

Mode-pairing quantum key distribution with multi-step advantage distillation

Shizhuo Li(李世卓), Xin Liu(刘馨), Zhenrong Zhang(张振荣), and Kejin Wei(韦克金)
Citatio: Chin. Phys. B, 2025, 34 (**9**): 090307. DOI: 10.1088/1674-1056/adf4a9
http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Mode-pairing quantum key distribution based on heralded pair-coherent source with passive decoy-states

Zhigang Shen(沈志冈), Yuting Lu(鲁雨婷), Yang Yu(余杨), and Shengmei Zhao(赵生妹)
Chin. Phys. B, 2025, 34 (**9**): 090304. DOI: 10.1088/1674-1056/adcf89

Improving the performance of reference-frame-independent measurement-device-independent quantum key distribution in hybrid channels

Yan-Mei Zhao(赵燕美), Chun Zhou(周淳), Xiao-Lei Jiang(姜晓磊), Yi-Fei Lu(陆宜飞), Yu Zhou(周雨), Hai-Tao Wang(汪海涛), Yang Wang(汪洋), Jia-Ji Li(李家骥), Yan-Yang Zhou(周砚扬), Hong-Wei Li(李宏伟), and Wan-Su Bao(鲍皖苏)
Chin. Phys. B, 2025, 34 (**5**): 050302. DOI: 10.1088/1674-1056/adbee4

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)
Chin. Phys. B, 2025, 34 (**4**): 040305. DOI: 10.1088/1674-1056/adbb5c

General multi-attack detection for continuous-variable quantum key distribution with local local oscillator

Zhuo Kang(康茁), Wei-Qi Liu(刘维琪), Jin Qi(齐锦), and Chen He(贺晨)
Chin. Phys. B, 2024, 33 (**5**): 050308. DOI: 10.1088/1674-1056/ad2bf2

Performance analysis of quantum key distribution using polarized coherent-states in free-space channel

Zengte Zheng(郑增特), Ziyang Chen(陈子扬), Luyu Huang(黄露雨),Xiangyu Wang(王翔宇), and Song Yu(喻松)
Chin. Phys. B, 2023, 32 (**3**): 030306. DOI: 10.1088/1674-1056/ac7450

SPECIAL TOPIC — Quantum communication and quantum network

Mode-pairing quantum key distribution with multi-step advantage distillation

Shizhuo Li(李世卓)[1], Xin Liu(刘馨)[1], Zhenrong Zhang(张振荣)[2], and Kejin Wei(韦克金)[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 June 2025; revised manuscript received 17 July 2025; accepted manuscript online 28 July 2025)

The advantage distillation (AD) technology has been proven to effectively improve the secret key rate and the communication distance of quantum key distribution (QKD). The mode-pairing quantum key distribution (MP-QKD) protocol can overcome a fundamental physical limit, known as the Pirandola–Laurenza–Ottaviani–Banchi bound, without requiring global phase-locking. In this work, we propose a method based on multi-step AD to further enhance the performance of MP-QKD. The simulation results show that, compared to one-step AD, multi-step AD achieves better performance in long-distance scenarios and can tolerate a higher quantum bit error rate. Specifically, when the difference between the communication distances from Alice and Bob to Charlie is 25 km, 50 km and 75 km, and the corresponding transmission distance exceeds 523 km, 512 km and 496 km, respectively, the secret key rate achieved by multi-step AD surpasses that of one-step AD. Our findings indicate that the proposed method can effectively promote the application of MP-QKD in scenarios with high loss and high error rate.

Keywords: mode-pairing quantum key distribution, multi-step advantage distillation, secret key rate

PACS: 03.67.Dd, 03.67.Hk, 03.67.–a

DOI: 10.1088/1674-1056/adf4a9 **CSTR:** 32038.14.CPB.adf4a9

1. Introduction

Quantum computing poses a significant threat to the security of traditional public key encryption based on computational complexity.[1] Quantum key distribution (QKD), grounded in the principles of quantum mechanics, enables two communicating parties to share random keys with information-theoretic security, which has attracted great attention in research.[2] Since the first QKD protocol was proposed,[3] substantial advancements have been achieved for higher secret key rates,[4–8] longer distances,[9–12] miniature setups,[13–15] and more scalable network deployment.[16–19]

Following the remarkable progress in QKD, the proposal of measurement-device-independent (MDI) QKD[20] represents a significant advancement, as it eliminates all security vulnerabilities associated with the detection side. However, the performance of most QKD protocols remains constrained by the fundamental limit known as the Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound,[21] which states that the maximum secret key rates achievable over a quantum channel cannot surpass the fundamental rate–distance limit of $O(\eta)$, where η denotes the transmittance of the quantum channel.

Twin-field (TF) QKD[22] is based on first-order optical interference and achieves a rate–distance scaling of $O(\sqrt{\eta})$, surpassing the PLOB bound and enabling a considerable key rate over long distances. Subsequently, numerous variants of the TF-QKD protocol have been proposed[23–29] and experimentally demonstrated.[9,11,30–34] However, TF-QKD requires precise frequency-locking and phase-locking techniques to achieve stable interference between two coherent states.[9,11,35–37] These requirements significantly increase system complexity and implementation difficulty, thereby limiting its practicality in real-world applications.

To address the global phase-locking challenge, two recent works, namely, mode-pairing (MP) QKD[38] and asynchronous MDI (AMDI),[39] were proposed almost simultaneously. These two protocols utilize the inherent stability during the pairing time, thereby overcoming the PLOB bound without requiring global phase stabilization. At present, these MDI-type QKD protocols have achieved a communication distance of up to 508 km,[10] with experimental demonstrations[40] and field tests.[41,42] Moreover, numerous efforts have been made to enhance their practical implementation,[42–49] and the strategy of asynchronous pairing has also been applied to other fields.[50,51]

Improving transmission distance and secret key rates has garnered significant attention in the field of QKD.[5,6,11,52–54] 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 is to divide the raw keys into several blocks and extract the highly correlated keys from the weakly correlated keys, thereby en-

†Corresponding author. E-mail: kjwei@gxu.edu.cn

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

hancing the correlation between the raw keys. The AD method has been applied to various QKD protocols[59–65] to extend transmission distances and improve tolerance to background noise. Recently, Hao *et al*. proposed a multi-step advantage distillation (MSAD) method to further improve the performance of the QKD protocol.[66] However, the impact of the MSAD method on the performance of the MP-QKD protocol remains to be thoroughly investigated.

This study improves the MP-QKD protocol by incorporating a MSAD method, extending the one-step advantage distillation (OSAD) approach. This scheme modifies the post-processing steps without changing the hardware of the actual MP-QKD system. In practical applications, MSAD can be integrated into the classical post-processing steps of MP-QKD by modifying the processing logic of the FPGA. The OSAD method divides the raw key into blocks to distinguish strongly correlated keys from weakly correlated ones. The MSAD method further refines this process by subdividing the blocks into smaller partitions. The simulation results show that MSAD can enhance the long-distance performance of the MP-QKD protocol. In particular, considering both symmetric and asymmetric channel scenarios, MSAD can contribute to improving the secret key rate and increasing the maximum tolerated quantum bit error rate (QBER) of the system.

The structure of this paper is as follows: Section 2 provides an overview of the MP-QKD protocol with OSAD method. Section 3 introduces MP-QKD protocol with the MSAD method. In Section 3, numerical simulation results are presented. Finally, we offer conclusions in Section 4.

2. MP-QKD with one-step advantage distillation

Here, we first review the MP-QKD protocol with the OSAD method.[44] A schematic of this scheme is presented in Fig. 1 and its specific steps are as follows.

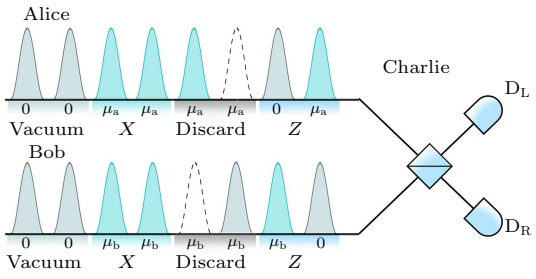


Fig. 1. Schematic of the MP-QKD protocol. Alice and Bob send coherent pulses to an untrusted relay, Charlie. Z-basis key generation is based on time-bin pairs where one pulse is vacuum (0) and the other has a nonzero intensity. The X-basis uses intensity pairs of (μ_a, μ_b), while (0,0) denotes a vacuum state. If data is missing for either party in a time bin, the corresponding data is discarded and the search continues to the next. D_L/D_R represent the detectors.

Step 1. State preparation Alice (Bob) generates n weak coherent pulses $|e^{i\theta_A^i}\sqrt{\lambda_A^i}\rangle(|e^{i\theta_B^i}\sqrt{\lambda_B^i}\rangle)$, where each pulse has intensity $\lambda_A^i \in \{\mu_a, 0\}$ ($\lambda_B^i \in \{\mu_b, 0\}$) and phase θ_A^i (θ_B^i) $\in [0, 2\pi)$. The index i denotes the time bin, with $i \in \{1, 2, \ldots, N\}$.

