

Measurement-device-independent quantum dialogue protocol with bidirectional identity authentication

Shi-Pu Gu(顾世浦), Jia-Wei Ying(应佳伟), Xing-Fu Wang(王兴福), Lan Zhou(周澜), and Yu-Bo Sheng(盛宇波)
Citation: Chin. Phys. B, 2025, 34 (**11**): 110308. DOI: 10.1088/1674-1056/addd81
http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Multi-hop quantum teleportation based on HSES via GHZ-like states

She-Xiang Jiang(蒋社想), Xiao-Long Wei(韦晓龙), Jin-Huan Li(李金欢), and Shuai-Shuai Li(李帅帅)
Chin. Phys. B, 2025, 34 (**1**): 010302. DOI: 10.1088/1674-1056/ad8db0

Quantum homomorphic broadcast multi-signature based on homomorphic aggregation

Xin Xu(徐鑫) and Ai-Han Yin(殷爱菡)
Chin. Phys. B, 2023, 32 (**7**): 070302. DOI: 10.1088/1674-1056/acac0e

Measurement-device-independent one-step quantum secure direct communication

Jia-Wei Ying(应佳伟), Lan Zhou(周澜), Wei Zhong(钟伟), and Yu-Bo Sheng(盛宇波)
Chin. Phys. B, 2022, 31 (**12**): 120303. DOI: 10.1088/1674-1056/ac8f37

Quantum private comparison of arbitrary single qubit states based on swap test

Xi Huang(黄曦), Yan Chang(昌燕), Wen Cheng(程稳), Min Hou(侯敏), and Shi-Bin Zhang(张仕斌)
Chin. Phys. B, 2022, 31 (**4**): 040303. DOI: 10.1088/1674-1056/ac4103

Measurement-device-independent quantum dialogue

Guo-Fang Shi(石国芳)
Chin. Phys. B, 2021, 30 (**10**): 100303. DOI: 10.1088/1674-1056/ac140a

---

Measurement-device-independent quantum dialogue protocol with bidirectional identity authentication

Shi-Pu Gu(顾世浦)[1,2], Jia-Wei Ying(应佳伟)[2], Xing-Fu Wang(王兴福)[1], Lan Zhou(周澜)[1,†], and Yu-Bo Sheng(盛宇波)[2,3]

[1] *College of Science, Nanjing University of Posts and Telecommunications, Nanjing* 210023, *China*
[2] *College of Electronic and Optical Engineering and College of Flexible Electronics (Future Technology), Nanjing University of Posts and Telecommunications, Nanjing* 210023, *China*
[3] *Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*

(Received 25 March 2025; revised manuscript received 19 May 2025; accepted manuscript online 28 May 2025)

Quantum dialogue (QD) realizes the real-time secure bidirectional quantum communication. Measurement-device-independent (MDI) QD can resist all possible attacks focusing on the imperfect measurement devices and enhance QD's practical security. However, in practical applications, any secure communication requires identity authentication as a prerequisite. In this paper, we propose an MDI QD protocol with bidirectional identity authentication. The practical communication parties can first authenticate the identity of each other simultaneously before the message exchange. In theory, our MDI QD protocol has unconditional security and the communication parties can exchange 1.5 bits of messages in each communication round with linear optical Bell state measurement. We numerically simulate the secrecy message capacity of our MDI QD protocol. Our protocol has two advantages. First, it can effectively resist the impersonation attack and enhance MDI QD's practical security. Second, it does not require keys to assist the message exchange and has relatively high efficiency. Our protocol has application potential in the future quantum communication field.

Keywords: measurement-device-independent quantum dialogue, quantum identity authentication, entanglement swapping

PACS: 03.67.Pp, 03.67.Hk, 03.65.Ud

DOI: 10.1088/1674-1056/addd81 **CSTR:** 32038.14.CPB.addd81

1. Introduction

Quantum secure direct communication (QSDC) is an important quantum communication branch.[1–3] QSDC can directly transmit secret messages through quantum channels without keys. The first QSDC protocol was proposed by Long *et al.*[1] It has also achieved great progresses in both theory and experiments.[4–23] In theory, the device-independent (DI),[5–8] measurement-device-independent (MDI),[4] receiver-device-independent (RDI),[10] and passive[11,12] QSDC protocols were proposed to enhance QSDC's practical security. In 2022, one-step QSDC protocol was put forward, which can reduce the message loss and simplify the experimental operation.[9] Recently, the quantum error correction code was introduced in QSDC to enhance its noise robustness.[13] In experiment, the single-photon and entanglement-based QSDC protocols were successively demonstrated in 2016 and 2017, respectively.[16,17] In 2022, QSDC achieved the communication distance of 100 km.[21] The QSDC network was also reported.[22] A recent work proposed a theory of one-way QSDC and successfully developed a practical system, advancing QSDC from a concept to the stage of practical application.[23]

QSDC can also be used to realize the bidirectional quantum direct communication, i.e., quantum dialogue (QD). In 2004, Nguyen *et al.*[24] proposed the first QD protocol. Since then, various QD protocols have been proposed.[25–33] Man *et al.*[25] proposed an improved QD protocol which could resist the intercept-resent attack. Subsequently, QD protocols based on entanglement swapping, single-photons, and continuous-variable two-mode squeezed vacuum states were proposed, respectively.[28,29] However, like QKD and QSDC, the practical security of QD protocols depends on two aspects. The first is the perfect devices, such as the ideal signal sources and single-photon detectors. The second is that both communication parties in quantum communication must be legal. Unfortunately, the practical signal sources and single-photon detectors are imperfect which will cause the security loophole for QSS,[34] such as the time-shift attack,[35,36] fake-sate attack,[37] and glare blinding attack.[38,39] The concept of MDI was first proposed in QKD system.[40–42] Later, MDI theory was exploited in QSDC and QD.[4,43–48] MDI QD protocols can resist all possible attacks from imperfect measurement devices and greatly enhance QD's practical security. In 2021, the reference-frame-independent (RFI) MDI QD protocol was proposed, which can eliminate the high requirement for the reference frames alignment in both parties' locations.[45] In

†Corresponding author. E-mail: zhoul@njupt.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.

