

Measurement-device-independent quantum key distribution with entanglement-assisted linear Bell state measurement

Cheng Zhang(张诚), Cheng Liu(刘成), Jiawei Ying(应佳伟), Shipu Gu(顾世浦), Lan Zhou(周澜), Yin Ma(马寅), Kang Gao(高亢), Hai Wei(魏海), Kai Wen(文凯), and Yubo Sheng(盛宇波)

Citation: Chin. Phys. B, 2026, 35 (**4**): 040310. DOI: 10.1088/1674-1056/ae3605
http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

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

Improved model on asynchronous measurement-device-independent quantum key distribution with realistic devices

Mingshuo Sun(孙铭烁), Chun-Hui Zhang(张春辉), Rui Zhang(章睿), Xing-Yu Zhou(周星宇), Jian Li(李剑), and Qin Wang(王琴)

Chin. Phys. B, 2024, 33 (**11**): 110302. DOI: 10.1088/1674-1056/ad757a

Security of the traditional quantum key distribution protocols with finite-key lengths

Bao Feng(冯宝), Hai-Dong Huang(黄海东), Yu-Xiang Bian(卞宇翔), Wei Jia(贾玮), Xing-Yu Zhou(周星宇), and Qin Wang(王琴)

Chin. Phys. B, 2023, 32 (**3**): 030307. DOI: 10.1088/1674-1056/ac9b33

Improvement of a continuous-variable measurement-device-independent quantum key distribution system via quantum scissors

Lingzhi Kong(孔令志), Weiqi Liu(刘维琪), Fan Jing(荆凡), Zhe-Kun Zhang(张哲坤), Jin Qi(齐锦), and Chen He(贺晨)

Chin. Phys. B, 2022, 31 (**9**): 090304. DOI: 10.1088/1674-1056/ac6dba

Performance analysis of continuous-variable measurement-device-independent quantum key distribution under diverse weather conditions

Shu-Jing Zhang(张淑静), Chen Xiao(肖晨), Chun Zhou(周淳), Xiang Wang(汪翔), Jian-Shu Yao(要建姝), Hai-Long Zhang(张海龙), Wan-Su Bao(鲍皖苏)

Chin. Phys. B, 2020, 29 (**2**): 020301. DOI: 10.1088/1674-1056/ab5efd

---

SPECIAL TOPIC — Quantum communication and quantum network

Measurement-device-independent quantum key distribution with entanglement-assisted linear Bell state measurement

Cheng Zhang(张诚)[1], Cheng Liu(刘成)[2], Jiawei Ying(应佳伟)[1], Shipu Gu(顾世浦)[1], Lan Zhou(周澜)[2], Yin Ma(马寅)[3,†], Kang Gao(高亢)[4], Hai Wei(魏海)[3,4], Kai Wen(文凯)[3,4], and Yubo Sheng(盛宇波)[1,‡]

[1] *College of Electronic and Optical Engineering, College of Flexible Electronics (Future Technology), Nanjing University of Posts and Telecommunications, Nanjing* 210023, *China*

[2] *College of Science, Nanjing University of Posts and Telecommunications, Nanjing* 210023, *China*

[3] *Beijing QBoson Quantum Technology Co. Ltd., Beijing* 100015, *China*

[4] *Quantum Science Center of Guangdong–Hong Kong–Macao Greater Bay Area, Shenzhen* 518045, *China*

(Received 22 October 2025; revised manuscript received 6 January 2026; accepted manuscript online 9 January 2026)

Measurement-device-independent quantum key distribution (MDI QKD) provides inherent immunity against attacks targeting practical measurement devices. Existing MDI QKD protocols all rely on Bell-state measurements (BSM) to establish correlations between the users. However, the success probability of linear-optics BSM is limited to 50%, which severely restricts the achievable key rate of MDI QKD. We propose a high-capacity MDI QKD protocol with entanglement-assisted linear-optical BSM. This protocol has three advantages. First, compared with the original MDI QKD, at least a 25% increase in the key rate can be achieved. Second, simulation results show that this protocol can effectively increase the maximum photon transmission distance of MDI QKD from 262 km to 272 km. Third, this protocol is feasible in a fully linear-optical system under current experimental conditions. Our protocol provides a potential approach for improving the performance of future quantum communication networks.

Keywords: measurement-device-independent quantum key distribution, linear-optical Bell state measurement, entanglement assistance

PACS: 03.67.–a, 03.67.Ac, 03.67.Hk, 03.67.Mn

DOI: 10.1088/1674-1056/ae3605 **CSTR:** 32038.14.CPB.ae3605

1. Introduction

Quantum information technology is a new type of technology that uses the principles of quantum mechanics for information processing, including quantum computing,[1] quantum sensing,[2] quantum communication,[3] and so on. Quantum communication also encompasses numerous research branches such as quantum key distribution (QKD),[4–24] quantum secure direct communication (QSDC),[25–29] quantum secret sharing (QSS),[30–33] quantum conference key agreement (QCKA),[34] and quantum signature (QS).[35,36] QKD is the closest to practical application among the branches of quantum communication. It was first introduced by Bennett *et al.* in 1984,[4] which allows two remote parties to share random keys with unconditional security in theory. Unfortunately, imperfect devices in practical experimental conditions introduce security loopholes in QKD systems, which can be exploited by the eavesdropper (Eve) to launch attacks.[37–46] Among all possible attacks, those targeting imperfect measurement devices (detectors) have the most severe consequences.[41–45] To eliminate security vulnerabilities from measurement devices, Lo *et al.*[47] and Braunstein *et al.*[48] independently proposed the measurement-device-independent (MDI) QKD protocols in 2012. By delegating all measurement operations to an untrusted third party, MDI QKD is immune to all attacks from measurement devices and can thus significantly enhance the security of practical QKD systems. Currently, MDI QKD has been extensively studied.[49–64] Beyond QKD, the MDI framework has also been extended to other quantum communication branches, such as QSDC[25–29] and QSS.[30–33]

Bell state measurement (BSM) plays a vital role in MDI QKD,[47–55] while also serving as a critical component in other quantum communication protocols, such as quantum teleportation[65,66] and quantum dense coding.[67,68] However, the performance of many quantum communication protocols is limited by BSM, as the success probability of BSM in linear optics is only 50%.[69,70] Therefore, it is crucial to increase the success probability of BSM. Barreiro *et al.*[71] and Hu *et al.*[72] utilized hyperentanglement and high-dimensional entanglement, respectively, to assist BSM and broke through the channel capacity limit of ultra-dense coding by increasing the success probability of BSM. In 2011, Grice proposed a theoretical model for linear-optical BSM that could achieve

†Corresponding author. E-mail: may@boseq.com

‡Corresponding author. E-mail: shengyb@njupt.edu.cn

© 2026 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

a maximum identification efficiency of $1-1/2^N$ using 2^N-2 auxiliary photons.[73] In 2014, Ewert *et al.* proposed a theoretical linear-optical BSM scheme based on two single-photon sources and six 50:50 beam splitters (BSs), which can realize a success probability of 75%.[74] In 2023, Bayerbach *et al.* proposed and experimentally demonstrated a linear-optical BSM scheme employing a pair of auxiliary entangled photons and two BSs, which can achieve a success probability of 62.5%.[75]

In this paper, we propose an MDI QKD protocol with entanglement-assisted linear-optical BSM.[75] Although the BSM scheme proposed in Ref. [74] theoretically achieves a higher success rate, it would greatly increase the complexity of the system and present greater challenges for experimental implementation. The BSM scheme in Ref. [75] has a much simpler structure and has already been experimentally demonstrated. Therefore, we adopt the BSM scheme in Ref. [75] in our MDI QKD protocol. We numerically analyze the performance of our MDI QKD protocol under practical experimental conditions. Our protocol achieves a maximum photon transmission distance of 272 km, surpassing the maximum transmission distance of 262 km of the original MDI QKD with non-assisted linear-optical BSM[47] under identical conditions. Our MDI QKD protocol reaches a 25% higher key rate than the original MDI QKD protocol within the photon transmission distance range of 210 km, while this advantage further increases beyond 210 km. Our protocol is the first to conduct an in-depth discussion on the effect of entanglement-assisted linear-optical BSM on MDI QKD and provides theoretical results, which explore a potential development direction of MDI QKD. Our MDI QKD protocol with entanglement-assisted linear-optical BSM has reference value for improving the performance of quantum communication networks.

The paper is organized as follows. In Section 2, we introduce our MDI QKD protocol with entanglement-assisted linear-optical BSM. In Section 3, we establish a numerical simulation model to estimate the secure key rate of our protocol. Finally, we draw a conclusion in Section 4.

2. The MDI QKD protocol with entanglement-assisted linear-optical BSM

The basic principle of the MDI QKD protocol with entanglement-assisted linear-optical BSM is shown in Fig. 1. The protocol operates through the following six steps.

Step 1 Alice and Bob each employ a single-photon source to generate single-photon states.

Step 2 After the single photon is prepared, both parties randomly encode the single photons in the Z basis ($Z=\{|H\rangle,|V\rangle\}$) or the X basis ($X=\{|+\rangle=\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle),|-\rangle=\frac{1}{\sqrt{2}}(|H\rangle-|V\rangle)\}$) using polarization modulators (PMs). Here, $|H\rangle$ and $|V\rangle$ represent the horizontal and vertical polarization states, respectively. The key encoding rule can be described as follows: $|H\rangle$ and $|+\rangle$ represent the classical key bit 0, while $|V\rangle$ and $|-\rangle$ represent the classical key bit 1.