Step 2. Measurement and announcement Alice and Bob send weak coherent pulses to an untrusted intermediary, Charlie. At each time bin i, Charlie interferes the incoming signals and records whether detector D_L and/or D_R respond. Charlie then broadcasts the detection status and the corresponding detection result.

Step 3. Mode pairing Steps 1 and 2 are repeated N times by Alice and Bob. For each valid detection, only rounds with a single click from either detector D_L or D_R are kept. These rounds are paired to determine the basis. The corresponding phase and intensity values from both rounds form a data pair. The resulting bases are compared and retained if they meet the sifting rules; otherwise, the pair is discarded.

Step 4. Basis sifting For each pair of time bins i and j, data are kept as a Z-basis event if one intensity is nonzero and the other is zero. If the intensities are (μ_a, μ_b), the data are considered for the X-basis; otherwise, such as $(0,0)$, they are discarded. Alice and Bob then disclose their basis choices and the total intensity for the pair. If the announced bases match and the data are not flagged for discarding, the pair is preserved.

Step 5. Key mapping For each Z-basis pair at time bins i and j, Alice assigns $\kappa_A = 0$ if the intensity pair is $(\mu_a, 0)$, and $\kappa_A = 1$ for $(0, \mu_b)$. For each X-basis, the key bit is derived from the relative phase difference $(\theta_A^i - \theta_A^j)$, expressed as $\phi_A + \pi\kappa_A$, where $\kappa_A = \{[(\theta_A^j - \theta_A^i)/\pi] \bmod 2\}$ and $\phi_A = (\theta_A^j - \theta_A^i) \bmod \pi$. Bob follows the same method to compute κ_B and ϕ_B. Both parties then announce ϕ_A and ϕ_B. If $\phi_A = \phi_B$, the pairing is kept; otherwise, it is discarded.

Step 6. Parameter estimation Alice and Bob use the retained Z-basis to extract the raw key. The bit error rate $E^{ZZ}_{(\mu_a,\mu_b)}$ is estimated from the Z-basis where the intensities are (μ_a, μ_b). By analyzing different intensity combinations, they estimate the gain of single-photon events $\bar{q}_{11}$ from the Z-basis data, and obtain the single-photon phase error rate $e^{XX}_{(1,1)}$ using the X-basis.

Step 7. Postprocessing This step involves several subtasks carried out in order:

- Alice and Bob determine the optimal block size b via numerical optimization.
- They divide their respective raw key sequences into blocks of size b, where the optimal block size b can be selected to improve the secret key rate, and denote the resulting sequences as $X = \{x_1, x_2, \ldots, x_b\}$ and $Y = \{y_1, y_2, \ldots, y_b\}$.
- For each block X, Alice selects a random bit $c \in \{0, 1\}$, computes $C = \{x_1 \oplus c, x_2 \oplus c, \ldots, x_b \oplus c\}$, and sends C to Bob.
- Upon receiving C, Bob calculates $C' = C \oplus Y$. If $C' = \{0, \ldots, 0\}$ or $\{1, \ldots, 1\}$, he replies with "Accept"; otherwise, with "Reject".
- If accepted, Alice and Bob retain x_1 and y_1 as key bits; if rejected, they discard the block.
- Finally, error correction and privacy amplification are performed to generate the final secret keys.

After the above steps, through information security theoretical analysis, the secret key rate is given by

$$\begin{aligned}\tilde{R} \geqslant & \max_{b} \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{1}{b} p_{\text{succ}} r_p(p,\Delta) r_s \\ & \times \left\{ (\overline{q}_{11})^b \left[1 - \left(\tilde{\lambda}_0 + \tilde{\lambda}_1\right) h\left(\frac{\tilde{\lambda}_0}{\tilde{\lambda}_0 + \tilde{\lambda}_1}\right) \right.\right. \\ & \left.\left. - \left(\tilde{\lambda}_2 + \tilde{\lambda}_3\right) h\left(\frac{\tilde{\lambda}_2}{\tilde{\lambda}_2 + \tilde{\lambda}_3}\right) \right] - f h\left(\tilde{E}^{ZZ}_{(\mu_a,\mu_b)}\right) \right\}, \quad (1)\end{aligned}$$

subject to

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

where $\sum_{n=0}^{3}\lambda_n = 1$, and each λ_n $(n = 0,1,2,3)$ denotes the weight of a Bell-state component that characterizes the quantum channel. The single-photon error rates in the X and Z bases are constrained by $\lambda_1 + \lambda_3 = e^{XX}_{(1,1)}$ and $\lambda_2 + \lambda_3 = e^{ZZ}_{(1,1)}$, respectively. The parameter p_{succ} represents the success probability of OSAD on a block of size b, and $E^{ZZ}_{(\mu_a,\mu_b)}$ denotes the effective error rate after the OSAD step. The observed QBER in the Z-basis is denoted by $E^{ZZ}_{(\mu_a,\mu_b)}$, while $r_p(p,\Delta)$ denotes the mode-pairing success rate as a function of the detection probability p and maximum pairing interval Δ. The parameter r_s is the probability that a detected event corresponds to a valid Z-basis pair, and $\overline{q}_{11}$ represents the estimated fraction of single-photon contributions among Z-basis detections. The details of the derivation of relevant parameters are presented in Appendix A, and the derivations for the original MP-QKD and the MP-QKD with OSAD are provided in Appendices B and C, respectively.

3. MP-QKD with multi-step advantage distillation

The following provides a detailed description of the specific steps involved in the MP-QKD with the MSAD method. The MSAD method modifies only the post-processing stage. Therefore, steps 1–6 of the proposed scheme remain the same as those in the MP-QKD with the OSAD method, and only step 7 is modified. The process of MP-QKD with the MSAD method is shown in Fig. 2, and the specific details are as follows.

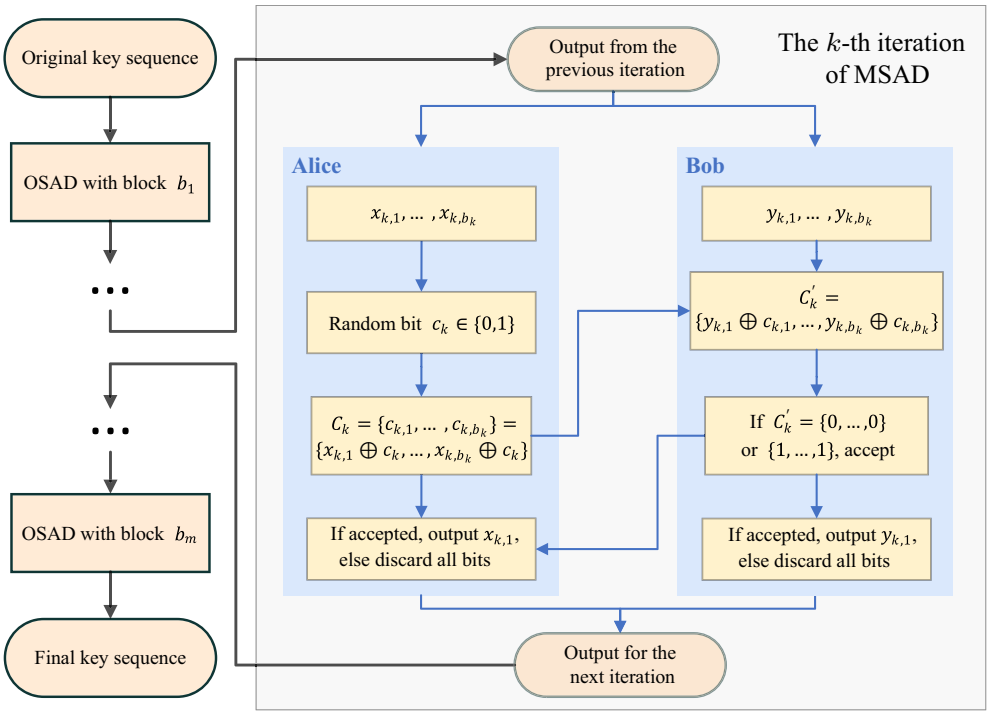


Fig. 2. Multi-step advantage distillation post-processing flowchart.

New step 7. In the MSAD protocol, Alice and Bob first obtain raw key sequences after the sifting step. They then perform multiple OSAD iterations, where each iteration takes as input the output of the previous one. Assume that MSAD consists of m such iterations, with a total block size $b = \prod_{i=1}^{m} b_i$, where each OSAD uses a configurable block size $b_1, b_2, \ldots, b_m$. The k-th iteration of the MSAD protocol is described in detail as follows.

• Alice and Bob determine the optimal block size b_k via numerical methods.

• Alice and Bob divide their input sequences into blocks of size b_k, denoted as $X_k = \{x_{k,1}, x_{k,2}, \ldots, x_{k,b_k}\}$ and $Y_k = \{y_{k,1}, y_{k,2}, \ldots, y_{k,b_k}\}$.

• For each block X_k, Alice randomly selects a bit $c_k \in \{0,1\}$, computes $C_k = \{x_{k,1} \oplus c_k, x_{k,2} \oplus c_k, \ldots, x_{k,b_k} \oplus c_k\}$, and sends it to Bob.

• Upon receiving C_k, Bob computes $C'_k = C_k \oplus Y_k$. He replies with "Accept" if $C'_k = \{0,0,\ldots,0\}$ or $\{1,1,\ldots,1\}$; otherwise, he responds with "Reject".