2021, a high-capacity hyperentanglement-based MDI QD[47] protocol was proposed, which can effectively increase MDI QD's secret message capacity. In 2024, Zhang *et al.* put forward the MDI QD with phase encoding.[48] However, previous MDI QD protocols cannot solve the communication parties legality authentication problem. The concept of quantum identity authentication (QIA) was proposed to authenticate the legality of practical communicators. The QIA protocols with single particles and entanglement[49–54] were proposed. In this way, introduce QIA into MDI QD is a promising method to solve MDI QD's communicator legality authentication problem.

In this paper, we propose an MDI QD protocol with bidirectional identity authentication. In this protocol, two practical communication parties first authenticate the identity of each other simultaneously. Only when the bidirectional identity authentication is passed, the parties will exchange the messages. In theory, our protocol has unconditional security and the communication parties can exchange 1.5 bits of messages in each communication round with linear optical Bell state measurement (BSM). We numerically simulate the secrecy message capacity of our MDI QD protocol. Our protocol has some advantages. First, our protocol can effectively resist the impersonation attack from the eavesdropper (Eve) and enhance MDI QD's practical security. Second, it does not require keys to assist the message exchange and has relatively high efficiency. Our MDI QD protocol with bidirectional identity authentication has application potential in the future quantum communication field.

This paper is organized as follows. In Section 2, we explain the basic principle of the MDI QD protocol with bidirectional identity authentication. In Section 3, a specific example is proposed. In Section 4, we perform the security analysis of our protocol. In Section 5, we numerically simulate its secret message capacity. Finally, we make some discussion and draw a conclusion in Section 6.

2. The MDI QD protocol with bidirectional identity authentication

Suppose that two legitimate parties Alice' and Bob' share the identity code strings K_{A} and K_{B} in advance with the method of QKD. K_{A} and K_{B} can be described as

$$\begin{aligned} K_{\mathrm{A}} &= (K_{\mathrm{A}1}, K_{\mathrm{A}2}, K_{\mathrm{A}3}, \ldots, K_{\mathrm{A}n}), \\ K_{\mathrm{B}} &= (K_{\mathrm{B}1}, K_{\mathrm{B}2}, K_{\mathrm{B}3}, \ldots, K_{\mathrm{B}n}), \end{aligned} \tag{1}$$

where n is a large number.

In the protocol, the actual communication parties Alice and Bob should first authenticate each other's identity. Here, we suppose that at least one practical communication party is legal. The basic principle of the MDI QD protocol with the bidirectional identity authentication is shown in Fig. 1, which includes the following 8 steps.

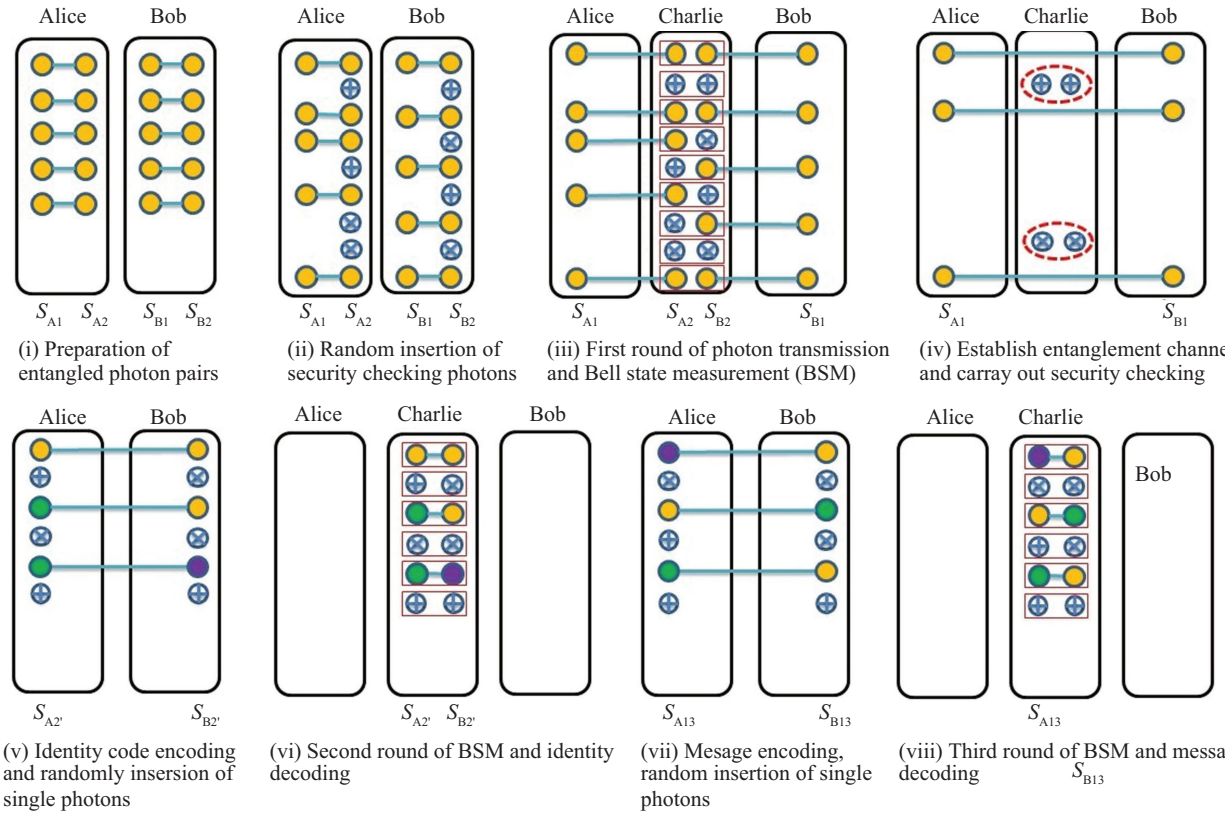


Fig. 1. Illustration of the MDI QD protocol with bidirectional identity authentication. The orange balls connected by solid line represent the initial entangled photon pairs, and the white balls with "+" and "×" represent the single photons under the Z and X basis, respectively. The green and purple balls represent the encoded photons.