Step 3 Alice and Bob send the encoded photons to the untrusted measurement party Charlie for entanglement-assisted linear-optical BSM.

Step 4 The measurement party consists of an entangled photon source and a BSM module, which is shown in Fig. 1. The entangled photon source generates identical entangled photon pairs in $|\phi^+\rangle=\frac{1}{\sqrt{2}}(|HH\rangle+|VV\rangle)$. The measurement module consists of two cascaded BSs, three polarizing beam splitters (PBSs), and six photon-number-resolving detectors. The photons from Alice and Bob enter the BSM module through the ports a_1 and b_1, respectively. The locally generated auxiliary entangled photon pair is injected through port b_2. After the four-photon interference process, the specific detector responses corresponding to the four Bell states and their probabilities are detailed in Table 1. Note that only the bold response combinations are exclusive detector responses that can be discriminated. Specifically, this entanglement-assisted linear-optical BSM protocol can realize 100% identification of $|\psi^+\rangle=\frac{1}{\sqrt{2}}(|HV\rangle+|VH\rangle)$ and $|\psi^-\rangle=\frac{1}{\sqrt{2}}(|HV\rangle-|VH\rangle)$, while 25% identification of $|\phi^+\rangle$ and $|\phi^-\rangle=\frac{1}{\sqrt{2}}(|HH\rangle-|VV\rangle)$. In this way, the entanglement-assisted linear-optical BSM increases the identification probability to 62.5%. After the measurement, Charlie announces the BSM results.

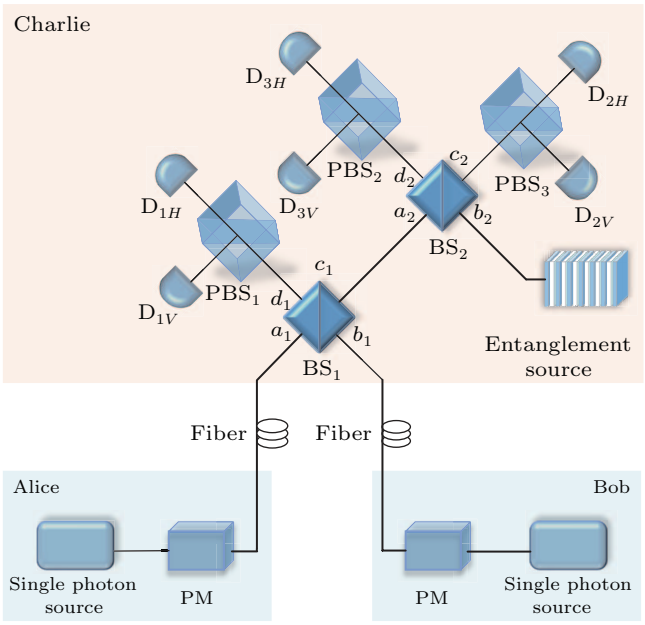


Fig. 1. Schematic diagram of the MDI QKD protocol with entanglement-assisted linear-optical BSM. The single-photon source prepares single photons, and the entanglement source prepares auxiliary Bell states.[75] The PBS transmits photons with horizontal polarization ($|H\rangle$) and reflects photons with vertical polarization ($|V\rangle$). The 50:50 beam splitter (BS) splits light equally into two paths. The polarization modulator (PM) encodes photons in the polarization degree of freedom. D_{1H}, D_{1V}, D_{2H}, D_{2V}, D_{3H}, and D_{3V} denote six photon-number-resolving detectors.

Table 1. Detector response combinations corresponding to the four Bell states in the entanglement-assisted BSM protocol. The superscript of each item indicates the number of photons detected by the corresponding detector. Only the bold response combinations are exclusive detector responses that can be discriminated.

$\|\phi^-\rangle$		$\|\phi^+\rangle$		$\|\psi^-\rangle$		$\|\psi^+\rangle$	
Result	Probability	Result	Probability	Result	Probability	Result	Probability
D_{2H}^4	$\frac{3}{64}$	D_{2H}^4	$\frac{3}{64}$	$\mathbf{D_{1H}D_{2V}^3}$	$\frac{3}{32}$	$\mathbf{D_{2H}^3D_{2V}}$	$\frac{3}{64}$
D_{2V}^4	$\frac{3}{64}$	D_{2V}^4	$\frac{3}{64}$	$\mathbf{D_{1H}D_{3V}^3}$	$\frac{3}{32}$	$\mathbf{D_{2H}D_{2V}^3}$	$\frac{3}{64}$
D_{3H}^4	$\frac{3}{64}$	D_{3H}^4	$\frac{3}{64}$	$\mathbf{D_{1H}D_{2V}D_{3H}^2}$	$\frac{1}{32}$	$\mathbf{D_{3H}^3D_{3V}}$	$\frac{3}{64}$
D_{3V}^4	$\frac{3}{64}$	D_{3V}^4	$\frac{3}{64}$	$\mathbf{D_{1H}D_{2V}D_{3V}^2}$	$\frac{1}{32}$	$\mathbf{D_{3H}D_{3V}^3}$	$\frac{3}{64}$
$D_{2H}^2D_{3H}^2$	$\frac{1}{32}$	$D_{2H}^2D_{3H}^2$	$\frac{1}{32}$	$\mathbf{D_{1H}D_{2H}^2D_{2V}}$	$\frac{1}{32}$	$\mathbf{D_{2V}^3D_{3H}}$	$\frac{3}{64}$
$D_{2V}^2D_{3V}^2$	$\frac{1}{32}$	$D_{2V}^2D_{3V}^2$	$\frac{1}{32}$	$\mathbf{D_{1H}D_{2H}^2D_{3V}}$	$\frac{1}{32}$	$\mathbf{D_{2V}D_{3H}^3}$	$\frac{3}{64}$
$\mathbf{D_{2H}^2D_{2V}D_{3V}}$	$\frac{1}{16}$	$\mathbf{D_{3H}^2D_{3V}^2}$	$\frac{1}{32}$	$\mathbf{D_{1H}D_{2V}^2D_{3V}}$	$\frac{1}{32}$	$\mathbf{D_{2H}^3D_{3V}}$	$\frac{3}{64}$
$\mathbf{D_{2V}D_{3H}^2D_{3V}}$	$\frac{1}{16}$	$\mathbf{D_{2H}^2D_{2V}^2}$	$\frac{1}{32}$	$\mathbf{D_{1H}D_{3H}^2D_{3V}}$	$\frac{1}{32}$	$\mathbf{D_{2H}D_{3V}^3}$	$\frac{3}{64}$
$\mathbf{D_{2H}D_{2V}^2D_{3H}}$	$\frac{1}{16}$	$\mathbf{D_{2H}^2D_{3V}^2}$	$\frac{1}{32}$	$\mathbf{D_{1H}D_{2H}D_{2V}D_{3H}}$	$\frac{1}{16}$	$\mathbf{D_{2H}D_{2V}^2D_{3V}}$	$\frac{1}{64}$
$\mathbf{D_{2H}D_{3H}D_{3V}^2}$	$\frac{1}{16}$	$\mathbf{D_{2V}^2D_{3H}^2}$	$\frac{1}{32}$	$\mathbf{D_{1H}D_{2H}D_{3H}D_{3V}}$	$\frac{1}{16}$	$\mathbf{D_{2H}^2D_{2V}D_{3H}}$	$\frac{1}{64}$
$D_{1H}^2D_{2H}^2$	$\frac{1}{32}$	$D_{1H}^2D_{2H}^2$	$\frac{1}{32}$	$\mathbf{D_{1V}D_{2H}^3}$	$\frac{3}{32}$	$\mathbf{D_{2V}D_{3H}D_{3V}^2}$	$\frac{1}{64}$
$D_{1H}^2D_{3H}^2$	$\frac{1}{32}$	$D_{1H}^2D_{3H}^2$	$\frac{1}{32}$	$\mathbf{D_{1V}D_{3H}^3}$	$\frac{3}{32}$	$\mathbf{D_{2H}D_{3H}^2D_{3V}}$	$\frac{1}{64}$
$D_{1H}^2D_{2V}^2$	$\frac{1}{32}$	$D_{1H}^2D_{2V}^2$	$\frac{1}{32}$	$\mathbf{D_{1V}D_{2H}D_{2V}^2}$	$\frac{1}{32}$	$\mathbf{D_{2V}^2D_{3H}D_{3V}}$	$\frac{1}{64}$
$D_{1H}^2D_{3V}^2$	$\frac{1}{32}$	$D_{1H}^2D_{3V}^2$	$\frac{1}{32}$	$\mathbf{D_{1V}D_{3H}D_{3V}^2}$	$\frac{1}{32}$	$\mathbf{D_{2H}D_{2V}D_{3H}^2}$	$\frac{1}{64}$
$D_{1H}^2D_{2V}D_{3V}$	$\frac{1}{16}$	$D_{1H}^2D_{2V}D_{3V}$	$\frac{1}{16}$	$\mathbf{D_{1V}D_{2H}D_{3V}^2}$	$\frac{1}{32}$	$\mathbf{D_{2H}D_{2V}D_{3V}^2}$	$\frac{1}{64}$
$D_{1H}^2D_{2H}D_{3H}$	$\frac{1}{16}$	$D_{1H}^2D_{2H}D_{3H}$	$\frac{1}{16}$	$\mathbf{D_{1V}D_{2H}D_{3H}^2}$	$\frac{1}{32}$	$\mathbf{D_{2H}^2D_{3H}D_{3V}}$	$\frac{1}{64}$
$D_{1V}^2D_{2H}^2$	$\frac{1}{32}$	$D_{1V}^2D_{2H}^2$	$\frac{1}{32}$	$\mathbf{D_{1V}D_{2H}^2D_{3H}}$	$\frac{1}{32}$	$\mathbf{D_{1H}D_{1V}D_{2H}^2}$	$\frac{1}{16}$
$D_{1V}^2D_{3H}^2$	$\frac{1}{32}$	$D_{1V}^2D_{3H}^2$	$\frac{1}{32}$	$\mathbf{D_{1V}D_{2V}^2D_{3H}}$	$\frac{1}{32}$	$\mathbf{D_{1H}D_{1V}D_{2V}^2}$	$\frac{1}{16}$
$D_{1V}^2D_{2V}^2$	$\frac{1}{32}$	$D_{1V}^2D_{2V}^2$	$\frac{1}{32}$	$\mathbf{D_{1V}D_{2H}D_{2V}D_{3V}}$	$\frac{1}{16}$	$\mathbf{D_{1H}D_{1V}D_{3H}^2}$	$\frac{1}{16}$
$D_{1V}^2D_{3V}^2$	$\frac{1}{32}$	$D_{1V}^2D_{3V}^2$	$\frac{1}{32}$	$\mathbf{D_{1V}D_{2V}D_{3H}D_{3V}}$	$\frac{1}{16}$	$\mathbf{D_{1H}D_{1V}D_{3V}^2}$	$\frac{1}{16}$
$D_{1V}^2D_{2H}D_{3H}$	$\frac{1}{16}$	$D_{1V}^2D_{2H}D_{3H}$	$\frac{1}{16}$	–	–	$\mathbf{D_{1H}D_{1V}D_{2H}D_{3H}}$	$\frac{1}{8}$
$D_{1V}^2D_{2V}D_{3V}$	$\frac{1}{16}$	$D_{1V}^2D_{2V}D_{3V}$	$\frac{1}{16}$	–	–	$\mathbf{D_{1H}D_{1V}D_{2V}D_{3V}}$	$\frac{1}{8}$
–	–	$\mathbf{D_{2H}D_{2V}D_{3H}D_{3V}}$	$\frac{1}{8}$	–	–	–	–

