

Asymmetric mode-pairing quantum key distribution with advantage distillation

Hai-Tao Wang(汪海涛), Chun Zhou(周淳), Yi-Fei Lu(陆宜飞), Chen-Peng Hao(郝辰鹏), Yan-Mei Zhao(赵燕美), Yan-Yang Zhou(周砚扬), Hong-Wei Li(李宏伟), and Wan-Su Bao(鲍皖苏)

Citation: Chin. Phys. B, 2025, 34 (**4**): 040305. DOI: 10.1088/1674-1056/adbb5c
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Mask-coding-assisted continuous-variable quantum direct communication with orbital angular momentum multiplexing

Zhengwen Cao(曹正文), Yujie Wang(王禹杰), Geng Chai(柴庚), Xinlei Chen(陈欣蕾), and Yuan Lu(卢缘)
Chin. Phys. B, 2025, 34 (**2**): 020308. DOI: 10.1088/1674-1056/ad9ff7

Improved reference-frame-independent quantum key distribution with intensity fluctuations

Zi-Qi Chen(陈子骐), Hao-Bing Sun(孙昊冰), Ming-Shuo Sun(孙铭烁), and Qin Wang(王琴)
Chin. Phys. B, 2025, 34 (**2**): 020302. DOI: 10.1088/1674-1056/ad99cb

Effect of pseudo-random number on the security of quantum key distribution protocol

Xiao-Liang Yang(杨晓亮), Yu-Qing Li(李毓擎), and Hong-Wei Li(李宏伟)
Chin. Phys. B, 2025, 34 (**2**): 020301. DOI: 10.1088/1674-1056/ad99c9

Multi-protocol relay chaining for large-scale quantum key distribution networks

Yuan Cao(曹原), Xiaosong Yu(郁小松), Yongli Zhao(赵永利), Chunhui Zhang(张春辉), Xingyu Zhou(周星宇), Jie Zhang(张杰), and Qin Wang(王琴)
Chin. Phys. B, 2025, 34 (**1**): 010310. DOI: 10.1088/1674-1056/ad9018

Security analysis of satellite-to-ground reference-frame-independent quantum key distribution with beam wandering

Chun Zhou(周淳), Yan-Mei Zhao(赵燕美), Xiao-Liang Yang(杨晓亮), Yi-Fei Lu(陆宜飞), Yu Zhou(周雨), Xiao-Lei Jiang(姜晓磊), Hai-Tao Wang(汪海涛), Yang Wang(汪洋), Jia-Ji Li(李家骥), Mu-Sheng Jiang(江木生), Xiang Wang(汪翔), Hai-Long Zhang(张海龙), Hong-Wei Li(李宏伟), and Wan-Su Bao(鲍皖苏)
Chin. Phys. B, 2024, 33 (**8**): 080306. DOI: 10.1088/1674-1056/ad51f6

SPECIAL TOPIC — Quantum communication and quantum network

Asymmetric mode-pairing quantum key distribution with advantage distillation

Hai-Tao Wang(汪海涛), Chun Zhou(周淳)†, Yi-Fei Lu(陆宜飞), Chen-Peng Hao(郝辰鹏), Yan-Mei Zhao(赵燕美), Yan-Yang Zhou(周砚扬), Hong-Wei Li(李宏伟), and Wan-Su Bao(鲍皖苏)

Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou 450001, *China*

(Received 31 December 2024; revised manuscript received 11 February 2025; accepted manuscript online 28 February 2025)

Mode-pairing quantum key distribution (MP-QKD) is an excellent scheme that can exceed the repeaterless rate-transmittance bound without complex phase locking. Nevertheless, MP-QKD usually needs to ensure that the communication distances of the two channels are equal. To address the problem, the asymmetric MP-QKD protocol is proposed. In this paper, we enhance the performance of the asymmetric MP-QKD protocol based on the advantage distillation (AD) method without modifying the quantum process. The simulation results show that the AD method can extend the communication distance by about 70 km in the case of asymmetry. And we observe that as the misalignment error increases, the AD method further increases the expandable communication distance. Our work can further enhance the robustness and promote the practical application of the asymmetric MP-QKD.

Keywords: quantum key distribution, asymmetric mode-pairing, advantage distillation

PACS: 03.67.Dd, 03.67.Hk, 03.67.–a

DOI: 10.1088/1674-1056/adbb5c **CSTR:** 32038.14.CPB.adbb5c

1. Introduction

Quantum key distribution (QKD),[1,2] based on the law of quantum mechanics, can provide the secret key of unconditionally theoretical security for two legitimate parties. Since the first QKD protocol was proposed in 1984,[1] great progress has been made both in theory[3–12] and experiment[13–24] in the past few decades.

Nevertheless, the imperfection of device will lead to the security vulnerabilities,[25] which can be utilized by eavesdroppers to steal key information. The loopholes in the detection side were once considered to be the most difficult problem in the practical QKD system. Fortunately, Lo *et al.* have proposed measurement-device-independent QKD (MDI-QKD) in 2012.[26] And the MDI-QKD protocol can address the loopholes in the detection side once and for all. The significant progresses[27–32] have been made in several aspects of the MDI-QKD. Besides the security, the key-rate performance is the critical issue in the actual implementation of QKD. Due to the inevitable and ubiquitous transmission loss occurring within the channel, the Pirandola–Laurenza–Ottaviani–Banchi bound (PLOB bound)[33] restricts the secret key rate.