Step 1. Alice prepares N entangled photon pairs randomly in $|\phi^+\rangle$ or $|\phi^-\rangle$, while Bob randomly prepares N entangled photon pairs randomly in $|\phi^+\rangle$ or $|\psi^+\rangle$ (N is much greater than the length of each identity code string n). $|\phi^\pm\rangle$ and $|\psi^+\rangle$ belong to four polarized Bell states as

$$\begin{aligned}|\psi^\pm\rangle &= \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle),\\ |\phi^\pm\rangle &= \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle),\end{aligned} \tag{2}$$

where $|H\rangle$ and$|V\rangle$ represent the horizontal and vertical polarization states, respectively. The entangled photon pairs form the photon sequences $S_{\rm A1}$ and $S_{\rm A2}$ ($S_{\rm B1}$ and $S_{\rm B2}$) in Alice's (Bob's) locations.

Step 2. Alice (Bob) prepares a large number of single photons randomly in the rectilinear (Z) basis or dialogue (X) basis as the security checking photons, which are represented as

$$\begin{aligned}Z =&\ \{|H\rangle, |V\rangle\},\\ X =&\ \{|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)\}.\end{aligned} \tag{3}$$

In this way, the single photons are randomly in four quantum states, $|H\rangle$, $|V\rangle$, $|+\rangle$, and $|-\rangle$. Alice (Bob) randomly inserts the single photons in the photon sequence $S_{\rm A2}$ ($S_{\rm B2}$).

Step 3. Alice and Bob send the photons in $S_{\rm A2}$ and $S_{\rm B2}$ sequences to the third party Charlie through quantum channels, and store the photons in $S_{\rm A1}$ and $S_{\rm B1}$ sequences in the quantum memories. Here, Charlie can be untrusted or even controlled by the eavesdropper (Eve). Charlie performs the complete Bell state measurement (CBSM) for the received photon pairs in turn and announces the measurement results.

Step 4. Alice and Bob announce the position and quantum state of each single photon in $S_{\rm A2}$ and $S_{\rm B2}$ sequences through classical channels. There are four cases as follows. First, if both the photons for the CBSM come from the entangled photon pairs, the corresponding photons in $S_{\rm A1}$ and $S_{\rm B1}$ sequences establish an entanglement channel through the entanglement swapping. We explain the cases of $|\phi^\pm\rangle_{S_{\rm A1}S_{\rm A2}} \otimes |\phi^+\rangle_{S_{\rm B1}S_{\rm B2}}$ and $|\phi^\pm\rangle_{S_{\rm A1}S_{\rm A2}} \otimes |\psi^+\rangle_{S_{\rm B1}S_{\rm B2}}$. The entanglement swapping processes can be described as follows:

$$\begin{aligned}|\phi^\pm\rangle_{S_{\rm A1}S_{\rm A2}} \otimes |\phi^+\rangle_{S_{\rm B1}S_{\rm B2}} &= \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle)_{S_{\rm A1}S_{\rm A2}} \otimes \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)_{S_{\rm B1}S_{\rm B2}}\\ &= \frac{1}{2}(|\phi^+\rangle_{S_{\rm A2}S_{\rm B2}} \otimes |\phi^\pm\rangle_{S_{\rm A1}S_{\rm B1}} + |\phi^-\rangle_{S_{\rm A2}S_{\rm B2}} \otimes |\phi^\mp\rangle_{S_{\rm A1}S_{\rm B1}} + |\psi^+\rangle_{S_{\rm A2}S_{\rm B2}} \otimes |\psi^\pm\rangle_{S_{\rm A1}S_{\rm B1}}\\ &\quad + |\psi^-\rangle_{S_{\rm A2}S_{\rm B2}} \otimes |\psi^\mp\rangle_{S_{\rm A1}S_{\rm B1}}),\\ |\phi^\pm\rangle_{S_{\rm A1}S_{\rm A2}} \otimes |\psi^+\rangle_{S_{\rm B1}S_{\rm B2}} &= \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle)_{S_{\rm A1}S_{\rm A2}} \otimes \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle)_{S_{\rm B1}S_{\rm B2}}\\ &= \frac{1}{2}(|\phi^+\rangle_{S_{\rm A2}S_{\rm B2}} \otimes |\psi^\pm\rangle_{S_{\rm A1}S_{\rm B1}} + |\phi^-\rangle_{S_{\rm A2}S_{\rm B2}} \otimes |\psi^\mp\rangle_{S_{\rm A1}S_{\rm B1}} + |\psi^+\rangle_{S_{\rm A2}S_{\rm B2}} \otimes |\phi^\pm\rangle_{S_{\rm A1}S_{\rm B1}}\\ &\quad + |\psi^-\rangle_{S_{\rm A2}S_{\rm B2}} \otimes |\phi^\mp\rangle_{S_{\rm A1}S_{\rm B1}}).\end{aligned} \tag{4}$$

Based on the CBSM results, Alice and Bob can construct the long-distance entanglement channel. Alice can only determinate the phase, and Bob can only determinate the parity of the constructed entanglement channel, respectively. As the initial Bell states are private, any external party, including Charlie can not obtain the information of the entanglement channel.

Second, if one of the two photons for the CBSM is a single photon and the other one is from the entangled photon pair, the CBSM result and the remaining photons in the entangled photon pair should be discarded. Third, if the two photons for the CBSM are both single photons with different generation bases, the CBSM result should be discarded.