Table 2. The quantum states from two parties and the post-selection operation corresponding to Charlie's measurement results.

Alice & Bob	Charlie			
	$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$
$\|HH\rangle_{ab}/\|VV\rangle_{ab}$	no bit flip	no bit flip	–	–
$\|HV\rangle_{ab}/\|VH\rangle_{ab}$	–	–	bit flip	bit flip

Step 5 Alice and Bob publicly announce their encoding bases for all photons and reveal the encoded states of the photons prepared in the X basis. If both photons are encoded in the Z basis, their encoded bits are used to generate the raw keys. From Table 2, when both photons are encoded in the Z basis, if the BSM result is $|\phi^{\pm}\rangle$, the users obtain $k_{\mathrm{A}} = k_{\mathrm{B}}$, where both Alice and Bob retain their encoded bits as the raw key. If the BSM result is $|\psi^{\pm}\rangle$, the users obtain $k_{\mathrm{A}} = k_{\mathrm{B}} \oplus 1$, where Alice keeps the original encoded bit while Bob flips his encoded bit to form the raw key. If both photons are encoded in the X basis, their encoded bits are used for security checking. In detail, the state $|++\rangle$ or $|--\rangle$ corresponds to the Bell state $|\phi^+\rangle$ or $|\psi^+\rangle$, while the state $|+-\rangle$ or $|-+\rangle$ corresponds to the Bell states $|\phi^-\rangle$ or $|\psi^-\rangle$. After security checking, Alice and Bob estimate the total quantum bit error rate (QBER) based on the test results. If the QBER is below a predefined threshold, they continue to the next step. Otherwise, they discard all raw keys and recheck the quantum channels. Alice and Bob repeat the above steps until they obtain a sufficient amount of raw keys.

Step 6 Alice and Bob perform error correction and privacy amplification on the raw keys to generate the final secure keys.

3. Key rate estimation of the MDI QKD with entanglement-assisted linear-optical BSM

3.1. Key rate estimation model

We now establish a numerical model to estimate the key rate of our MDI QKD protocol with entanglement-assisted linear-optical BSM under the condition of ideal single-photon sources. In the asymptotic limit (neglecting finite-size effects), the secure key rate is given by Ref. [76]

$$R \geq Y_{11}^{Z}\left[1 - H(e_{11}^{X}) - fH(e_{11}^{Z})\right], \tag{1}$$

where Y_{11}^{Z} is the single-photon yield, e_{11}^{Z} (e_{11}^{X}) is the bit error rate for single-photon emission in the Z (X) basis, f is the error-correction efficiency factor, and $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function.

We define the single-photon yields of correct and erroneous measurement outcomes as Y_{11}^{C} and Y_{11}^{E}, respectively. Given the use of photon-number-resolving detectors at the measurement station, we assume

(i) negligible loss in the local entanglement source;

(ii) the detector response rate is 100%;

(iii) the situation where a detector has two or more dark counts simultaneously is ignored.

Under the condition of an ideal single-photon source, there are three photon-distribution situations at the measurement end: (I) both photons arrive, (II) only one photon arrives, and (III) neither photon arrives. We now discuss the measurement outcomes in these three cases, respectively.

(I) Both photons arrive at the BSM devices In this case, the relationship between the BSM results and the encoded photons is shown in Table 3. In detail, when the state of the two photons is $|HH\rangle_{ab}$ or $|VV\rangle_{ab}$, the theoretical BSM result is $1/\sqrt{2}(|\phi^+\rangle+|\phi^-\rangle)$. For example, by combining the measurement probabilities of each BSM result shown in Table 1, we obtain the probabilities

$$\begin{aligned}&P_{HH}^{\phi^+}=\frac{1}{16}(1-p_{\rm d})^4+\frac{1}{16}(1-p_{\rm d})^2,\ P_{HH}^{\phi^-}=\frac{1}{8}(1-p_{\rm d})^3,\\&P_{HH}^{\psi^+}=0,\ P_{HH}^{\psi^-}=0.\end{aligned}\tag{2}$$

When the state of the two photons is $|HV\rangle_{ab}$ or $|VH\rangle_{ab}$, the theoretical BSM result is $1/\sqrt{2}(|\psi^+\rangle+|\psi^-\rangle)$. For example, by combining the measurement probabilities of each BSM result in Table 1, we obtain

$$\begin{aligned}&P_{HV}^{\phi^+}=0,\ P_{HV}^{\phi^-}=0,\\&P_{HV}^{\psi^-}=\frac{3}{16}(1-p_{\rm d})^4+\frac{3}{16}(1-p_{\rm d})^3+\frac{1}{8}(1-p_{\rm d})^2,\\&P_{HV}^{\psi^+}=\frac{3}{16}(1-p_{\rm d})^4+\frac{3}{16}(1-p_{\rm d})^3+\frac{1}{8}(1-p_{\rm d})^2.\end{aligned}\tag{3}$$

When the state of the two photons is $|++\rangle_{ab}$ or $|--\rangle_{ab}$, the theoretical BSM result is $1/\sqrt{2}(|\phi^+\rangle+|\psi^+\rangle)$. We take $|++\rangle_{ab}$ as an example and obtain

$$\begin{aligned}&P_{++}^{\phi^+}=\frac{1}{16}(1-p_{\rm d})^4+\frac{1}{16}(1-p_{\rm d})^2,\ P_{++}^{\phi^-}=0,\\&P_{++}^{\psi^+}=\frac{3}{16}(1-p_{\rm d})^4+\frac{3}{16}(1-p_{\rm d})^3+\frac{1}{8}(1-p_{\rm d})^2,\\&P_{++}^{\psi^-}=0.\end{aligned}\tag{4}$$

When the state of the two photons is $|+-\rangle_{ab}$ or $|-+\rangle_{ab}$, the theoretical BSM result is $1/\sqrt{2}(|\phi^-\rangle+|\psi^-\rangle)$. Considering $|+-\rangle_{ab}$, we obtain

$$\begin{aligned}&P_{+-}^{\phi^+}=0,\ P_{+-}^{\phi^-}=\frac{1}{8}(1-p_{\rm d})^3,\ P_{+-}^{\psi^+}=0,\\&P_{+-}^{\psi^-}=\frac{3}{16}(1-p_{\rm d})^4+\frac{3}{16}(1-p_{\rm d})^3+\frac{1}{8}(1-p_{\rm d})^2.\end{aligned}\tag{5}$$

Here, $p_{\rm d}$ is the dark-counting rate, and P_{AB}^{Φ} ($AB\in\{HH,HV,++,+-\}$ and $\Phi\in\{\phi^+,\phi^-,\psi^+,\psi^-\}$) represents the probability of obtaining the BSM result $|\Phi\rangle$ when Charlie receives two photons in the $|AB\rangle_{ab}$ state. The states $|VV\rangle_{ab}$, $|VH\rangle_{ab}$, $|--\rangle_{ab}$, and $|-+\rangle_{ab}$ yield the same results as $|HH\rangle_{ab}$, $|HV\rangle_{ab}$, $|++\rangle_{ab}$, and $|+-\rangle_{ab}$, respectively.

