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

Jia-Wei Ying(应佳伟)[1,2], Lan Zhou(周澜)[3], Wei Zhong(钟伟)[2], and Yu-Bo Sheng(盛宇波)[1,2,†]

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

[2] *Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210003, *China*

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

(Received 2 June 2022; revised manuscript received 21 July 2022; accepted manuscript online 5 September 2022)

The one-step quantum secure direct communication (QSDC) (*Sci. Bull.* **67**, 367 (2022)) can effectively simplify QSDC's operation and reduce message loss. For enhancing its security under practical experimental condition, we propose two measurement-device-independent (MDI) one-step QSDC protocols, which can resist all possible attacks from imperfect measurement devices. In both protocols, the communication parties prepare identical polarization-spatial-mode two-photon hyperentangled states and construct the hyperentanglement channel by hyperentanglement swapping. The first MDI one-step QSDC protocol adopts the nonlinear-optical complete hyperentanglement Bell state measurement (HBSM) to construct the hyperentanglement channel, while the second protocol adopts the linear-optical partial HBSM. Then, the parties encode the photons in the polarization degree of freedom and send them to the third party for the hyperentanglement-assisted complete polarization Bell state measurement. Both protocols are unconditionally secure in theory. The simulation results show the MDI one-step QSDC protocol with complete HBSM attains the maximal communication distance of about 354 km. Our MDI one-step QSDC protocols may have potential applications in the future quantum secure communication field.

Keywords: measurement-device-independent, one-step quantum secure direct communication, hyperentanglement Bell state measurement, hyperentanglement-assisted complete polarization Bell state measurement

PACS: 03.67.Pp, 03.67.Hk, 03.65.Ud **DOI:** 10.1088/1674-1056/ac8f37

1. Introduction

In the 21st century, the information security has been widely concerned. Quantum communication based on the basic principle of quantum mechanics can provide an absolute security guarantee of the communication. Quantum communication began as the research on quantum key distribution (QKD).[1–3] QKD can distribute secure keys between two distant parties, which was first proposed in 1984.[1] Combined with extra one-time pad and the one-way classical communication, the communication parties can realize the secure communication. During past decades, QKD has made great progress in both theory[4–14] and experiment.[15–23] For example, in the theory aspect, the device-independent (DI) QKD[4] and measurement-device-independent (MDI) QKD can efficiently enhance QKD's security under practical imperfect experimental condition.[4–9] The twin-field (TF) QKD improves the key rate-transmittance bound from linear to square root.[14] In the experimental aspect, Yin *et al.* in 2020 built a time-phase encoding system to implement the four-intensity decoy-state BB84 QKD protocol.[15] In 2021, Chen *et al.* realized the space-to-ground quantum communication network over 4600 km.[16] Recently, the chip-based QKD[18] and TF-QKD experiment over an 830-km fibre[23] were also reported. Besides QKD, there appears to be some important branches of quantum communication, such as quantum teleportation (QT),[24–28] quantum secret sharing (QSS),[29–33] and quantum secure direct communication.[34–54] QT enables a communication party to send the encoded messages to a remote party without sending the encoded particle itself. In QSS, a dealer can distribute the keys to multiple participants. All the participants can obtain the keys only by cooperation.

Quantum secure direct communication (QSDC) which will be detailed here is a new quantum secure communication mode. It can directly transmit secure messages between two communication parties without keys. Meanwhile, QSDC can also realize the task of QKD. The first QSDC protocol known as the efficient QSDC protocol was proposed by Long and Liu in 2000.[34] In 2003 and 2004, the typical two-step QSDC protocol based on Einstein–Podolsky–Rosen pairs and the QSDC protocol based on single photons (DL04 protocol) were successively proposed.[35,36] In 2005, Wang *et al.* proposed the QSDC protocol with high-dimension quantum superdense coding.[37] The DL04 protocol and two-step QSDC protocol were experimentally demonstrated in 2016 and 2017, respectively.[38,39] In recent few years, QSDC has developed rapidly in both theory and experiment.[40–54] In theory, DI-QSDC and MDI-QSDC were put forward, which can largely enhance QSDC's security under practical experimental condition.[41–44] In 2021, Long and Zhang adopted the mask-

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

© 2022 Chinese Physical Society and IOP Publishing Ltd

ing technology in QSDC to increase its capacity, communication distance, and tolerable error rate greatly.[49] In the experimental aspect, a 15-user QSDC network with any two users being 40 km apart was realized in 2021.[51] Later, researchers achieved the QSDC over a 100-km fiber with time-bin and phase quantum states.[53]

In 2021, the one-step QSDC[52] based on polarization-spatial-mode-hyperentanglement was proposed, where the communication parties only require to transmit photons in the quantum channel once to construct the hyperentanglement channel. Then, the message sender encodes his messages in the polarization degree of freedom (DOF) and the parties perform the nonlocal complete polarization Bell state measurement (BSM) assisted by the spatial-mode entanglement.[55] The message receiver can read out the encoded messages according to the BSM results. The one-step QSDC can effectively simplify QSDC's operation and reduce message loss. However, similar to previous QSDC protocols, the one-step QSDC requires perfect and trusted experimental devices. For enhancing its security in practical imperfect experimental condition, in this paper, we propose two MDI one-step QSDC protocols, which can resist all possible attacks from practical imperfect measurement devices. In both MDI one-step QSDC protocols, the communication parties are only responsible for preparing polarization-spatial-mode hyperentanglement and hyper-encoded single photons and for encoding. All the measurement tasks are handed over to the third party. The parties first construct the hyperentanglement channel by the hyperentanglement swapping method. In the first MDI one-step QSDC protocol, we adopt the complete hyperentanglement Bell state measurement (HBSM) with the help of the cross-Kerr nonlinearity, while in the second protocol, we adopt the feasible linear-optical partial HBSM. Then, the message sender encodes his messages in the polarization DOF of his remaining photons and the receiver randomly encodes his photons. As they cannot measure the photons, they should send the encoded photons to the measurement party for the complete polarization BSM assisted by the spatial-mode entanglement. Then, the receiver can finally read out the encoded messages according to the BSM results and his own encodings. Our two MDI one-step QSDC protocols have potential applications in the future quantum secure communication field.

The structure of this paper is organized as follows. In Section 2, we explain our first MDI one-step QSDC protocol. In Section 3, we briefly explain the second MDI one-step QSDC protocol and analyze the influence from the adoption of linear-optical partial HBSM on its message transmission and security. In Section 4, we analyze the security of our MDI one-step QSDC protocols. In Section 5, we simulate the secret message capacity of the first MDI one-step QSDC protocol. In Section 6, we make some discussion and conclusion.

2. The MDI one-step QSDC protocol with the nonlinear complete HBSM

In this section, we explain our MDI one-step QSDC protocol with the complete HBSM. As shown in Fig. 1, there are three parties in our protocol. Alice (A) and Bob (B) are the message sender and receiver, respectively. Charlie (C) is an untrusted third party, who can even be controlled by the eavesdropper (Eve). The whole protocol can be described as follows.