• Depending on the "Accept" or "Reject" result, Alice and Bob keep $x_{k,1}$ and $y_{k,1}$ as key bits or discard the full block of size b_k.

• After completing the k-th iteration, Alice and Bob obtain sequences X_{k+1} and Y_{k+1}, which are either used as input for the following iteration or sent for error correction as part of the final key.

After new step 7, highly correlated bits can be separated from weakly correlated information and the secret key rate of the MP-QKD with MSAD can be modified as follows:

$$
\begin{aligned}
R \geq & \max_{b_1,b_2,\ldots,b_m} \min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3} \frac{1}{b_1 b_2 \cdots b_m} p_1 p_2 \cdots p_m r_p(p,\Delta) r_s \\
& \times \left\{ (\overline{q}_{11})^b \left[1 - \left(\tilde{\lambda}_0 + \tilde{\lambda}_1\right) h\left(\frac{\tilde{\lambda}_0}{\tilde{\lambda}_0 + \tilde{\lambda}_1}\right) \right.\right. \\
& \left.\left. - \left(\tilde{\lambda}_2 + \tilde{\lambda}_3\right) h\left(\frac{\tilde{\lambda}_2}{\tilde{\lambda}_2 + \tilde{\lambda}_3}\right) \right] - f h\left(\tilde{E}^{ZZ}_{(\mu_a,\mu_b)}\right) \right\} \qquad (3)
\end{aligned}
$$

subject to

$$
\begin{aligned}
p_k &= \left(1 - E^{ZZ}_{(\mu_a,\mu_b,k-1)}\right)^{b_k} + \left(E^{ZZ}_{(\mu_a,\mu_b,k-1)}\right)^{b_k}, \\
\tilde{E}^{ZZ}_{(\mu_a,\mu_b,k)} &= \frac{\left(E^{ZZ}_{(\mu,\mu,k-1)}\right)^{b_k}}{\left(1 - E^{ZZ}_{(\mu_a,\mu_b,k-1)}\right)^{b_k} + \left(E^{ZZ}_{(\mu_a,\mu_b,k-1)}\right)^{b_k}}, \qquad (4)
\end{aligned}
$$

and

$$
\begin{aligned}
\tilde{\lambda}_{m,0} = \tilde{\lambda}_0 &= \frac{(\lambda_0+\lambda_1)^b + (\lambda_0-\lambda_1)^b}{2p_{\text{succ}}}, \\
\tilde{\lambda}_{m,1} = \tilde{\lambda}_1 &= \frac{(\lambda_0+\lambda_1)^b - (\lambda_0-\lambda_1)^b}{2p_{\text{succ}}}, \\
\tilde{\lambda}_{m,2} = \tilde{\lambda}_2 &= \frac{(\lambda_2+\lambda_3)^b + (\lambda_2-\lambda_3)^b}{2p_{\text{succ}}}, \\
\tilde{\lambda}_{m,3} = \tilde{\lambda}_3 &= \frac{(\lambda_2+\lambda_3)^b - (\lambda_2-\lambda_3)^b}{2p_{\text{succ}}}, \qquad (5)
\end{aligned}
$$

where p_k represents the probability of a successful advantage distillation on a block of size b_k, $\tilde{E}^{ZZ}_{(\mu_a,\mu_b,k)}$ represents the error rate after the k-th iteration after the AD postprocessing step. The complete derivation can be found in Appendix D.

4. Simulation

In this section, to investigate the performance of the MP-QKD with the MSAD method, we use the parameters in Table 1 for numerical simulation, which are sourced from Ref. [38].

Table 1. List of parameters used for numerical simulations. η_d denotes the detection efficiency, α denotes the loss coefficient of the fiber, p_d denotes the detector dark count rate, f denotes the error correction, and e_d denotes the misalignment error.

η_d	α	p_d	f	e_d
20%	0.20 dB/km	1.2×10^{-8}	1.15	4%

4.1. Symmetric scenarios

Most of the experimental demonstrations are performed in the laboratory over symmetric fiber spools.[10,11,40] For this type of symmetric channel scenario, we analyze the impact of MSAD on the performance of MP-QKD ($\Delta L = L_a - L_b = 0$). In this case, the intensities sent by Alice and Bob are equal, i.e., $\mu_a = \mu_b = \mu$.

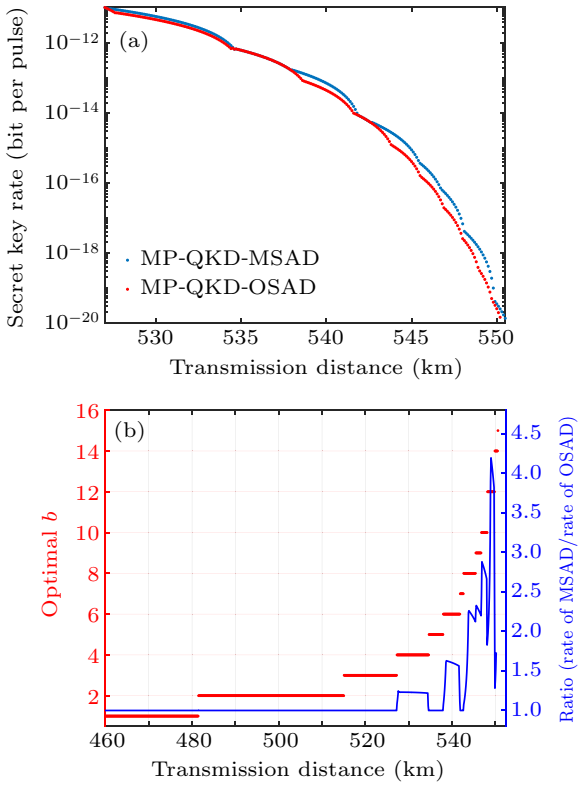


Fig. 3. Performance comparison between the proposed scheme (MP-QKD-MSAD) and MP-QKD protocol using OSAD (MP-QKD-OSAD) assuming $\Delta = 10^6$. (a) Relationship between the secret key rate and the total transmission distance. (b) Relationship between optimal block size b and transmission distance, as well as the relationship between the ratio of the secret key rate achieved by the proposed scheme to that of the MP-QKD protocol using OSAD and the total transmission distance.

As shown in Fig. 3, when the transmission distance exceeds 527 km, the secret key rate obtained using MSAD becomes greater than or equal to that achieved with OSAD. Within the distance range of 534 km to 543 km, the secret

key rates of MSAD and OSAD are equal at some distances. The reason is that the optimal block size b is a prime number, and MSAD can only perform a single round of grouping, that is, the key is divided into b blocks in the first round, which is equivalent to using the blocking strategy of OSAD. When the transmission distance is greater than 543 km, MSAD is effectively executed, and the secret key rate of MSAD is greater than that of OSAD.

At approximately 550 km, a significant decline is observed in the key rate ratio between the proposed scheme and the MP-QKD protocol using OSAD in Fig. 3(b). This is because MSAD cannot perform multi-step processing based on the prime number 13, but it can implement multi-step processing using the adjacent composite number 12. However, this processing reduces the performance advantage of MSAD, further leading to the observed decline in key rate ratio.

As shown in Table 2, when the key rate is on the order of 10^{-13} and the communication distance is 539 km, the secret key rate using the MSAD method is 1.6 times higher than that using the OSAD method. When the communication distance is 549 km, the secret key rate of the MSAD method is about 4 times higher than that of the OSAD method.

Table 2. Comparison of secret key rates for MP-QKD with MSAD and OSAD at the transmission distances of 539 km and 549 km. The ratio shows the improvement factor of MSAD over OSAD.

Transmission distance	Protocol	Optimal block size	QBER	Secret key rate	Ratio
539	OSAD	6	0.1225	8.22×10^{-14}	1.629
	MSAD	2×3	0.1244	1.34×10^{-13}	
549	OSAD	12	0.1352	3.03×10^{-19}	4.196
	MSAD	$2\times2\times3$	0.1364	1.27×10^{-18}	

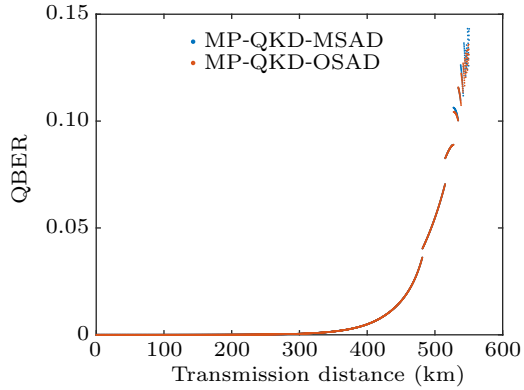


Fig. 4. Comparison of the maximum tolerated QBER of the proposed scheme and MP-QKD protocol using OSAD assuming $\Delta = 10^6$.

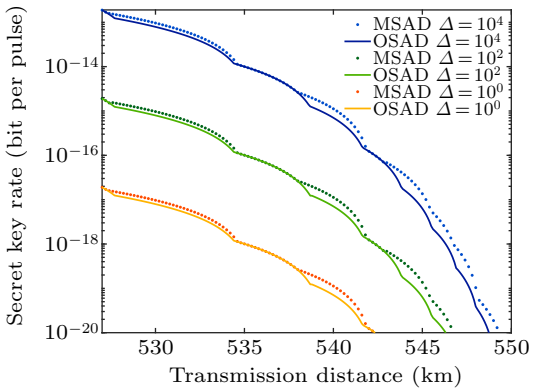


Fig. 5. The performance of the proposed scheme corresponding to different maximum pairing intervals Δ.