(II) Only one photon arrives at the BSM devices In this case, dark counting must occur for a successful response. Due to the randomness of dark counting, each of the four BSM results has a probability of occurring. The probability of obtaining each BSM result is calculated by combining Table 1 with the probability of dark-count occurrence. It should be particularly noted that dark counting can only occur on detectors that did not register a photon click, and thus it can only increase the photon number by one. Therefore, in the case of photon loss, response results corresponding to two or more photons detected by a single detector cannot occur.

For example, when the input photon state is $|H\rangle_a|0\rangle_b$, $|V\rangle_a|0\rangle_b$, $|0\rangle_a|H\rangle_b$, or $|0\rangle_a|V\rangle_b$, we obtain

$$\begin{aligned}&P_{V0}^{\phi^+}=P_{0V}^{\phi^+}=P_{0H}^{\phi^+}=P_{H0}^{\phi^+}=\frac{1}{16}(1-p_{\rm d})^2p_{\rm d}\times2,\\&P_{V0}^{\phi^-}=P_{0V}^{\phi^-}=P_{0H}^{\phi^-}=P_{H0}^{\phi^-}=\frac{1}{32}(1-p_{\rm d})^3p_{\rm d}\times4,\\&P_{V0}^{\psi^+}=P_{0V}^{\psi^+}=P_{0H}^{\psi^+}=P_{H0}^{\psi^+}=\frac{1}{8}(1-p_{\rm d})^2p_{\rm d}\times2\\&\qquad+\frac{1}{16}(1-p_{\rm d})^3p_{\rm d}\times4\\&\qquad+\frac{1}{32}(1-p_{\rm d})^3p_{\rm d}\times8\\&\qquad+\frac{3}{32}(1-p_{\rm d})^4p_{\rm d}\times4,\\&P_{V0}^{\psi^-}=P_{0V}^{\psi^-}=P_{0H}^{\psi^-}=P_{H0}^{\psi^-}=\frac{1}{16}(1-p_{\rm d})^3p_{\rm d}\times6\\&\qquad+\frac{1}{8}(1-p_{\rm d})^2p_{\rm d}+\frac{1}{32}(1-p_{\rm d})^3p_{\rm d}\times6\\&\qquad+\frac{3}{32}(1-p_{\rm d})^4p_{\rm d}\times2+\frac{1}{16}(1-p_{\rm d})^2p_{\rm d}\times2.\end{aligned}\tag{6}$$

When the incoming photon state is $|+\rangle_a|0\rangle_b$, $|-\rangle_a|0\rangle_b$, $|0\rangle_a|+\rangle_b$, or $|0\rangle_a|-\rangle_b$, we obtain

$$\begin{aligned}&P_{-0}^{\phi^+}=P_{0-}^{\phi^+}=P_{0+}^{\phi^+}=P_{+0}^{\phi^+}=\frac{1}{2}P_{H0}^{\phi^+}+\frac{1}{2}P_{V0}^{\phi^+},\\&P_{-0}^{\phi^-}=P_{0-}^{\phi^-}=P_{0+}^{\phi^-}=P_{+0}^{\phi^-}=\frac{1}{2}P_{H0}^{\phi^-}+\frac{1}{2}P_{V0}^{\phi^-},\\&P_{-0}^{\psi^+}=P_{0-}^{\psi^+}=P_{0+}^{\psi^+}=P_{+0}^{\psi^+}=\frac{1}{2}P_{H0}^{\psi^+}+\frac{1}{2}P_{V0}^{\psi^+},\\&P_{-0}^{\psi^-}=P_{0-}^{\psi^-}=P_{0+}^{\psi^-}=P_{+0}^{\psi^-}=\frac{1}{2}P_{H0}^{\psi^-}+\frac{1}{2}P_{V0}^{\psi^-}.\end{aligned}\tag{7}$$

Here, P_{AB}^{Φ} ($AB\in\{H0,V0,0H,0V,+0,-0,0+,0-\}$ and $\Phi\in\{\phi^+,\phi^-,\psi^+,\psi^-\}$) represents the probability of obtaining the BSM result $|\Phi\rangle$ when Charlie receives one photon from Alice or Bob.

(III) Neither photon arrives at the BSM devices When both input photons are lost, the successful response is completely randomly triggered by the dark counting. In this way, all the four BSM results may occur, and the number of detector responses in Table 1 that cannot be obtained further increases.

In this case, the input state is $|0\rangle_a|0\rangle_b$, and we can obtain

$$P_{00}^{\phi^+}=\frac{1}{4}\times(1-p_{\rm d})^2p_{\rm d}^2\times2,$$

$$
\begin{aligned}
P_{00}^{\phi^-} &= \frac{1}{8}\times(1-p_{\rm d})^3 p_{\rm d}^2\times 4,\\
P_{00}^{\psi^+} &= \frac{1}{8}\times(1-p_{\rm d})^3 p_{\rm d}^2\times 12+\frac{1}{4}\times(1-p_{\rm d})^2 p_{\rm d}^2\times 2,\\
P_{00}^{\psi^-} &= \frac{1}{8}\times(1-p_{\rm d})^3 p_{\rm d}^2\times 12+\frac{1}{4}\times(1-p_{\rm d})^2 p_{\rm d}^2\times 4. \quad (8)
\end{aligned}
$$

When the photon transmission loss occurs, based on Refs. [47,77], the correct yield Y_{AB}^{C} and error yield Y_{AB}^{E} for each possible photon state combination ($AB\in\{HH,VV,HV,VH,++,--,+-,-+\}$) according to Table 3 are given by

$$
\begin{aligned}
Y_{VV}^{C}=Y_{HH}^{C} &= \eta_a\eta_b\times(P_{HH}^{\phi^+}+P_{HH}^{\phi^-})+\eta_a(1-\eta_b)\times(P_{H0}^{\phi^+}+P_{H0}^{\phi^-})\\
&\quad+\eta_b(1-\eta_a)\times(P_{0H}^{\phi^+}+P_{0H}^{\phi^-})+(1-\eta_a)(1-\eta_b)\times(P_{00}^{\phi^+}+P_{00}^{\phi^-}),\\
Y_{VV}^{E}=Y_{HH}^{E} &= \eta_a\eta_b\times(P_{HH}^{\psi^+}+P_{HH}^{\psi^-})+\eta_a(1-\eta_b)\times(P_{H0}^{\psi^+}+P_{H0}^{\psi^-})\\
&\quad+\eta_b(1-\eta_a)\times(P_{0H}^{\psi^+}+P_{0H}^{\psi^-})+(1-\eta_a)(1-\eta_b)\times(P_{00}^{\psi^+}+P_{00}^{\psi^-}),\\
Y_{VH}^{C}=Y_{HV}^{C} &= \eta_a\eta_b\times(P_{HV}^{\psi^+}+P_{HV}^{\psi^-})+\eta_a(1-\eta_b)\times(P_{H0}^{\psi^+}+P_{H0}^{\psi^-})\\
&\quad+\eta_b(1-\eta_a)\times(P_{0V}^{\psi^+}+P_{0V}^{\psi^-})+(1-\eta_a)(1-\eta_b)\times(P_{00}^{\psi^+}+P_{00}^{\psi^-}),\\
Y_{VH}^{E}=Y_{HV}^{E} &= \eta_a\eta_b\times(P_{HV}^{\phi^+}+P_{HV}^{\phi^-})+\eta_a(1-\eta_b)\times(P_{H0}^{\phi^+}+P_{H0}^{\phi^-})\\
&\quad+\eta_b(1-\eta_a)\times(P_{0V}^{\phi^+}+P_{0V}^{\phi^-})+(1-\eta_a)(1-\eta_b)\times(P_{00}^{\phi^+}+P_{00}^{\phi^-}),\\
Y_{--}^{C}=Y_{++}^{C} &= \eta_a\eta_b\times(P_{++}^{\phi^+}+P_{++}^{\psi^+})+\eta_a(1-\eta_b)\times(P_{+0}^{\phi^+}+P_{+0}^{\psi^+})\\
&\quad+\eta_b(1-\eta_a)\times(P_{0+}^{\phi^+}+P_{0+}^{\psi^+})+(1-\eta_a)(1-\eta_b)\times(P_{00}^{\phi^+}+P_{00}^{\psi^+}),\\
Y_{--}^{E}=Y_{++}^{E} &= \eta_a\eta_b\times(P_{++}^{\phi^-}+P_{++}^{\psi^-})+\eta_a(1-\eta_b)\times(P_{+0}^{\phi^-}+P_{+0}^{\psi^-})\\
&\quad+\eta_b(1-\eta_a)\times(P_{0+}^{\phi^-}+P_{0+}^{\psi^-})+(1-\eta_a)(1-\eta_b)\times(P_{00}^{\phi^-}+P_{00}^{\psi^-}),\\
Y_{-+}^{C}=Y_{+-}^{C} &= \eta_a\eta_b\times(P_{+-}^{\phi^-}+P_{+-}^{\psi^-})+\eta_a(1-\eta_b)\times(P_{+0}^{\phi^-}+P_{+0}^{\psi^-})\\
&\quad+\eta_b(1-\eta_a)\times(P_{0-}^{\phi^-}+P_{0-}^{\psi^-})+(1-\eta_a)(1-\eta_b)\times(P_{00}^{\phi^-}+P_{00}^{\psi^-}),\\
Y_{-+}^{E}=Y_{+-}^{E} &= \eta_a\eta_b\times(P_{+-}^{\phi^+}+P_{+-}^{\psi^+})+\eta_a(1-\eta_b)\times(P_{+0}^{\phi^+}+P_{+0}^{\psi^+})\\
&\quad+\eta_b(1-\eta_a)\times(P_{0-}^{\phi^+}+P_{0-}^{\psi^+})+(1-\eta_a)(1-\eta_b)\times(P_{00}^{\phi^+}+P_{00}^{\psi^+}). \quad (9)
\end{aligned}
$$

Table 3. The Bell state measurement results corresponding to the input single photon states.