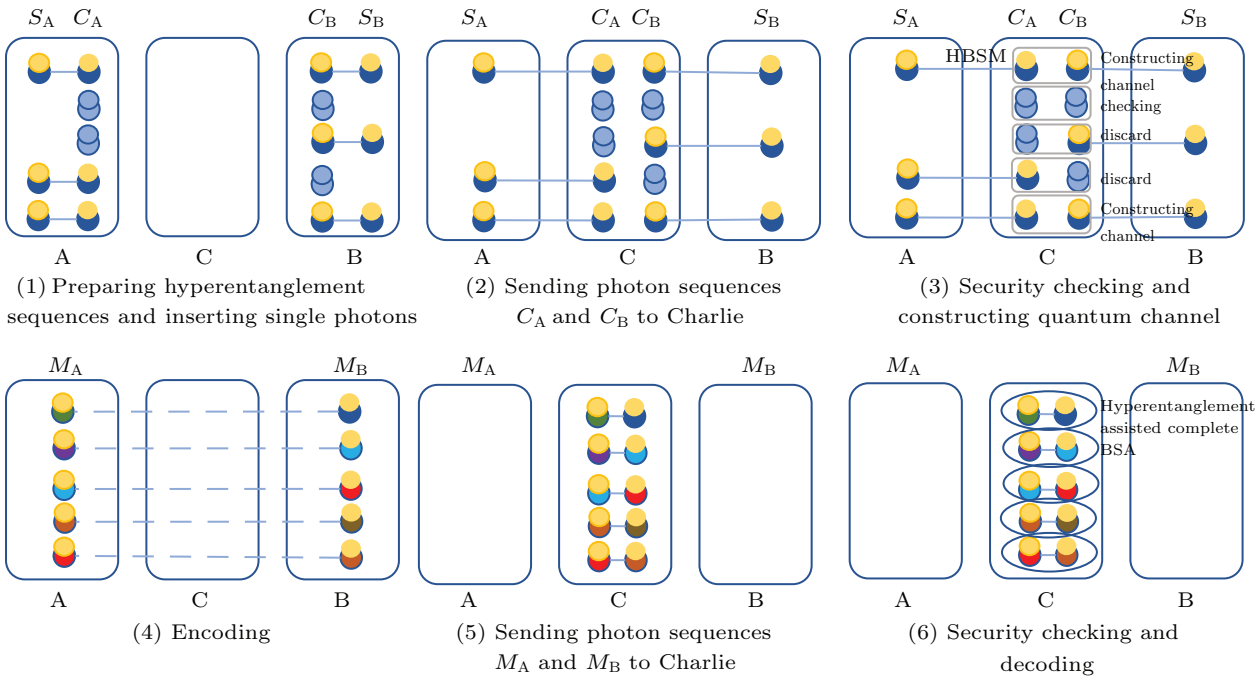


Fig. 1. Illustration of the first MDI one-step QSDC protocol. A, B, C stand for Alice, Bob, and Charlie, respectively. The pattern of yellow and blue balls represents the initial hyperentangled state $|\psi_P^+\rangle|\psi_S^+\rangle_A$ prepared by Alice and Bob. The pattern of two blue balls represents the hyper-encoded single photon. The solid and dashed lines represent the initial and the constructed hyperentanglement, respectively.

Step 1: Alice and Bob both prepare n (n is large) identical polarization-spatial-mode hyperentangled photon pairs in $|\Psi\rangle = |\psi_{\rm P}^{+}\rangle \otimes |\psi_{\rm S}^{+}\rangle$. Alice (Bob) takes one photon from each hyperentangled photon pair to form an ordered photon sequence $S_{\rm A}$ ($S_{\rm B}$) and takes the other photons to form the ordered photon sequence $C_{\rm A}$ ($C_{\rm B}$). Then, Alice (Bob) prepares m polarization-spatial-mode hyper-encoded single photons and inserts them randomly into the sequence $C_{\rm A}$ ($C_{\rm B}$). In this way, there are n photons in sequence $S_{\rm A}$ ($S_{\rm B}$) and $n+m$ photons in sequence $C_{\rm A}$ ($C_{\rm B}$). The single photons are randomly prepared in the rectilinear basis $Z_{\rm P}$ ($Z_{\rm S}$) and diagonal basis $X_{\rm P}$ ($X_{\rm S}$) in the polarization (spatial-mode) DOF. $Z_{\rm P}$ and $X_{\rm P}$ can be described as

$$\begin{aligned} Z_{\rm P} &= \{|H\rangle, |V\rangle\}, \\ X_{\rm P} &= \left\{ |+_{\rm P}\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), |-_{\rm P}\rangle \right. \\ &\quad \left. = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) \right\}, \end{aligned} \tag{1}$$

where $|H\rangle$ and $|V\rangle$ represent the horizontal and vertical polarization, respectively. $Z_{\rm S}$ and $X_{\rm S}$ in Alice's and Bob's locations can be respectively written as

$$\begin{aligned} Z_{\rm SA} &= \{|a_1'\rangle, |a_2'\rangle\}, \\ X_{\rm SA} &= \left\{ |+_{\rm S}\rangle_{\rm A} = \frac{1}{\sqrt{2}}(|a_1'\rangle + |a_2'\rangle), |-_{\rm S}\rangle_{\rm A} \right. \\ &\quad \left. = \frac{1}{\sqrt{2}}(|a_1'\rangle - |a_2'\rangle) \right\}, \\ Z_{\rm SB} &= \{|b_1'\rangle, |b_2'\rangle\}, \\ X_{\rm SB} &= \left\{ |+_{\rm S}\rangle_{\rm B} = \frac{1}{\sqrt{2}}(|b_1'\rangle + |b_2'\rangle), |-_{\rm S}\rangle_{\rm B} \right. \\ &\quad \left. = \frac{1}{\sqrt{2}}(|b_1'\rangle - |b_2'\rangle) \right\}, \end{aligned} \tag{2}$$

where $|a_1'\rangle$, $|a_2'\rangle$, $|b_1'\rangle$, and $|b_2'\rangle$ represent different spatial modes in $C_{\rm A}$ and $C_{\rm B}$ sequences, respectively.

The Bell states in the polarization and spatial-mode DOFs have the forms of

$$\begin{aligned} |\phi_{\rm P}^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle), \\ |\psi_{\rm P}^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle), \\ |\phi_{\rm S}^{\pm}\rangle_{\rm A} &= \frac{1}{\sqrt{2}}(|a_1 a_1'\rangle \pm |a_2 a_2'\rangle), \\ |\psi_{\rm S}^{\pm}\rangle_{\rm A} &= \frac{1}{\sqrt{2}}(|a_1 a_2'\rangle \pm |a_2 a_1'\rangle), \\ |\phi_{\rm S}^{\pm}\rangle_{\rm B} &= \frac{1}{\sqrt{2}}(|b_1 b_1'\rangle \pm |b_2 b_2'\rangle), \\ |\psi_{\rm S}^{\pm}\rangle_{\rm B} &= \frac{1}{\sqrt{2}}(|b_1 b_2'\rangle \pm |b_2 b_1'\rangle). \end{aligned} \tag{3}$$

Here, $|a_1\rangle$, $|a_2\rangle$, $|b_1\rangle$, and $|b_2\rangle$ are different spatial modes in $S_{\rm A}$ and $S_{\rm B}$ sequences, respectively.

Step 2: Alice and Bob send the photons in sequences $C_{\rm A}$ and $C_{\rm B}$ to the third party Charlie. After Charlie receiving the photons, he performs the complete HBSM with the help of the cross-Kerr nonlinearity[56] on each photon pair.

