SCIENCE CHINA
Physics, Mechanics & Astronomy

• Article •

May 2022 Vol. 65 No. 5: 250311
https://doi.org/10.1007/s11433-021-1863-9

One-step device-independent quantum secure direct communication

Lan Zhou[1], and Yu-Bo Sheng[2,3*]

[1] *School of Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;*
[2] *College of Electronic and Optical Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;*
[3] *Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*

Received December 23, 2021; accepted January 21, 2022; published online March 10, 2022

Device-independent quantum secure direct communication (DI-QSDC) can relax the security assumptions about the devices' internal working, and effectively enhance QSDC's security. In this paper, we put forward the first hyperentanglement-based one-step DI-QSDC protocol. In this protocol, the communication parties adopt the nonlocal hyperentanglement-assisted complete Bell state analysis, which enables the photons to transmit in the quantum channel for only one round. The one-step DI-QSDC can directly transmit 2 bits of messages by a hyperentangled photon pair, and is unconditionally secure in theory. Compared with the original DI-QSDC protocol (Sci. Bull. 65, 12 (2020)), the one-step DI-QSDC protocol can simplify the experiment and reduce the message loss. In particular, with the help of the hyperentanglement heralded amplification and the hyperentanglement purification, the message loss and the message error caused by the channel noise can be completely eliminated, and the communication distance can be largely extended. By using the photon source with a repetition rate of 10 GHz, the one-step DI-QSDC's secret message capacity under 50 km communication distance achieves about 7 bit/s with the initial fidelity in each degree of freedom of 0.8. Combined with the quantum repeater, it is possible for researchers to realize the one-step DI-QSDC with an arbitrarily long distance.

device-independent quantum secure direct communication, hyperentanglement, nonlocal Bell state analysis

PACS number(s): 03.67.Mn, 03.67.-a, 42.50.Dv

Citation: L. Zhou, and Y.-B. Sheng, One-step device-independent quantum secure direct communication, Sci. China-Phys. Mech. Astron. **65**, 250311 (2022), https://doi.org/10.1007/s11433-021-1863-9

1 Introduction

Quantum secure communication provides an absolute approach to guarantee communication security. There are some main branches of quantum secure communication, such as quantum key distribution (QKD) [1-14], quantum secure direct communication (QSDC) [15-18], and quantum secret sharing (QSS) [19, 20]. QKD is the earliest and most widely researched branch of quantum secure communication, which is used to distribute secure keys between two communication parties. QSS allows the sender to split a key into several parts. The sender distributes each part of a key to a party. The parties can read out the key only when they cooperate with each other [19, 20]. Different from QKD and QSS, QSDC allows the message sender to directly transmit secret messages to the message receiver without keys. On the other hand, QSDC can also achieve the function of QKD [21]. QSDC was first proposed by Long et al. [15] in 2002. In 2003 and 2004, Deng et al. [16, 17] proposed the entanglement-

*Corresponding author (email: shengyb@njupt.edu.cn) based two-step QSDC protocol and the single-photon-based QSDC protocol, respectively. In the past few years, QSDC has made important progress in experiments [22-27]. In 2016, Hu et al. [22] demonstrated the single-photon-based QSDC using frequency coding. In 2017, researchers realized the entanglement-based QSDC with quantum memory [23]. Soon later, the first long-distance QSDC experiment was achieved by Zhu et al. [24]. In 2021, Qi et al. [27] reported their work on a 15-user QSDC network with any two users being 40 km apart. Besides the experiment progress, QSDC has also gained great development in theory [28-40]. The measurement-device-independent (MDI) QSDC and the device-independent (DI) QSDC were proposed in 2018 and 2020, respectively [29, 33], which could effectively enhance QSDC's security in the practical experimental condition.

Similar to DI-QKD [41-48], DI-QSDC only requires two fundamental assumptions, that is to say, quantum physics is correct and no unwanted signal can escape from the laboratories. In the original DI-QSDC protocol [33], Alice needs to generate a large amount of two-photon entangled states. Both photons in each photon pair have to be sent to Bob by two rounds of photon transmission processes, respectively. Only when Bob obtains both photons of an encoded photon pair, can he obtain the encoded messages by performing the local Bell state analysis (BSA). In this way, we call the original DI-QSDC protocol the two-step DI-QSDC protocol. The security of each photon transmission round only relies on the observation of data that conclusively violates a Bell (typically, the Clauser-Horne-Shimony-Holt (CHSH)) inequality [49, 50]. However, the photon loss and decoherence caused by the environment would deteriorate the quality of the nonlocal correlations between the photons, which will provide an opportunity for the eavesdropper to intercept some encoded messages without being detected, and cause the message loss and the message error. It is noteworthy that, unlike QKD, the communication parties cannot use the post processing method to correct the message error, for QSDC transmits meaningful messages, not random keys. The message error and the message loss problems seriously limit the practical application of the two-step DI-QSDC.