Input single photon state		Results of BSM			
Alice	Bob	$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$
$\|H\rangle$	$\|H\rangle$	1/2	1/2	0	0
$\|V\rangle$	$\|V\rangle$	1/2	1/2	0	0
$\|H\rangle$	$\|V\rangle$	0	0	1/2	1/2
$\|V\rangle$	$\|H\rangle$	0	0	1/2	1/2
$\|+\rangle$	$\|+\rangle$	1/2	0	1/2	0
$\|-\rangle$	$\|-\rangle$	1/2	0	1/2	0
$\|+\rangle$	$\|-\rangle$	0	1/2	0	1/2
$\|-\rangle$	$\|+\rangle$	0	1/2	0	1/2

Here $\eta_a=10^{-\alpha L_{ac}/10}$ and $\eta_b=10^{-\alpha L_{bc}/10}$ represent the transmission efficiency of photons emitted by Alice and Bob through the optical fiber channel, respectively. α represents the fiber attenuation coefficient and L_{ac} (L_{bc}) represents the channel distance from Alice (Bob) to Charlie. We assume $L_{ac}=L_{bc}=L$, and thus $\eta_a=\eta_b=10^{-\alpha L/10}$.

Then, the total yield $Y_{11}^{Z(X)}$ in the $Z(X)$ basis is given by

$$
Y_{11}^{Z}=Y_{11}^{ZC}+Y_{11}^{ZE},\quad Y_{11}^{X}=Y_{11}^{XC}+Y_{11}^{XE}, \quad (10)
$$

where

$$
\begin{aligned}
Y_{11}^{ZC} &= \frac{1}{4}\left(Y_{HH}^{C}+Y_{VV}^{C}+Y_{HV}^{C}+Y_{VH}^{C}\right),\\
Y_{11}^{ZE} &= \frac{1}{4}\left(Y_{HH}^{E}+Y_{VV}^{E}+Y_{HV}^{E}+Y_{VH}^{E}\right),\\
Y_{11}^{XC} &= \frac{1}{4}\left(Y_{++}^{C}+Y_{--}^{C}+Y_{+-}^{C}+Y_{-+}^{C}\right),\\
Y_{11}^{XE} &= \frac{1}{4}\left(Y_{++}^{E}+Y_{--}^{E}+Y_{+-}^{E}+Y_{-+}^{E}\right). \quad (11)
\end{aligned}
$$

Accounting for the basis misalignment probability $e_{\rm d}^{Z(X)}$, the QBER $e_{11}^{Z(X)}$ becomes

$$
\begin{aligned}
e_{11}^{Z} &= \frac{e_{\rm d}^{Z}Y_{11}^{ZC}+(1-e_{\rm d}^{Z})Y_{11}^{ZE}}{Y_{11}^{Z}},\\
e_{11}^{X} &= \frac{e_{\rm d}^{X}Y_{11}^{XC}+(1-e_{\rm d}^{X})Y_{11}^{XE}}{Y_{11}^{X}}. \quad (12)
\end{aligned}
$$

By substituting Eqs. (10) and (12) into Eq. (1), the lower bound of the secure key rate R can be obtained.

3.2. Analysis of simulation results

The key rate is numerically simulated using the parameters listed in Table 4. We provide the secure key rates of our

MDI QKD protocol with entanglement-assisted linear-optical BSM and the original MDI QKD protocol[47] versus the photon transmission distance L between Charlie and Alice (or Bob) in Fig. 2.

It is found that the maximal photon transmission distance of our MDI QKD protocol is about 272 km, which is longer than that of the original MDI QKD protocol (about 262 km). The key rate curves demonstrate consistent parallelism, and the key rate of our MDI QKD protocol is always about 25% higher than that of the original MDI QKD protocol. When the photon transmission distance exceeds 210 km, the attenuation rate of the key rate of the original MDI QKD protocol increases significantly. Therefore, the key rate advantage of our MDI QKD protocol is more pronounced at long distances.

Table 4. Simulation parameters. Here, $p_{\rm d}$ is the dark count rate of detectors; $e_{\rm d}^{Z(X)}$ denotes the misalignment probability of $Z(X)$ basis; f is the error correction inefficiency; α is the standard fiber loss coefficient.

$p_{\rm d}$	$e_{\rm d}^{Z}$	$e_{\rm d}^{X}$	f	α
10^{-7}	1.5%	1.5%	1.16	0.2 dB/km

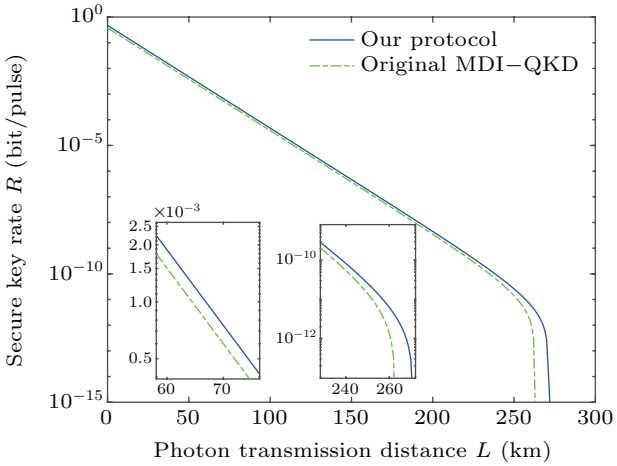


Fig. 2. Secure key rates of our MDI QKD protocol with entanglement-assisted linear-optical BSM and the original MDI QKD protocol[47] versus the photon transmission distance L.

We also compare e_{11}^{Z} and Y_{11}^{Z} of our MDI QKD protocol with the original MDI QKD protocol in Figs. 3(a) and 3(b), respectively.

It can be seen from Fig. 3(a) that e_{11}^{Z} of the two MDI QKD protocols remains at about 1.5% when $L < 160$ km, and the difference between the two curves is negligible. After $L > 160$ km, the difference in e_{11}^{Z} between the two protocols increases. When $L > 200$ km, e_{11}^{Z} of the original protocol becomes significantly higher than that of our protocol.

It can also be observed in Fig. 3(b) that Y_{11}^{Z} of both MDI QKD protocols maintains a relatively stable trend within the range of 270 km. Within 230 km, Y_{11}^{Z} of our protocol is about 25% higher than that of the original MDI QKD protocol. This explains why the key rate of our MDI QKD protocol is 25% higher than that of the original protocol for photon transmission distances up to 210 km in Fig. 2.

Based on the above discussion, the reason why the two MDI QKD protocols maintain a stable key rate difference of 25% when $L < 200$ km is that their e_{11}^{Z} values are very close within this range, so the key rate curves are mainly determined by Y_{11}^{Z}. When $L > 200$ km, the difference in key rates between the two MDI QKD protocols gradually increases, although the difference in Y_{11}^{Z} remains small. Therefore, the key rate curve is mainly affected by e_{11}^{Z}. The increase in e_{11}^{Z} for our MDI QKD protocol is much slower than that of the original protocol, resulting in a longer maximum photon transmission distance. This occurs because photon loss becomes significant at long distances, and the contribution of dark counts to error responses dominates. Due to the use of photon-number-resolving detectors, some responses cannot be triggered by dark counts in our protocol, so the proportion of error responses is smaller than that of the original protocol.

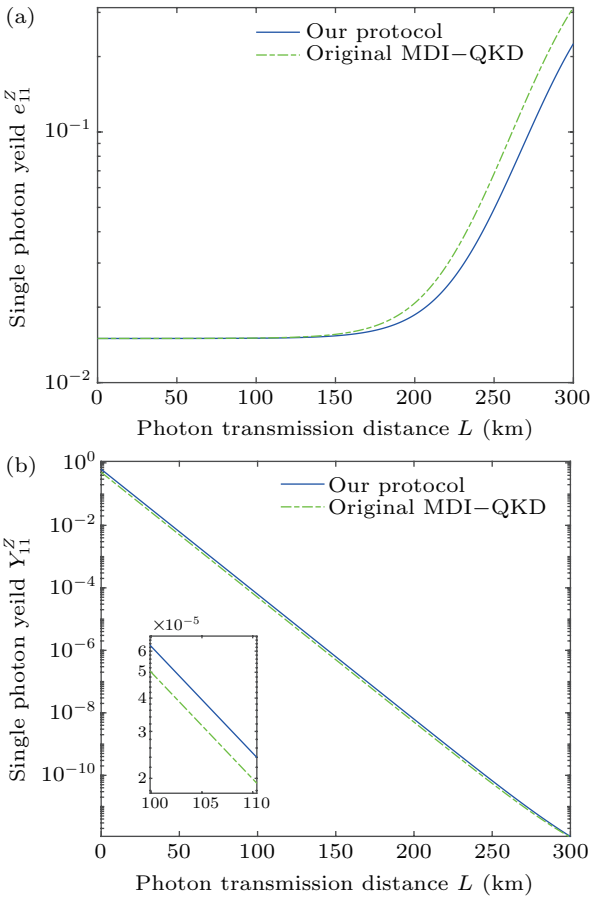


Fig. 3. Simulation results of our MDI QKD protocol with entanglement-assisted linear-optical BSM and the original MDI QKD protocol. (a) Single-photon QBER e_{11}^{Z} of our MDI QKD protocol and the original MDI QKD protocol as a function of the photon transmission distance L. (b) Single-photon yield Y_{11}^{Z} of our MDI QKD protocol and the original MDI QKD protocol.

