long distance.

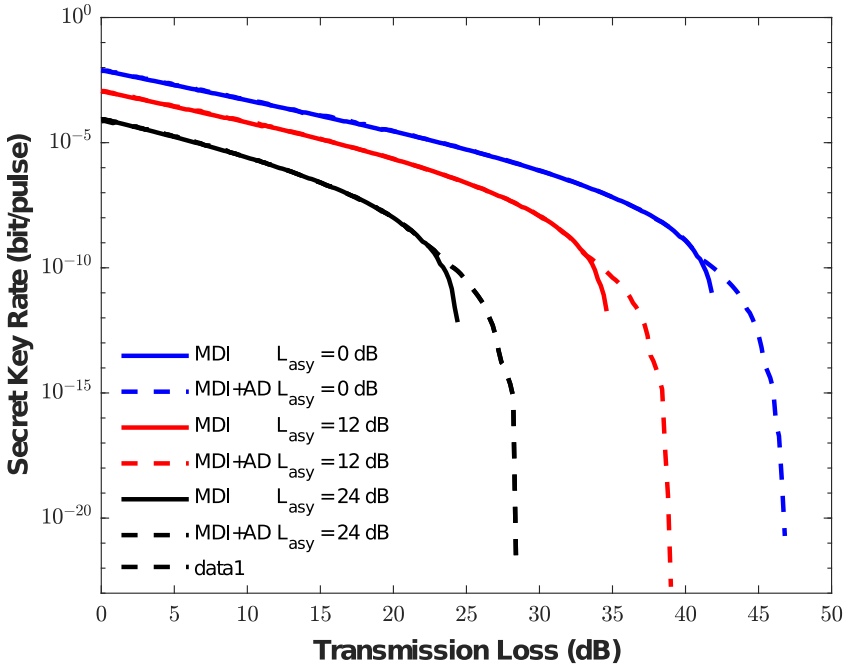

Figure 1. Comparison of the secret key generation rate versus the transmission loss. The value L_{asy} is the loss difference of Alice to Charlie and Bob to Charlie. The different colors represent loss difference, which is L_{asy} = 0 dB, L_{asy} = 12 dB, and L_{asy} = 24 dB, respectively. The solid line represents the secret key without the AD method, and the dotted line represents the secret key with the AD method.

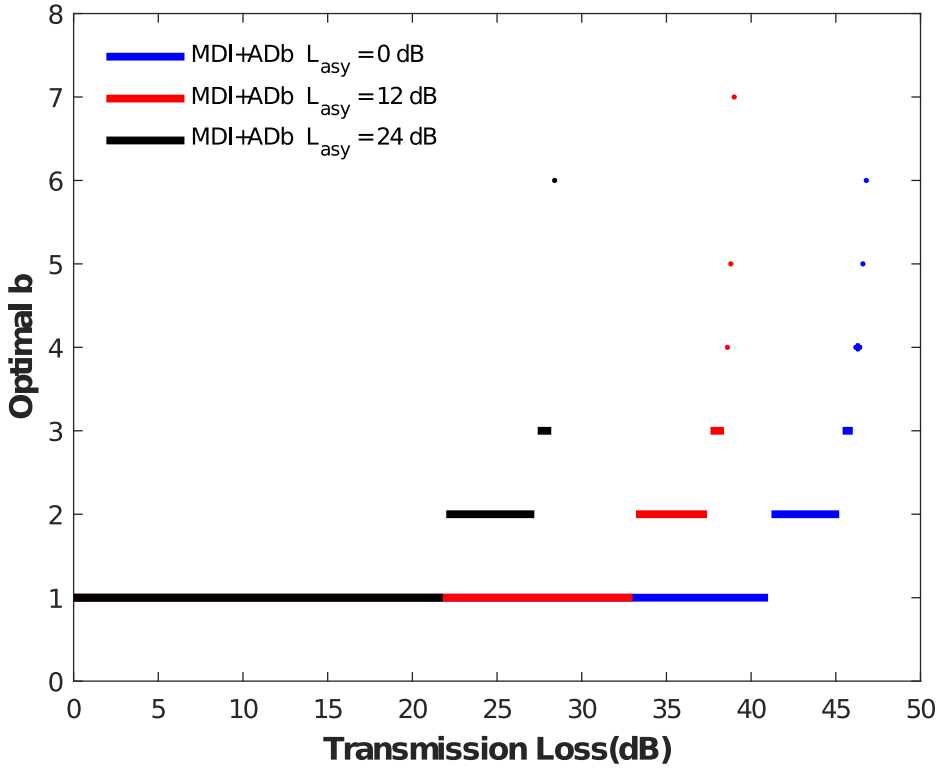

Figure 2. Results of the optimal b versus the transmission loss. The black, red, and blue represent the values L_{asy} = 0 dB, L_{asy} = 12 dB, and L_{asy} = 24 dB, respectively. When value b is not equal to 1, the AD method can further improve the secret key rate and transmission distance of the asymmetric MDI-QKD protocol.