The researchers have proposed the twin-field QKD (TF-QKD)[34] and its various variants[35–38] to improve the secret key rate performance and exceed the PLOB bound. However, TF-QKD and its variants need global phase locking to complete stable optical interference between coherent states, which is an extremely difficult problem in practical applications. So, the complexity of system implementation is greatly increased. Afterwards, mode-pairing QKD (MP-QKD) proposed in 2022,[39] also called asynchronous MDI-QKD,[40] not only broke the PLOB bound, but also was immune to the need for global phase locking. Moreover, MP-QKD gets the same exceptional protocol performance of TF-OKD and also the same practicability as MDI-QKD. Subsequently, researchers have demonstrated the feasibility of utilizing asynchronous MDI-QKD or MP-QKD to build quantum communication networks theoretically[41–43] and experimentally.[44,45]

In most QKD systems, only symmetric scenarios are considered for simplicity where the distance between the channels of the two communication parties is equal. In reality, due to the constraints of geographical environment and the alteration in the location of the two communicating sides, the distances between the intermediate party and the two communication parties are unequal, resulting in different channel transmittances. To address this problem, Zhu *et al.*[46] proposed the asymmetric MP-QKD protocol. However, due to its asymmetric characteristics, its performance is not as good as that of the original symmetric scheme. So, it would be of significant value to enhance the performance of asymmetric MP-QKD by exploiting advanced technologies. Because of the excellent improvement of the advantage distillation method for asynchronous MDI-QKD[47] and MP-QKD[48] in symmetric channels, we explore the improvement effect of advantage distillation method on asymmetric MP-QKD.

†Corresponding author. E-mail: winmaxsky@163.com

© 2025 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

The advantage distillation (AD) method,[49] originally proposed in the field of classical cryptography, can be expanded to the field of quantum cryptography. The advantage distillation method, as a highly practical scheme, can significantly enhance the performance of QKD protocols.[50–55] When utilizing the AD method, Alice and Bob split their raw key into blocks of size b, and separate highly correlated bits from the weakly correlated information, which increases the correlation between the raw keys and improves the error tolerance. In this paper, we further enhance the performance of recently proposed asymmetric MP-QKD through combining with the AD method. According to the simulation results in the asymptotic case, it can be found that the maximum communication distance can be improved from 474 km to 544 km, from 438 km to 508 km, from 394 km to 462 km, respectively, when the difference between the distances of two communication parties is 50 km, 100 km, 150 km. Obviously, the analysis results demonstrate that the AD method is robust to the increase of asymmetry. Moreover, our simulation results demonstrate that the AD method can significantly extend communication distance and improve the secret key rate, particularly when channel loss and misalignment error are high. Remarkably, the AD method only changes the classical post-processing stage and does not change the hardware of the practical asymmetric MP-QKD system. The AD method can be conveniently employed to the current asymmetric MP-QKD system.

The rest of the article is arranged as follows. In Section 2, we briefly introduce the original asymmetric MP-QKD protocol. Then, we conduct the security analysis of the asymmetric MP-QKD with AD. In Section 3, we present the numerical simulation results and discussion in various scenarios. Finally, the conclusion is made in Section 4.

2. Security analysis

2.1. Asymmetric MP-QKD

Here, we briefly revisit the original asymmetric MP-QKD protocol that was introduced in Ref. [46]. The diagrammatic sketch of the asymmetric MP-QKD is depicted in Fig. 1 and its detailed procedure is outlined as follows.

Step 1. State preparation Alice prepares a weak coherent pulse $|\sqrt{\mu_{\rm a}^i}\,{\rm e}^{{\rm i}\phi_{\rm a}^i}\rangle$, with the intensity $\mu_{\rm a}^i$ chosen from $\{0,\mu_{\rm a}\}$ and the phase $\phi_{\rm a}^i$ uniformly selected from $[0,2\pi)$. Similarly, Bob prepares a weak coherent pulse $|\sqrt{\mu_{\rm b}^i}\,{\rm e}^{{\rm i}\phi_{\rm b}^i}\rangle$, with the intensity $\mu_{\rm b}^i$ chosen from $\{0,\mu_{\rm b}\}$ and the phase $\phi_{\rm b}^i$ uniformly selected from $[0,2\pi)$.

Step 2. Measurement The weak coherent light pulses are transmitted to Charlie by Alice and Bob. Then, Charlie conducts interference measurements on the received pulses and openly declares the results of measurements from detectors L and R. The terms $L_{\rm a}$ and $L_{\rm b}$ are defined as the communication distances from Alice to Charlie and from Bob to Charlie. For simplicity and without loss of generality, we assume $L_{\rm a} < L_{\rm b}$.

Step 3. Mode pairing Alice and Bob perform Step 1 and Step 2 a total of N rounds. For each successfully detected round, there is only one detector response in the two detectors. Then, two clicked rounds are grouped as a pair by Alice and Bob. Then, Alice and Bob calculate the interval between the first and second successfully detected rounds. When the interval is less than or equal to ξ, they retain a successfully detected pair and calculate the interval between the third and the fourth successfully detected rounds. Otherwise, the first successfully detected round is discarded, then they calculate the interval between the second and the third successfully detected rounds. Until the last successfully detected round, they complete the mode pairing. The pairing strategy is depicted in Fig. 2.

Step 4. Basis sifting For two grouped rounds labeled with indices i and j, Alice records them as the Z pair when the intensities meet $\mu_{\rm a}^i+\mu_{\rm a}^j=\mu_{\rm a}$, as the X pair when their intensities satisfy $\mu_{\rm a}^i=\mu_{\rm a}^j=\mu_{\rm a}$, or as "0" pair when their intensities satisfy $\mu_{\rm a}^i=\mu_{\rm a}^j=0$. Similarly, Bob records them as the Z pair when the intensities meet $\mu_{\rm b}^i+\mu_{\rm b}^j=\mu_{\rm b}$, as the X pair when their intensities satisfy $\mu_{\rm b}^i=\mu_{\rm b}^j=\mu_{\rm b}$, or as "0" pair when their intensities satisfy $\mu_{\rm b}^i=\mu_{\rm b}^j=0$. Subsequently, the bases corresponding to each pair of data are declared by Alice and Bob. If the declared bases are uniformly either X or Z and share the same time bins, they will be retained; whereas otherwise, they will be discarded.