4. Conclusion

In summary, we propose an MDI QKD protocol with entanglement-assisted linear-optical BSM. The entanglement-assisted linear-optical BSM can achieve 100% identification of $|\psi^{\pm}\rangle$ and 25% identification of $|\phi^{\pm}\rangle$, resulting in a total

identification probability of 62.5%. Moreover, this scheme has already been experimentally validated.[75] We develop a numerical model to estimate the key rate of our MDI QKD protocol and compare it with the original MDI QKD protocol using non-assisted linear-optical BSM under ideal single-photon source conditions. Simulation results show that the adoption of entanglement-assisted linear-optical BSM effectively increases the maximum photon transmission distance of the MDI QKD protocol from 262 km to 272 km. The key generation rate improves at different photon transmission distances; within 210 km, the key generation rate of our MDI QKD protocol is 25% higher than that of the original MDI QKD protocol.[47] This 25% improvement is due to the success probability of 62.5% achieved by the entanglement-assisted linear-optical BSM, compared to 50% for the non-assisted version.

Our protocol is the first to provide an in-depth discussion on the effect of entanglement-assisted linear BSM on MDI QKD and to offer theoretical results, exploring a potential development direction for MDI QKD. The entanglement-assisted method could also be applied to GHZ-state measurements, potentially improving the performance of MDI QSS.[30] Despite the inevitable reduction in key rate when using practical single-photon and entangled photon sources, the entanglement-assisted linear-optical BSM maintains a success probability of 57.9% under realistic experimental conditions,[75] enabling the protocol to achieve a higher key rate even with non-ideal sources. Over the past few years, research on single-photon sources has achieved significant progress; contemporary quantum-dot-based single-photon sources offer near-perfect multi-photon suppression, effectively approximating the performance of an ideal single-photon source for our protocol.[78,79] Based on these features, our MDI QKD protocol with entanglement-assisted linear-optical BSM holds potential for improving the performance of future quantum communication networks.

Appendix A: The principle derivation of entanglement-assisted linear BSM

In this section, we will elaborate on the process of BSM assisted by a pair of entangled photons, with the entangled state being $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$. First, we derive the interference process of two-photon states from Alice and Bob at BS_1 and BS_2 (for the convenience of calculation, we use the form of creation operators for derivation)

$$\begin{aligned}
|\phi^+\rangle_{a_1b_1} &= \frac{1}{\sqrt{2}}\left(a_{1H}^\dagger b_{1H}^\dagger + a_{1V}^\dagger b_{1V}^\dagger\right)|\text{vac}\rangle \xrightarrow{BS_1} \frac{1}{2\sqrt{2}}\left(c_{1H}^{\dagger 2} + c_{1V}^{\dagger 2} - d_{1H}^{\dagger 2} - d_{1V}^{\dagger 2}\right)|\text{vac}\rangle \\
&\xrightarrow{BS_2} \left[\frac{1}{4\sqrt{2}}\left(c_{2H}^{\dagger 2} + c_{2V}^{\dagger 2} + d_{2H}^{\dagger 2} + d_{2V}^{\dagger 2} + 2c_{2H}^\dagger d_{2H}^\dagger + 2c_{2V}^\dagger d_{2V}^\dagger\right) - \frac{1}{2\sqrt{2}}\left(d_{1H}^{\dagger 2} + d_{1V}^{\dagger 2}\right)\right]|\text{vac}\rangle, \qquad \text{(A1)} \\
|\phi^-\rangle_{a_1b_1} &= \frac{1}{\sqrt{2}}\left(a_{1H}^\dagger b_{1H}^\dagger - a_{1V}^\dagger b_{1V}^\dagger\right)|\text{vac}\rangle \xrightarrow{BS_1} \frac{1}{2\sqrt{2}}\left(c_{1H}^{\dagger 2} - c_{1V}^{\dagger 2} - d_{1H}^{\dagger 2} + d_{1V}^{\dagger 2}\right)|\text{vac}\rangle \\
&\xrightarrow{BS_2} \left[\frac{1}{4\sqrt{2}}\left(c_{2H}^{\dagger 2} - c_{2V}^{\dagger 2} + d_{2H}^{\dagger 2} - d_{2V}^{\dagger 2} + 2c_{2H}^\dagger d_{2H}^\dagger - 2c_{2V}^\dagger d_{2V}^\dagger\right) - \frac{1}{2\sqrt{2}}\left(d_{1H}^{\dagger 2} - d_{1V}^{\dagger 2}\right)\right]|\text{vac}\rangle, \qquad \text{(A2)} \\
|\psi^+\rangle_{a_1b_1} &= \frac{1}{\sqrt{2}}\left(a_{1H}^\dagger b_{1V}^\dagger + a_{1V}^\dagger b_{1H}^\dagger\right)|\text{vac}\rangle \xrightarrow{BS_1} \frac{1}{\sqrt{2}}\left(c_{1H}^\dagger c_{1V}^\dagger - d_{1H}^\dagger d_{1V}^\dagger\right)|\text{vac}\rangle \\
&\xrightarrow{BS_2} \left[\frac{1}{2\sqrt{2}}\left(c_{2H}^\dagger c_{2V}^\dagger + d_{2H}^\dagger d_{2V}^\dagger + c_{2H}^\dagger d_{2V}^\dagger + c_{2V}^\dagger d_{2H}^\dagger\right) - \frac{1}{\sqrt{2}}\left(d_{1H}^\dagger d_{1V}^\dagger\right)\right]|\text{vac}\rangle, \qquad \text{(A3)} \\
|\psi^-\rangle_{a_1b_1} &= \frac{1}{\sqrt{2}}\left(a_{1H}^\dagger b_{1V}^\dagger - a_{1V}^\dagger b_{1H}^\dagger\right)|\text{vac}\rangle \xrightarrow{BS_1} \frac{1}{\sqrt{2}}\left(c_{1V}^\dagger d_{1H}^\dagger - c_{1H}^\dagger d_{1V}^\dagger\right)|\text{vac}\rangle \\
&\xrightarrow{BS_2} \frac{1}{2}\left[\left(c_{2V}^\dagger + d_{2V}^\dagger\right)d_{1H}^\dagger - \left(c_{2H}^\dagger + d_{2H}^\dagger\right)d_{1V}^\dagger\right]|\text{vac}\rangle. \qquad \text{(A4)}
\end{aligned}$$

Then we derive the interference process of the auxiliary photons at BS_2

$$|\text{Aux}\rangle_{b_2b_2} = \frac{1}{2}\left(b_{2H}^{\dagger 2} + b_{2V}^{\dagger 2}\right)|\text{vac}\rangle \xrightarrow{BS_2} \frac{1}{4}\left(c_{2H}^{\dagger 2} + c_{2V}^{\dagger 2} + d_{2H}^{\dagger 2} + d_{2V}^{\dagger 2} - 2c_{2H}^\dagger d_{2H}^\dagger - 2c_{2V}^\dagger d_{2V}^\dagger\right)|\text{vac}\rangle. \qquad \text{(A5)}$$

By combining the above two processes, we can obtain the final output state

$$\begin{aligned}
|\phi^+\rangle_{a_1b_1} \otimes |\text{Aux}\rangle_{b_2b_2} \rightarrow\ & \frac{1}{8\sqrt{2}}\left(c_{2H}^{\dagger 2}c_{2V}^{\dagger 2} + d_{2H}^{\dagger 2}d_{2V}^{\dagger 2} + c_{2H}^{\dagger 2}d_{2V}^{\dagger 2} + c_{2V}^{\dagger 2}d_{2H}^{\dagger 2} - 4c_{2H}^\dagger c_{2V}^\dagger d_{2H}^\dagger d_{2V}^\dagger\right)|\text{vac}\rangle \\
&+ \left[\frac{1}{16\sqrt{2}}\left(c_{2H}^{\dagger 4} + c_{2V}^{\dagger 4} + d_{2H}^{\dagger 4} + d_{2V}^{\dagger 4} - 2c_{2H}^{\dagger 2}d_{2H}^{\dagger 2} - 2c_{2V}^{\dagger 2}d_{2V}^{\dagger 2}\right)\right. \\
&\left. - \frac{1}{8\sqrt{2}}\left(d_{1H}^{\dagger 2}c_{2H}^{\dagger 2} + d_{1H}^{\dagger 2}c_{2V}^{\dagger 2} + d_{1H}^{\dagger 2}d_{2H}^{\dagger 2} + d_{1H}^{\dagger 2}d_{2V}^{\dagger 2} - 2d_{1H}^{\dagger 2}c_{2H}^\dagger d_{2H}^\dagger - 2d_{1H}^{\dagger 2}c_{2V}^\dagger d_{2V}^\dagger\right.\right.
\end{aligned}$$

$$-d_{1V}^{\dagger 2}c_{2H}^{\dagger 2}+d_{1V}^{\dagger 2}c_{2V}^{\dagger 2}+d_{1V}^{\dagger 2}d_{2H}^{\dagger 2}+d_{1V}^{\dagger 2}d_{2V}^{\dagger 2}-2d_{1V}^{\dagger 2}c_{2H}^{\dagger}d_{2H}^{\dagger}-2d_{1V}^{\dagger 2}c_{2V}^{\dagger}d_{2V}^{\dagger}\Big)\Big]|\mathrm{vac}\rangle, \tag{A6}$$