Forth, if the two photons for the CBSM are both single photons with the same generation basis, Alice and Bob can perform the first round of security checking according to the CBSM result. In detail, if two single photons are both in Z basis, say, $|H\rangle|V\rangle$, $|V\rangle|H\rangle$, $|H\rangle|H\rangle$, or $|V\rangle|V\rangle$. The BSM process can be written as

$$|H\rangle|V\rangle = \frac{1}{\sqrt{2}}(|\psi^+\rangle + |\psi^-\rangle),\ \ |V\rangle|H\rangle = \frac{1}{\sqrt{2}}(|\psi^+\rangle - |\psi^-\rangle),\ \ |H\rangle|H\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\phi^-\rangle),\ \ |V\rangle|V\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\phi^-\rangle). \tag{5}$$

If the CBSM result of $|H\rangle|V\rangle$ and $|V\rangle|H\rangle$ is $|\phi^\pm\rangle$, or the BSM result result of $|H\rangle|H\rangle$ and $|V\rangle|V\rangle$ is $|\psi^\pm\rangle$, both parties can determine that an error occurrs. If two single photons are both in X basis, say, $|+\rangle|+\rangle$, $|+\rangle|-\rangle$, $|-\rangle|+\rangle$, or $|-\rangle|-\rangle$. The CBSM process can be written as

$$|+\rangle|+\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\psi^+\rangle),\ \ |+\rangle|-\rangle = \frac{1}{\sqrt{2}}(|\phi^-\rangle - |\psi^-\rangle),\ \ |-\rangle|+\rangle = \frac{1}{\sqrt{2}}(|\phi^-\rangle + |\psi^-\rangle),\ \ |-\rangle|-\rangle = \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\psi^+\rangle). \tag{6}$$

If the CBSM result is different from the above formulas, both parties determine that an error occurs. After the security checking, Alice and Bob estimate the error rate. If the error rate exceeds the tolerable threshold, the first round of photon transmission is not secure. The parties should discard the communication. If the error rate is lower than the tolerable threshold, the parties proceed to the next step.

Step 5. Alice randomly selects enough number of photons in S_{A1} sequence as the authentication photons and announces their positions. The two parties distill the authentication photon pairs to form the photon sequences S_{AI1} and S_{BI1}. Alice encodes the photons in S_{AI1} sequence using parity-encoding rule. Bob encodes the photons in S_{BI1} sequence based on the phase-coding rule. The parity-encoding rule is that $U_0 = I = |H\rangle\langle H| + |V\rangle\langle V|$ represents the identity code 0 and $U_{\mathrm{b}} = \sigma_x = |H\rangle\langle V| + |V\rangle\langle H|$ represents the identity code 1. The phase-coding rule is that $U_0 = I$ represents the identity code 0 and $U_{\mathrm{p}} = \sigma_z = |H\rangle\langle H| - |V\rangle\langle V|$ represents the identity code 1. Then, Alice and Bob randomly generate a large number of security checking single photons in Z basis or X basis, and randomly insert them into the sequences S_{AI1} and S_{BI1} to form the sequences $S_{\mathrm{AI1}'}$ and $S_{\mathrm{BI1}'}$.

Step 6. Alice and Bob send the sequences $S_{\mathrm{AI1}'}$ and $S_{\mathrm{BI1}'}$ to Charlie for the second round of CBSM. Charlie announces all the CBSM results. Then, Alice and Bob announce the locations and quantum states of the the security checking. Similar as step 4, there are also four cases. First, if both the photons for the CBSM are from an encoded entangled pair, Alice and Bob can read out the encoded identity code based on the CBSM result.

Second, if the photons for the CBSM are from different entangled pairs, or one photon is the single photon and the other photon is from the encoded entangled pair, Alice and Bob should discard the CBSM results and the encoded identity codes. Third, if both photons are single photons in different generation basis, the parties should discard the CBSM results. Forth, if both photons for the CBSM are the single photons in the same generation basis, the CBSM results are used for the second round of security checking, which is the same as that in step 4. The parties go to the next step only when the security checking is passed.

It is noticed that some identity codes may be discarded due to the mismatch of photons for the CBSM. In practical implementation, Alice and Bob should record the positions of the lost identity codes. They should repeat the above steps until they check all the identity codes from each other. Then, they estimate the error rate of each other's identity codes. If the error rate of one practical party's identity code is lower than the tolerable threshold, the practical party can be authenticated as the legal party. Only when both practical parties are legal, the parties go to the next step. Otherwise, the communication should be discarded.

Step 7. Alice and Bob distill the remained photons in sequences S_{A1} and S_{B1} for the message coding, respectively. Similarly as step 5, Alice encodes the remained photons in S_{A1} sequence based on the parity-encoding rule, and Bob encodes the remained photons in S_{B1} sequence based on the phase-coding rule. For Alice, U_0 represents the message 0 and U_{b} represents the message 1. For Bob, U_0 represents the message 0 and U_{p} represents the message 1. After encoding, they each randomly prepare a large number of single photons in Z or X basis and randomly insert the single photons in S_{A1} and S_{B1} sequences to form new sequences S_{AI3} and S_{BI3}.

Step 8. The photons in S_{AI3} and S_{BI3} sequences are sent to Charlie for the third round of CBSM. After the CBSM, Alice and Bob announce the positions and quantum states of the inserted single photons. If both photons are single photons in the same generation basis, the CBSM result is used for security checking, similar as step 4. If both photons are from the same entangled photon pair, Alice and Bob can read out each other's encoded messages. For example, if the initial entangled state is $|\psi^-\rangle_{S_{\mathrm{A1}}S_{\mathrm{B1}}}$ (Alice only knows its phase and Bob only knows its parity) and the announced CBSM result is $|\psi^+\rangle_{S_{\mathrm{A1}}S_{\mathrm{B1}}}$. Alice can deduce that Bob's operation is U_{p} corresponding to the classical message 1 while Bob can deduce Alice's operation is U_0 corresponding to the classical message 0. It is noticed that only when the third security checking is passed, Alice and Bob will preserve the transmitted messages. If the security checking is not passed, they should discard the transmitted message. If the photons for the CBSM are single photons in different generation basis, one photon is the single photon and the other photon is from the entangled photon pair, or single photons from two different entangled photon pairs, the CBSM results and the encoded messages should be discarded.

Some encoded messages may be also discarded due to the mismatch of the photons. Alice and Bob should record the lost messages and repeat the protocol until they obtain all the messages.