Step 5. Key mapping For each Z pair at locations i and j, Alice sets the raw key as $\kappa_{\rm a}=0$ when $(\mu_{\rm a}^i,\mu_{\rm a}^j)=(0,\mu_{\rm a})$ and $\kappa_{\rm a}=1$ if $(\mu_{\rm a}^i,\mu_{\rm a}^j)=(\mu_{\rm a},0)$. For every X pair at positions i and j, the raw key is acquired from the relative phase $(\phi_{\rm a}^j-\phi_{\rm a}^i)=\theta_{\rm a}+\pi\kappa_{\rm a}$, where the key is $\kappa_{\rm a}=\lfloor[\phi_{\rm a}^j-\phi_{\rm a}^i/\pi] \bmod 2\rfloor$ and the alignment angle is $\theta_{\rm a}=(\phi_{\rm a}^j-\phi_{\rm a}^i) \bmod 2$. Bob obtains the raw key bit $\kappa_{\rm b}$ and calculates $\theta_{\rm b}$ in a similar way. For the X pairs, if the click of the detector is the same, Bob keeps the key $\kappa_{\rm b}$;

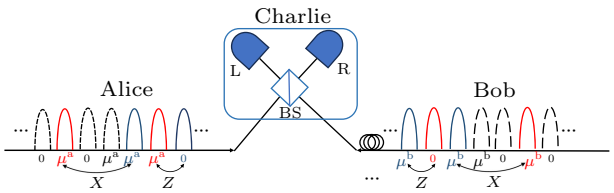


Fig. 1. Schematic diagram of the asymmetric MP-QKD scheme. Alice (Bob) prepares weakly coherent pulses with random intensity $\mu_i^{\rm a}\in\{0,\mu^{\rm a}\}$ ($\mu_i^{\rm b}\in\{0,\mu^{\rm b}\}$) and random phase $\phi_i^{\rm a}$ ($\phi_i^{\rm b}$) $\in[0,2\pi)$, which are then sent to Charlie. Upon performing an interference measurement and announcing the detection results, Alice and Bob pair the successfully detected pulses and ascertain their corresponding encoding bases. They utilize the Z-pairs for key generation and employ other data for parameter estimation. The term $L_{\rm a}$ and $L_{\rm b}$ are defined as the communication distances from Alice to Charlie and from Bob to Charlie. For simplicity and without loss of generality, we assume $L_{\rm a}<L_{\rm b}$. The successfully detected and undetected pulses are represented by solid lines and dashed lines, respectively. Red and blue pulses represent the front and rear pulses in the successful pair, and black pulses denote the pulses of failed pairing.

Pairing strategy

Input: Charlie's announced detection results D_i for $i=1$ to N; maximal pairing interval ξ.

Output: Kpairs; front- and rear-pulse locations (l_k,r_k) for the k-th pair, where $k=1$ to K.

Initialize the pairing index $k=1$; initialize the flag $f=0$.
for $i=1$ **to** N **do** ⟹ Traversing all locations
  if $f=0$ **then** ⟹ Searching for the front-pulse location
    if $D_i=0$ **then** ⟹ Successful detection
      Set the temporary front−pulse location to $l_k=i$, set the flag to $f=1$.
    end if
  else ⟹ Searching the rear-pulse location
    if $D_i=1$ **then** ⟹ Successful detection
      Set the rear-pulse location to $r_k=i$; update the pairing index to $k=k+1$; reset the flag to $f=0$.
    else if $l_k-i\geq\xi$ **then** ⟹ Pairing interval exceeding ξ
      Reset the flag to $f=0$.
    end if
  end if
end if
Set the total number of pairs to $K=k+1$.

Fig. 2. Detailed description of pairing strategy.

otherwise, if the click of the detector is different, Bob flips $\kappa_{\rm b}$. The alignment angles $\theta_{\rm a}$ and $\theta_{\rm b}$ in the X pairs are declared by Alice and Bob. If $\theta_{\rm a}=\theta_{\rm b}$, they retain the data pairs; otherwise, they discard the data pairs.

Step 6. Parameter estimation Alice and Bob utilize the Z pairs for key generation. Then, they use the data of Z pairs and X pairs to calculate the single-photon pair ratio $\bar{q}_{(1,1)}$ in all Z pairs, the single-photon pair phase error rate $e^{XX}_{(1,1)}$ and the quantum bit error rate $E^{ZZ}_{(\mu_{\rm a},\mu_{\rm b})}$ of the Z pairs.

Step 7. Postprocessing Alice and Bob carry out error correction and privacy amplification procedures on the raw key data, yielding the final secret key.

After completing the aforementioned steps, the formula for the secret key rate in asymmetric MP-QKD can be reformulated as follows:[46]

$$R=r_{\rm p}(p,\xi)r_{\rm s}\{\bar{q}_{11}[1-H(e^{XX}_{(1,1)})]-fH(E^{ZZ}_{(\mu_{\rm a},\mu_{\rm b})})\},\quad(1)$$

where $E^{ZZ}_{(\mu_{\rm a},\mu_{\rm b})}$ is the bit error rate, $r_{\rm p}(p,\xi)$ is the pairing rate contributed by each round. The term $r_{\rm s}$ indicates the probability that a generated pair is a Z pair. The single-photon phase error rate is denoted by $e^{XX}_{(1,1)}$, and $\bar{q}_{11}$ refers to the single-photon pair ratio within all Z pairs. The efficiency of error correction process is represented by f. The maximum pairing interval is denoted as ξ, and the probability that the emitted pulse results in a successful detection click is p. The binary Shannon entropy function is given by $h(x)=-x\log_2(x)-(1-x)\log_2(1-x)$.