Step 3: Charlie announces the HBSM result for each photon pair. Alice and Bob announce the positions and quantum states of the hyper-encoded photons. If one photon for the HBSM is the hyper-encoded single photon and the other one is from the hyperentangled photon pair, Alice and Bob will discard the HBSM result and the corresponding photon in $S_{\rm A}$ or $S_{\rm B}$ sequence. If both photons for the HBSM are from the hyperentangled photon pairs, after the HBSM, the corresponding remained photons in $S_{\rm A}$ and $S_{\rm B}$ sequences can construct the hyperentanglement channel with the hyperentanglement swapping. In detail, the whole photon state can be written as

$$\begin{aligned} &|\psi_{\rm P}^{+}\rangle |\psi_{\rm S}^{+}\rangle_{\rm A} \otimes |\psi_{\rm P}^{+}\rangle |\psi_{\rm S}^{+}\rangle_{\rm B} \\ &= \frac{1}{2}\big(|\psi_{\rm P}^{+}\rangle_{S_{\rm A}S_{\rm B}} |\psi_{\rm P}^{+}\rangle_{C_{\rm A}C_{\rm B}} - |\psi_{\rm P}^{-}\rangle_{S_{\rm A}S_{\rm B}} |\psi_{\rm P}^{-}\rangle_{C_{\rm A}C_{\rm B}} \\ &\quad + |\phi_{\rm P}^{+}\rangle_{S_{\rm A}S_{\rm B}} |\phi_{\rm P}^{+}\rangle_{C_{\rm A}C_{\rm B}} - |\phi_{\rm P}^{-}\rangle_{S_{\rm A}S_{\rm B}} |\phi_{\rm P}^{-}\rangle_{C_{\rm A}C_{\rm B}} \big) \\ &\quad \otimes \frac{1}{2}\big(|\psi_{\rm S}^{+}\rangle_{S_{\rm A}S_{\rm B}} |\psi_{\rm S}^{+}\rangle_{C_{\rm A}C_{\rm B}} - |\psi_{\rm S}^{-}\rangle_{S_{\rm A}S_{\rm B}} |\psi_{\rm S}^{-}\rangle_{C_{\rm A}C_{\rm B}} \\ &\quad + |\phi_{\rm S}^{+}\rangle_{S_{\rm A}S_{\rm B}} |\phi_{\rm S}^{+}\rangle_{C_{\rm A}C_{\rm B}} - |\phi_{\rm S}^{-}\rangle_{S_{\rm A}S_{\rm B}} |\phi_{\rm S}^{-}\rangle_{C_{\rm A}C_{\rm B}} \big). \end{aligned} \tag{4}$$

For example, if the HBSM result is $|\psi_{\rm P}^{+}\rangle \otimes |\psi_{\rm S}^{-}\rangle_{C_{\rm A}C_{\rm B}}$, the hyperentangled state between Alice and Bob is $|\psi_{\rm P}^{+}\rangle_{S_{\rm A}S_{\rm B}} \otimes |\psi_{\rm S}^{-}\rangle_{S_{\rm A}S_{\rm B}}$. The constructed hyperentangled states in sequences $S_{\rm A}$ and $S_{\rm B}$ are known to all.

If both photons for the HBSM are hyper-encoded photons, the HBSM results can be used for security checking. As shown in Ref. [7], there are two possible cases. First, if the two single photons are generated with different bases in both DOFs, the HBSM results and the encodings in both DOFs cannot be used for security checking. For example, for the photon pair in $|H\rangle|a_1'\rangle \otimes |+_{\rm P}\rangle|+_{\rm S}\rangle_{\rm B}$, the whole photon state will evolve to

$$\begin{aligned} &|H\rangle |a_1'\rangle \otimes |+_{\rm P}\rangle |+_{\rm S}\rangle_{\rm B} \\ &= \frac{1}{2}(|HH\rangle + |HV\rangle) \otimes \big(|a_1' b_1'\rangle + |a_1' b_2'\rangle\big) \\ &= \frac{1}{2}\Big(|\phi_{\rm P}^{+}\rangle_{C_{\rm A}C_{\rm B}} + |\phi_{\rm P}^{-}\rangle_{C_{\rm A}C_{\rm B}} + |\psi_{\rm P}^{+}\rangle_{C_{\rm A}C_{\rm B}} + |\psi_{\rm P}^{-}\rangle_{C_{\rm A}C_{\rm B}}\Big) \\ &\quad \otimes \frac{1}{2}\Big(|\phi_{\rm S}^{+}\rangle_{C_{\rm A}C_{\rm B}} + |\phi_{\rm S}^{-}\rangle_{C_{\rm A}C_{\rm B}} + |\psi_{\rm S}^{+}\rangle_{C_{\rm A}C_{\rm B}} + |\psi_{\rm S}^{-}\rangle_{C_{\rm A}C_{\rm B}}\Big). \end{aligned} \tag{5}$$

It can be found that the HBSM result may obtain all the sixteen hyperentangled Bell states with the same probability and the parties cannot detect whether an error occurs in each DOF. As a result, the parties have to discard the HBSM results and the encodings in both DOFs.

Table 1. Possible BSM results and corresponding probability in the polarization DOF.

Bit encoding		BSM results and probabilities			
Alice	Bob	$\|\phi_{\rm P}^{+}\rangle$	$\|\phi_{\rm P}^{-}\rangle$	$\|\psi_{\rm P}^{+}\rangle$	$\|\psi_{\rm P}^{-}\rangle$
$\|H\rangle$	$\|H\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	0	0
$\|H\rangle$	$\|V\rangle$	0	0	$\frac{1}{2}$	$\frac{1}{2}$
$\|V\rangle$	$\|H\rangle$	0	0	$\frac{1}{2}$	$\frac{1}{2}$
$\|V\rangle$	$\|V\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	0	0
$\|+_{\rm P}\rangle$	$\|+_{\rm P}\rangle$	$\frac{1}{2}$	0	$\frac{1}{2}$	0
$\|+_{\rm P}\rangle$	$\|-_{\rm P}\rangle$	0	$\frac{1}{2}$	0	$\frac{1}{2}$
$\|-_{\rm P}\rangle$	$\|+_{\rm P}\rangle$	0	$\frac{1}{2}$	0	$\frac{1}{2}$
$\|-_{\rm P}\rangle$	$\|-_{\rm P}\rangle$	$\frac{1}{2}$	0	$\frac{1}{2}$	0

Table 2. Possible BSM results and the corresponding probability in the spatial-mode DOF.

Bit encoding		BSM results and probabilities			
Alice	Bob	$\|\phi_{\rm S}^{+}\rangle$	$\|\phi_{\rm S}^{-}\rangle$	$\|\psi_{\rm S}^{+}\rangle$	$\|\psi_{\rm S}^{-}\rangle$
$\|a_1'\rangle$	$\|b_1'\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	0	0
$\|a_1'\rangle$	$\|b_2'\rangle$	0	0	$\frac{1}{2}$	$\frac{1}{2}$
$\|a_2'\rangle$	$\|b_1'\rangle$	0	0	$\frac{1}{2}$	$\frac{1}{2}$
$\|a_2'\rangle$	$\|b_2'\rangle$	$\frac{1}{2}$	$\frac{1}{2}$	0	0
$\|+_{\rm S}\rangle_{\rm A}$	$\|+_{\rm S}\rangle_{\rm B}$	$\frac{1}{2}$	0	$\frac{1}{2}$	0
$\|+_{\rm S}\rangle_{\rm A}$	$\|-_{\rm S}\rangle_{\rm B}$	0	$\frac{1}{2}$	0	$\frac{1}{2}$
$\|-_{\rm S}\rangle_{\rm A}$	$\|+_{\rm S}\rangle_{\rm B}$	0	$\frac{1}{2}$	0	$\frac{1}{2}$
$\|-_{\rm S}\rangle_{\rm A}$	$\|-_{\rm S}\rangle_{\rm B}$	$\frac{1}{2}$	0	$\frac{1}{2}$	0