3. A specific example of the MDI QD protocol with bidirectional identity authentication

In Section 2, our MDI-QD protocol requires the CBSM to distinguish all the four polarization Bell states. However, the CBSM is still a challenging under current experimental condition. For enhancing its practicality, we replace the CBSM with partial linear optical BSM to realize the MDI-QD. The partial BSM can only distinguish two polarization Bell states $|\psi^{\pm}\rangle$, but cannot distinguish the phase of $|\phi^{\pm}\rangle$. We provide the specific implementation of our MDI-QD protocol with the partial BSM in Fig. 2. In security checking and entanglement channel construction processes, if the partial BSM obtains $|\phi^{\pm}\rangle$,

the communication parties will discard the results and the corresponding remaining photons. Only when Charlie obtains the conclusive BSM results, the BSM results are used for security checking and entanglement channel construction. In the identity authentication and message decoding processes, as Alice performs the parity encoding, the adoption of the partial BSM would not influence Alice's message transmission. However, as Bob performs the phase encoding, when the BSM obtains the unconclusive results ($|\phi^{\pm}\rangle$), the parties have to discard Bob's corresponding messages. Bob should record the positions of the discarded messages and encode the messages on the next communication rounds until all the lost messages are successfully transmitted to Alice. In statistics, we assume that the partial BSM obtains the unconclusive results with the probability of $1/2$. In this case, Alice and Bob can exchange 1.5 bit of messages per communication round.

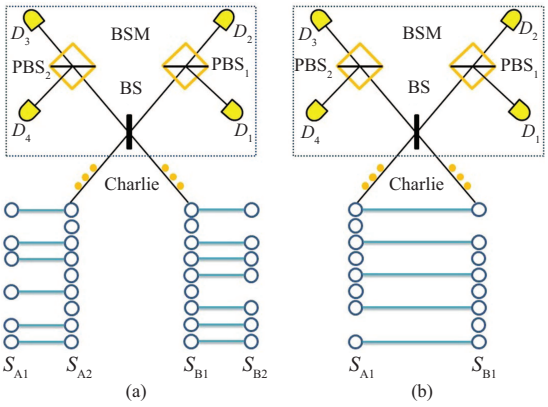


Fig. 2. The specific implementation of our MDI-QD protocol with practical partial Bell state measurement. Here, BS and PBS represent the 50 : 50 beam splitter and the polarization beam splitter, respectively. D_i $(i = 1,2,3,4)$ is the single photon detector. The clicks in D_1D_3 or D_2D_4 correspond to the Bell state $|\psi^-\rangle$, while the clicks in D_1D_2 or D_3D_4 correspond to the Bell state $|\psi^+\rangle$.

Here, we provide a specific example of our MDI QD protocol with bidirectional identity authentication. We neglect the security checking processes for simplicity.

First, suppose that the identity code string of the legal party Alice' is $\{0,1,1,0,1,0,0,\ldots\}$ and that of the legal party Bob' is $\{1,1,0,0,1,0,1,\ldots\}$. The practical parties Alice and Bob should send their identity code string to each other to authenticate their identity. For guaranteeing the security of their identity code strings, the identity code strings are one-time pad. We take the case that Alice and Bob exchange the first identity codes 0 and 1 for example.

Suppose that Alice generates the Bell state $|\phi^+\rangle_{S_{A1}S_{A2}}$ and Bob generates the Bell state $|\psi^+\rangle_{S_{B1}S_{B2}}$. They send the photons in S_{A2} and S_{B2} sequences to Charlie for the BSM. The entanglement swapping process is shown in Eq. (4). Suppose the BSM result is $|\psi^+\rangle_{S_{A2}S_{B2}}$, so that Alice and Bob can construct the entanglement channel as $|\phi^+\rangle_{S_{A1}S_{B1}}$ (Alice can only determinate the phase $+$, and Bob can only determinate the parity $|\phi\rangle$ of the Bell state). Then, Alice and Bob encode their identity code 0 and 1 on the entangled photon pair with the unitary operations I and U_p, respectively. After encoding, they send the photons in S_{A1} and S_{B1} sequences to Charlie for the BSM. According to the BSM result $|\psi^+\rangle_{S_{A1}S_{B1}}$, Alice can deduce Bob's operation as U_p and Bob can obtain Alice's operation as I, so that they can exchange the identity codes 0 and 1, respectively.

Then, Alice and Bob encode their messages on the message entangled photon pairs. Suppose that Alice's message is 1 and Bob's message is 1, and the initial entangled photon pair in S_{A1} and S_{B1} sequences is in $|\phi^-\rangle_{S_{A1}S_{B1}}$. Under this case, Alice and Bob perform the operations U_b and U_p on their photons, respectively, and the quantum state of the encoded photon pair is transformed to $|\psi^+\rangle_{S_{A1}S_{B1}}$. After Charlie announcing his BSM result, the parties can deduce the operations from each other and exchange the secure messages.

4. Security analysis

In this section, we will discuss the security of our MDI QD protocol with bidirectional identity authentication. We consider the case that during the communication process, Eve may pretend to be a legal communication party to steal the messages (impersonation attack), or perform the collective attack (intercept-measure-resend attack). We will show that our protocol is secure against above two attacks.

(i) Impersonation Attack. In step 5 and step 6 of our protocol, the practical parties Alice and Bob should exchange their own identity codes. Considering the channel noise and imperfect quantum state generation may cause the error of identity authentication, for any party, only when the error rate of the identity code is lower than the tolerable threshold, the identity authentication is passed. If the practical communication party is not the legal party, he may guess the wrong identity code with the probability of 50%, so that the illegal party can successfully impersonate Alice (Bob) with the probability of $(\frac{1}{2})^n$. As the number (n) of the identity codes is large, the probability $(\frac{1}{2})^n$ approximates 0. In this way, our protocol can effectively resist the impersonation attack. Moreover, as the identity code string of each party is one-time pad, even if one illegal party obtains the identity code string of the legitimate one, he cannot use the identity code string to impersonate the legal party.

(ii) Collective attack. The security of our MDI-QD protocol against the collective attack is the same as that of the MDI QSDC protocol.[4] As all the measurements are performed by the untrusted third party Charlie, our protocol can resist all possible attacks from the measurement device. However, Eve can intercept the photons during the photon transmission process with certain probability. He randomly uses Z basis or X basis to measure the intercepted photons. Then, he generates new photons based on his measurement results and sends

the new photons to Charlie for the BSM. Eve's attack would threaten the communication security and disturb the communication. However, the above attack can be detected by the security checking. After each photon transmission process, the parties would perform the security checking. As Eve has no information about the position of the security checking photons during the photon transmission process, he may inevitably intercept some of the security checking photons. He may guess wrong measurement basis with the probability of 50%. If Eve chooses the wrong basis, Charlie's BSM result will be wrong with the probability of $1/2$. Thus, the probability of Eve being detected is $(1/2)^2 = 1/4$. Actually, as the number of security checking photons is very large, the total probability of Eve being detected is $1-(3/4)^M$, which is approximately 1. On the other hand, Eve can control Charlie to deliberately announce wrong BSM result with certain probability, which would also disturb the message transmission. However, as Charlie does not know the positions of the security checking photons, the case that he deliberately announces wron BSM result would also increase the error rate of security checking, and thus being detected by the communication parties.