2.2. Asymmetric MP-QKD with AD

The AD method has demonstrated its superiority in some QKD protocols.[50–55] In this section, we extend the AD method to asymmetric MP-QKD and conduct a thorough security analysis. Based on the information theory, we analyze the security of the asymmetric MP-QKD with the AD method. Initially, Alice and Bob prepare the quantum state $|1,0\rangle^{i,j}$ and $|1,0\rangle^{j,i}$ as the Z basis and $|+\rangle=(|1,0\rangle^{i,j}+|0,1\rangle^{i,j})/\sqrt{2}$ and $|-\rangle=(|1,0\rangle^{i,j}-|0,1\rangle^{i,j})/\sqrt{2}$ as the X basis. These states are transmitted to Charlie via the quantum channel. The notation $|1,0\rangle^{i,j}=|1\rangle^{i}|0\rangle^{j}$ indicates the presence of a single photon in time-bin i and the absence of a photon in time-bin j. Before the measurement is performed, the whole quantum system can be given by the following quantum state:

$$|\Psi\rangle_{\rm ABE}=\sum_{j=1}^{4}\sqrt{\lambda_j}|\Phi_j\rangle_{\rm AB}\otimes|e_j\rangle_{\rm E},\quad(2)$$

where

$$\begin{aligned}
|\Phi_1\rangle&=\frac{1}{\sqrt{2}}(|1,0\rangle^{i,j}_{\rm A}|1,0\rangle^{i,j}_{\rm B}+|0,1\rangle^{i,j}_{\rm A}|0,1\rangle^{i,j}_{\rm B}),\\
|\Phi_2\rangle&=\frac{1}{\sqrt{2}}(|1,0\rangle^{i,j}_{\rm A}|1,0\rangle^{i,j}_{\rm B}-|0,1\rangle^{i,j}_{\rm A}|0,1\rangle^{i,j}_{\rm B}),\\
|\Phi_3\rangle&=\frac{1}{\sqrt{2}}(|1,0\rangle^{i,j}_{\rm A}|0,1\rangle^{i,j}_{\rm B}+|0,1\rangle^{i,j}_{\rm A}|1,0\rangle^{i,j}_{\rm B}),\\
|\Phi_4\rangle&=\frac{1}{\sqrt{2}}(|1,0\rangle^{i,j}_{\rm A}|0,1\rangle^{i,j}_{\rm B}-|0,1\rangle^{i,j}_{\rm A}|1,0\rangle^{i,j}_{\rm B}),
\end{aligned}\quad(3)$$

and $\lambda_1+\lambda_2+\lambda_3+\lambda_4=1$. The single-photon error rates in the Z basis and X basis are respectively bounded by $\lambda_3+\lambda_4=e^{Z}_{11}$ and $\lambda_2+\lambda_4=e^{X}_{11}$. Here, subscripts A and B represent modes "Alice" and "Bob", respectively; and $|e_j\rangle_{\rm E}$ denotes the orthonormal basis of Hilbert space $\mathscr{H}_{\rm E}$. If the measurement outcomes of Alice and Bob are $xy\in\{00,11,01,10\}$, the quantum

states that Eve can get are as follows:

$$
\begin{aligned}
|\varphi_{0,0}\rangle &= \frac{1}{\sqrt{2}}(\sqrt{\lambda_1}|e_1\rangle + \sqrt{\lambda_2}|e_2\rangle),\\
|\varphi_{1,1}\rangle &= \frac{1}{\sqrt{2}}(\sqrt{\lambda_1}|e_1\rangle - \sqrt{\lambda_2}|e_2\rangle),\\
|\varphi_{0,1}\rangle &= \frac{1}{\sqrt{2}}(\sqrt{\lambda_3}|e_3\rangle + \sqrt{\lambda_4}|e_4\rangle),\\
|\varphi_{1,0}\rangle &= \frac{1}{\sqrt{2}}(\sqrt{\lambda_3}|e_3\rangle - \sqrt{\lambda_4}|e_4\rangle).
\end{aligned} \tag{4}
$$

After Eve's disruption of the quantum channel, Alice and Bob conduct orthonormal measurements on $\mathscr{H}_{\mathrm{A}}$ and $\mathscr{H}_{\mathrm{B}}$, resulting in the density operator σ_{XYE} for the entire system

$$
\sigma_{XYE} = \sum_{x,y} |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes |\varphi_{x,y}\rangle\langle\varphi_{x,y}|. \tag{5}
$$

Note that Eve may control the quantum channel, she can select the optimal parameters $\{\lambda_1,\lambda_2,\lambda_3,\lambda_4\}$ to reduce the secret key rate as long as λ_j $(j=1,2,3,4)$ is bounded by the quantum bit error rate (QBER) in different bases. Based on the preceding analysis, we can get

$$
\begin{aligned}
H(\sigma_{XE}) &= 1 + h(\lambda_1+\lambda_2),\\
H(\sigma_E) &= h(\lambda_1+\lambda_2) + (\lambda_1+\lambda_2)h\left(\frac{\lambda_1}{\lambda_1+\lambda_2}\right)\\
&\quad + (\lambda_3+\lambda_4)h\left(\frac{\lambda_3}{\lambda_3+\lambda_4}\right),\\
H(X|Y) &= h(\lambda_1+\lambda_2).
\end{aligned} \tag{6}
$$

Therefore, the secret key rate formula can be written as

$$
\begin{aligned}
R &\geq \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} S(X|E) - H(X|Y)\\
&= \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} H(\sigma_{XE}) - H(\sigma_E) - H(X|Y)\\
&= \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} 1 - (\lambda_1+\lambda_2)h\left(\frac{\lambda_1}{\lambda_1+\lambda_2}\right)\\
&\quad -(\lambda_1+\lambda_2)h\left(\frac{\lambda_1}{\lambda_1+\lambda_2}\right) - h(\lambda_1+\lambda_2),
\end{aligned} \tag{7}
$$