Recently, a feasible one-step QSDC protocol has been proposed [40], where the message sender only needs to transmit photons in the quantum channel for one round. To further relax the security assumptions and enhance the security of the one-step QSDC in a practical scenario, we proposed the first one-step DI-QSDC protocol. In this protocol, the receiver Bob prepares a large amount of polarization-spatial-mode hyperentangled two-photon pairs and distributes the hyperentanglement to the sender Alice through the practical quantum channel for only one round. They perform the CHSH test in each degree of freedom (DOF) to ensure the security of the photon transmission. Then, Alice encodes her messages in the polarization DOF of the photons. After encoding, the parties adopt the nonlocal complete polarization BSA assisted by the spatial entanglement [51-54]. Bob can obtain the encoded messages according to the BSA results. This one-step DI-QSDC protocol is unconditionally secure in theory. It has some attractive advantages. First, it can simplify the operation of DI-QSDC. Second, it can effectively reduce DI-QSDC's message loss. In particular, when combined with the hyperentanglement heralded amplification and the hyperentanglement purification, the message loss and the message error caused by the channel noise can be completely eliminated.

This paper is organized as follows. In sect. 2, we explain this one-step DI-QSDC protocol in detail. In sect. 3, we simulate the secrete message capacity of this one-step DI-QSDC protocol against the collective attacks. In sect. 4, we propose a modified one-step DI-QSDC protocol with the hyperentanglement heralded amplification and the hyperentanglement purification. In sect. 5, we make a discussion and provide a conclusion in sect. 6.

2 One-step DI-QSDC protocol

The security of the one-step DI-QSDC protocol does not rely on any detailed description, or trust, of the inner workings of users' devices. Figure 1 provides the schematic principle of the one-step DI-QSDC protocol. It uses the polarization-spatial-mode hyperentangled photon pairs. The four Bell states in polarization DOF have the form of

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

where $|H\rangle$ and $|V\rangle$ represent the horizontal polarization and the vertical polarization, respectively. Meanwhile, in the spatial-mode DOF, the four Bell states in Bob's location are

$$\begin{aligned}|\phi_{\rm sB}^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|b_1 b_1'\rangle \pm |b_2 b_2'\rangle),\\ |\psi_{\rm sB}^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|b_1 b_2'\rangle \pm |b_2 b_1'\rangle),\end{aligned} \tag{2}$$

where b_1, b_2, b_1' and b_2' represent the spatial modes in Bob's location.

Step 1 Bob prepares an ordered N polarization-spatial-mode hyperentangled photon pairs in $|\Phi^+\rangle_i = |\phi_{\rm p}^+\rangle \otimes |\phi_{\rm sB}^+\rangle$ ($i = 1, 2, \ldots, N$). He divides the N hyperentangled photon pairs into two photon sequences, the traveling (T) photon sequence $[T_1, T_2, T_3, \ldots, T_N]$ and the home (H) photon sequence $[H_1, H_2, H_3, \ldots, H_N]$. Then, he sends the T photons