Second, if the two single photons are generated with the same basis in a DOF, the BSM results and the encodings in this DOF can be used for security checking. The possible BSM results and the corresponding success probability in the polarization DOF and spatial-mode DOF are listed in Table 1 and Table 2, respectively. For example, for the quantum state $|H\rangle|a_1'\rangle\otimes|+_{\rm P}\rangle|b_2'\rangle$ or $|H\rangle|a_1'\rangle\otimes|H\rangle|b_1'\rangle$, the photon state can be written as

$$\begin{aligned}&|H\rangle\,|a_1'\rangle\otimes|+_{\rm P}\rangle\,|b_2'\rangle=\frac{1}{\sqrt{2}}\left(|HH\rangle+|HV\rangle\right)\otimes|a_1'b_2'\rangle\\&=\frac{1}{2}\left(|\phi_{\rm P}^{+}\rangle_{C_{\rm A}C_{\rm B}}+|\phi_{\rm P}^{-}\rangle_{C_{\rm A}C_{\rm B}}+|\psi_{\rm P}^{+}\rangle_{C_{\rm A}C_{\rm B}}+|\psi_{\rm P}^{-}\rangle_{C_{\rm A}C_{\rm B}}\right)\\&\otimes\frac{1}{\sqrt{2}}\left(|\psi_{\rm S}^{+}\rangle_{C_{\rm A}C_{\rm B}}+|\psi_{\rm S}^{-}\rangle_{C_{\rm A}C_{\rm B}}\right),\end{aligned}\tag{6}$$

$$\begin{aligned}&|H\rangle\,|a_1'\rangle\otimes|H\rangle\,|b_1'\rangle=|HH\rangle\otimes|a_1'b_1'\rangle\\&=\frac{1}{\sqrt{2}}\left(|\phi_{\rm P}^{+}\rangle_{C_{\rm A}C_{\rm B}}+|\phi_{\rm P}^{-}\rangle_{C_{\rm A}C_{\rm B}}\right)\\&\otimes\frac{1}{\sqrt{2}}\left(|\phi_{\rm S}^{+}\rangle_{C_{\rm A}C_{\rm B}}+|\phi_{\rm S}^{-}\rangle_{C_{\rm A}C_{\rm B}}\right).\end{aligned}\tag{7}$$

It can be found that when the two photons have the same basis in a DOF, the BSM result in this DOF only has two possible Bell states. If Charlie obtains the other result, the parties can ensure that an error occurs in this DOF. As a result, when the photons have the same basis in a DOF, the BSM result in this DOF can be used for security checking. After the security checking, the parties estimate the bit error rate in both DOFs. If the bit error rate in any DOF exceeds a certain threshold, the photon transmission is unsafe and the parties have to discard the communication. Otherwise, they will ensure that the photon transmission is secure and go to the next step.

Step 4: Alice performs one of the four unitary operations on the photons in $S_{\rm A}$ sequence to encode her messages in the polarization DOF. The four unitary operations have the form of

$$\begin{aligned}U_0&=I=|H\rangle\langle H|+|V\rangle\langle V|,\\U_1&=\delta_z=|H\rangle\langle H|-|V\rangle\langle V|,\\U_2&=\delta_x=|H\rangle\langle V|+|V\rangle\langle H|,\\U_3&=\mathrm{i}\delta_y=|H\rangle\langle V|-|V\rangle\langle H|,\end{aligned}\tag{8}$$

where U_0, U_1, U_2, and U_3 represent four classical messages 00, 01, 10, and 11, respectively. Meanwhile, she randomly selects some photon pairs as the second round of security checking photon pairs and performs random operations on them. In order to prevent message leakage, Bob also randomly performs one of the above four unitary operations on all the photons in $S_{\rm B}$ sequence. We call the encoded photon sequences as $M_{\rm A}$ and $M_{\rm B}$, respectively.

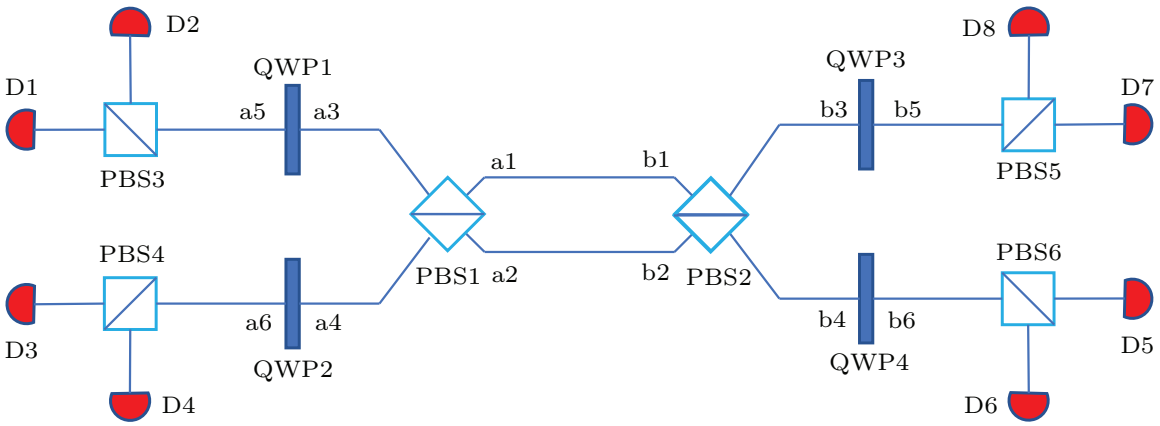


Fig. 2. The basic principle of the complete polarization BSM assisted by spatial-mode entanglement. Here, PBS represents the polarization beam splitter, which can totally transmit the photon in $|H\rangle$ and totally reflect the photon in $|V\rangle$. QWP means the quarter wave plate, which makes $|H\rangle\rightarrow\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)$ and $|V\rangle\rightarrow\frac{1}{\sqrt{2}}(|H\rangle-|V\rangle)$. D$i$ ($i=1,2,\ldots,8$) represents the single photon detector.

Table 3. The polarization Bell states corresponding to the detector responses with different spatial-mode entangled states.

Spatial-mode Bell state	Detector response	Polarization Bell state
$\|\phi_S^+\rangle_{M_AM_B}$ or $\|\psi_S^+\rangle_{M_AM_B}$	$D_1D_5/D_3D_7/D_2D_6/D_4D_8$	$\|\phi_P^+\rangle_{M_AM_B}$
	$D_2D_5/D_4D_7/D_1D_6/D_3D_8$	$\|\phi_P^-\rangle_{M_AM_B}$
	$D_3D_5/D_1D_7/D_4D_6/D_2D_8$	$\|\psi_P^+\rangle_{M_AM_B}$
	$D_4D_5/D_3D_6/D_2D_7/D_1D_8$	$\|\psi_P^-\rangle_{M_AM_B}$
$\|\phi_S^-\rangle_{M_AM_B}$ or $\|\psi_S^-\rangle_{M_AM_B}$	$D_2D_5/D_4D_7/D_1D_6/D_3D_8$	$\|\phi_P^+\rangle_{M_AM_B}$
	$D_1D_5/D_3D_7/D_2D_6/D_4D_8$	$\|\phi_P^-\rangle_{M_AM_B}$
	$D_4D_5/D_3D_6/D_2D_7/D_1D_8$	$\|\psi_P^+\rangle_{M_AM_B}$
	$D_3D_5/D_1D_7/D_4D_6/D_2D_8$	$\|\psi_P^-\rangle_{M_AM_B}$

Step 5: Alice and Bob send the photons in sequences M_A and M_B to Charlie. After receiving the photons, Charlie performs the complete polarization BSM assisted by the spatial entanglement on each photon pair.[2] The basic principle of such BSM is shown in Fig. 2. The polarization Bell states corresponding to the detector responses with different spatial-mode entangled states are shown in Table 3. In this way, according to the detector responses, Charlie can completely distinguish four polarization Bell states in Eq. (3).

Step 6: Charlie announces his BSM results and Alice announces the positions and operations on the security checking photon pairs. For the message transmission photon pairs, Bob can deduce Alice's coding operation combining the BSM result with his own random operation, thus can finally read out the encoded message. For the security checking photon pairs, Bob can estimate the error rate. If the bit error rate exceeds a certain threshold, the photon transmission is unsafe and the parties have to discard the communication and the transmitted messages. Otherwise, if the bit error rate is lower than the threshold, they ensure that the photon transmission is secure and keep the transmitted messages.