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

Notably, after conducting the error correction, all errors are rectified by Alice and Bob, we have

$$
H(X|Y) \leq f h(E^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})}), \tag{8}
$$

where $h(E^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})})$ is the maximum information leakage during the error correction process. Based on the information theory, the secret key rate formula of the asymmetric MP-QKD protocol can be rewritten as

$$
\begin{aligned}
R \geq \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} & r_{\mathrm{p}}(p,\xi)\, r_{\mathrm{s}} \Bigg\{ \bar{q}_{11} \Bigg[1 - (\lambda_1+\lambda_2)\, h\left(\frac{\lambda_1}{\lambda_1+\lambda_2}\right)\\
& - (\lambda_1+\lambda_2)\, h\left(\frac{\lambda_1}{\lambda_1+\lambda_2}\right) \Bigg] - f h\left(E^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})}\right) \Bigg\},
\end{aligned} \tag{9}
$$

where the bit error rate of the Z pairs is $E^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})}$, $r_{\mathrm{p}}(p,\xi)$ is the expected pair rate contributed by each round, the term r_{s} signifies the probability that a generated pair is a Z pair, the error correction efficiency is f. And the variable $\bar{q}_{11}$ refers to the expected single-photon pair ratio in all Z pairs.

In the AD step, Alice and Bob split their raw key into blocks consisting of b bits, denoted as $\{x_1,x_2,\ldots,x_b\}$ and $\{y_1,y_2,\ldots,y_b\}$. Alice randomly chooses a bit $c\in\{0,1\}$ and transmits the sequence of messages $m=\{m_1,m_2,\ldots,m_b\} = \{x_1\oplus c, x_2\oplus c,\ldots,x_b\oplus c\}$ to Bob via the authenticated classical channel. The block is accepted by Alice and Bob if Bob declares that the computation of $\{m_1\oplus y_1, m_2\oplus y_2,\ldots,m_b\oplus y_b\}$ is either $\{0,0,\ldots,0\}$ or $\{1,1,\ldots,1\}$. Subsequently, they retain the first bits x_1 and y_1 as the raw key. Consequently, the corresponding successful probability of the AD process on a block of size b can be expressed as

$$
q_{\mathrm{succ}} = \left(E^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})}\right)^b + \left(1 - E^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})}\right)^b. \tag{10}
$$

When executing the AD step, the QBER $E^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})}$ in the Z basis can be substituted by $E'^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})} = (E^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})})^b/q_{\mathrm{succ}}$, and the quantum state of the whole system composed of Alice, Bob, and Eve can be given by

$$
|\Psi'\rangle_{\mathrm{ABE}} = \sum_{j=1}^{4} \sqrt{\lambda'_j}\,|\Phi_j\rangle_{\mathrm{AB}} \otimes |e_j\rangle_{\mathrm{E}}, \tag{11}
$$

where

$$
\begin{aligned}
\lambda'_1 &= \frac{(\lambda_1+\lambda_2)^b + (\lambda_1-\lambda_2)^b}{2p_{\mathrm{succ}}},\\
\lambda'_2 &= \frac{(\lambda_1+\lambda_2)^b - (\lambda_1-\lambda_2)^b}{2p_{\mathrm{succ}}},\\
\lambda'_3 &= \frac{(\lambda_3+\lambda_4)^b + (\lambda_3-\lambda_4)^b}{2p_{\mathrm{succ}}},\\
\lambda'_1 &= \frac{(\lambda_3+\lambda_4)^b - (\lambda_3-\lambda_4)^b}{2p_{\mathrm{succ}}},
\end{aligned} \tag{12}
$$

and $p_{\mathrm{succ}} = (\lambda_1+\lambda_2)^b + (\lambda_3+\lambda_4)^b$. Therefore, the secret key rate formula of the asymmetric MP-QKD protocol with the AD method can be rewritten as follows:

$$
\begin{aligned}
R \geq \max_b \min_{\lambda_1,\lambda_2,\lambda_3,\lambda_4} & \frac{1}{b} q_{\mathrm{succ}} r_{\mathrm{p}}(p,\xi)\, r_{\mathrm{s}} \Bigg\{ (\bar{q}_{11})^b\\
& \times \Bigg[1 - \left(\lambda'_1+\lambda'_2\right) h\left(\frac{\lambda'_1}{\lambda'_1+\lambda'_2}\right)\\
& - \left(\lambda'_3+\lambda'_4\right) h\left(\frac{\lambda'_3}{\lambda'_3+\lambda'_4}\right) \Bigg] - f h\left(E'^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})}\right) \Bigg\}.
\end{aligned} \tag{13}
$$

Then, we compute the necessary parameters in order to estimate the secret key rate. The parameters are subject to

$$
e^{XX}_{(1,1)} = \lambda_2+\lambda_4, \quad e^{ZZ}_{(1,1)} = \lambda_3+\lambda_4, \tag{14}
$$

$$q_{\rm succ} = \left(E^{ZZ}_{(\mu_{\rm a},\mu_{\rm b})}\right)^b + \left(1-E^{ZZ}_{(\mu_{\rm a},\mu_{\rm b})}\right)^b, \tag{15}$$

$$E'^{ZZ}_{(\mu_{\rm a},\mu_{\rm b})} = \frac{\left(E^{ZZ}_{(\mu_{\rm a},\mu_{\rm b})}\right)^b}{\left(E^{ZZ}_{(\mu_{\rm a},\mu_{\rm b})}\right)^b + \left(1-E^{ZZ}_{(\mu_{\rm a},\mu_{\rm b})}\right)^b}. \tag{16}$$

3. Numerical simulation

In this section, we numerically simulate the performance of the asymmetric MP-QKD with the AD method in the asymptotic case and analyze the simulation results. Here, we assume the fiber transmittance to be given by $\eta = 10^{-\alpha L/10}$, where α represents the fiber loss coefficient, $\eta_{\rm d}$ denotes the efficiency of the single-photon detector, $p_{\rm d}$ stands for the dark count rate, and f signifies the error correction efficiency. The maximum pairing interval is set to ξ. The misalignment error is defined as $e_{\rm d}$. $L_{\rm a}$ and $L_{\rm b}$ denote the communication distances from Alice to Charlie and from Bob to Charlie. The term $\Delta_L := L_{\rm b} - L_{\rm a}$ is defined as the difference in the communication distances from Alice and Bob to Charlie. The experimental parameters[46] fixed in the following numerical simulations are detailed in Table 1.