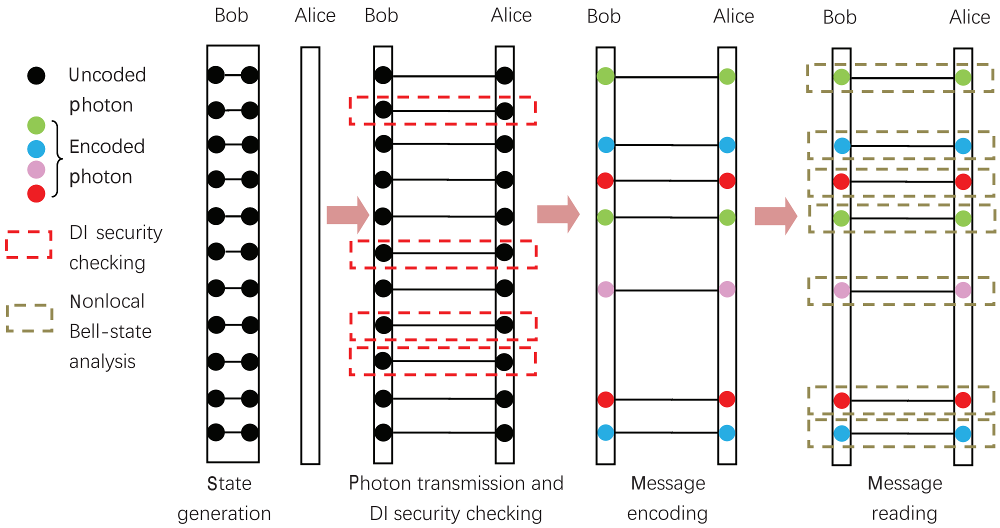

Figure 1 (Color online) The basic diagram of the one-step DI-QSDC protocol. The message receiver Bob prepares N pairs of polarization-spatial-mode hyperentangled photons in $|\phi^+_{\rm p}\rangle \otimes |\phi^+_{\rm sB}\rangle$. He sends one photon of each photon pair to the message sender Alice. The security of the photon transmission process is guaranteed by the CHSH test (the red dotted box). Then, Alice encodes messages in the polarization DOF. Both parties perform the nonlocal complete polarization Bell state analysis (the grey dotted box) and Bob can finally obtain the encoded messages.

to Alice through the quantum channel and stores the H photons into the quantum memory devices.

Step 2 After all the T photons are sent to Alice, if there is no eavesdropping or error, the two parties share the hyperentangled state $|\Phi^+\rangle_i = |\phi^+_{\rm p}\rangle \otimes |\phi^+_{\rm sAB}\rangle$, where $|\phi^+_{\rm sAB}\rangle$ belongs to the spatial-mode Bell states as:

$$\begin{aligned} |\phi^{\pm}_{\rm sAB}\rangle &= \frac{1}{\sqrt{2}}(|a_1b_1\rangle \pm |a_2b_2\rangle), \\ |\psi^{\pm}_{\rm sAB}\rangle &= \frac{1}{\sqrt{2}}(|a_1b_2\rangle \pm |a_2b_1\rangle), \end{aligned} \tag{3}$$

where a_1 and a_2 represent two spatial modes in Alice's location. Alice stores all her photons in quantum memory devices. Then, she randomly selects some photon pairs as the security checking photon pairs and announces their positions through a classical channel. Both parties extract the security checking photons and measure them with the bases chosen randomly in both DOFs. In both DOFs, Alice has four possible measurements bases as $A_0 = \sigma_z$, $A_1 = \frac{\sigma_z+\sigma_x}{2}$, $A_2 = \frac{\sigma_z-\sigma_x}{2}$, and $A_3 = \sigma_x$. Bob has two possible measurements bases $B_1 = \sigma_z$ and $B_2 = \sigma_x$ [45, 46]. All the measurement results $A' = \{A'_{0\rm p(s)}, A'_{1\rm p(s)}, A'_{2\rm p(s)}, A'_{3\rm p(s)}\}$ and $B' = \{B'_{1\rm p(s)}, B'_{2\rm p(s)}\}$ have the binary outcomes $+1$ and -1. If Alice or Bob obtains an inconclusive result (the photon detectors do not click any photon), she or he randomly sets the measurement result to be $+1$ or -1. We suppose the marginals are random for each measurement. After the measurements, the parties announce their measurement bases and measurement results in both DOFs.

There are four different cases. In the first case, Alice chooses $A_{1\rm p(s)}$ or $A_{2\rm p(s)}$. The parties use their measurement results to estimate the CHSH polynomial in polarization (spatial-mode) DOF as:

$$\begin{aligned} S_{\rm p} &= \langle A'_{1\rm p}B'_{1\rm p}\rangle + \langle A'_{1\rm p}B'_{2\rm p}\rangle + \langle A'_{2\rm p}B'_{1\rm p}\rangle - \langle A'_{2\rm p}B'_{2\rm p}\rangle, \\ S_{\rm s} &= \langle A'_{1\rm s}B'_{1\rm s}\rangle + \langle A'_{1\rm s}B'_{2\rm s}\rangle + \langle A'_{2\rm s}B'_{1\rm s}\rangle - \langle A'_{2\rm s}B'_{2\rm s}\rangle. \end{aligned} \tag{4}$$

$\langle A'_{i\rm p(s)}B'_{j\rm p(s)}\rangle$ is defined as the probability (P) of $A'_{i\rm p(s)} = B'_{j\rm p(s)}$ subtracts that of $A'_{i\rm p(s)} \neq B'_{j\rm p(s)}$ ($i = 1, 2$, $j = 1, 2$). In the second case, Alice chooses $A_{0\rm p(s)}$ and Bob chooses $B_{1\rm p(s)}$. They use their measurement results to estimate the bit-flip error rate ($Q_{\rm p(s)1}$) in the polarization (spatial-mode) DOF as:

$$\begin{aligned} Q_{\rm p1} &= P(A'_{0\rm p} \neq B'_{1\rm p}), \\ Q_{\rm s1} &= P(A'_{0\rm s} \neq B'_{1\rm s}). \end{aligned} \tag{5}$$

In the third case, Alice chooses $A_{3\rm p(s)}$ and Bob chooses $B_{2\rm p(s)}$. They use the measurement results to estimate the phase-flip error rate ($Q_{\rm p(s)2}$) in the polarization (spatial-mode) DOF as:

$$\begin{aligned} Q_{\rm p2} &= P(A'_{3\rm p} \neq B'_{2\rm p}), \\ Q_{\rm s2} &= P(A'_{3\rm s} \neq B'_{2\rm s}). \end{aligned} \tag{6}$$

In the last case, Alice chooses $A_{0\rm p(s)}$ and Bob chooses $B_{2\rm p(s)}$, or Alice chooses $A_{3\rm p(s)}$ and Bob chooses $B_{1\rm p(s)}$. The parties discard their measurement results.