$$|\phi^{-}\rangle_{a_1b_1}\otimes|\mathrm{Aux}\rangle_{b_2b_2}\rightarrow\frac{1}{4\sqrt{2}}\left(c_{2H}^{\dagger 2}c_{2V}^{\dagger}d_{2V}^{\dagger}-c_{2H}^{\dagger}c_{2V}^{\dagger 2}d_{2H}^{\dagger}+c_{2H}^{\dagger}d_{2H}^{\dagger}d_{2V}^{\dagger 2}-c_{2V}^{\dagger}d_{2H}^{\dagger 2}d_{2V}^{\dagger}\right)|\mathrm{vac}\rangle$$
$$+\Bigg[\frac{1}{16\sqrt{2}}\left(c_{2H}^{\dagger 4}+c_{2V}^{\dagger 4}+d_{2H}^{\dagger 4}+d_{2V}^{\dagger 4}-2c_{2H}^{\dagger 2}d_{2H}^{\dagger 2}-2c_{2V}^{\dagger 2}d_{2V}^{\dagger 2}\right)$$
$$-\frac{1}{8\sqrt{2}}\Big(d_{1H}^{\dagger 2}c_{2H}^{\dagger 2}+d_{1H}^{\dagger 2}c_{2V}^{\dagger 2}+d_{1H}^{\dagger 2}d_{2H}^{\dagger 2}+d_{1H}^{\dagger 2}d_{2V}^{\dagger 2}-2d_{1H}^{\dagger 2}c_{2H}^{\dagger}d_{2H}^{\dagger}-2d_{1H}^{\dagger 2}c_{2V}^{\dagger}d_{2V}^{\dagger}$$
$$-d_{1V}^{\dagger 2}c_{2H}^{\dagger 2}+d_{1V}^{\dagger 2}c_{2V}^{\dagger 2}+d_{1V}^{\dagger 2}d_{2H}^{\dagger 2}+d_{1V}^{\dagger 2}d_{2V}^{\dagger 2}-2d_{1V}^{\dagger 2}c_{2H}^{\dagger}d_{2H}^{\dagger}-2d_{1V}^{\dagger 2}c_{2V}^{\dagger}d_{2V}^{\dagger}\Big)\Bigg]|\mathrm{vac}\rangle, \tag{A7}$$

$$|\psi^{+}\rangle_{a_1b_1}\otimes|\mathrm{Aux}\rangle_{b_2b_2}\rightarrow\Bigg[\frac{1}{8\sqrt{2}}\Big(c_{2H}^{\dagger 3}c_{2V}^{\dagger}+c_{2H}^{\dagger}c_{2V}^{\dagger 3}+c_{2V}^{\dagger 3}d_{2H}^{\dagger}+c_{2V}^{\dagger}d_{2H}^{\dagger 3}+c_{2H}^{\dagger 3}d_{2V}^{\dagger}+c_{2H}^{\dagger}d_{2V}^{\dagger 3}+d_{2H}^{\dagger 3}d_{2V}^{\dagger}$$
$$+d_{2H}^{\dagger}d_{2V}^{\dagger 3}-c_{2H}^{\dagger 2}c_{2V}^{\dagger}d_{2H}^{\dagger}-c_{2H}^{\dagger}c_{2V}^{\dagger 2}d_{2V}^{\dagger}-c_{2H}^{\dagger}d_{2H}^{\dagger 2}d_{2V}^{\dagger}-c_{2V}^{\dagger}d_{2H}^{\dagger}d_{2V}^{\dagger 2}-c_{2H}^{\dagger 2}d_{2H}^{\dagger}d_{2V}^{\dagger}$$
$$-c_{2H}^{\dagger}c_{2V}^{\dagger}d_{2V}^{\dagger 2}-c_{2H}^{\dagger}c_{2V}^{\dagger}d_{2H}^{\dagger 2}-c_{2V}^{\dagger 2}d_{2H}^{\dagger}d_{2V}^{\dagger}\Big)-\frac{1}{4\sqrt{2}}\Big(d_{1H}^{\dagger}d_{1V}^{\dagger}c_{2H}^{\dagger 2}+d_{1H}^{\dagger}d_{1V}^{\dagger}c_{2V}^{\dagger 2}$$
$$+d_{1H}^{\dagger}d_{1V}^{\dagger}d_{2H}^{\dagger 2}+d_{1H}^{\dagger}d_{1V}^{\dagger}d_{2V}^{\dagger 2}-2d_{1H}^{\dagger}d_{1V}^{\dagger}c_{2H}^{\dagger}d_{2H}^{\dagger}-2d_{1H}^{\dagger}d_{1V}^{\dagger}c_{2V}^{\dagger}d_{2V}^{\dagger}\Big)\Bigg]|\mathrm{vac}\rangle, \tag{A8}$$

$$|\psi^{-}\rangle_{a_1b_1}\otimes|\mathrm{Aux}\rangle_{b_2b_2}\rightarrow\frac{1}{8}\Big(d_{1H}^{\dagger}c_{2V}^{\dagger 3}+d_{1H}^{\dagger}d_{2V}^{\dagger 3}+d_{1H}^{\dagger}c_{2V}^{\dagger}d_{2H}^{\dagger 2}+d_{1H}^{\dagger}c_{2H}^{\dagger 2}c_{2V}^{\dagger}+d_{1H}^{\dagger}c_{2H}^{\dagger 2}d_{2V}^{\dagger}-d_{1H}^{\dagger}c_{2V}^{\dagger 2}d_{2V}^{\dagger}$$
$$+d_{1H}^{\dagger}d_{2H}^{\dagger 2}d_{2V}^{\dagger}-d_{1H}^{\dagger}c_{2V}^{\dagger}d_{2V}^{\dagger 2}-2d_{1H}^{\dagger}c_{2H}^{\dagger}d_{2H}^{\dagger}d_{2V}^{\dagger}-2d_{1H}^{\dagger}c_{2H}^{\dagger}c_{2V}^{\dagger}d_{2V}^{\dagger}-d_{1V}^{\dagger}c_{2H}^{\dagger 3}$$
$$-d_{1V}^{\dagger}d_{2H}^{\dagger 3}+d_{1V}^{\dagger}c_{2H}^{\dagger}d_{2H}^{\dagger 2}-d_{1V}^{\dagger}c_{2H}^{\dagger}d_{2V}^{\dagger 2}+d_{1V}^{\dagger}c_{2H}^{\dagger 2}d_{2H}^{\dagger}-d_{1V}^{\dagger}c_{2V}^{\dagger 2}d_{2H}^{\dagger}-d_{1V}^{\dagger}c_{2H}^{\dagger}c_{2V}^{\dagger 2}$$
$$-d_{1V}^{\dagger}d_{2H}^{\dagger}d_{2V}^{\dagger 2}+2d_{1V}^{\dagger}c_{2H}^{\dagger}c_{2V}^{\dagger}d_{2V}^{\dagger}+2d_{1V}^{\dagger}c_{2V}^{\dagger}d_{2H}^{\dagger}d_{2V}^{\dagger}\Big)|\mathrm{vac}\rangle. \tag{A9}$$

From the above results, it can be seen that among the output states corresponding to $|\phi^{\pm}\rangle_{a_1b_1}$, only the first term on the right side of the equation can be recognized, while all the output states corresponding to $|\psi^{\pm}\rangle_{a_1b_1}$ can be recognized. The probabilities of all output results, after calculation, are shown in Table 1.

Acknowledgments

Project supported by the National Natural Science Foundation of China (Grant Nos. 12574393, 12175106, and 92365110), the Research Initiation Fund of the Quantum Science Center of the Guangdong–Hong Kong–Macao Greater Bay Area (Grant No. QD2305001), and the Postgraduate Research & Practice Innovation Program of Jiangsu Province (Grant No. KYCX23-0989).