Table 1. Simulation parameters.

Variable	Parameter	Simulation value
α	fiber loss coefficient	0.2
$\eta_{\rm d}$	single-photon detector efficiency	20%
$e_{\rm d}$	misalignment error	4%
f	error correction Efficiency	1.15
$p_{\rm d}$	dark count rate	1.2×10^{-8}
ξ	maximal interval	1×10^{6}

For the sake of simplicity, we only consider the asymptotic scenario in the simulation. The detailed calculation for the parameters is described as follows:[27,46]

$$r_{\rm p}(p,\xi) = \left[\frac{1}{p[1-(1-p)^{\xi}]} + \frac{1}{p}\right]^{-1},$$

$$p \approx \frac{\eta_{\rm a}u_{\rm a} + \eta_{\rm b}u_{\rm b}}{2},$$

$$r_{\rm s} = \frac{1}{8}\frac{1}{p^2}\Big\{\left[1-(1-2p_{\rm d})\,{\rm e}^{-\eta_{\rm a}u_{\rm a}}\right]\left[1-(1-2p_{\rm d})\,{\rm e}^{-\eta_{\rm b}u_{\rm b}}\right] + 2p_{\rm d}\left[1-(1-2p_{\rm d})\,{\rm e}^{-\eta_{\rm a}u_{\rm a}-\eta_{\rm b}u_{\rm b}}\right]\Big\},$$

$$\bar{q}_{11} = \frac{1}{8}\frac{{\rm e}^{-\mu_{\rm a}}\mu_{\rm a}{\rm e}^{-\mu_{\rm b}}\mu_{\rm b}}{r_{\rm s}p^2}\Big\{\left[1-(1-2p_{\rm d})\,(1-\eta_{\rm a})\right] \times\left[1-(1-2p_{\rm d})\,(1-\eta_{\rm b})\right] + 2p_{\rm d}[1-(1-2p_{\rm d})(1-\eta_{\rm a})(1-\eta_{\rm b})]\Big\},$$

$$E^{ZZ}_{(\mu_{\rm a},\mu_{\rm b})} = \frac{1}{4}\frac{1}{r_{\rm s}p^2}p_{\rm d}[1-(1-2p_{\rm d})\,{\rm e}^{-\eta_{\rm a}u_{\rm a}-\eta_{\rm b}u_{\rm b}}],$$

$$Y_{(1,1)} = (1-p_{\rm d})^2\left[\frac{\eta_{\rm a}\eta_{\rm b}}{2} + (2\eta_{\rm a}+2\eta_{\rm b}-3\eta_{\rm a}\eta_{\rm b})\,p_{\rm d} + 4\,(1-\eta_{\rm a})\,(1-\eta_{\rm b})\,p_{\rm d}^2\right],$$

$$e_{(1,1)} = \frac{e_0 Y_{(1,1)} - (e_0-e_{\rm d})(1-p_{\rm d})^2\frac{\eta_{\rm a}\eta_{\rm b}}{2}}{Y_{(1,1)}}, \tag{17}$$

where $\eta_{\rm a}$ and $\eta_{\rm b}$ are the channel transmittances. The misalignment error $e_{\rm d}$ is the inevitable intrinsic factor in the actual QKD system. The misalignment error $e_{\rm d}$ has an effect on the interference, which may lead to phase drift. However, the Z basis does not interfere, so the calculation of QBER $E^{ZZ}_{(\mu_{\rm a},\mu_{\rm b})}$ does not consider $e_{\rm d}$. The effect of $e_{\rm d}$ is considered in the single-photon phase error rate $e_{(1,1)}$. Subsequently, we conduct simulations to assess the performance of asymmetric MP-QKD with AD in the asymptotic scenario, utilizing Eqs. (10)–(17) under various conditions.

Initially, we analyze the performance of the asymmetric MP-QKD protocol both with and without the AD method under asymptotic condition. The comparative results for $\Delta_L = 0$, 50 km, 100 km, 150 km are presented in Fig. 3. Figure 3 illustrates that the performance of the asymmetric MP-QKD with AD is consistent with that without AD in a short distance. However, with the increase in communication distance, the secret key rate of the original asymmetric MP-QKD experiences a swift decline. When $\Delta_L = 100$ km, the AD method has an obvious advantage at the communication distance of about 433 km, and the maximum communication distance reaches 508 km, resulting in a maximum distance increase of 70 km. As illustrated in simulation results, we can find that the maximum communication distance is improved from 488 km to 554 km, from 474 km to 544 km and from 394 km to 462 km, when $\Delta_L = 0$ km, 50 km, 150 km.

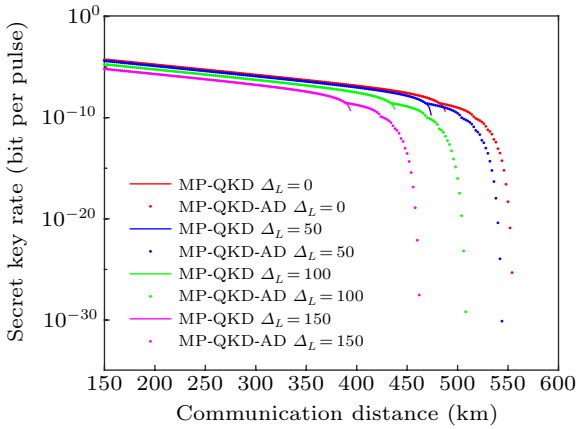


Fig. 3. The comparison of asymmetric MP-QKD performance with and without AD and the relationship between the secret key rate and the communication distance ($L_{\rm a}+L_{\rm b}$) assuming $\lambda = 10^6$ and $e_{\rm d} = 4\%$. The red, blue, green and magenta lines correspond to the secret key rates of the asymmetric MP-QKD protocol for $\Delta_L = 0$, $\Delta_L = 50$ km, $\Delta_L = 100$ km and $\Delta_L = 150$ km, respectively. The dash lines and solid lines respectively indicate the secret key rate of asymmetric MP-QKD with and without AD.