Additionally, we also further investigate the specific effects of the AD method on an asymmetric MDI-QKD under various values L_{asy}, and the results are shown in Figure 3. We describe the meaning of Figure 3 and give a detailed definition of the improved percentage. Generally, when the degree of asymmetry is large, the deterioration of the key rate becomes more obvious. However, after the AD method is used, it can be clearly seen in Figure 3 that the improvement effect of the AD method becomes more obvious with the increase of the degree of asymmetry. For example, the improved percentage can reach about 35% when the value L_{asy} = 35 dB, which means that AD method can better solve some transmission performance bottlenecks of the entire network.

By the above analysis, the AD method indeed can increase the propagation distance when the number of pulse pairs $N = 10^{11}$. In order to further analyze the finite size effects, we give the simulation results in Figure 4 under different values of N when the value L_{asy} = 12 dB. As can be seen from Figure 4, the AD method improves the performance of the asymmetric MDI-QKD protocol under various finite-size effects. Even though there is a large statistical fluctuation when the number of pulse pairs $N = 10^{10}$, the AD method can still tolerate transmission losses of more than 5 dB, which means that AD method can also be more adaptable with finite-size cases.

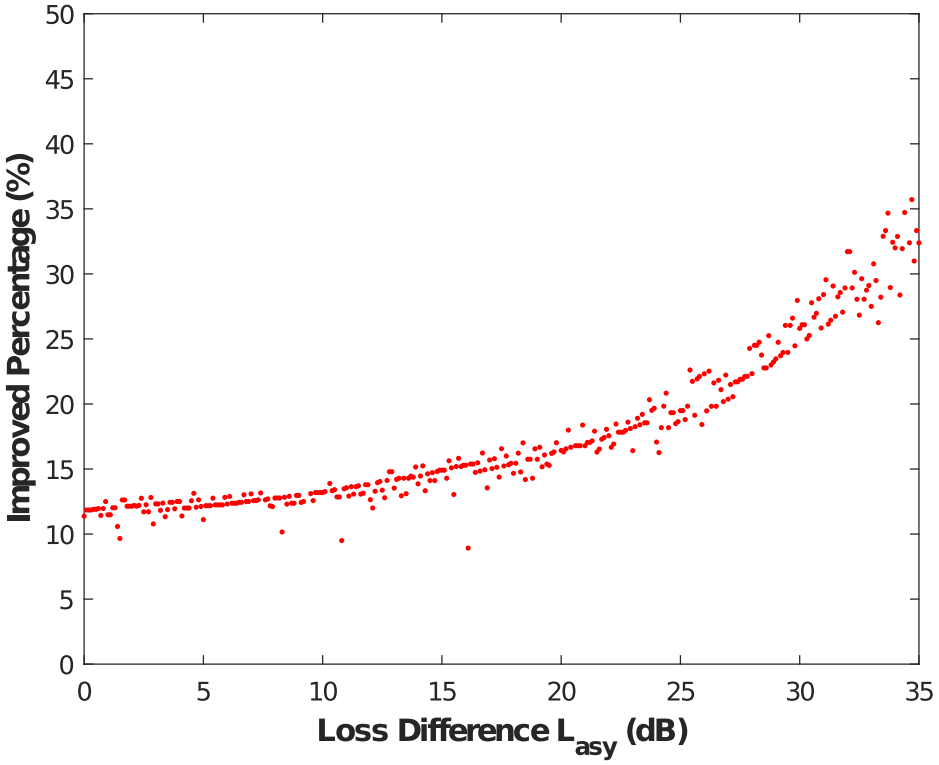

Figure 3. Results of the value L_{asy} versus the improved percentage. The improved transmission loss is the difference of the maximum transmission loss of the asymmetric MDI-QKD with and without the AD method, and we define the improved percentage as the difference divided by the latter. With the increasing degree of asymmetry, the improved percentage also becomes better.