Furthermore, we compare the maximum tolerated QBER of the MP-QKD protocol using MSAD and OSAD in Fig. 4. The simulation results show that the maximum tolerated QBER of the proposed scheme has increased to 0.1432, while the maximum tolerated QBER of the MP-QKD protocol using OSAD is only 0.1358. We also analyze the performance of the proposed scheme under different maximum pairing intervals Δ. Figure 5 indicates that across different maximum pairing intervals, MSAD can increase the secret key rate of MP-QKD at long distances.

4.2. Symmetric scenarios

In practical applications, variations in geographical location and environmental conditions often lead to unequal channel attenuation between the two communicating parties and intermediate nodes.[41,67] Therefore, it is essential to consider asymmetric channels in the scheme design. Next, we will further analyze the influence of MSAD on MP-QKD performance in the asymmetric case ($L_a \neq L_b$). In this case, the intensities sent by Alice and Bob are not equal, i.e., $\mu_a \neq \mu_b$.

In Fig. 6, we analyze the performance of the MP-QKD protocol using MSAD under varying degrees of asymmetry in the communication distances from Alice and Bob to Charlie (ΔL). As a concrete example, we consider three sets of channels at $\Delta L = 25$ km, 50 km, and 75 km, and the corresponding transmission distances exceed 523 km, 512 km, and 496 km, respectively, the secret key rate achieved using MSAD becomes greater than or equal to that obtained with OSAD. The detailed results at 524 km and 534 km for $\Delta L = 50$ km are shown in Table 3. These results demonstrate that using MSAD can improve the secret key rate of the MP-QKD protocol over long transmission distances in asymmetric scenarios. Furthermore, the degree of channel asymmetry does not significantly affect the performance improvement of MSAD.

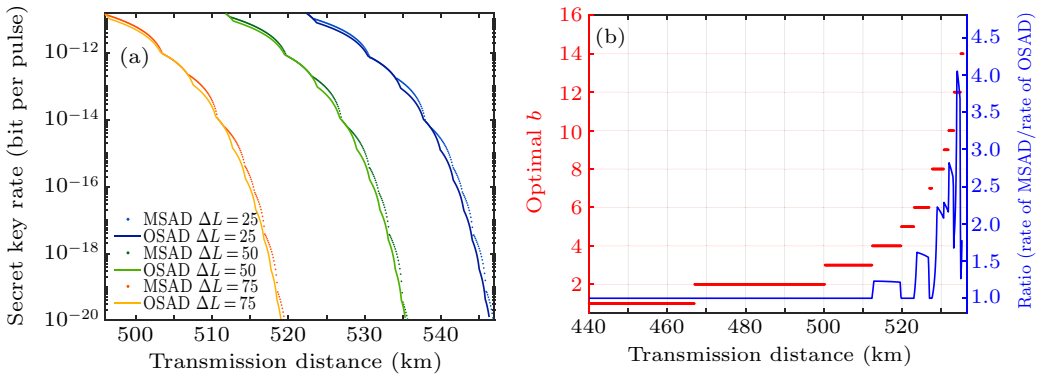


Fig. 6. Performance comparison between asymmetric MP-QKD protocol using OSAD and MSAD assuming $\Delta = 10^6$. (a) Relationship between the secret key rate and the total transmission distance under varying degrees of asymmetry in the communication distances from Alice and Bob to Charlie (ΔL). (b) At $\Delta L = 50$ km, the relationship between optimal block size b and transmission distance, as well as the relationship between the ratio of the secret key rate achieved by the proposed scheme to that of MP-QKD protocol using OSAD and the total transmission distance.

Table 3. Comparison of secret key rates for MP-QKD with MSAD and OSAD at the transmission distances of 524 km and 534 km when $\Delta L = 50$ km. The ratio shows the improvement factor of MSAD over OSAD.

Transmission distance	Protocol	Optimal block size	QBER	Secret key rate	Ratio
524	OSAD	6	0.1205	9.47×10^{-14}	1.616
	MSAD	2×3	0.1224	1.53×10^{-13}	
534	OSAD	12	0.1320	2.84×10^{-19}	4.049
	MSAD	$2\times2\times3$	0.1331	1.15×10^{-18}	

5. Discussion and conclusion

In conclusion, this paper proposes a scheme for improving the performance of MP-QKD by using the MSAD method, and simulates its performance in both symmetric and asymmetric cases. The simulation results show that, compared with the MP-QKD scheme using OSAD, the proposed scheme can achieve a higher secret key rate over long transmission distances and tolerate a QBER of up to 0.1432. This scheme does not require any modifications to the original hardware, requiring only adjustments to the classical post-processing process. Therefore, it can be readily applied to existing MP-QKD systems to enhance long-distance transmission performance.

In future work, we can further investigate the advantageous distillation framework proposed in Ref. [68] and explore methods or block strategies to increase the secret key rate.

Appendix A: Details of the simulation model

According to Refs. [38,44,45], we can derive the model and the final secret key rate of the MP-QKD protocol as follows.

The following calculations are performed under the asymptotic limits and the assumption of perfect decoy-state estimation. Let's assume that the probability of Alice (Bob) randomly selecting intensity $\{0,\mu_{\rm a}\}$ ($\{0,\mu_{\rm b}\}$) is close to 1/2, and the probability of the decoy intensity $\nu_{\rm a}$ ($\nu_{\rm b}$) can be ignored. We represent the coherent pulse sent by Alice (Bob) in the i-th round as $|\sqrt{z_A^i\mu_{\rm a}}\,{\rm e}^{{\rm i}\theta_A^i}\rangle$ ($|\sqrt{z_B^i\mu_{\rm b}}\,{\rm e}^{{\rm i}\theta_B^i}\rangle$), where $z^i_{A(B)}$ denotes the random variable of intensity and $\theta^i_{A(B)}$ denotes the random phase. The intensity setting for i-th round can be denoted as the following vector:

$$z^i := \left[z_A^i, z_B^i\right] = [0,1],[1,0],[0,0],[1,1]. \tag{A1}$$

Alice and Bob transmit weak coherent optical pulses to Charlie over a typical attenuated channel, with the channel is i.i.d. in each round. Then, Alice and Bob pair the successfully clicked pulses and sifting their bases. For the pulse pair indexed by (i,j), we define $\tau^{i,j} = [\tau_A^{i,j}, \tau_B^{i,j}] := [z_A^i \oplus z_A^j, z_B^i \oplus z_B^j]$, where $\oplus$ denotes the bit-wise addition modulo 2. When $\tau^{i,j} = [1,1]$, the (i,j) pair is set to be an effective Z pair.

In the i-th round, the click events of the $\rm D_L$ and $\rm D_R$ detectors can be denoted as $\left(L^i, R^i\right)$. The successful click variable is $C^i := L^i \oplus R^i$, where $C^i = 1$ indicates a successful click. The detection probability can be denoted as

$$\Pr\left(C^i = 1 \mid z^i\right) \approx 1 - (1-2p_{\rm d})\exp\left[-\left(\eta_{\rm a}\mu_{\rm a}z_A^i + \eta_{\rm b}\mu_{\rm b}z_B^i\right)\right], \tag{A2}$$

where $\eta_{\rm a}$ ($\eta_{\rm b}$) represents the channel transmittance from Alice (Bob) to Charlie.

The expected successful click probability of each round is

$$\begin{aligned} p :&= \Pr\left(C^i = 1\right) = \sum_{z^i}\Pr\left(C^i = 1 \mid z^i\right)\Pr\left(z^i\right) \\ &= \frac{1}{4}\sum_{z^i}\Pr(C^i = 1 \mid z^i) \approx \frac{\eta_{\rm a}\mu_{\rm a} + \eta_{\rm b}\mu_{\rm b}}{2}, \end{aligned} \tag{A3}$$

and given a maximum pairing interval Δ, the expected success probability of mode-pairing per round is given by

$$r_p(p,\Delta) = \left[\frac{1}{p[1-(1-p)^{\Delta}} + \frac{1}{p}\right]^{-1}. \tag{A4}$$

The phase-randomized coherent states emitted by the i-th round can be viewed as a linear superposition of photon-number states. When Alice and Bob transmit photon number states $|n_A^i\rangle$ and $|n_B^i\rangle$ respectively, the detection probability is

$$\Pr\left(C^i=1\mid n^i\right)\approx 1-(1-2p_{\rm d})\left(1-\eta_{\rm a}\right)^{n_A^i}\left(1-\eta_{\rm b}\right)^{n_B^i}. \quad \text{(A5)}$$