5. Numerical simulation of the MDI-QD protocol's secret message capacity under practical experimental condition.

In this section, we simulate the secret message capacity (C_s) of our MDI-DQ protocol with bidirectional identity authentication in the practical imperfect experimental condition. C_s is defined as the amount of transmitted correct and secure qubits divided by the total amount of the encoded photon pair. With the partial BSM, one encoded photon pair can transmit 1.5 bits of secrete messages in theory. In practical condition, we must consider all the practical imperfect factors, such as the imperfect photon source, imperfect photon detector and channel noise. In this way, C_s can be lower bounded by[55]

$$C_s \geq 1.5\left\{Q_2^{1,1}[1-H(e_2^{1,1})]-Q_{t1}H(E_{t1})\right\}. \tag{7}$$

Here, Q_{t1} and E_{t1} are the total gain and total error rate after one round of photon transmission, and $Q_2^{n,m}$ and $e_2^{n,m}$ represent the gain and error rate after two rounds of photon transmission corresponding to Alice generating n entangled photon pairs while Bob generating m entangled photon pairs.

Here, we suppose that each party adopts the practical spontaneous parametric down-conversion (SPDC) source to generate the entangled photon pairs. As $p' \ll 1$, we only consider that the source generates the vacuum state with the probability of $1-p'-p'^2$, one entangled photon pair with the probability of p' and two entangled photon pairs with the probability of p'^2 ($p' \sim 10^{-3}$),[56] and neglect the higher order term.

Here, we suppose that Alice and Bob employ the optical switch and quantum nondemolition detection (QND) gate constructed with the cross-Kerr nonlinearities on the two emitted photon pulses. Only when each SPDC source emits exactly one entangled photon pair, the optical switch will let the photon enter the partial BSM devices, so that we can obtain $Q_{t1} = Q_1^{1,1}$ and $E_{t1} = e_1^{1,1}$. In this way, equation (7) can be simplified to

$$C_s = 1.5\left\{Q_2^{1,1}[1-H(e_2^{1,1})]-Q_1^{1,1}H(e_1^{1,1})\right\}. \tag{8}$$

Next, we calculate $Q_1^{1,1}$, $Q_2^{1,1}$, $e_1^{1,1}$, and $e_2^{1,1}$. We suppose that Charlie locates in the middle of Alice and Bob, and the distance between Charlie and Alice (Bob) is d. As a result, the channel transmission efficiency is $t_a = t_b = 10^{-\alpha d/10}$, where α =0.2 db/km for a standard optical fiber. After each photon transmission, we set the basis misalignment error rates as e_m. We also consider the decoherence caused by the channel noise. Suppose that the decoherence may cause the bit-flip error or phase-flip error with the same probability of $(1-F)/2$ after each photon transmission. We take the target entangled state $|\phi^+\rangle$ as an example. After the first and second round of photon transmissions, the entangled states degrade to the mixed states as

$$\begin{aligned}\rho_1 &= F|\phi^+\rangle\langle\phi^+| + \frac{1-F}{2}|\psi^+\rangle\langle\psi^+| + \frac{1-F}{2}|\phi^-\rangle\langle\phi^-|,\\ \rho_2 &= \left[F^2+\frac{(1-F)^2}{2}\right]|\phi^+\rangle\langle\phi^+| + F(1-F)|\psi^+\rangle\langle\psi^+| + F(1-F)|\phi^-\rangle\langle\phi^-| + \frac{(1-F)^2}{2}|\psi^-\rangle\langle\psi^-|.\end{aligned} \tag{9}$$

In addition, we define the inherent efficiency η_{l1} as the product of the coupling efficiency (η_c) between the photon and the fiber, the detection efficiency η_d of the single photon detector. In this way, we can obtain the error rate $e_1^{1,1}$ and the yield $Y_1^{1,1}$ after the first photon transmission round as given in the following expressions:

$$Y_1^{1,1} = t_a t_b \eta_{l1}^2 = 10^{-2\alpha d/10} \times \eta_{l1}^2,$$

$$e_1^{1,1} = 1 - F(1-e_m). \tag{10}$$

After the construction of entanglement channel, Alice and Bob distill the remaining photons from quantum memory devices for encoding. Then, they send the encoded photons to Charlie for the partial BSM. We set the inherent efficiency η_{l2} as the product of η_c, η_d, and the efficiency (η_m) of the quantum memory. The error rate $e_2^{1,1}$ and the yield $Y_2^{1,1}$ after the second

round of photon transmission can be calculated as follows:

$$Y_2^{1,1} = t_a t_b \eta_{l2}^2 = 10^{-2\alpha d/10} \times \eta_{l2}^2,$$
$$e_2^{1,1} = 1 - [F^2 + \frac{(1-F)^2}{2}](1-e_m)^2. \quad (11)$$

Based on above calculation, $Q_1^{1,1}$ and $Q_2^{1,1}$ can be derived as

$$Q_1^{1,1} = p' Y_1^{1,1}, \qquad Q_2^{1,1} = p' Y_1^{1,1} Y_2^{1,1}. \quad (12)$$

Taking Eqs. (10)–(12) to Eq. (8), we can calculate the lower bound of C_s.

In Fig. 3, we provide C_s per pulse altered with the communication distance $2d$ from Alice to Bob. We set that $p' = 10^{-3}$,[56] $e_m = 1.5\%$,[57] $\eta_{11} = 90\%$ and $\eta_{12} = 81\%$, and adjust F =1, 0.98, respectively. It can be found that the fidelity F seriously influence the C_s and maximum communication distance. When F =1 and 0.98, the maximum communication distances of our MDI QD protocol are about 33.6 km and 14 km, respectively. When $F = 1$, C_s under the communication distance of 5 km and 10 km are about 2.97×10^{-4} and 1.70×10^{-4}, respectively. When $F = 0.98$, C_s under the communication distance of 5 km and 10 km are about 1.13×10^{-4} and 3.69×10^{-5}, respectively.