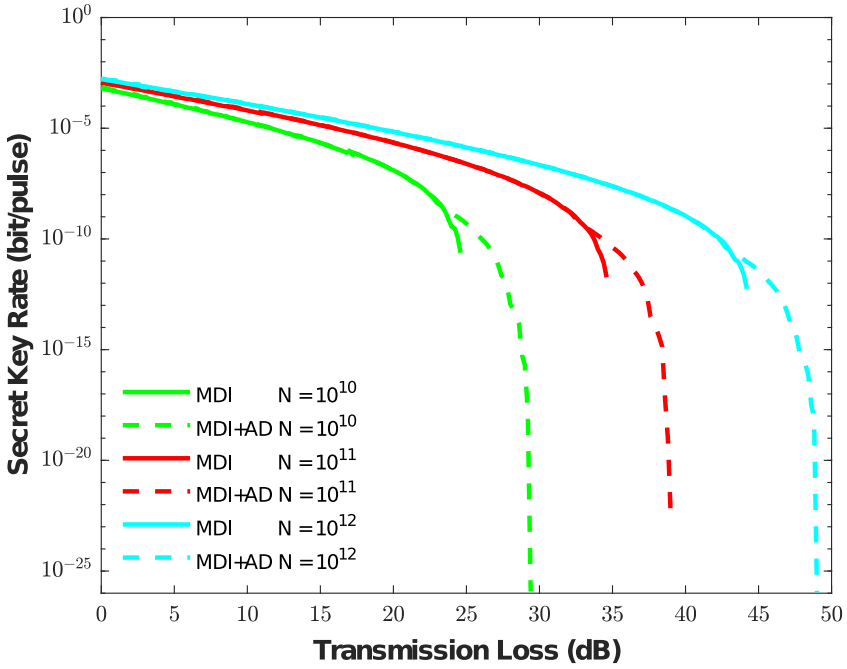

Figure 4. Comparison of the secret key generation rate versus the transmission loss when the value L_{asy} = 12 dB. The different colors represent the values $N = 10^{10}$, $N = 10^{11}$, and $N = 10^{12}$, respectively. The solid line represents the secret key without the AD method, and the dotted line represents the secret key with the AD method.

4. Conclusions

The AD method, a classical algorithm based on information theory, can be combined with QKD without changing the existing system structure. Specifically, the AD method can be combined with an asymmetric seven-intensity MDI-QKD to improve the robustness effectively, so as to distinguish and extract highly correlated bit pairs from the weakly correlated information as the final secret key. The AD method has a better performance for the asymmetric MDI-QKD protocol. The greater the degree of asymmetry, the better the improvement of the AD method. The AD method can also improve the performance of the asymmetric MDI-QKD protocol under various finite-size effects, and can be more adaptable with finite-size cases. Our work may play a role in measurement-device-independent networks.

Author Contributions: Conceptualization, J.L. and Q.W.; Methodology, K.Z., J.L., H.D., C.Z. and Q.W.; Software, K.Z., J.L., H.D. and C.Z.; Validation, K.Z., J.L., H.D., X.Z., C.Z. and Q.W.; Formal analysis, K.Z., J.L., X.Z. and C.Z.; Investigation, J.L. and C.Z.; Resources, Q.W.; Data curation, K.Z., J.L., X.Z. and C.Z.; Writing—original draft, K.Z. and X.Z.; Writing—review & editing, J.L., H.D., X.Z. and Q.W.; Visualization, K.Z. and J.L.; Supervision, X.Z. and Q.W.; Project administration, Q.W.; Funding acquisition, X.Z. and Q.W. All authors have read and agreed to the published version of the manuscript.

Funding: We gratefully acknowledge the financial support from the National Natural Science Foundation of China (12074194, 12104240, 62101285); Industrial Prospect and Key Core Technology Projects of Jiangsu provincial key R&D Program (E2022071); Natural Science Foundation of Jiangsu Province (BK20192001, BK20210582); Postgraduate Research & Practice Innovation Program of Jiangsu Province (KYCX20_0726); Natural Science Foundation of the Jiangsu Higher Education Institutions(21KJB140014), and NUPTSF (NY220122, NY220123).