Without loss of generality, we regard the i-th and j-th rounds as a pair. Since the detection of all rounds are identical and i.i.d, we ignored the subscript. The probability of the intensity setting z caused by a successful click is

$$\begin{aligned}\Pr\left(z\mid C=1\right)&=\frac{\Pr\left(z,C=1\right)}{\Pr\left(C=1\right)}\\&=\frac{\Pr\left(C=1\mid z\right)\Pr\left(z\right)}{\sum_{z'}\Pr\left(C=1\mid z'\right)\Pr\left(z'\right)}\\&=\frac{\Pr\left(C=1\mid z\right)}{\sum_{z'}\Pr\left(C=1\mid z'\right)}.\end{aligned} \quad \text{(A6)}$$

When $\tau_{i,j}=[1,1]$, the successfully clicked pairs are regarded as Z-basis events. Therefore, four possible configurations of z^i and z^j are

$$\left[z^i,z^j\right]\in\{[00,11],[01,10],[10,01],[11,00]\}, \quad \text{(A7)}$$

where $\mathrm{Err}:=\{[00,11],[11,00]\}$ are the two configurations that cause bit errors. To simplify the symbolic expression, we define several events as follows:

$$\begin{aligned}&\Pr(C)=\Pr(\text{Pair Clicked}):=\Pr\left(C^i=C^j=1\right)=p^2,\\&\Pr(E)=\Pr(\text{Pair Effective}):=\Pr\left(z^i\oplus z^j=11\right),\\&\Pr(\mathrm{Err})=\Pr(\text{Pair Erroneous}):=\Pr\left(\left[z^i,z^j\right]\in\mathrm{Err}\right),\\&\Pr(S)=\mathrm{P}(\text{Single-photon Pair}):=\Pr\left(n^i\oplus n^j=11\right).\end{aligned} \quad \text{(A8)}$$

Next, we will consider the calculation of the Z-basis pairs ratio r_s, which can be expressed as follows:

$$\begin{aligned}r_s&=\Pr(E\mid C)=\Pr\left(z^i\oplus z^j=11\mid C^i=1,C^j=1\right)\\&=\sum_{z^i\oplus z^j=11}\Pr\left(z^i\mid C^i=1\right)\Pr\left(z^j\mid C^j=1\right)\\&=\frac{1}{16}\frac{1}{p^2}\sum_{z^i\oplus z^j=11}\Pr\left(C^i=1\mid z^i\right)\Pr\left(C^j=1\mid z^j\right)\\&=\frac{1}{8}\frac{1}{p^2}\left[1-(1-2p_{\rm d})\exp\left(-\eta_{\rm a}\mu_{\rm a}\right)\right]\\&\quad\times\left[1-(1-2p_{\rm d})\exp\left(-\eta_{\rm b}\mu_{\rm b}\right)\right].\end{aligned} \quad \text{(A9)}$$

The expected quantum bit error rate of Z-basis pairs is

$$\begin{aligned}E^{ZZ}_{(\mu_{\rm a},\mu_{\rm b})}&=\Pr(\mathrm{Err}\mid E,C)\\&=\frac{\Pr(\mathrm{Err},E\mid C)}{\Pr(E\mid C)}=\frac{\Pr(\mathrm{Err}\mid C)}{\Pr(E\mid C)}\\&=r_s^{-1}\Pr\left(\left[z^i,z^j\right]\in\mathrm{Err}\mid C^i=C^j=1\right)\\&=r_s^{-1}\sum_{\left[z^i,z^j\right]\in\mathrm{Err}}\Pr\left(z^i\mid C^i=1\right)\Pr\left(z^j\mid C^j=1\right)\\&=\frac{1}{16}\frac{1}{r_sp^2}\sum_{\left[z^i,z^j\right]\in\mathrm{Err}}\Pr\left(C^i=1\mid z^i\right)\Pr\left(C^j=1\mid z^j\right)\\&=\frac{1}{4r_sp^2}p_{\rm d}\left[1-(1-2p_{\rm d})e^{-\eta_{\rm a}\mu_{\rm a}-\eta_{\rm b}\mu_{\rm b}}\right].\end{aligned} \quad \text{(A10)}$$

The expected single-photon pair ratio in the effective Z-basis pairs can be written as follows:

$$\begin{aligned}\bar{q}_{11}&=\Pr(S\mid E,C)=\frac{\Pr(S,E,C)}{\Pr(E,C)}=\frac{1}{r_sp^2}\Pr(S,E,C)\\&=\frac{1}{r_sp^2}\sum_{z^i,z^j}\Pr(S,E,C\mid z^i,z^j)\Pr(z^i,z^j)\\&=\frac{1}{16r_sp^2}\sum_{z^i\oplus z^j=11}\Pr(S,C\mid z^i,z^j)\\&=\frac{1}{16r_sp^2}\sum_{z^i\oplus z^j=11}\Pr(C\mid S,z^i,z^j)\Pr(S\mid z^i,z^j)\\&=\frac{P_{\mu_{\rm a}}(1)P_{\mu_{\rm b}}(1)}{16r_sp^2}\sum_{z^i\oplus z^j=11}\Pr\left(C^i=1\mid n^i=z^i\right)\\&\quad\times\Pr\left(C^j=1\mid n^j=z^j\right)\\&=\frac{P_{\mu_{\rm a}}(1)P_{\mu_{\rm b}}(1)}{8r_sp^2}\left[1-(1-2p_{\rm d})\left(1-\eta_{\rm a}\right)\right]\\&\quad\times\left[1-(1-2p_{\rm d})\left(1-\eta_{\rm b}\right)\right],\end{aligned} \quad \text{(A11)}$$

where $P_\mu(k)=\mathrm{e}^{-\mu}\mu^k/k!$ is the Poisson distribution.

We adopt the deception state estimation method in Ref. [69], and the gain and error rate of X-basis can be expressed as follows:

$$\begin{aligned}Y_{(1,1)}&=(1-p_{\rm d})^2\left[\frac{\eta_{\rm a}\eta_{\rm b}}{2}+(2\eta_{\rm a}+2\eta_{\rm b}-3\eta_{\rm a}\eta_{\rm b})p_{\rm d}\right.\\&\quad\left.+4(1-\eta_{\rm a})(1-\eta_{\rm b})p_{\rm d}^2\right],\\e^{XX}_{(1,1)}&=\frac{\left[e_0Y_{(1,1)}-(e_0-e_{\rm d})(1-p_{\rm d})^2\frac{\eta_{\rm a}\eta_{\rm b}}{2}\right]}{Y_{(1,1)}},\end{aligned} \quad \text{(A12)}$$

where $e_0=1/2$ is the error caused by vacuum pulses.

Appendix B: Security of MP-QKD based on quantum information theory

According to the security proof given in Ref. [38], the final secret key rate of MP-QKD can be estimated as follows:

$$R=r_p(p,\Delta)r_s\left\{\bar{q}_{11}\left[1-h\left(e^{XX}_{(1,1)}\right)\right]-fh\left(E^{ZZ}_{(\mu_{\rm a},\mu_{\rm b})}\right)\right\}. \quad \text{(B1)}$$

In order to further understand the improvement of secret key rate using the MSAD method, we re-analyze Eq. (B1) using quantum information theory[70,71]

$$R=\min_{\sigma_{AB}\in\Gamma}S(X\mid E)-H(X\mid Y), \quad \text{(B2)}$$

where Γ denotes the set of all two-qubit density operators σ_{AB} defined over the Hilbert space $\mathcal{H}_A\otimes\mathcal{H}_B$, with dimensions 2×2. The term $S(X\mid E)$ is the conditional von Neumann entropy that quantifies the uncertainty of the eavesdropper Eve about Alice's measurement result X, while $H(X\mid Y)$ is the

classical Shannon entropy quantifying Bob's uncertainty about X given his own outcome Y.

Before Alice and Bob perform their measurements, the quantum system is represented by the following state:

$$|\Psi\rangle_{ABE} := \sum_{n=0}^{3} \sqrt{\lambda_n} |\Phi_n\rangle_{AB} \otimes |e_n\rangle_E, \tag{B3}$$

where λ_n are non-negative real coefficients satisfying $\sum_{n=0}^{3} \lambda_n = 1$. These coefficients characterize the quantum channel by representing the weight of each Bell component in the shared bipartite state. They are further constrained by the observed single-photon error rates in the X and Z bases: specifically, the phase error rate e_X and the bit error rate e_Z are related to the Bell-diagonal coefficients via $\lambda_1 + \lambda_3 = e_X$ and $\lambda_2 + \lambda_3 = e_Z$, where e_X and e_Z denote the error rate in the X-basis and Z-basis, respectively. Subscripts A and B indicate the modes associated with Alice and Bob, respectively. The set $|e_n\rangle_E$ forms an orthonormal basis spanning a four-dimensional Hilbert space $\mathcal{H}_E$.