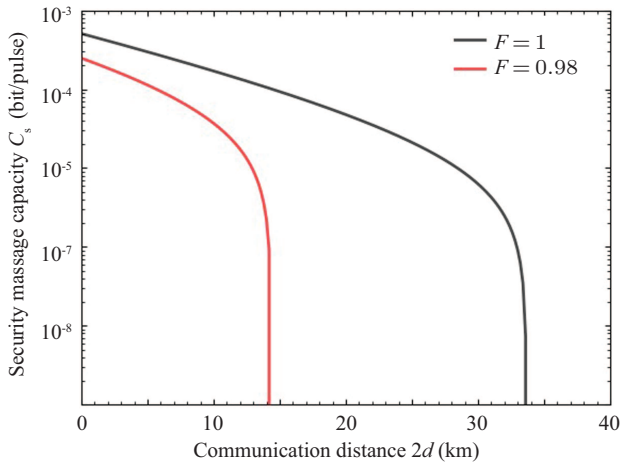


Fig. 3. The secrete message capacity (C_s) per pulse altered with the communication distance $2d$ from Alice to Bob. Here, we suppose that Alice and Bob use the SPDC sources to generate entangled states with $p' = 10^{-3}$. During each photon transmission process, we set the basis misalignment error rate as $e_m = 1.5\%$, the inherent efficiency as $\eta_{11} = 90\%$ and $\eta_{12} = 81\%$. We adjust the fidelity F =1, 0.98, respectively.

6. Discussion and summary

It is interesting to compare our MDI QD protocol with previous MDI QD protocols.[44–48] In the paper, we first introduce the bidirectional identity authentication in the MDI QD, which enables two practical communication parties to authenticate the identity of each other simultaneously. Once the authentication of any party is not passed, the other party will discard the communication. In this way, our MDI QD protocol can effectively resist the impersonation attack, which can further enhance MDI QD's practical security. Besides that, some previous MDI QD protocols require the communication parties to share a sequence of keys by QKD in advance.[44,45] However, Eve can attack the key distribution process taking use of the practical imperfect measurement devices. It will open the security loophole for the QD process.

The MDI QD protocols in Ref. [48] does not require any keys in advance, where each communication round uses six pairs of polarized Bell states and three rounds of BSM, and Alice and Bob can totally exchange 2 bits of messages in theory. Our MDI QD protocol does not require keys to assist the message exchange either. Each communication round uses two pairs of polarized Bell states and two rounds of BSM. The parties can also exchange 1.5 bits of messages in theory. In this way, under the same experimental condition (SPDC source and noisy channels), we can obtain that the raw value of C_s of our MDI QD protocol is 16 orders of magnitude higher than that of the protocol in Ref. [48]. In this way, our MDI QD protocol is more efficient than that in Ref. [48].

QM is also a key element of our MDI QD protocol. The photons in S_{A1} and S_{B1} sequences should be stored in QM devices and distilled sequentially for identity code encoding and message encoding, respectively. QM technique has developed rapidly in recent years.[58–61] In 2019, Guo *et al.* realized the high-performance atomic Raman memory with the memory efficiency of above 82.0% for 6 ns-20 ns optical pulses and the fidelity of up to 98.0%.[58] Soon later, the experiment of the coherent light storage in an atomic frequency comb memory over 1 hour was reported.[60] Based on above progresses in QM, our MDI QD protocol with bidirectional identity authentication has application potential in the near future.

In conclusion, QD can realize the real-time secure bidirectional communication. MDI QD can resist all possible attacks from imperfect measurement devices and enhance QD's security under practical imperfect experimental condition. However, similar as the other quantum communication branches, only when the practical communication parties are legal, the practical security of MDI QD can be ensured. In the paper, we propose the MDI QD protocol with bidirectional identity authentication. The practical communication parties first authenticate the identity of each other simultaneously. Only when the bidirectional identity authentication is passed, the parties will exchange the messages. In our MDI QD protocol, the communication parties can exchange 1.5 bits of messages in each communication round with practical linear optical BSM in theory. The security of each photon transmission is guaranteed by the security checking. Our MDI QD protocol has unconditional security in theory. We numerically simulated its secrecy message capacity. The simulation results show that when F =1 and 0.98, the maximum communication distances of our MDI QD protocol are about 33.6 km and

14 km, respectively. Compared with previous MDI QD protocols, our protocol has some advantages. First, our MDI QD protocol can effectively resist Eve's impersonation attack and enhance MDI QD's practical security. Second, it does not require keys to assist the message exchange and has relatively high efficiency. Based on above features, our MDI QD protocol has application potential in the future quantum communication field.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant Nos. 12175106 and 92365110) and the Postgraduate Research and Practice Innovation Program of Jiangsu Province, China (Grant No. KYCX23-0987).