$S_{\rm p(s)} \leq 2$ (the well-known CHSH inequality) indicates that the parties' measurement results in polarization (spatial-mode) DOF are classically correlated. In this case, there exists a trivial attack for Eve to eavesdrop on all the photons without being detected, so that the photon transmission process is not secure. Therefore, if $S_{\rm p(s)} \leq 2$, the parties have to discard the communication. On the other hand, $S_{\rm p} > 2$ and $S_{\rm s} > 2$ indicate that the parties' measurement results in both DOFs are non-locally correlated, and they can bound

Eve's photon interception rate. If $S_{\rm p}$ ($S_{\rm s}$) reaches the maximal value of $2\sqrt{2}$, the parties share the maximally entangled state $|\phi^+_{\rm p}\rangle$ ($|\phi^+_{\rm sAB}\rangle$). Under this case, Eve's photon interception rate can be reduced to zero [55]. Therefore, if both $S_{\rm p} > 2$ and $S_{\rm s} > 2$, the parties regard the photon transmission process to be secure.

Step 3 When the parties ensure the security of the photon transmission process, they extract the stored photons from the memory devices. Alice encodes her messages by performing the four unitary operations $U_{0\rm p}$, $U_{1\rm p}$, $U_{2\rm p}$, and $U_{3\rm p}$ on her photons. The four unitary operations can be written as:

$$\begin{aligned}
U_{0\rm p} &= I_{\rm p} = |H\rangle\langle H| + |V\rangle\langle V|,\\
U_{1\rm p} &= \sigma_{z\rm p} = |H\rangle\langle H| - |V\rangle\langle V|,\\
U_{2\rm p} &= \sigma_{x\rm p} = |V\rangle\langle H| + |H\rangle\langle V|,\\
U_{3\rm p} &= i\sigma_{x\rm p} = |H\rangle\langle V| - |V\rangle\langle H|.
\end{aligned} \tag{7}$$

$U_{0\rm p}$, $U_{1\rm p}$, $U_{2\rm p}$, and $U_{3\rm p}$ can make $|\phi^+_{\rm p}\rangle$ evolve to $|\phi^+_{\rm p}\rangle$, $|\phi^-_{\rm p}\rangle$, $|\psi^+_{\rm p}\rangle$, and $|\psi^-_{\rm p}\rangle$, respectively. We define that $U_{0\rm p}$, $U_{1\rm p}$, $U_{2\rm p}$, and $U_{3\rm p}$ represent the classical messages 00, 01, 10, and 11, respectively. Meanwhile, Bob also randomly performs one of the four above unitary operations on each of his photons.

Step 4 Alice and Bob perform the nonlocal polarization BSA assisted with the entanglement in the spatial mode DOF. The diagram of the nonlocal BSA is shown in Figure 2. The parties can distinguish four Bell states in the polarization DOF heralded by the detector responses. We provide the specific formula derivation in Appendix A1. With the spatial entanglement of $|\phi^+_{\rm sAB}\rangle$, the polarization BSA results and the corresponding detector responses are shown in Table 1. After the measurement, only Alice announces her detector clicks in the classical channel. Bob can obtain the BSA results based on their detector responses, and read out Alice's messages combined with his own unitary operations. For example, when the detectors D_1 and D_6 click photons and Bob's unitary operation is $U_{2\rm p}$, Bob can obtain that the polarization BSA result is $|\phi^-_{\rm p}\rangle$. Combined with his unitary operation, Bob can deduce Alice's unitary operation to be $U_{3\rm p}$, corresponding to the message of 11.