The set $|\Phi_n\rangle$ consists of the four Bell states, which in the context of MP-QKD are defined over the temporal mode pair (i, j) as

$$\begin{aligned}
|\Phi_0\rangle &= \frac{1}{\sqrt{2}} \left(|1,0\rangle_A^{i,j} |1,0\rangle_B^{i,j} + |0,1\rangle_A^{i,j} |0,1\rangle_B^{i,j} \right), \\
|\Phi_1\rangle &= \frac{1}{\sqrt{2}} \left(|1,0\rangle_A^{i,j} |1,0\rangle_B^{i,j} - |0,1\rangle_A^{i,j} |0,1\rangle_B^{i,j} \right), \\
|\Phi_2\rangle &= \frac{1}{\sqrt{2}} \left(|1,0\rangle_A^{i,j} |0,1\rangle_B^{i,j} + |0,1\rangle_A^{i,j} |1,0\rangle_B^{i,j} \right), \\
|\Phi_3\rangle &= \frac{1}{\sqrt{2}} \left(|1,0\rangle_A^{i,j} |0,1\rangle_B^{i,j} - |0,1\rangle_A^{i,j} |1,0\rangle_B^{i,j} \right).
\end{aligned} \tag{B4}$$

As the quantum channel is under Eve's control, the states accessible to her depend on the joint measurement outcomes of Alice and Bob. Specifically, when their outcomes are 00, 11, 01, or 10, Eve's corresponding quantum states are given by

$$\begin{aligned}
|\varphi_{0,0}\rangle &= \frac{1}{\sqrt{2}} (\sqrt{\lambda_0} |e_0\rangle + \sqrt{\lambda_1} |e_1\rangle), \\
|\varphi_{1,1}\rangle &= \frac{1}{\sqrt{2}} (\sqrt{\lambda_0} |e_0\rangle - \sqrt{\lambda_1} |e_1\rangle), \\
|\varphi_{0,1}\rangle &= \frac{1}{\sqrt{2}} (\sqrt{\lambda_2} |e_2\rangle + \sqrt{\lambda_3} |e_3\rangle), \\
|\varphi_{1,0}\rangle &= \frac{1}{\sqrt{2}} (\sqrt{\lambda_2} |e_2\rangle - \sqrt{\lambda_3} |e_3\rangle).
\end{aligned} \tag{B5}$$

Thereafter, Alice and Bob can obtain the density operator σ_{XYE} of the entire system

$$\sigma_{XYE} = \sum_{x,y} |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes |\varphi_{x,y}\rangle\langle\varphi_{x,y}|. \tag{B6}$$

The associated entropic quantities are computed as follows:

$$\begin{aligned}
H(\sigma_{XE}) &= 1 + h(\lambda_0 + \lambda_1), \\
H(\sigma_E) &= h(\lambda_0 + \lambda_1) + (\lambda_0 + \lambda_1) h\left(\frac{\lambda_0}{\lambda_0 + \lambda_1} \right) \\
&\quad + (\lambda_2 + \lambda_3) h\left(\frac{\lambda_2}{\lambda_2 + \lambda_3} \right), \\
H(X \mid Y) &= h(\lambda_0 + \lambda_1),
\end{aligned} \tag{B7}$$

where $h(x)$ denotes the binary entropy function, defined as $h(x) = -x \log_2 x - (1-x) \log_2 (1-x)$.

Consequently, the resulting expression for the key rate is given by

$$\begin{aligned}
R &\geqslant \min_{\lambda_0, \lambda_1, \lambda_2, \lambda_3} S(X \mid E) - H(X \mid Y) \\
&= \min_{\lambda_0, \lambda_1, \lambda_2, \lambda_3} H(\sigma_{XE}) - H(\sigma_E) - H(X \mid Y) \\
&= \min_{\lambda_0, \lambda_1, \lambda_2, \lambda_3} 1 - (\lambda_0 + \lambda_1) h\left(\frac{\lambda_0}{\lambda_0 + \lambda_1} \right) \\
&\quad - (\lambda_2 + \lambda_3) h\left(\frac{\lambda_2}{\lambda_2 + \lambda_3} \right) - h(\lambda_0 + \lambda_1).
\end{aligned} \tag{B8}$$

In the ideal case, assuming $e_X = e_Z = Q$, we have

$$\begin{aligned}
&\lambda_0 = 1 - 2Q + \lambda_3, \quad \lambda_1 = Q - \lambda_3, \quad \lambda_2 = Q - \lambda_3, \\
&\sum_{n=0}^{3} \lambda_n = 1.
\end{aligned} \tag{B9}$$

Substituting these relations into the key rate expression, we obtain

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

It can be shown that this function is minimized when $\lambda_3 = Q^2$, which leads to the optimal Bell coefficients

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

In practical MP-QKD systems, phase-randomized weak coherent sources are typically used. Alice and Bob extract the final key from successfully paired Z-basis events and apply the decoy-state method to counter photon-number-splitting attacks. Eve's potential information leakage is bounded by $fh(E^{ZZ}_{(\mu_a, \mu_b)})$, which quantifies the information Eve may gain during error correction. Therefore, the secret key rate is given by

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

where $r_p(p, \Delta)$ is the pairing success probability, r_s is the Z-basis sifting factor, $\bar{q}_{11}$ is the fraction of single-photon contributions, and $E^{ZZ}_{(\mu_a, \mu_b)}$ is the estimated QBER in the Z-basis for signal-state pairs.

Appendix C: Security of MP-QKD with OSAD

In this appendix, we analyze the security of MP-QKD using OSAD in post-processing. Alice and Bob divide their raw key strings into blocks of size b, denoted respectively as $\{x_1,x_2,\ldots,x_b\}$ and $\{y_1,y_2,\ldots,y_b\}$. Alice chooses a random bit $c\in\{0,1\}$ and computes $c_i=x_i\oplus c$ for $i=1,\ldots,b$, then sends the message $C=\{c_1,\ldots,c_b\}$ to Bob via an authenticated classical channel. Bob accepts the block if and only if $\{c_1\oplus y_1,\ldots,c_b\oplus y_b\}\in\{0,1\}$, i.e., all values are the same. Then both parties retain the first bit x_1 and y_1 as part of their distilled raw key. The success probability of this distillation process is given by

$$p_{\mathrm{succ}}=\left(E^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})}\right)^b+\left(1-E^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})}\right)^b, \tag{C1}$$

where $E^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})}$ is the bit error rate of Z-pairs.

Since the security of the key depends on the single-photon components, only blocks where all b pulses are single-photon pairs contribute to the final key. The probability of this event is $(\bar{q}_{11})^b$.

The corresponding overall error rate after OSAD becomes

$$\tilde{E}^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})}=\frac{\left(E^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})}\right)^b}{\left(E^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})}\right)^b+\left(1-E^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})}\right)^b}. \tag{C2}$$

Given these, the final key rate under OSAD is

$$\begin{aligned}\tilde{R}\geqslant&\max_b\min_{\lambda_0,\lambda_1,\lambda_2,\lambda_3}\frac{1}{b}p_{\mathrm{succ}}r_p(p,\delta)r_s\\&\times\left\{(\bar{q}_{11})^b\left[1-\left(\tilde{\lambda}_0+\tilde{\lambda}_1\right)h\left(\frac{\tilde{\lambda}_0}{\tilde{\lambda}_0+\tilde{\lambda}_1}\right)\right.\right.\\&\left.\left.-\left(\tilde{\lambda}_2+\tilde{\lambda}_3\right)h\left(\frac{\tilde{\lambda}_2}{\tilde{\lambda}_2+\tilde{\lambda}_3}\right)\right]-fh\left(\tilde{E}^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}})}\right)\right\},\end{aligned} \tag{C3}$$

subject to the constraints

$$\lambda_1+\lambda_3=e^{XX}_{(1,1)},\quad \lambda_2+\lambda_3=e^{ZZ}_{(1,1)}, \tag{C4}$$

and the updated Bell coefficients after OSAD are

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

Appendix D: Security of MP-QKD with MSAD

In this appendix, we extend the advantage distillation analysis of the MP-QKD protocol to the multi-step scenario, referred to as MSAD. This technique enhances security and robustness by applying the OSAD procedure iteratively. The MSAD protocol increases the success probability of distilled keys while maintaining the Bell-diagonal structure of the underlying quantum state.[66]

Let the number of OSAD iterations be m, where each iteration k ($k=1,2,\ldots,m$) uses a block size b_k. The total block size is therefore defined as $b=\prod_{k=1}^m b_k$. In our simulations, the final number of iterations is determined by comparing the maximum secret key rates achieved at different iteration rounds.

The input to each MSAD iteration is the output of the previous one. At each iteration k, Alice and Bob group their respective key strings into blocks of size b_k, apply the standard OSAD procedure, and generate a shorter, more correlated raw key. This process is repeated for m times.

Let $\tilde{\lambda}_{k,n}$ denote the Bell state weight after the k-th iteration for $n\in\{0,1,2,3\}$, and let p_k denote the success probability of the k-th iteration. The recursion is initialized by setting $\tilde{\lambda}_{0,n}=\lambda_n$ as the original channel parameters estimated from decoy-state analysis.