To facilitate understanding, we explain our protocol in a specific example. Here, we neglect the security checking for simplicity. First, Alice and Bob prepare polarization-spatial-mode hyperentanglement in $|\psi_P^+\rangle|\psi_S^+\rangle_A$, $|\psi_P^+\rangle|\psi_S^+\rangle_B$, respectively. They send the photons in C_A and C_B sequences to Charlie for the HBSM. According to Eq. (4), we suppose that the HBSM result is $|\phi_P^+\rangle_{C_AC_B}|\psi_S^+\rangle_{C_AC_B}$. In this case, Alice and Bob can infer that they share the hyperentangled state as $|\phi_P^+\rangle_{S_AS_B}|\psi_S^+\rangle_{S_AS_B} = \frac{1}{\sqrt{2}}(|HH\rangle+|VV\rangle)\otimes\frac{1}{\sqrt{2}}(|a_1b_2\rangle+|a_2b_1\rangle)$. If Alice wants to transmit the message 10 to Bob, she will perform U_2 on her photon in the sequence S_A. We suppose that the random operation performed by Bob is U_1. After these operations, the state shared by Alice and Bob becomes $|\psi_P^-\rangle_{M_AM_B}|\psi_S^+\rangle_{M_AM_B} = \frac{1}{\sqrt{2}}(|HV\rangle-|VH\rangle)\otimes\frac{1}{\sqrt{2}}(|a_1b_2\rangle+|a_2b_1\rangle)$. Then, they send the encoded photons to Charlie for the complete polarization BSM. According to the detector responses, Charlie can deduce the polarization Bell state and then announces it to Alice and Bob. Combined with his own operation, Bob can obtain that the polarization Bell state encoded by Alice is $|\psi_P^+\rangle$, so that the encoded messages is 10. In our protocol, with the complete HBSM and complete polarization BSM, Alice can transmit 2 bits of classical messages to Bob in each communication round. However, the complete HBSM protocol based on cross-Kerr nonlinearity[56] is still of challenge under current experimental condition.

3. The second MDI one-step QSDC protocol with the linear-optical partial HBSM

For enhancing the practicability of the MDI one-step QSDC protocol, we propose the second MDI one-step QSDC protocol, which adopts the linear-optical partial HBSM protocol in Ref. [57] in step 2. The linear-optical partial HBSM protocol can distinguish 12 of the 16 hyperentangled Bell states assisted by the time-bin DOF. The distinguishable 12 hyperentangled states are $|\phi_P^\pm\rangle\otimes|\phi_S^\pm\rangle$, $|\psi_P^\pm\rangle\otimes|\psi_S^\pm\rangle$, and $|\psi_P^\pm\rangle\otimes|\phi_S^\pm\rangle$. For the other 4 hyperentangled Bell states $|\phi_P^\pm\rangle\otimes|\psi_S^\pm\rangle$, this HBSM protocol can only distinguish $|\psi_S^\pm\rangle$ but cannot distinguish $|\phi_P^\pm\rangle$.[57] This partial HBSM protocol only requires linear-optical elements, and is feasible with current experimental technology.

Then, we analyze the influence from adopting the linear-optical partial HBSM protocol on the security and communication efficiency of our MDI one-step QSDC. If the HBSM obtains one of the four hyperentangled states $|\phi_P^\pm\rangle\otimes|\psi_S^\pm\rangle$, the situation that the partial HBSM cannot distinguish $|\phi_P^\pm\rangle$ would influence the security checking and the construction of hyperentanglement channel. As shown in Table 1, during the security checking process of step 3, if both parties use the rectilinear basis, $|\phi_P^\pm\rangle$ both correspond to the even parity $|H\rangle|H\rangle$ and $|V\rangle|V\rangle$. In this case, the situation that Charlie cannot distinguish $|\phi_P^\pm\rangle$ will not cause error in the polarization DOF, so that the encoded bits and the BSM result in the polarization DOF can still be used in the security checking. On the other hand, if both parties use the diagonal basis, $|\phi_P^+\rangle$ corresponds to the even parity $|+_P\rangle|+_P\rangle$ and $|-_P\rangle|-_P\rangle$, while $|\phi_P^-\rangle$ corresponds to the odd parity $|+_P\rangle|-_P\rangle$ and $|-_P\rangle|+_P\rangle$. As a result, if Charlie randomly announces $|\phi_P^+\rangle$ or $|\phi_P^-\rangle$, it may cause error in the polarization DOF. As a result, for avoiding the error caused by the partial HBSM, the parties have to discard the encoded bits and the BSM result in the polarization DOF when Charlie obtains $|\phi_P^\pm\rangle\otimes|\psi_S^\pm\rangle$, but only use the BSM result and the encoding bits in the spatial-mode DOF to check the se-

curity. On the other hand, in the hyperentanglement swapping process, if Charlie obtains $|\phi_{\rm P}^{\pm}\rangle \otimes |\psi_{\rm S}^{\pm}\rangle$, the communication parties cannot determine the constructed quantum state in the polarization DOF, which may make Bob obtain wrong messages by comparing the constructed quantum state and encoded quantum state in the polarization DOF. For avoiding the message error, the parties have to discard the corresponding hyperentangled photons in $S_{\rm A}$ and $S_{\rm B}$ sequences. As Charlie may obtain $|\phi_{\rm P}^{\pm}\rangle \otimes |\psi_{\rm S}^{\pm}\rangle$ with the probability of 1/4, Alice can transmit 1.5 bits of classical messages to Bob in each communication round in statistics.

4. Security analysis

Now, we analyze the security of our MDI one-step QSDC protocols in theory. In the protocols, all the measurement tasks are handed over to the third measurement party Charlie, who can be even controlled by Eve and the measurement results are public to all. We show the relationship among the first HBSM result in the polarization DOF, the complete polarization BSM result and Alice's and Bob's joint operations in Table 4. We set the HBSM result in the polarization DOF as $|\psi^{+}\rangle$ for simplicity. If the HBSM obtains the other result, we can obtain the similar results. From Table 4, the BSM result is independent of Alice's bit value. One can read out Alice's encoded message only by combining the BSM result with Bob's operation. As Bob's random operation is private, only Bob can obtain the encoded messages. Meanwhile, if Charlie deliberately announces wrong HBSM or BSM result, Bob may read out wrong messages according to the measurement results. However, as Charlie does not know the positions of the security checking photons before announcing the measurement results, his dishonest behavior may increase the error rate. In this way, his dishonest behavior can be detected by the communication parties. Based on the above analysis, our protocol can resist all the possible attacks from the imperfect measurement devices and the measurement party.

Table 4. The relationship among the HBSM result in the polarization DOF, the complete polarization BSM result and Alice's and Bob's joint operation. Here, we set the HBSM result in the polarization DOF as $|\psi^{+}\rangle$ for simplicity.