3 The secrete message capacity of the one-step DI-QSDC protocol against the collective attacks

In the one-step DI-QSDC protocol, we require that Eve obeys the laws of quantum physics. Meanwhile, he cannot obtain the information of both parties' local operations or change the parties' measurement results. In this way, we can even assume that Eve can control the entanglement source and know both parties' measurement results. As Eve does not know Bob's random unitary operations, he still cannot read out the encoded messages. In the security checking process, the parties can only use the observed relation between the measurement basis (input) and the measurement result (outcome) to bound Eve's knowledge. Here, we consider the collective attack, in which Eve performs the same attack on each system of Alice and Bob. In this way, all the photon pairs have the same form after the photon transmission. We assume that the total photon state shared by Alice, Bob, and Eve has the product form of $|\Gamma_{\rm ABE}\rangle = |\tau_{\rm ABE}\rangle^{\otimes n}$, where $|\tau_{\rm ABE}\rangle = |\tau_{\rm ABEp}\rangle \otimes |\tau_{\rm ABEs}\rangle$ and n means the number of the hyperentangled photon pairs after the photon transmission. We also require that the parties' measurement results are only a function of the current inputs.

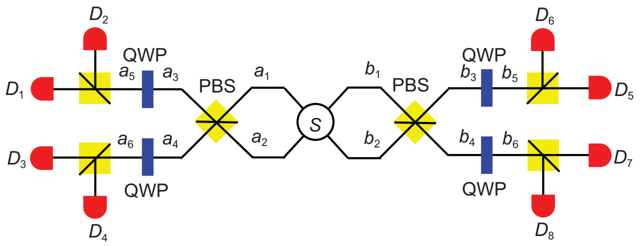

Figure 2 (Color online) The diagram of the nonlocal Bell state analysis in the polarization DOF assisted by the spatial entanglement [51]. PBS represents the polarization beam splitter, which can totally transmit the horizontally polarized photon and reflect the vertically polarized photon. QWP means the quarter wave plate, which can make the Hadamard operation in the polarization DOF. D_1-D_8 represent the single photon detectors.

Table 1 The polarization Bell states corresponding to the detector responses

BSA result	Detector responses			
$\lvert\phi^+_{\rm p}\rangle$	D_1D_5	D_2D_6	D_3D_7	D_4D_8
$\lvert\phi^-_{\rm p}\rangle$	D_1D_6	D_2D_5	D_3D_8	D_4D_7
$\lvert\psi^+_{\rm p}\rangle$	D_1D_7	D_2D_8	D_3D_5	D_4D_6
$\lvert\psi^-_{\rm p}\rangle$	D_1D_8	D_2D_7	D_3D_6	D_4D_5

As the photons only transmit in the quantum channel for one round, the security analysis of the one-step DI-QSDC protocol is quite similar to that of the DI-QKD [42, 43]. We define the secrete message capacity ($E_{\rm c}$) as the amount of the transmitted correct and secure messages divided by the total amount of the encoded hyperentangled photon pairs. We can only use the observed parameters $Q_{\rm p1}$, $Q_{\rm p2}$, $Q_{\rm s1}$, $Q_{\rm s2}$, $S_{\rm p}$, and $S_{\rm s}$. Although we have specified a particular state to produce these correlations, in the practical application, we do not assume anything about the implementation of the correlations.

We first research the ideal scenario. In the ideal quantum scenario, if there is no eavesdropping, all the photons can be transmitted to Alice correctly. As a result, the CHSH polynomials in both DOFs meet $S_{\rm p} = S_{\rm s} = 2\sqrt{2}$, and the error rates meet $Q_{\rm p1} = Q_{\rm p2} = Q_{\rm s1} = Q_{\rm s2} = 0$. In this case, any eavesdropping behavior during the photon transmission process would result in a decline in the CHSH polynomials and a rise in the error rates in both DOFs, thus can be easily detected during the security checking. In this way, the one-step DI-QSDC protocol is unconditionally secure. As each encoded polarization Bell state encodes 2 bits of messages, the value of E_c is 2.

Next, we consider the security of the one-step DI-QSDC protocol with the practical imperfect devices and the noisy channel. According to the Csiszár-Körner theory [56], we can obtain E_c as:

$$E_c = 2(I_{AB} - I_{AE}), \tag{8}$$

where I_{AB} and I_{AE} represent the mutual information between Alice and Bob, and between Alice and Eve, respectively. I_{AB} can be calculated as:

$$I_{AB} = 1 - h(Q_{pt}). \tag{9}$$

Here, h is the binary entropy with the form of

$$h(x) = -x\log_2 x - (1-x)\log_2(1-x), \tag{10}$$

and Q_{pt} represents the total error rate in the polarization DOF.