To delve deeper into the reasons for the AD method enhancing the secret key rate in the long-distance case, we present Fig. 4 with respect to b. We observe that, at a distance of $\Delta_L = 100$ km, the value of b changes from 1 to 2 at about

433 km, illustrating that the AD method begins to work at this moment. As the communication distance increases, more noise is introduced and the correlation of the raw key becomes worse, we need the AD method to obtain a larger b value to improve the correlation. Moreover, the results are similar when $\Delta_L = 0$ km, $\Delta_L = 100$ km or $\Delta_L = 150$ km. Therefore, the use of the AD method can significantly enhance the performance of asymmetric MP-QKD over a long distance.

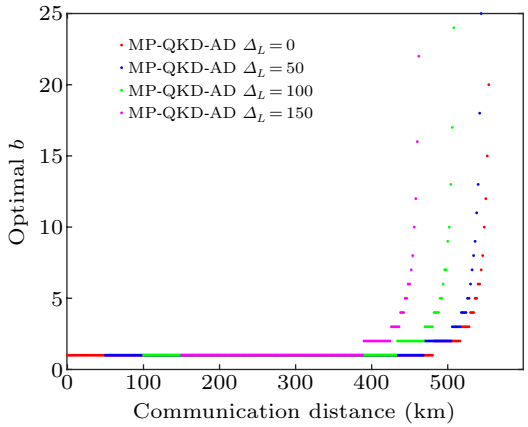


Fig. 4. Results of the optimal b versus the communication distance between Alice and Bob in asymmetric MP-QKD with AD. The red, blue, green and magenta scattered points represent the values $\Delta_L = 0$ km, $\Delta_L = 50$ km, $\Delta_L = 100$ km and $\Delta_L = 150$ km, respectively.

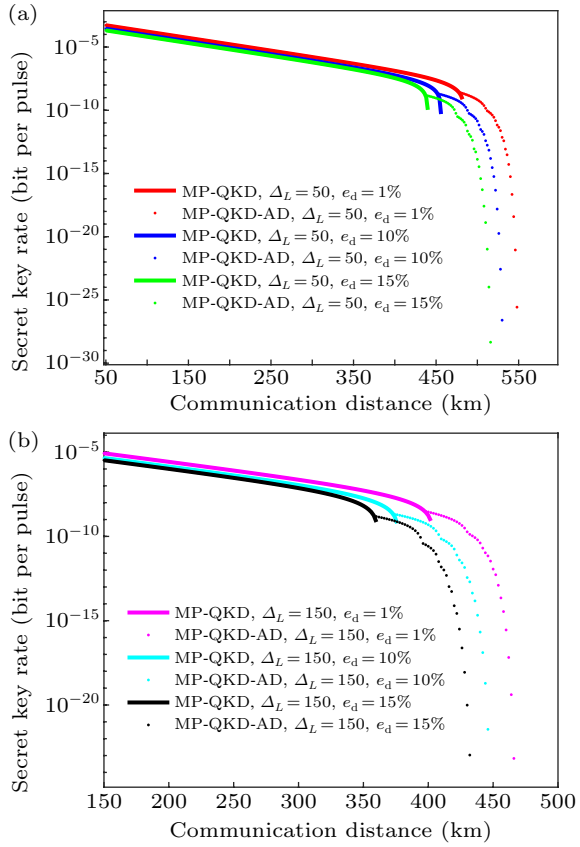


Fig. 5. The performance of the asymmetric MP-QKD with AD under various e_d. The solid and dotted lines in different colors indicate the performances of the asymmetric MP-QKD with AD and without AD for different e_d, respectively. Relationship between the secret key rate and the communication distance $(L_a + L_b)$ when (a) $\Delta_L = 50$ km and (b) $\Delta_L = 150$ km.

Finally, we analyze the influence of the misalignment error e_d on the performance of the asymmetric MP-QKD with the AD method when $\Delta_L = 50$ km and 150 km. The simulation results are depicted in Fig. 5. As shown in Fig. 5(a), we set the difference between communication distances $\Delta_L = 50$ km and the misalignment error $e_d = 1\%$, 10%, 15%. We observe that the maximal communication distance increases by 66 km, 76 km and 78 km, respectively, when $e_d = 1\%$, 10%, 15%. As illustrated in Fig. 5(b), we set the difference between two communication distances $\Delta_L = 150$ km. The maximal communication distance increases by 66 km, 74 km and 76 km when $e_d = 1\%$, 10%, 15%, respectively. The simulation results imply that the distance extension of the scheme with the AD method gradually increases as the misalignment error rises. Furthermore, with the increase of the difference between the two communication distances, the extension of distance is almost not reduced, which shows the robustness of the AD method.

4. Conclusion

In summary, we extend the AD method to the asymmetric MP-QKD scheme and investigate the effect of the AD method on the performance of the asymmetric MP-QKD. The simulation results demonstrate that the AD method can substantially extend the communication distance and enhance the secret key rate for real-life MP-QKD particularly when the channel losses and misalignment errors are high. Additionally, we find that the AD method can still promote the performance evidently when accounting for misalignment error and difference between the communication distances. Thus, our analysis results clearly reveal that the AD method is not only practical but also robust to variations in asymmetric communication distances. In particular, the AD method is free of the hardware modifications of MP-QKD, it may be easily adopted in current systems. We anticipate that our research can promote the applications of actual asymmetric MP-QKD systems.