First HBSM	Second BSM	Bob's operation	Alice's operation	Encoded message
$\|\psi_{\rm P}^{+}\rangle_{C_{\rm A}C_{\rm B}}$	$\|\psi_{\rm P}^{+}\rangle_{M_{\rm A}M_{\rm B}}$	U_0	U_0	00
		U_1	U_1	01
		U_2	U_2	10
		U_3	U_3	11
	$\|\psi_{\rm P}^{-}\rangle_{M_{\rm A}M_{\rm B}}$	U_0	U_1	01
		U_1	U_0	00
		U_2	U_3	11
		U_3	U_2	10
	$\|\phi_{\rm P}^{+}\rangle_{M_{\rm A}M_{\rm B}}$	U_0	U_2	10
		U_1	U_3	11
		U_2	U_0	00
		U_3	U_1	01
	$\|\phi_{\rm P}^{-}\rangle_{M_{\rm A}M_{\rm B}}$	U_0	U_3	11
		U_1	U_2	10
		U_2	U_1	01
		U_3	U_0	00

Then, we consider a common attack mode, say, the intercept-resend attack. For achieving the goal of MDI, the parties require to transmit photons in quantum channels twice. During the first photon transmission process, Eve can intercept some photons from Alice. For avoiding detection, he prepares some single photons and sends them to Charlie to make the HBSM. In this way, Alice actually constructs the hyperentangled channel with Eve. During the second photon transmission process, Eve also intercepts the corresponding photons of the intercepted photons in the first photon transmission, so that he can finally obtain Alice's encoded messages by performing the polarization BSM. In the protocol, the communication security is guaranteed by two rounds of security checking. During the first photon transmission process, as the randomly encoded security checking photons are randomly inserted into the $C_{\rm A}$ and $C_{\rm B}$ sequences, Eve may steal some security checking photons inevitably. As Eve does not know the generation basis of the single photons, he can only randomly choose Z or X basis to measure the photons in both DOFs and generate a new photon according to his measurement result. When Eve chooses wrong basis, his new generated photon may cause wrong HBSM result and increase the error rate, so that the parties can detect Eve's attack. As long as the security of the first photon transmission process can be guaranteed, Eve cannot steal meaningful messages even if she could steal some photons during the second photon transmission process. Meanwhile, Charlie (Eve) cannot obtain the encoded messages from the HBSM and polarization BSM results, because he does not know Bob's random encoding in the polarization DOF. However, the intercept-resend attack in the second photon transmission process would make Charlie obtain wrong BSM results and disturb the communication. We set the second se-

curity checking to guarantee the security of the second photon transmission process. As a result, with the help of two rounds of security checking, the security and correctness of the messages can be guaranteed. Our protocols can resist the intercept-resend attack in theory.

Third, we consider another common attack, the Trojan horse attack, in which the attacker inserts his own photons into the photon sequences to steal the encoded messages. In our protocol, with the help of the entanglement swapping, the photons to be encoded are always in Alice's and Bob's locations before the encoding. In this way, the eavesdropper cannot insert photons into these photon sequences to steal the encoded messages, so that our protocols can also resist the Trojan horse attack.

5. Simulation of the MDI one-step QSDC protocol's secrete message capacity

In this section, we simulate the secrete message capacity ($C_{\rm s}$) of our first MDI one-step QSDC protocol with the complete HBSM in Ref. [56]. $C_{\rm s}$ is defined as the amount of transmitted correct and secure qubits divided by the total amount of the encoded photon pair. As one encoded photon pair can transmit 2 bits of secrete messages, in the ideal scenario, it is obvious that $C_{\rm s}=2Q_{\rm P}^{1,1}$, where $Q_{\rm P}^{1,1}$ represents the gain in the polarization DOF when the photon sources in both parties' locations generate one target hyperentangled photon pair. On the other hand, in practical condition, we must consider all the practical imperfect factors, such as the imperfect photon source, imperfect photon detector and homodyne measurement, and basis misalignment. In this way, $C_{\rm s}$ in a realistic setup will be given by[3,4]

$$C_{\rm s}=2\{Q_{\rm P}^{1,1}[1-H(e_{\rm tP}^{1,1})]-Q_{\rm tP}H(E_{\rm tP})\}. \tag{9}$$

Here, $e_{\rm tP}^{1,1}$ is the total error rate in the polarization DOF when the photon source in each party's location generates one target hyperentangled photon pair. $Q_{\rm tP}$ and $E_{\rm tP}$ are the total gain and total error rate in the polarization DOF, where $Q_{\rm tP}=\sum_{n,m}Q_{\rm P}^{n,m}$ and $E_{\rm tP}=\sum_{n,m}Q_{\rm P}^{n,m}e_{\rm tP}^{n,m}/Q_{\rm tP}$. Here, we suppose that each party adopts the practical spontaneous parametric down-conversion (SPDC) source to generate the hyperentangled photon pair $|\Psi\rangle$ with a probability of p' ($p'\sim 10^3$).[58] As $p'\ll 1$, we only consider the vacuum state, one-pair and two-pair emission, and neglect the higher order term. The generated hyperentangled photon states can be written as

$$\begin{aligned}\rho \approx\ & (1-p'-p'^2)|{\rm vac}\rangle\langle{\rm vac}|+p'|\Psi\rangle\langle\Psi|\\ & +p'^2|\Psi^{\otimes 2}\rangle\langle\Psi^{\otimes 2}|.\end{aligned} \tag{10}$$

Here, we suppose that Alice and Bob can employ a optical switch and the quantum nondemolition detection (QND) gate constructed with the cross-Kerr nonlinearities on the two emitted pulses. Only when each SPDC source emits exactly one hyperentangled photon pair, the optical switch will let the photon go to the HBSM. With the QND gate, the two-pair emission case can not enter the HBSM, and we can obtain $Q_{\rm tP}=Q_{\rm P}^{1,1}$ and $E_{\rm tP}=e_{\rm tP}^{1,1}$. In this way, we can simplify $C_{\rm s}$ to

$$C_{\rm s}=2Q_{\rm P}^{1,1}[1-2H(e_{\rm tP}^{1,1})]. \tag{11}$$

Then, we calculate $Q_{\rm P}^{1,1}$ and $e_{\rm tP}^{1,1}$. 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 $\alpha=0.2$ dB/km for a standard optical fiber. Based on the previous experimental data given in Ref. [59], after the first photon transmission, we set the polarization and spatial-mode misalignment error rates as $e_{\rm mP}=e_{\rm mS}=1.5\%$. Meanwhile, the parties can distinguish all the polarization-spatial-mode hyperentangled states based on the homodyne measurement, which is proved to be highly efficient (quite close to 100%).[60–62] However, in practical cases it will inevitably introduce the inherent loss and error. According to Ref. [61], the error rate ($e_{\rm d}$) of the homodyne measurement can be reduced to 1% with the weak cross-Kerr nonlinearities in an NV-diamond system, so that we set $e_{\rm d}=1\%$. In addition, we define the inherent efficiency η_{l1} as the product of the coupling efficiency ($\eta_{\rm c}$) between the photon and the fiber, and the efficiency ($\eta_{\rm h}$) of the homodyne measurement, say, $\eta_{l1}=\eta_{\rm c}\eta_{\rm h}$. Here, we set $\eta_{l1}=98\%$. In this way, we can obtain the error rate $e_{\rm P1}^{1,1}$ ($e_{\rm S1}^{1,1}$) in polarization (spatial-mode) DOF and the yield $Y_1^{1,1}$ after the complete HBSM as

$$\begin{aligned}Y_1^{1,1} &= t_at_b\eta_{l1}^2=10^{-2\alpha d/10}\eta_{l1}^2,\\ e_{\rm P1}^{1,1} &= 1-\frac{t_{\rm a}t_{\rm b}\eta_{l1}^2(1-e_{\rm d})^2(1-e_{\rm mP})^2}{Y_1^{1,1}},\\ e_{\rm S1}^{1,1} &= 1-\frac{t_{\rm a}t_{\rm b}\eta_{l1}^2(1-e_{\rm d})^2(1-e_{\rm mS})^2}{Y_1^{1,1}}.\end{aligned} \tag{12}$$