In the practical experiment, we have to consider the photon loss and the decoherence. The photon loss can be divided into two categories, the local loss and the transmission loss. The local loss represents the photon loss occurring within the users' laboratory. We define the local efficiency η_l as the product of the coupling efficiency η_c between the photon source and the fiber, the efficiency η_m of the quantum memory device, and the detection efficiency η_d of the photon detector, $\eta_l = \eta_c\eta_m\eta_d$. The transmission loss means the photon loss occurring during the photon transmission process. The photon transmission rate has the form of $\eta_t = 10^{-\alpha d/10}$ ($\alpha = 0.2$ dB/km, and d is the communication distance between two parties). The decoherence effect during the photon transmission process would degrade the entanglement and increase the bit-flip error rate and the phase-flip error rate in each DOF. Here, we consider a general white-noise model in both DOFs, where the maximally entangled states $|\phi_p^+\rangle$ and $|\phi_s^+\rangle$ degrade to the mixed states as:

$$\begin{aligned}\rho_p &= F_p|\phi_p^+\rangle\langle\phi_p^+| + \frac{1-F_p}{3}(|\psi_p^+\rangle\langle\psi_p^+| + |\phi_p^-\rangle\langle\phi_p^-| \\ &\quad + |\psi_p^-\rangle\langle\psi_p^-|), \\ \rho_s &= F_s|\phi_{sAB}^+\rangle\langle\phi_{sAB}^+| + \frac{1-F_s}{3}(|\psi_{sAB}^+\rangle\langle\psi_{sAB}^+| \\ &\quad + |\phi_{sAB}^-\rangle\langle\phi_{sAB}^-| + |\psi_{sAB}^-\rangle\langle\psi_{sAB}^-|).\end{aligned} \tag{11}$$

In this way, after the photon transmission, the parties finally share N pairs of mixed states as:

$$\begin{aligned}\rho_{out} &= \eta_t\eta_l^2\rho_p\otimes\rho_s + \frac{1}{4}\eta_l(1-\eta_t\eta_l)(|H\rangle\langle H| + |V\rangle\langle V|) \\ &\quad \otimes(|b_1\rangle\langle b_1| + |b_2\rangle\langle b_2|) + \frac{1}{4}\eta_t\eta_l(1-\eta_l)(|H\rangle\langle H| + |V\rangle\langle V|) \\ &\quad \otimes(|a_1\rangle\langle a_1| + |a_2\rangle\langle a_2|) + (1-\eta_l)(1-\eta_t\eta_l)|\text{vac}\rangle\langle\text{vac}|.\end{aligned} \tag{12}$$

In theory, if there is no eavesdropping, the error rates and CHSH polynomials in both DOFs can be calculated as [41-43]:

$$\begin{aligned}Q_{p1} + Q_{p2} &= \frac{1}{2}(1-\eta_t\eta_l^2) + \eta_t\eta_l^2(1-F_p) \\ &= \frac{1}{2}(1+\eta_t\eta_l^2 - 2\eta_t\eta_l^2F_p), \\ S_p &= 2\sqrt{2}\eta_t\eta_l^2F_p, \\ Q_{s1} + Q_{s2} &= \frac{1}{2}(1-\eta_t\eta_l^2) + \eta_t\eta_l^2(1-F_s) \\ &= \frac{1}{2}(1+\eta_t\eta_l^2 - 2\eta_t\eta_l^2F_s), \\ S_s &= 2\sqrt{2}\eta_t\eta_l^2F_s.\end{aligned} \tag{13}$$

We first calculate Q_{pt}. If the bit-flip error or phase-flip error occurs in a DOF, it would make the BSA obtain the wrong result, thus making Bob obtain the wrong messages. It is noticed that when the entanglement in both DOFs suffers from the same kind of error, Bob can still read out the correct messages (The specific derivation is shown in Appendix A2). In the white-noise model, we have $Q_{p1} = Q_{p2}$ and $Q_{s1} = Q_{s2}$. In this way, we can calculate Q_{pt} as:

$$\begin{aligned}Q_{pt} &= 1-(1-Q_{p1}-Q_{p2})(1-Q_{s1}-Q_{s2}) \\ &\quad - Q_{p1}Q_{s1} - Q_{p2}Q_{s2} \\ &= 2Q_{s1} + 2Q_{p1} - 6Q_{s1}Q_{p1}.\end{aligned} \tag{14}$$

When $S_s > 2$ and $S_p > 2$, we can estimate the Holevo quantities in the spatial-mode and polarization DOFs by

$$\begin{aligned}\chi(S_s) &\le h\left(\frac{1+\sqrt{(S_s/2)^2-1}}{2}\right), \\ \chi(S_p) &\le h\left(\frac{1+\sqrt{(S_p/2)^2-1}}{2}\right),\end{aligned} \tag{15}$$