Acknowledgments

Project supported by the National Natural Science Foundation of China (Grant Nos. 61505261, 62101597, 61605248, and 61675235), the National Key Research and Development Program of China (Grant No. 2020YFA0309702), the China Postdoctoral Science Foundation (Grant No. 2021M691536), the Natural Science Foundation of Henan Province (Grant Nos. 202300410534 and 202300410532), and the Anhui Initiative in Quantum Information Technologies.

References

[1] Bennett C H and Brassard G 1984 *Quantum cryptography: Public key distribution and coin tossing* (New York: IEEE) p. 175
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[3] Lo H K and Chau H F 1999 *Science* **283** 2050
[4] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[5] Kraus B, Gisin N and Renner R 2005 *Phys. Rev. Lett.* **95** 080501
[6] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[7] Wang X B 2003 *Phys. Rev. Lett.* **94** 230503
[8] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[9] Braunstein S L and Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[10] Zhang C X, Wu D, Cui P W, *et al.* 2023 *Chin. Phys. B* **32** 124207
[11] Ma H Q, Han Y X, Dou T Q and Li P Y 2023 *Chin. Phys. B* **32** 020304
[12] Luo H, Wang Y J, Ye W, *et al.* 2022 *Chin. Phys. B* **31** 020306
[13] Peng C Z, Zhang J, Yang D, *et al.* 2007 *Phys. Rev. Lett.* **98** 010505
[14] Wang S, Chen W, Guo J F, *et al.* 2012 *Opt. Lett.* **37** 1008
[15] Liu Y, Chen T Y, Wang L J, *et al.* 2013 *Phys. Rev. Lett.* **111** 130502
[16] Tang Y L, Yin H L, Chen S J, *et al.* 2014 *Phys. Rev. Lett.* **113** 190501
[17] Wang S, Yin Z Q, Chen W, *et al.* 2015 *Nat. Photon.* **9** 832
[18] Takesue Hi, Sasaki T, Tamaki K and Koashi M 2015 *Nat. Photon.* **9** 827
[19] Wang C, Song X T, Yin Z Q, *et al.* 2015 *Phys. Rev. Lett.* **115** 160502
[20] Yin H L, Chen T Y, Yu Z W, *et al.* 2016 *Phys. Rev. Lett.* **117** 190501
[21] Tang Y L, Yin H L, Zhao Q, *et al.* 2016 *Phys. Rev. X* **6** 011024
[22] Wang C, Yin Z Q, Wang S, *et al.* 2017 *Optica* **4** 1016
[23] Liao S K, Cai W Q, Liu W Y, *et al.* 2017 *Nature* **549** 43
[24] Grünenfelder F, Boaron A, Resta G V, *et al.* 2023 *Nat. Photon.* **17** 422
[25] Xu F H, Ma X F, Zhang Q, *et al.* 2020 *Rev. Mod. Phys.* **92** 025002
[26] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[27] Ma X F and Razavi M 2012 *Phys. Rev. A* **86** 062319
[28] Yu Z W, Zhou Y H and Wang X B 2013 *Phys. Rev. A* **88** 062339
[29] Curty M, Xu F H, Cui W, *et al.* 2014 *Nat. Commun.* **5** 3732
[30] Yin Z Q, Fung C H F, Ma X F, *et al.* 2014 *Phys. Rev. A* **90** 052319
[31] Yin Z Q, Wang S, Chen W, *et al.* 2014 *Quantum Inf. Process.* **13** 1237
[32] Yu Z W, Zhou Y H and Wang X B 2015 *Phys. Rev. A* **91** 032318
[33] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 1
[34] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[35] Ma X F, Zeng P and Zhou H Y 2018 *Phys. Rev. X* **8** 031043
[36] Lin J and Lütkenhaus N 2018 *Phys. Rev. A* **98** 042332
[37] Wang X B, Yu Z W and Hu X L 2018 *Phys. Rev. A* **98** 062323
[38] Cui C H, Yin Z Q, Wang R, *et al.* 2019 *Phys. Rev. Appl.* **11** 034053
[39] Zeng P, Zhou H Y, Wu W J and Ma X F 2022 *Nat. Commun.* **13** 3903
[40] Xie Y M, Lu Y S, Weng C X, *et al.* 2022 *PRX Quantum* **3** 020315
[41] Xie Y M, Bai J L, Lu Y S, *et al.* 2023 *Phys. Rev. Appl.* **19** 054070
[42] Bai J L, Xie Y M, Fu Y, *et al.* 2023 *Opt. Lett.* **48** 3551
[43] Zhou L, Lin J P, Xie Y M, *et al.* 2023 *Phys. Rev. Lett.* **130** 250801
[44] Zhu H T, Huang Y Z, Liu H, *et al.* 2023 *Phys. Rev. Lett.* **130** 030801
[45] Ge C F, Zhou L, Lin J P, *et al.* 2024 *Quantum Sci. Technol.* **10** 015046
[46] Lu Z Y, Wang G, Li C and Cao Z 2024 *Phys. Rev. A* **109** 012401
[47] Luo D, Liu X, Qin K B, *et al.* 2024 *Phys. Rev. A* **110** 022605
[48] Liu X, Luo D, Zhang Z R and Wei K J 2023 *Phys. Rev. A* **107** 062613
[49] Maurer U M 1993 *IEEE Trans. Inf. Theory* **39** 733
[50] Tan E Y Z, Lim C C W and Renner R 2020 *Phys. Rev. Lett.* **124** 020502
[51] Li H W, Zhang C M, Jiang M S and Cai Q Y 2022 *Commun. Phys.* **5** 53
[52] Wang R Q, Zhang C M, Yin Z Q, *et al.* 2022 *New J. Phys.* **24** 073049
[53] Li H W, Wang R Q, Zhang C M and Cai Q Y 2023 *Quantum* **7** 1201
[54] Zhu J R, Zhang C M, Wang R and Li H W 2023 *Opt. Lett.* **48** 542
[55] Jiang X L, Wang Y, Li J J, *et al.* 2023 *Opt. Express* **31** 9196