References

[1] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[2] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[3] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[4] 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
[5] Zhou L, Sheng Y B and Long G L 2020 *Sci. Bull.* **65** 12
[6] Zhou L and Sheng Y B 2022 *Sci. China Phys. Mech. Astron.* **65** 250311
[7] Zhou L, Xu B W, Zhong W and Sheng Y B 2023 *Phys. Rev. Appl.* **19** 014036
[8] Zeng H, Du M M, Zhong W, Zhou L and Sheng Y B 2024 *Funda. Res.* **4** 851
[9] Sheng Y B, Zhou L and Long G L 2022 *Sci. Bull.* **67** 367
[10] Liu C, Zhang C, Gu S P, Wang X F, Zhou L and Sheng Y B 2025 *Sci. China Phys. Mech. Astron.* **68** 250311
[11] Ying J W, Zhao P, Zhong W, Du M M, Li X Y, Shen S T, Zhang A L, Zhou L and Sheng Y B 2024 *Phys. Rev. Appl.* **22** 024040
[12] Ying J W, Wang J Y, Xiao Y X, Gu S P, Wang X F, Zhong W, Du M M, Li X Y, Shen S T, Zhang A L, Zhou L and Sheng Y B 2025 *Sci. China Phys. Mech. Astron.* **68** 240312
[13] Ding C W, Wang W Y, Zhang W D, Zhou L and Sheng Y B 2025 *Appl. Phys. Lett.* **126** 024002
[14] Cao Z W, Zhang Y J, Chai G, Liang Z T, Chen X L, Wang L and Wang Y J 2025 *Chin. Phys. B* **34** 030303
[15] Cao Z W, Wang Y J, Chai G, Chen X L and Lu Y 2025 *Chin. Phys. B* **34** 020308
[16] Hu J Y, Yu B, Jing M Y, Xiao L T, Jia S T, Qin G Q and Long G L 2016 *Light Sci. Appl.* **5** e16144
[17] Zhang W, Ding D S, Sheng Y B, Zhou L, Shi B S and Guo G C 2017 *Phys. Rev. Lett.* **118** 220501
[18] Zhu F, Zhang W, Sheng Y B and Huang Y D 2017 *Sci. Bull.* **62** 1519
[19] Qi R Y, Sun Z, Lin Z S, Niu P H, Hao W T, Song L Y, Huang Q, Gao J C, Yin L G and Long G L 2019 2019 *Light Sci. Appl.* **8** 22
[20] Long G L and Zhang H R 2021 *Sci. Bull.* **66** 1267
[21] Zhang H R, Sun Z, Qi R Y, Yin L G, Long G L and Lu J H 2022 *Light Sci. Appl.* **11** 83
[22] Qi Z T, Li Y H, Huang Y W, Feng J, Zheng Y L and Chen X F 2021 *Light Sci. Appl.* **10** 183
[23] Pan D, Liu Y C, Niu P H, Zhang H R, Zhang F H, Wang M, Song X T, Chen X W, Zheng C and Long G L 2025 *Sci. Adv.* **11** eadt4627
[24] Nguyen B A 2004 *Phys. Lett. A* **328** 6
[25] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 22
[26] Yang Y G and Wen Q Y 2007 *Sci. China Phys. Mech. Astron.* **50** 558
[27] Shi G F, Xi X Q and Tian X L 2009 *Opt. Commun.* **282** 2460
[28] Shi G F, Xi X Q and Hu M L 2010 *Opt. Commun.* **283** 1984
[29] Zhou N R, Li J F, Yu Z B, Gong L H and Farouk A 2017 *Quant. Inf. Process.* **16** 4
[30] Zhu P H, Zhong W, Du M M, Li X Y, Zhou L and Sheng Y B 2024 *Chin. Phys. B* **33** 030302
[31] Lin J, Chang C Y, Tsai C W and Yang C W 2024 *EPJ Quantum Technol.* **11** 87
[32] Wang Y Y, Yang T H, Xu J and Chen X G 2024 *Quant. Inf. Process.* **23** 13
[33] Pan T J, Zhou R G and Zhang X X 2024 *Quantum Inf. Process.* **23** 365
[34] Xu F H, Ma X F, Zhang Q, Lo H K and Pan J W 2020 *Rev. Mod. Phys.* **92** 025002
[35] Qi B, Fung C H F, Lo H K and Ma X F 2007 *Quantum Inf. Comput.* **7** 73
[36] Jain N, Wittmann C, Lydersen L, *et al*. 2011 *Phys. Rev. Lett.* **107** 110501
[37] Makarov V, Anisimov A and Skaar J 2006 *Phys. Rev. A* **74** 022313
[38] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 686
[39] Makarov V 2009 *New J. Phys.* **11** 065003
[40] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[41] Tamaki K and Lo H K 2012 *Phys. Rev. A* **85** 042307
[42] Xu F H, Curty M, Qi B and Lo H K 2013 *New J. Phys.* **15** 113007
[43] Maitra A 2017 *Quant. Inf. Process.* **16** 305
[44] Das N and Paul G 2020 *Int. J. Quantum Inf.* **18** 2050038
[45] Basak J, Maitra A and Maitra S 2021 *Quantum Inf. Process.* **20** 361
[46] Shi G F 2021 *Chin. Phys. B* **30** 100303
[47] Han K Q, Zhou L, Zhong W and Sheng Y B 2021 *Quantum Inf. Process.* **20** 280
[48] Zhang C, Zhou L, Zhong W, Du M M and Sheng Y B 2024 *Quantum Inf. Process.* **23** 52
[49] Mihara T 2002 *Phys. Rev. A* **65** 052326
[50] Zhang X L 2009 *Chin. Sci. Bull.* **54** 2018
[51] Ma H X, Huang P, Bao W S and Zeng G H 2016 *Quantum Inf. Process.* **15** 2605
[52] Dutta A and Pathak A 2022 *Quantum Inf. Process.* **21** 369
[53] Zhou N R, Zeng G H, Zeng W J and Zhu F C 2005 *Opt. Commun.* **254** 380
[54] Zhang Z S, Zeng G H, Zhou N R and Xiong J 2006 *Phys. Lett. A* **356** 199
[55] Ying J W, Zhou L, Zhong W and Sheng Y B 2022 *Chin. Phys. B* **31** 120303
[56] Hu X M, Huang C X, Sheng Y B, Zhou L, Liu B H, Guo Y, Zhang C, Xing W B, Huang Y F, Li C F and Guo G C 2021 *Phys. Rev. Lett.* **126** 010503
[57] Tang Z Y, Liao Z F, Xu F H, Qi B, Li Q and Lo H K 2014 *Phys. Rev. Lett.* **112** 190503
[58] Guo J X, Feng X T, Yang P Y, Yu Z F, Chen L Q, Yuan C H and Zhang W P 2019 *Nat. Commun.* **10** 148
[59] Wang Y F, Li J F, Zhang S C, Su K Y, Zhou Y R, Liao K Y, Du S W, Yan H and Zhu S L 2019 *Nat. Photon.* **13** 346
[60] Ma Y, Ma Y, Ma Y Z, Zhou Z Q, Li C F and Guo G C 2021 *Nat. Commun.* **12** 2381
[61] Zhang X Y, Zhang B, Wei S H, Li H, Liao J Y, Li C, Deng G W, Wang Y, Song H Z and You L X 2023 *Sci. Adv.* **9** eadf4587