To describe the evolution of the Bell-diagonal state through multiple iterations of advantage distillation, we define a recursive update rule for the Bell coefficients. In the final iteration, denoted as iteration m, the Bell coefficients $\tilde{\lambda}_{m,n}$ for $n\in\{0,1,2,3\}$ are computed recursively based on the output of the previous iteration $m-1$. The update equations are given by

$$\begin{aligned}\tilde{\lambda}_{k,0}&=\frac{\left(\tilde{\lambda}_{k-1,0}+\tilde{\lambda}_{k-1,1}\right)^{b_k}+\left(\tilde{\lambda}_{k-1,0}-\tilde{\lambda}_{k-1,1}\right)^{b_k}}{2p_k},\\\tilde{\lambda}_{k,1}&=\frac{\left(\tilde{\lambda}_{k-1,0}+\tilde{\lambda}_{k-1,1}\right)^{b_k}-\left(\tilde{\lambda}_{k-1,0}-\tilde{\lambda}_{k-1,1}\right)^{b_k}}{2p_k},\\\tilde{\lambda}_{k,2}&=\frac{\left(\tilde{\lambda}_{k-1,2}+\tilde{\lambda}_{k-1,3}\right)^{b_k}+\left(\tilde{\lambda}_{k-1,2}-\tilde{\lambda}_{k-1,3}\right)^{b_k}}{2p_k},\\\tilde{\lambda}_{k,3}&=\frac{\left(\tilde{\lambda}_{k-1,2}+\tilde{\lambda}_{k-1,3}\right)^{b_k}-\left(\tilde{\lambda}_{k-1,2}-\tilde{\lambda}_{k-1,3}\right)^{b_k}}{2p_k},\end{aligned} \tag{D1}$$

where $p_k=(\tilde{\lambda}_{k-1,0}+\tilde{\lambda}_{k-1,1})^{b_k}+(\tilde{\lambda}_{k-1,2}+\tilde{\lambda}_{k-1,3})^{b_k}$ is the success probability of the final iteration. The recursion begins with $\tilde{\lambda}_{0,n}=\lambda_n$.

As shown in the proof of Proposition 2 in the Ref. [66], take $\tilde{\lambda}_{m,0}$ as an example, we have

$$\begin{aligned}\tilde{\lambda}_{m,0}&=\frac{\left(\tilde{\lambda}_{m-1,0}+\tilde{\lambda}_{m-1,1}\right)^{b_m}+\left(\tilde{\lambda}_{m-1,0}-\tilde{\lambda}_{m-1,1}\right)^{b_m}}{2p_m}\\&=\frac{\left(\tilde{\lambda}_{m-2,0}+\tilde{\lambda}_{m-2,1}\right)^{b_{m-1}b_m}+\left(\tilde{\lambda}_{m-2,0}-\tilde{\lambda}_{m-2,1}\right)^{b_{m-1}b_m}}{2p_m\left(p_{m-1}\right)^{b_m}}\\&=\cdots\end{aligned}$$

$$= \frac{(\lambda_0+\lambda_1)^b + (\lambda_0-\lambda_1)^b}{\delta}, \tag{D2}$$

where δ is given by

$$\begin{aligned}
\delta &= 2p_m\,(p_{m-1})^{b_m}\cdots(p_1)^{b_2\cdots b_m} \\
&= 2\left[\left(\tilde{\lambda}_{m-1,0}+\tilde{\lambda}_{m-1,1}\right)^{b_m} + \left(\tilde{\lambda}_{m-1,2}+\tilde{\lambda}_{m-1,3}\right)^{b_m}\right] \\
&\quad\times(p_{m-1})^{b_m}\cdots(p_1)^{b_m\cdots b_2} \\
&= 2\left[\left(\tilde{\lambda}_{m-2,0}+\tilde{\lambda}_{m-2,1}\right)^{b_m b_{m-1}} + \left(\tilde{\lambda}_{m-2,2}+\tilde{\lambda}_{m-2,3}\right)^{b_m b_{m-1}}\right] \\
&\quad\times(p_{m-2})^{b_m b_{m-1}}\cdots(p_1)^{b_m\cdots b_2} \\
&= \cdots \\
&= 2\left[(\lambda_0+\lambda_1)^b + (\lambda_2+\lambda_3)^b\right] \\
&= 2p_{\mathrm{succ}}.
\end{aligned} \tag{D3}$$

This leads to the following closed-form expressions for the final Bell-state weights after all m iterations of MSAD:

$$\begin{aligned}
\tilde{\lambda}_{m,0} = \tilde{\lambda}_0 &= \frac{(\lambda_0+\lambda_1)^b + (\lambda_0-\lambda_1)^b}{2p_{\mathrm{succ}}}, \\
\tilde{\lambda}_{m,1} = \tilde{\lambda}_1 &= \frac{(\lambda_0+\lambda_1)^b - (\lambda_0-\lambda_1)^b}{2p_{\mathrm{succ}}}, \\
\tilde{\lambda}_{m,2} = \tilde{\lambda}_2 &= \frac{(\lambda_2+\lambda_3)^b + (\lambda_2-\lambda_3)^b}{2p_{\mathrm{succ}}}, \\
\tilde{\lambda}_{m,3} = \tilde{\lambda}_3 &= \frac{(\lambda_2+\lambda_3)^b - (\lambda_2-\lambda_3)^b}{2p_{\mathrm{succ}}}.
\end{aligned} \tag{D4}$$

These expressions indicate that, although the recursive update applies step by step, the final output after m iterations can be directly determined from the original Bell-diagonal state and the total block size. This result ensures that the entropy terms in the final key rate remain unchanged for a given b, while the overall success probability is enhanced via multi-step distillation.

The QBER after k iterations is denoted as

$$\tilde{E}^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}},k)} = \frac{\left(\tilde{E}^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}},k-1)}\right)^{b_k}}{\left(\tilde{E}^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}},k-1)}\right)^{b_k} + \left(1-\tilde{E}^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}},k-1)}\right)^{b_k}}. \tag{D5}$$

Then, the asymptotic secret key rate after MSAD is expressed as

$$\begin{aligned}
R \geqslant \max_{b_1 b_2\cdots b_m}\min_{\lambda_0\lambda_1\lambda_2\lambda_3} &\frac{1}{b_1 b_2\cdots b_m} p_1 p_2\cdots p_m r_p(p,\Delta) r_s \\
&\times\left\{(\overline{q}_{11})^b\left[1-\left(\tilde{\lambda}_0+\tilde{\lambda}_1\right)h\left(\frac{\tilde{\lambda}_0}{\tilde{\lambda}_0+\tilde{\lambda}_1}\right)\right.\right. \\
&\left.\left.-\left(\tilde{\lambda}_2+\tilde{\lambda}_3\right)h\left(\frac{\tilde{\lambda}_2}{\tilde{\lambda}_2+\tilde{\lambda}_3}\right)\right] - f h\left(\tilde{E}^{ZZ}_{(\mu_{\mathrm{a}},\mu_{\mathrm{b}},m)}\right)\right\}.
\end{aligned} \tag{D6}$$

Acknowledgments

This study was supported by the National Natural Science Foundation of China (Grant Nos. 62171144 and 62031024), Guangxi Science Foundation (Grant Nos. 2025GXNSFAA069137 and GXR-1BGQ2424005), and Innovation Project of Guangxi Graduate Education (Grant No. YCBZ2025064).

References

[1] Shor P W 1994 *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science* (IEEE, New York) pp. 124–134
[2] Zhang C X, Wu D, Cui P W, Ma J C, Wang Y and An J M 2023 *Chin. Phys. B* **32** 124207
[3] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York) pp. 175–179
[4] Wei K, Li W, Tan H, Li Y, Min H, Zhang W J, Li H, You L, Wang Z, Jiang X, Chen T Y, Liao S K, Peng C Z, Xu F and Pan J W 2020 *Phys. Rev. X* **10** 031030
[5] Grünenfelder F, Boaron A, Resta G V, Perrenoud M, Rusca D, Barreiro C, Houlmann R, Sax R, Stasi L, El-Khoury S, Hänggi E, Bosshard N, Bussières F and Zbinden H 2023 *Nat. Photon.* **17** 422
[6] Li W, Zhang L, Tan H, Lu Y, Liao S K, Huang J, Li H, Wang Z, Mao H K, Yan B, *et al.* 2023 *Nat. Photon.* **17** 416
[7] Zhang L, Li W, Pan J, Lu Y, Li W, Li Z P, Huang Y, Ma X, Xu F and Pan J W 2025 *Phys. Rev. X* **15** 021037
[8] Shao S F, Zhou L, Lin J, Minder M, Ge C, Xie Y M, Shen A, Yan Z, Yin H L and Yuan Z 2025 *Phys. Rev. X* **15** 021066
[9] Wang S, Yin Z Q, He D Y, Chen W, Wang R Q, Ye P, Zhou Y, Fan-Yuan G J, Wang F X, Chen W, *et al.* 2022 *Nat. Photon.* **16** 154
[10] Zhou L, Lin J, Xie Y M, Lu Y S, Jing Y, Yin H L and Yuan Z 2023 *Phys. Rev. Lett.* **130** 250801
[11] Liu Y, Zhang W J, Jiang C, Chen J P, Zhang C, Pan W X, Ma D, Dong H, Xiong J M, Zhang C J, Li H, Wang R C, Wu J, Chen T Y, You L, Wang X B, Zhang Q and Pan J W 2023 *Phys. Rev. Lett.* **130** 210801
[12] Li Y, Cai W Q, Ren J G, Wang C Z, Yang M, Zhang L, Wu H Y, Chang L, Wu J C, Jin B, *et al.* 2025 *Nature* **640** 47
[13] Beutel F, Brückerhoff-Plückelmann F, Gehring H, Kovalyuk V, Zolotov P, Goltsman G and Pernice W H P 2022 *Optica* **9** 1121
[14] Wei K, Hu X, Du Y, Hua X, Zhao Z, Chen Y, Huang C and Xiao X 2023 *Photon. Res.* **11** 1364
[15] Du Y, Li B H, Hua X, Cao X Y, Zhao Z, Xie F, Zhang Z, Yin H L, Xiao X and Wei K 2025 *Light Sci. Appl.* **14** 108
[16] Liao S K, Cai W Q, Handsteiner J, Liu B, Yin J, Zhang L, Rauch D, Fink M, Ren J G, Liu W Y, Li Y, Shen Q, Cao Y, Li F Z, Wang J F, Huang Y M, Deng L, Xi T, Ma L, Hu T, Li L, Liu N L, Koidl F, Wang P, Chen Y A, Wang X B, Steindorfer M, Kirchner G, Lu C Y, Shu R, Ursin R, Scheidl T, Peng C Z, Wang J Y, Zeilinger A and Pan J W 2018 *Phys. Rev. Lett.* **120** 030501
[17] Avesani M, Foletto G, Padovan M, Calderaro L, Agnesi C, Bazzani E, Berra F, Bertapelle T, Picciariello F, Santagiustina F B L, Scalcon D, Scriminich A, Stanco A, Vedovato F, Vallone G and Villoresi P 2022 *J. Lightwave Technol.* **40** 1658
[18] Fitzke E, Bialowons L, Dolejsky T, Tippmann M, Nikiforov O, Walther T, Wissel F and Gunkel M 2022 *PRX Quantum* **3** 020341
[19] Huang C, Chen Y, Luo T, He W, Liu X, Zhang Z and Wei K 2024 *Sci. China-Phys. Mech. Astron.* **67** 240312
[20] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[21] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 1
[22] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[23] Ma X, Zeng P and Zhou H 2018 *Phys. Rev. X* **8** 031043
[24] Wang X B, Yu Z W and Hu X L 2018 *Phys. Rev. A* **98** 062323
[25] Chistiakov V, Kozubov A, Gaidash A, Gleim A and Miroshnichenko G 2019 *Opt. Express* **27** 36551
[26] Cui C, Yin Z Q, Wang R, Chen W, Wang S, Guo G C and Han Z F 2019 *Phys. Rev. Appl.* **11** 034053
[27] Zhang C M, Xu Y W, Wang R and Wang Q 2020 *Phys. Rev. Appl.* **14** 064070
[28] Zhou L, Lin J, Jing Y and Yuan Z 2023 *Nat. Commun.* **14** 928
[29] Ma H, Han Y, Dou T and Li P 2023 *Chin. Phys. B* **32** 020304