which were proven in refs. [42, 43]. In this way, we can obtain that the upper bound of Eve's photon interception rate equals the minimum value between $\chi(S_s)$ and $\chi(S_p)$. In the practical experimental condition, the entanglement in the spatial-mode DOF often has stronger noise robustness than that in the polarization DOF [57], so that it is naturally $F_s > F_p$. In this way, we can obtain $S_s > S_p$ and $\chi(S_s) < \chi(S_p)$. In practical applications, we can utilize $\chi(S_s)$ to bound Eve's photon interception rate. When Eve intercepts some photons sent from Bob, he prepares some hyperentangled photon pairs in $|\Phi^+\rangle = |\phi_p^+\rangle\otimes|\phi_s^+\rangle$ and sends one photon of each photon pair to Alice through a high-quality quantum channel. After Alice encodes her messages on these photons, Eve and Alice make the nonlocal polarization BSA, and Eve can finally obtain Alice's encoded messages according to their measurement results. Therefore, we can bound the message leakage rate (I_{AE}) of the one-step DI-QSDC protocol by

$$I_{\mathrm{AE}} = \chi(S_{\mathrm{s}}) \le h\left(\frac{1+\sqrt{(S_{\mathrm{s}}/2)^2-1}}{2}\right), \tag{16}$$

which equals DI-QKD's key leakage rate [43].

Taking eqs. (14) and (16) to eq. (8), we can bound the secrete message capacity E_{c} as:

$$\begin{aligned} E_{\mathrm{c}} \ge 2\Bigg[&1 - h(2Q_{\mathrm{s1}} + 2Q_{\mathrm{p1}} - 6Q_{\mathrm{s1}}Q_{\mathrm{p1}}) \\ &- h\left(\frac{1+\sqrt{(S_{\mathrm{s}}/2)^2-1}}{2}\right)\Bigg]. \end{aligned} \tag{17}$$

Meanwhile, we can also obtain the message loss rate (r_{loss}) and the message error rate (r_{error}) of the one-step DI-QSDC protocol as:

$$\begin{aligned} r_{\mathrm{loss}} &= 1 - \eta_{\mathrm{t}}\eta_{\mathrm{l}}^2, \\ r_{\mathrm{error}} &= Q_{\mathrm{pt}}. \end{aligned} \tag{18}$$

It is noticed that as the one-step DI-QSDC protocol reduces the photon transmission rounds, its r_{loss} is lower than that of the original two-step DI-QSDC protocol ($r_{\mathrm{loss0}} = 1 - \eta_{\mathrm{t}}^2\eta_{\mathrm{l}}^2$).

Next, we compare this one-step DI-QSDC protocol with the DI-QKD protocol [42, 43] and the original two-step DI-QSDC protocol [33]. The bit error rate Q_{QKD} and the secret key generation rate R of the DI-QKD protocol can be calculated as [42, 43]:

$$\begin{aligned} Q_{\mathrm{QKD}} &= \frac{1}{2}(1 - \eta_{\mathrm{t}}\eta_{\mathrm{l}}^2 F_{\mathrm{p}}), \\ R &\ge 1 - h(Q_{\mathrm{QKD}}) - h\left(\frac{1+\sqrt{(S_{\mathrm{p}}/2)^2-1}}{2}\right). \end{aligned} \tag{19}$$

In the two-step DI-QSDC protocol [33], the total error rate Q_{t} and the secrecy message capacity E_{c0} can be calculated as:

$$\begin{aligned} Q_{\mathrm{t}} &= \frac{1}{2}(1 + \eta_{\mathrm{t}}^2\eta_{\mathrm{l}}^2 - 2\eta_{\mathrm{t}}^2\eta_{\mathrm{l}}^2 F_{\mathrm{p}}^2), \\ E_{\mathrm{c0}} &\ge 2\left[1 - H(Q_{\mathrm{t}}) - h\left(\frac{1+\sqrt{(S_{\mathrm{p}}/2)^2-1}}{2}\right)\right]. \end{aligned} \tag{20}$$

In Figure 3, we show the values of Q_{pt}, Q_{t}, and Q_{QKD} as a function of the communication distance d. In Figure 4, we provide the values of E_{c}, E_{c0}, and R altered with d. We set the local efficiency $\eta_{\mathrm{l}} = 0.98$. In the one-step DI-QSDC protocol, we control $F_{\mathrm{p}} = F_{\mathrm{s}} = 1$ and 0.98, while in the two-step DI-QSDC protocol and the DI-QKD protocol, we control $F_{\mathrm{p}} = 1$ and 0.98, respectively. It can be found that Q_{QKD} is the lowest, for DI-QKD only relies on the entanglement in one DOF and the photons only transmit in the quantum channel for one round. The two-step DI-QSDC protocol also relies on the entanglement in one DOF, but the photons should transmit in the quantum channel for two rounds, which will increase the error rate. The one-step DI-QSDC protocol adopts the hyperentanglement in two DOFs. The error in any DOF would increase Q_{pt}, so that Q_{pt} is higher than Q_{t} and Q_{QKD} even though the photons only transmit in the quantum channel for one round. The values of Q_{pt}, Q_{t},