After the construction of hyperentanglement channel, Alice and Bob distill the remaining photons from quantum memory devices and encode on them. Then, they send the encoded photons to Charlie for the complete polarization BSM. This BSM only requires the linear optical elements and the single photon detectors. We set the inherent efficiency η_{l2} as the product of the coupling efficiency ($\eta_{\rm c}$) and the efficiency ($\eta_{\rm m}$) of the quantum memory, say, $\eta_{l2}=\eta_{\rm c}\eta_{\rm m}$. Here, we also set $\eta_{l2}=98\%$. In addition, from recent reports,[63,64] the superconducting nanowire single-photon detectors (SNSPD) can be 90% efficiency at 1550 nm ($\eta_d=90\%$) with the background count rate of $Y_0=6.02\times10^{-6}$. In this way, we can obtain the error rate $e_{\rm P2}^{1,1}$ in polarization DOF and the yield $Y_2^{1,1}$ after the complete polarization BSM as

$$Y_2^{1,1} = (1-Y_0)^2[t_at_b\eta_{l2}^2\eta_d^2$$

$$+2Y_0(t_a\eta_{l2}\eta_d+t_b\eta_{l2}\eta_d-t_at_b\eta_{l2}^2\eta_d^2)$$
$$+4Y_0^2(1-t_a\eta_{l2}\eta_d)(1-t_{ab}\eta_{l2}\eta_d)],$$
$$e_{\rm P2}^{1,1} = 1-\frac{t_at_b\eta_{l2}^2\eta_d^2(1-e_{\rm mP})^2(1-e_{\rm mS})^2}{Y_2^{1,1}}. \quad (13)$$

In this way, we can obtain $Q_{\rm P}^{1,1}$ and $e_{\rm tP}^{1,1}$ as follows:

$$Q_{\rm P}^{1,1} = p'Y_1^{1,1}Y_2^{1,1},$$
$$e_{\rm tP}^{1,1} = \frac{1}{2}[1-(1-e_{\rm P1}^{1,1})(1-e_{\rm S1}^{1,1})(1-e_{\rm P2}^{1,1})]. \quad (14)$$

Taking Eq. (14) into Eq. (11), we can finally calculate the value of $C_{\rm s}$.

In Fig. 3, we provide the value of $\log C_{\rm s}$ per pulse altered with the photon transmission distance d from Charlie to Alice (Bob). It can be found that with the complete HBSM and linear optical complete polarization BSM, the maximal photon transmission distance can reach about 177 km, so that the maximal communication distance is about 354 km.

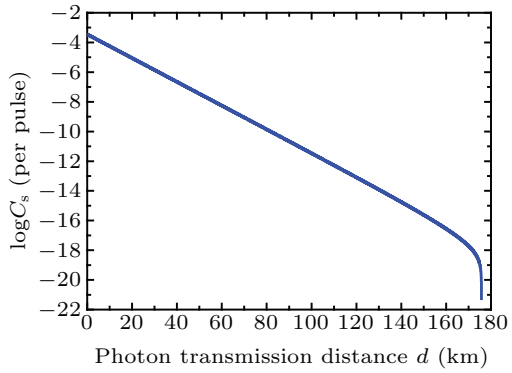


Fig. 3. The secrete message capacity ($\log C_{\rm s}$) per pulse altered with the photon transmission distance d from Charlie to Alice (Bob). Here, we suppose that Alice and Bob use the SPDC sources to generate hyperentangled states with $p'=10^{-3}$. During each photon transmission process, we set the misalignment error rates in both DOFs as $e_{\rm mP}=e_{\rm mS}=1.5\%$. We also set the inherent efficiencies as $\eta_{l1}=\eta_{l2}=98\%$, the error rate of the homodyne measurement as $e_d=1\%$, the single photon detector in the complete polarization BSM process is 90% efficient with the dark-ground count rate as $Y_0=6.02\times10^{-6}$.

6. Discussion and conclusion

In this paper, we propose two MDI one-step QSDC protocols based on the polarization-spatial-mode hyperentanglement. In our protocols, both Alice and Bob require photon state generation and the encoding. All the measurement tasks are handed over to the third party Charlie. In this way, our protocols can resist all possible attacks from practical imperfect measurement devices. In both protocols, with the help of the HBSM, Alice and Bob can construct the deterministic hyperentanglement channel by the hyperentanglement swapping. Then, after Alice's and Bob's encoding, they send the encoded photons to Charlie for the complete polarization BSM assisted by the spatial-mode entanglement. Bob can finally read out Alice's encoding messages based on Charlie's measurement results and his own encoding. In the first protocol, with the help of the complete HBSM, Alice can transmit two bits of messages to Bob by consuming two pairs of hyperentangled states. In the second MDI one-step QSDC protocol, with the practical partial HBSM, Alice can transmit 1.5 bits of messages to Bob by consuming two pairs of hyperentangled states in statistics.

Here, the HBSM is the key element of our protocols. With the complete HBSM, our first MDI one-step protocol can achieve the higher capacity. Besides the HBSM in Ref. [56], there are other complete HBSM protocols with nonlinear optical elements, such as the cross-Kerr nonlinearity and artificial atoms.[65–68] The nonlinear optical elements have gained great progress in recent years.[69–73] In 2016, Beck *et al.* obtained a large conditional cross-phase shift of $\pi/6$ between signal fields stored in an atomic quantum memory.[70] Soon later, Tiarks *et al.* reported the strong interactions in Rydberg electromagnetically induced transparency (EIT) experiments, which can create a large controlled phase shift of 3.3 ± 0.2 rad, with the control pulses containing an average of 0.6 photons.[72] In 2020, Sinclair *et al.* reported the cross-Kerr nonlinearity in a free-space medium based on the Rydberg atoms and EIT technology. They obtained the nonlinear phases as 8 mrad/nW of signal power, corresponding to a χ^3 of 10^{-8} m^2/V^2.[73] In this way, with the experimental development of the nonlinear optical elements, it is possible to realize the complete BSM in the near future.

In conclusion, for enhancing one-step QSDC's security under practical experimental condition, we propose two MDI one-step QSDC protocols, which can resist all possible attacks from the imperfect measurement device. In the MDI one-step QSDC protocols, Alice and Bob prepare a large number of identical polarization-spatial-mode two-photon hyperentangled states. Then, they send one photon of each hyperentangled photon pair to the third party Charlie to make the HBSM. In this way, Alice and Bob can construct the hyperentanglement channel with the hyperentanglement swapping. The first MDI one-step QSDC protocol uses the nonlinear complete HBSM to construct the hyperentanglement channel, while the second protocol uses the linear-optical partial HBSM. Then, Alice encodes her messages on her remaining photons in the polarization DOF by performing unitary operations and Bob also randomly operates his remaining photons to prevent message leakage. After encodings, Alice and Bob send their photons to Charlie. Charlie performs the linear-optical complete polarization BSM assisted by the spatial-mode entanglement on each photon pair and announces his measurement results. Combining Charlie's measurement results with his own random operations, Bob can finally deduce Alice's messages. Both the MDI one-step QSDC protocols are unconditionally secure in theory. In the first MDI one-step QSDC protocol, Alice can transmit 2 bits of message to Bob by using two hy-

perentangled photon pairs. In the second protocol, with the feasible linear-optical partial HBSM, Alice can transmit 1.5 bits of message to Bob by using two hyperentangled photon pairs in statistics. Our one-step MDI-QSDC protocols, especially the second protocol, may have potential applications in the near future.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant Nos. 11974189 and 12175106), the Natural Science Foundation of the Jiangsu Higher Education Institutions of China (Grant No. 20KJB140001), and the Postgraduate Research & Practice Innovation Program of Jiangsu Province, China (Grand No. KYCX22-0963).