References

[1] Bennett C H and DiVincenzo D P 2000 *Nature* **404** 247
[2] Degen C L, Reinhard F and Cappellaro P 2017 *Rev. Mod. Phys.* **89** 035002
[3] Gisin N and Thew R 2007 *Nat. Photonics* **1** 165
[4] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. Comput. Syst. Signal Process*, Bangalore, India, pp. 175
[5] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[6] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[7] Scarani V, Acín A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
[8] Zhao Y, Qi B, Ma X F, Lo H K and Qian L 2006 *Phys. Rev. Lett.* **96** 070502
[9] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 *Nat. Photonics* **7** 378
[10] Ma X F, Zeng P and Zhou H 2018 *Phys. Rev. X* **8** 031043
[11] 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, Zhu Y G, Morozov P V, Divochiy A V, Zhou Z, Guo G C and Han Z F 2022 *Nat. Photonics* **16** 154
[12] Huang C F, Chen Y, Jin L, Chen Y, Geng M, Wang J, Zhang Z and Wei K 2022 *Phys. Rev. A* **105** 012421
[13] Lin X, Wang R, Wang S, Yin Z Q, Chen W, Guo G C and Han Z F 2022 *Phys. Rev. Lett.* **129** 050506
[14] Li W, Zhang L, Tan H, Lu Y, Liao S K, Huang J, Li H, Wang Z, Mao H K, Yan B, Li Q, Liu Y, Zhang Q, Peng C Z, You L, Xu F and Pan J W 2023 *Nat. Photonics* **17** 416
[15] Wei K J, Hu X, Du Y Q, Hua X, Zhao Z, Chen Y, Huang C F and Xiao X 2023 *Photon. Res.* **11** 1364
[16] Huang A Q, Mizutani A, Lo H K, Makarov V and Tamaki K 2023 *Phys. Rev. Appl.* **19** 014048
[17] Feng B, Huang H D, Bian Y X, Jia W, Zhou X Y and Wang Q 2023 *Chin. Phys. B* **32** 030307
[18] Zhou C, Wang H T, Lu Y F, Jiang X L, Zhao Y M, Zhou Y, Wang Y, Li J J, Zhou Y Y, Wang X, Li H W and Bao W S 2024 *Chin. Phys. B* **33** 100302
[19] Zhang C X, Li J G, Wang Y, Chen W, Zhang J S and An J M 2025 *Chin. Phys. B* **34** 050303
[20] Liu C, Li Y, Wang H Y, Shi K Y, Ma D, Zhang Y J and Ma H Q 2025 *Chin. Phys. Lett.* **42** 010301
[21] Xu H X, Wang S H, Wang C L and Zhang P 2025 *Chin. Phys. Lett.* **42** 010303
[22] Li Y, Cai W Q, Ren J G, *et al.* 2025 *Nature* **640** 47
[23] Daniil Trefilov, Xoel Sixto, Víctor Zapatero, Anqi Huang, Marcos Curty, Vadim Makarov 2025 *Optica Quantum* **3** 417
[24] Chen Y, Huang C F, Lin G S, Huang S, Zhang Z R and Wei K J 2025 *J. Lightwave Technol.* **43** 5032
[25] Niu P H, Zhou Z R, Lin Z S, Sheng Y B, Yin L G and Long G L 2018 *Sci. Bull.* **63** 1345
[26] Zhou Z R, Sheng Y B, Niu P H, Yin L G, Long G L and Hanzo L 2020 *Sci. China Phys. Mech. Astron.* **63** 230362
[27] Ying J W, Zhou L, Zhong W and Sheng Y B 2022 *Chin. Phys. B* **31** 120303
[28] Pan D, Long G L, Yin L G, Sheng Y B, Ruan D, Ng S X, Lu J H and Hanzo L 2024 *IEEE Commun. Surv. Tutor.* **26** 1898

[29] Shukla C, Shukla A, Chatzinotas S and Nesladek M 2025 *AAPPS Bull.* **35** 20
[30] Fu Y, Yin H L, Chen T Y and Chen Z B 2015 *Phys. Rev. Lett.* **114** 090501
[31] Ju X X, Zhong W, Sheng Y B and Zhou L 2023 *Chin. Phys. B* **31** 100302
[32] Liu T G, Lai J C, Li Z H and Li T 2025 *Phys. Rev. Appl.* **23** 034057
[33] Zhang Q, Ying J W, Wang Z J, Zhong W, Du M M, Shen S T, Li X Y, Zhang A L, Gu S P, Wang X F, Zhou L and Sheng Y B 2025 *Phys. Rev. A* **111** 012603
[34] Lu Y S, Yin H L, Xie Y M, Fu Y and Chen Z B 2025 *Rep. Prog. Phys.* **88** 067901
[35] Yin H L, Fu Y, Li C L, Weng C X, Li B H, Gu J, Lu Y S, Huang S and Chen Z B 2022 *Natl. Sci. Rev.* **10** nwac228
[36] 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
[37] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[38] Ashkenazy A, Idan Y, Korn D, Fixler D, Dayan B and Cohen E 2024 *Adv. Quantum Technol.* **7** 2300437
[39] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev. A* **73** 022320
[40] Jain N, Anisimova E, Khan I, Makarov V, Marquardt C and Leuchs G 2014 *New J. Phys.* **16** 123030
[41] Qi B, Fung C H F, Lo H K and Ma X F 2007 *Quant. Inf. Comput.* **7** 073
[42] Zhao Y, Fung C H F, Qi B, Chen C and Lo H K 2008 *Phys. Rev. A* **78** 042333
[43] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photonics* **4** 686
[44] Wu Z H, Huang A Q, Chen H, Sun S H, Ding J F, Qiang X G, Fu X, Xu P and Wu J 2020 *Opt. Express* **28** 25574
[45] Xu F H, Ma X F, Zhang Q, Lo H K and Pan J W 2020 *Rev. Mod. Phys.* **92** 025002
[46] Gnanapandithan A, Qian L and Lo H K 2025 *Phys. Rev. Lett.* **134** 130802
[47] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[48] Braunstein S L and Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[49] Xu F H, Curty M, Qi B and Lo H K 2013 *New J. Phys.* **15** 113007
[50] Liu Y, Chen T Y, Wang L J, Liang H, Shentu G L, Wang J, Cui K, Yin H L, Liu N L, Li L, Ma X, Pelc J S, Fejer M M, Peng C Z, Zhang Q and Pan J W 2013 *Phys. Rev. Lett.* **111** 130502
[51] Tang Z Y, Liao Z F, Xu F H, Qi B, Qian L and Lo H K 2014 *Phys. Rev. Lett.* **112** 190503
[52] Yin H L, Chen T Y, Yu Z W, Liu H, You L X, Zhou Y H, Chen S J, Mao Y, Huang M Q, Zhang W J, Chen H, Li M J, Nolan D, Zhou F, Jiang X, Wang Z, Wang X B and Pan J W 2016 *Phys. Rev. Lett.* **117** 190501
[53] Tang G Z, Sun S H, Li C Y 2019 *Chin. Phys. Lett.* **36** 070301
[54] Wei K J, Li W, Tan H, Li Y, Min H, Zhang W J, Li H, You L X, Wang Z, Jiang X, Chen T Y, Liao S K, Peng C Z, Xu F H and Pan J W 2020 *Phys. Rev. X* **10** 031030
[55] Fan-Yuan G J, Lu F Y, Wang S, Yin Z Q, He D Y, Chen W, Wang Z H, Huang X J, Zhou Z, Wang Z H, Teng J, Guo G C and Han Z F 2022 *Optica* **9** 812
[56] Zeng P, Zhou H Y, Wu W J and Ma X F 2022 *Nat. Commun.* **13** 3903
[57] 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
[58] Zhu H T, Huang Y, Liu H, Zeng P, Zou M, Dai Y, Tang S, Li H, You L X, Wang Z, Chen Y A, Ma X, Chen T Y, and Pan J W 2023 *Phys. Rev. Lett.* **130** 030801
[59] Sun M H, Zhang C H, Ding H J, Zhou X Y, Li J and Wang Q 2023 *Phys. Rev. Appl.* **20** 024029
[60] Lu F Y, Ye P, Wang Z H, Wang S, Yin Z Q, Wang R, Huang X J, Chen W, He D Y, Fan-Yuan G J, Guo G C and Han Z F 2023 *Optica* **10** 520
[61] Sun M S, Zhang C H, Zhang R, Zhou X Y, Li J and Wang Q 2024 *Chin. Phys. B* **33** 110302
[62] Zhan X H, Zhong Z Q, Ma J Y, Wang S, Zhang Q, Chen W, Bian Z F, Huang X J, Han Z F, Chou C W, Zhang L J and Guo G C 2025 *npj Quantum Inf.* **11** 73
[63] Zhao Y M, Zhou C, Jiang X L, Lu Y F, Zhou Y, Wang H T, Wang Y, Li J J, Zhou Y Y, Li H and Bao W S 2025 *Chin. Phys. B* **34** 050302
[64] Shao S F, Zhou L, Lin J P, Minder M, Ge C F, Xie Y M, Shen A, Yan Z, Yin H L, Yuan Z 2025 *Phys. Rev. X* **15** 021066
[65] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895
[66] Bouwmeester D, Pan J W, Mattle K, Eibl M, Weinfurter H and Zeilinger A 1997 *Nature* **390** 575
[67] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[68] Mattle K, Weinfurter H, Kwiat P G and Zeilinger A 1996 *Phys. Rev. Lett.* **76** 4656
[69] Braunstein S L and Mann A 1995 *Phys. Rev. A* **51** R1727
[70] Calsamiglia J and Lütkenhaus N 2001 *Appl. Phys. B* **72** 67
[71] Barreiro J T, Wei T C and Kwiat P G 2008 *Nat. Phys.* **4** 282
[72] Hu X M, Guo Y, Liu B H, Huang Y F, Li C F and Guo G C 2018 *Sci. Adv.* **4** eaat9304
[73] Grice W P 2011 *Phys. Rev. A* **84** 042331
[74] Ewert F and van Loock P 2014 *Phys. Rev. Lett.* **113** 140403
[75] Bayerbach M J, D'Aurelio S E, van Loock P and Barz S 2023 *Sci. Adv.* **9** eadf4080
[76] Gottesman N L D, Lo H K and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[77] Ma X F and Razavi M 2012 *Phys. Rev. A* **86** 062319
[78] Wang H, He Y M, Chung T H, Hu H, Yu Y, Chen S, Ding X, Chen M C, Qin J, Yang X, Liu R Z, Duan Z C, Li J P, Gerhardt S, Winkler K, Jurkat J, Wang L J, Gregersen N, Huo Y H, Dai Q, Yu S, Höfling S, Lu C Y and Pan J W 2019 *Nat. Photonics* **13** 770
[79] Moczala-Dusanowska M, Dusanowski L, Iff O, Huber T, Kuhn S, Czyszanowski T, Schneider C and Höfling S 2020 *ACS Photonics* **7** 3474