[30] Zhong X, Hu J, Curty M, Qian L and Lo H K 2019 *Phys. Rev. Lett.* **123** 100506
[31] Pittaluga M, Minder M, Lucamarini M, Sanzaro M, Woodward R I, Li M J, Yuan Z and Shields A J 2021 *Nat. Photon.* **15** 530
[32] Clivati C, Meda A, Donadello S, Virz`i S, Genovese M, Levi F, Mura A, Pittaluga M, Yuan Z, Shields A J, *et al.* 2022 *Nat. Commun.* **13** 157
[33] Li W, Zhang L, Lu Y, Li Z P, Jiang C, Liu Y, Huang J, Li H, Wang Z, Wang X B, Zhang Q, You L, Xu F and Pan J W 2023 *Phys. Rev. Lett.* **130** 250802
[34] Chen J P, Zhou F, Zhang C, Jiang C, Chen F X, Huang J, Li H, You L X, Wang X B, Liu Y, Zhang Q and Pan J W 2024 *Phys. Rev. Lett.* **132** 260802
[35] Fang X T, Zeng P, Liu H, Zou M, Wu W, Tang Y L, Sheng Y J, Xiang Y, Zhang W, Li H, *et al.* 2020 *Nat. Photon.* **14** 422
[36] Chen J P, Zhang C, Liu Y, Jiang C, Zhang W J, Han Z Y, Ma S Z, Hu X L, Li Y H, Liu H, *et al.* 2021 *Nat. Photon.* **15** 570
[37] Du H, Paraiso T K, Pittaluga M, Lo Y S, Dolphin J A and Shields A J 2024 *Optica* **11** 1385
[38] Zeng P, Zhou H, Wu W and Ma X 2022 *Nat. Commun.* **13** 1
[39] Xie Y M, Lu Y S, Weng C X, Cao X Y, Jia Z Y, Bao Y, Wang Y, Fu Y, Yin H L and Chen Z B 2022 *PRX Quantum* **3** 020315
[40] Zhu H T, Huang Y, Liu H, Zeng P, Zou M, Dai Y, Tang S, Li H, You L, Wang Z, Chen Y A, Ma X, Chen T Y and Pan J W 2023 *Phys. Rev. Lett.* **130** 030801
[41] Zhu H T, Huang Y, Pan W X, Zhou C W, Tang J, He H, Cheng M, Jin X, Zou M, Tang S, Ma X, Chen T Y and Pan J W 2024 *Optica* **11** 883
[42] Li Z, Dou T, Cheng M, Liu Y and Tang J 2024 *Opt. Lett.* **49** 6609
[43] Wang Z H, Wang R, Yin Z Q, Wang S, Lu F Y, Chen W, He D Y, Guo G C and Han Z F 2023 *Commun. Phys.* **6** 265
[44] Liu X, Luo D, Zhang Z and Wei K 2023 *Phys. Rev. A* **107** 062613
[45] Lu Z, Wang G, Li C and Cao Z 2024 *Phys. Rev. A* **109** 012401
[46] Cui W, Yang C, Huang G and Jiao R 2024 *Phys. Scr.* **99** 085112
[47] Luo D, Liu X, Qin K, Zhang Z and Wei K 2024 *Phys. Rev. A* **110** 022605
[48] Zhou X Y, Hu J R, Zhang C H and Wang Q 2025 *Opt. Lett.* **50** 249
[49] Lu Y F, Wang Y, Li H W, Jiang M S, Zhang X X, Zhang Y Y, Zhou Y, Jiang X L, Wang H T, Zhao Y M, Zhou C and Bao W S 2025 *Phys. Rev. Res.* **7** 023102
[50] Li C L, Yin H L and Chen Z B 2024 *Rep. Prog. Phys.* **87** 127901
[51] Lu Y S, Yin H L, Xie Y M, Fu Y and Chen Z B 2025 *Rep. Prog. Phys.* **88** 067901
[52] Wang W, Xu F and Lo H K 2019 *Phys. Rev. X* **9** 041012
[53] Jiang C, Hu X L, Yu Z W and Wang X B 2022 *Photon. Res.* **10** 1703
[54] Liu X, Luo D, Luo Z, Li S, Zhang Z and Wei K 2024 *Phys. Rev. Appl.* **22** 064018
[55] Maurer U 1993 *IEEE Trans. Inf. Theory* **39** 733
[56] Gottesman D and Lo H K 2003 *IEEE Trans. Inf. Theory* **49** 457
[57] Ma X, Fung C H F, Dupuis F, Chen K, Tamaki K and Lo H K 2006 *Phys. Rev. A* **74** 032330
[58] Khatri S and Lütkenhaus N 2017 *Phys. Rev. A* **95** 042320
[59] Tan E Y Z, Lim C C W and Renner R 2020 *Phys. Rev. Lett.* **124** 020502
[60] Li H W, Zhang C M, Jiang M S and Cai Q Y 2022 *Commun. Phys.* **5** 53
[61] Wang R Q, Zhang C M, Yin Z Q, Li H W, Wang S, Chen W, Guo G C and Han Z F 2022 *New J. Phys.* **24** 073049
[62] Hu L W, Zhang C M and Li H W 2023 *Quantum Inf. Process.* **22** 77
[63] Zhou Y, Wang R Q, Zhang C M, Yin Z Q, Wang Z H, Wang S, Chen W, Guo G C and Han Z F 2024 *Phys. Rev. Appl.* **21** 014036
[64] Zhang C M, Wang Z, Wu Y D, Zhu J R, Wang R and Li H W 2024 *Phys. Rev. A* **109** 052432
[65] Wang H T, Zhou C, Lu Y F, Hao C P, Zhao Y M, Zhou Y Y, Li H W and Bao W S 2025 *Chin. Phys. B* **34** 040305
[66] Hao C P, Liu Y, Wang Y, Zhou C, Zhou Y Y, Bao W S and Li H W 2024 *Quantum Inf. Process.* **23** 148
[67] Li Y H, Li S L, Hu X L, Jiang C, Yu Z W, Li W, Liu W Y, Liao S K, Ren J G, Li H, You L, Wang Z, Yin J, Xu F, Zhang Q, Wang X B, Cao Y, Peng C Z and Pan J W 2023 *Phys. Rev. Lett.* **131** 100802
[68] Du Z, Liu G, Zhang X and Ma X 2024 *Quantum Sci. Technol.* **10** 015050
[69] Ma X and Razavi M 2012 *Phys. Rev. A* **86** 062319
[70] Renner R 2008 *Int. J. Quantum Inf.* **6** 1
[71] Li H W, Chen W, Huang J Z, Yao Y, Liu D, Li F Y, Wang S, Yin Z Q, He D Y, Zhou Z, Li Y H, Yu N H and Han Z F 2012 *Sci. Sin.: Phys. Mech. Astron.* **42** 1237