References

[1] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers Systems, and Signal Processing*, December 10–12, 1984, Bangalore, India, pp. 175–179
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Lo H K, Chau H and Ardehali M 2005 *J. Cryptol.* **18** 133
[4] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[5] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[6] Dellantonio L, Sørensen A S and Bacco D 2018 *Phys. Rev. A* **98** 062301
[7] Cui Z X, Zhong W, Zhou L and Sheng Y B 2019 *Sci. China Phys. Mech. Astron.* **62** 110311
[8] Xu F H, Ma X F, Zhang Q, Lo H K and Pan J W 2020 *Rev. Mod. Phys.* **92** 025002
[9] Ke Z J, Wang Y T, Yu S, *et al.* 2020 *Chin. Phys. B* **29** 080301
[10] Jin A R, Zeng P, Penty R V and Ma X F 2021 *Phys. Rev. Appl.* **16** 034017
[11] Sun Z Q, Han Y X, Dou T Q, *et al.* 2021 *Chin. Phys. B* **30** 110303
[12] Chen X T, Zhang L P, Chang S K, Zhang H and Hu L Y 2021 *Chin. Phys. B* **30** 060304
[13] Luo H, Wang Y J, Ye W, Zhong H, Mao Y Y and Guo Y 2022 *Chin. Phys. B* **31** 020306
[14] Wang X B, Yu Z W and Hu X L 2019 *Phys. Rev. A* **98** 062323
[15] Yin H L, Liu P, Dai W W, *et al.* 2020 *Opt. Express* **28** 29479
[16] Chen Y A, Zhang Q, Chen T Y, *et al.* 2021 *Nature* **589** 214
[17] Yin Z Q, Lu F Y, Teng J, Wang S, Chen W, Guo G C and Han Z F 2021 *Fundamental Res.* **1** 93
[18] Kwek L C, Cao L, Luo W, Wang Y X, Sun S H, Wang X B and Liu A Q 2021 *AAPPS Bull.* **31** 15
[19] Guo H, Li Z Y, Yu S and Zhang Y C 2021 *Fundamental Res.* **1** 96
[20] Li B H, Xie Y M, Li Z, *et al.* 2021 *Opt. Lett.* **46** 5529
[21] Liu W B, Li C L, Xie Y M, *et al.* 2021 *PRX Quantum* **2** 040334
[22] Xie Y M, Lu Y S, Weng C X, *et al.* 2022 *PRX Quantum* **3** 020315
[23] Wang S, Yin Z Q, He D Y, *et al.* 2022 *Nat. Photon.* **16** 154
[24] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895
[25] Bouwmeester D, Pan J W, Mattle K, Eibl M, Weinfurter H and Zeilinger A 1997 *Nature* **390** 575
[26] Quan Q, Zhao M J, Fei S M, Fan H, Yang W L, Wang T J and Long G L 2020 *Quantum Inf. Process.* **19** 205
[27] Yan Z H, Qin J L, Qin Z Z, Su X L, Jia X J, Xie C D and Peng K C 2021 *Fundamental Res.* **1** 43
[28] Pandey R K, Prakash R and Prakash H 2021 *Quantum Inf. Process.* **20** 322
[29] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[30] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[31] Williams B P, Lukens J M, Peters N A, Qi B and Grice W P 2019 *Phys. Rev. A* **99** 062311
[32] Wu X D, Wang Y J and Huang D 2020 *Phys. Rev. A* **101** 022301
[33] Lipinska V, Murta G, Ribeiro J and Wehner S 2020 *Phys. Rev. A* **101** 032332
[34] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[35] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[36] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[37] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev. A* **71** 044305
[38] 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
[39] Zhang W, Ding D S, Sheng Y B, Zhou L, Shi B S and Guo G C 2017 *Phys. Rev. Lett.* **118** 220501
[40] Zhu F, Zhang W, Sheng Y B and Huang Y D 2017 *Sci. Bull.* **62** 1519
[41] Zhou L, Sheng Y B and Long G L 2020 *Sci. Bull.* **65** 12
[42] Zhou Z R, Sheng Y B, Niu P H, Yin L G and Long G L 2020 *Sci. China Phys. Mech. Astron.* **63** 230362
[43] Niu P H, Zhou Z R, Lin Z S, Sheng Y B, Yin L G and Long G L 2020 *Sci. Bull.* **63** 1345
[44] Wu X D, Zhou L, Zhong W and Sheng Y B 2020 *Quantum Inf. Process.* **19** 10354
[45] Hu J Y, Yang L, Wu S X, *et al.* 2020 *Europhys. Lett.* **129** 10004
[46] Li T and Long G L 2020 *New J. Phys.* **22** 063017
[47] Liu L, Niu J L, Fan C R, Feng X T and Wang C 2020 *Quantum Inf. Process.* **19** 404
[48] Pan D, Lin Z S, Wu J W, *et al.* 2020 *Photon. Res.* **8** 1522
[49] Long G L and Zhang H R 2021 *Sci. Bull.* **66** 1267
[50] Cao Z W, Wang L, Liang K X, *et al.* 2021 *Phys. Rev. Appl.* **16** 024012
[51] Qi Z T, Li Y H, Huang W Y, *et al.* 2021 *Light: Sci. Appl.* **10** 183
[52] Sheng Y B, Zhou L and Long G L 2022 *Sci. Bull.* **67** 367
[53] Zhang H R, Sun Z, Qi R Y, Yin L G, Long G L and Lu J H 2022 *Light: Sci. Appl.* **11** 83
[54] Zhou L and Sheng Y B 2022 *Sci. China Phys. Mech. Astron.* **65** 250311
[55] Walborn S P, Pádua S and Monken C H 2003 *Phys. Rev. A* **68** 042313
[56] Sheng Y B, Deng F G and Long G L 2010 *Phys. Rev. A* **82** 032318
[57] Gao C Y, Ren B C, Zhang Y X, Ai Q and Deng F G 2020 *Appl. Phys. Express* **13** 027004
[58] Hu X M, Huang C X, Sheng Y B, *et al.* 2021 *Phys. Rev. Lett.* **126** 010503
[59] Tang Z Y, Liao Z F, Xu F H, Qi B, Qian L and Lo H K 2014 *Phys. Rev. Lett.* **112** 190503
[60] Nemoto K and Munro W J 2004 *Phys. Rev. Lett.* **93** 250502
[61] Munro W J, Nemoto K, Beausoleil R G and Spiller T P 2005 *Phys. Rev. A* **71** 033819
[62] Loock P V 2011 *Laser Photon. Rev.* **5** 167
[63] Zhang W J, You L X, Li H, Huang J, Lv C L, Zhang L, Liu X Y, Wu J J, Wang Z and Xie X M 2017 *Sci. China Phys. Mech. Astron.* **60** 120314
[64] Zhang X Y, Zhang W J, Zhou H, *et al.* 2022 *IEEE J. Sel. Top. Quantum Electron.* **28** 3803708
[65] Li X H and Gohse S 2016 *Opt. Express* **24** 18388
[66] Li X H and Gohse S 2016 *Phys. Rev. A* **93** 022302
[67] Liu Q, Wang G Y, Ai Q, Zhang M and Deng F G 2016 *Sci. Rep.* **6** 22016
[68] Wang G Y, Reng B C, Deng F G and Long G L 2019 *Opt. Express* **27** 8994
[69] Hoi I C, Kockum A F and Palomaki T 2013 *Phys. Rev. Lett.* **111** 053601
[70] Beck K M, Hosseini M, Duan Y and Vuletić V 2016 *Proc. Natl. Acad. Sci. USA* **113** 9740
[71] He B, Sharypov A V, Sheng J T, Simon C and Xiao M 2014 *Phys. Rev. Lett.* **112** 133606
[72] Tiarks D, Schmidt S, Rempe G and Dürr S 2016 *Sci. Adv.* **2** e1600036
[73] Sinclair J, Angulo D, Lupu-Gladstein N, Bonsma-Fisher K and Steinberg A M 2020 *Phys. Rev. Res.* **1** 033193