Institutional Review Board Statement: Not applicable.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 9–12 December 1984.
2. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef] [PubMed]
3. Bennett, C.H.; Brassard, G.; Mermin, N.D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **1992**, *68*, 557. [CrossRef] [PubMed]
4. Lutkenhaus, N.; Jahma, M. Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack. *New J. Phys.* **2002**, *4*, 44. [CrossRef]
5. Lo, H.K.; Ma, X.F.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef]
6. Wang, X.B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef]
7. Wang, X.B. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Phys. Rev. A* **2013**, *87*, 12320. [CrossRef]
8. Yu, Z.W.; Zhou, Y.H.; Wang, X.B. Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method. *Phys. Rev. A* **2015**, *91*, 032318. [CrossRef]
9. Zhang, C.H.; Zhang, C.M.; Wang, Q. Improving the Performance of Practical Decoy-State Measurement-Device-Independent Quantum Key Distribution with Biased Basis Choice. *Theor. Comput. Phys.* **2018**, *70*, 331. [CrossRef]
10. Lo, H.K. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
11. Zhou, Y.H.; Yu, Z.W.; Wang, X.B. Making the decoy-state measurement-device independent quantum key distribution practically useful. *Phys. Rev. A* **2016**, *93*, 042324. [CrossRef]
12. Liu, H.; Wang, W.; Wei, K.; Fang, X.T.; Li, L.; Liu, N.L.; Liang, H.; Zhang, S.J.; Zhang, W.; Li, H.; et al. Experimental Demonstration of High-Rate Measurement-Device-Independent Quantum Key Distribution over Asymmetric Channels. *Phys. Rev. Lett.* **2019**, *122*, 160501. [CrossRef]
13. Chen, Y.P.; Liu, J.Y.; Sun, M.S.; Zhou, X.Y.; Zhang, C.H.; Li, J.; Wang, Q. Experimental measurement-device-independent quantum key distribution with the double-scanning method. *Opt. Lett.* **2021**, *46*, 3729–3732. [CrossRef]
14. Jiang, C.; Yu, Z.W.; Hu, X.L.; Wang, X.B. Higher key rate of measurement-deviceindependent quantum key distribution through joint data processing. *Phys. Rev. A* **2021**, *103*, 012402. [CrossRef]
15. Lu, F.Y.; Wang, Z.H.; Yin, Z.Q.; Wang, S.; Wang, R.; Guo, G.C.; Han, Z.F. Unbalanced-basis-misalignment-tolerant measurement-device-independent quantum key distribution. *Optica* **2022**, *9*, 886–893. [CrossRef]
16. Cao, Y.; Li, Y.H.; Yang, K.X.; Jiang, Y.F.; Li, S.L.; Hu, X.L.; Abulizi, M.; Li, C.L.; Zhang, W.J.; Sun, Q.C.; et al. Long-Distance Free-Space Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2020**, *125*, 260503. [CrossRef] [PubMed]
17. Wei, K.J.; Li, W.; Tan, H.; Li, Y.; Min, H.; Zhang, W.J.; Li, H.; You, L.X.; Wang, Z.; Jiang, X.; et al. High-Speed Measurement-Device-Independent Quantum Key Distribution with Integrated Silicon Photonics. *Phys. Rev. X* **2020**, *10*, 031030. [CrossRef]
18. Jie, G.; Yuan, F.; Lu, F.Y.; Wang, S.; Yin, Z.Q.; He, D.Y.; Chen, W.; Zhou, Z.; Wang, H.Z.; Teng, J.; et al. Robust and Adaptable Quantum Key Distribution Network without Trusted Nodes. *Optica* **2022** *9*, 812.
19. Wang, W.Y.; Xu, F.H.; Lo, H.K. Asymmetric Protocols for Scalable High-Rate Measurement-Device-Independent Quantum Key Distribution Networks. *Phys. Rev. X* **2019**, *9*, 041012. [CrossRef]
20. Renner, R. Security of quantum key distribution. *Int. J. Quant. Inf.* **2008**, *6*, 1–127. [CrossRef]
21. Wang, R.Q.; Zhang, C.M.; Yin, Z.Q.; Li, H.W.; Wang, S.; Chen, W.; Guo, G.C.; Han, Z.F. Phase-matching quantum key distribution with advantage distillation. *New J. Phys.* **2022**, *24*, 73049. [CrossRef]
22. Li, H.W.; Zhang, C.M.; Jiang, M.S.; Cai, Q.Y. Improving the performance of practical decoy-state quantum key distribution with advantage distillation technology. *Commun. Phys.* **2022**, *5*, 53. [CrossRef]
23. Li, H.W.; Wang, R.Q.; Zhang, C.M.; Cai, Q.Y. Improving the performance of twin-field quantum key distribution with advantage distillation technology. *arXiv* **2022**, arXiv:2202.10059.
24. Xu, F.H.; Curty, M.; Qi, B.; Lo, H.K. Practical aspects of measurement-device-independent quantum key distribution. *New J. Phys.* **2013**, *15*, 113007. [CrossRef]
25. Wang, Q.; Wang, X.B. Simulating of the measurement-device independent quantum key distribution with phase randomized general sources. *Sci. Rep.* **2014**, *4*, 4612. [CrossRef]