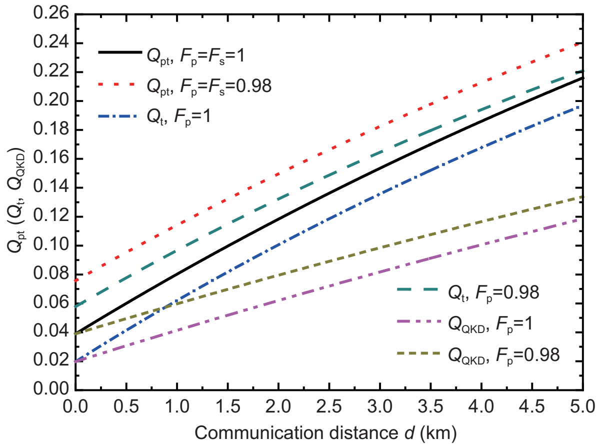

Figure 3 (Color online) Q_{pt} of the one-step DI-QSDC protocol, Q_{t} of the two-step DI-QSDC [33], and Q_{QKD} of the DI-QKD protocol [43] altered with the communication distance d. Here, we set the local efficiency $\eta_{\mathrm{l}} = 0.98$. In the two-step DI-QSDC protocol and the DI-QKD protocol, we control $F_{\mathrm{p}} = 1, 0.98$, while in the one-step DI-QSDC protocol, we control $F_{\mathrm{p}} = F_{\mathrm{s}} = 1, 0.98$, respectively.

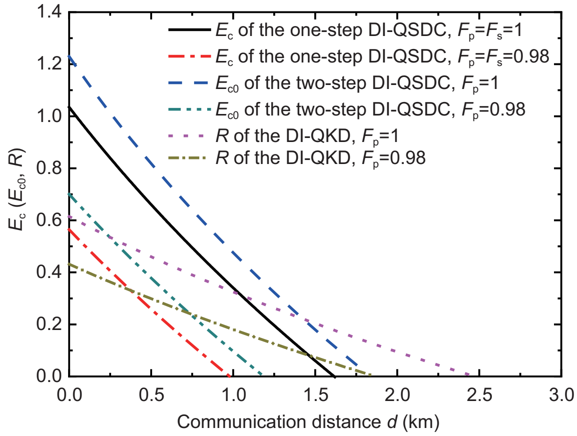

Figure 4 (Color online) E_{c} of the one-step DI-QSDC protocol, E_{c0} of the two-step DI-QSDC protocol [33], and R of the DI-QKD protocol [43] altered with the communication distance d. Here, we consider the local efficiency $\eta_{\mathrm{l}} = 0.98$. In the DI-QKD protocol and the two-step DI-QSDC protocol, we control $F_{\mathrm{p}} = 1, 0.98$, while in this one-step DI-QSDC protocol, we control $F_{\mathrm{p}} = F_{\mathrm{s}} = 1, 0.98$, respectively.

and $Q_{\rm QKD}$ influence the secrecy message capacity and key generation rate. In Figure 4, $E_{\rm c}$, $E_{\rm c0}$, and R all reduce largely with the growth of the communication distance, and $E_{\rm c}$ is slightly lower than $E_{\rm c0}$. In relatively low communication distance, $E_{\rm c}$ and $E_{\rm c0}$ are higher than R, because each photon pair in the one-step DI-QSDC protocol and the two-step DI-QSDC protocol can transmit 2 bits of messages, while each photon pair in the DI-QKD protocol can only generate 1 bit of key. With the growth of communication distance, DI-QKD's advantage in the low error rate makes R exceed $E_{\rm c}$ and $E_{\rm c0}$. Meanwhile, the maximal communication distances of the one-step DI-QSDC protocol are about 1.61 and 0.96 km corresponding to $F_{\rm p} = F_{\rm s} = 1$ and 0.98, respectively, which are lower than those of the two-step DI-QSDC protocol and the DI-QKD protocol. On the other hand, considering $F_{\rm p} = F_{\rm s}$, the threshold value of $F_{\rm p}$ ($F_{\rm s}$) is about 0.923. If $F_{\rm p}$ ($F_{\rm s}$) is lower than 0.923, no correct messages can be transmitted to Bob.

4 The modified one-step DI-QSDC protocol

From the above section, the photon transmission loss and decoherence caused by the channel noise largely reduce the secrecy message capacity and even threaten the security of the one-step DI-QSDC protocol. To solve these two problems, we propose a modified one-step DI-QSDC protocol assisted with the hyperentanglement heralded amplification and the hyperentanglement purification.

In 2019, our group proposed a heralded amplification protocol for an arbitrary polarization-spatial-mode hyperentangled state as [58]:

$$|\varphi\rangle = (\alpha|HH\rangle + \beta|VV\rangle) \otimes (\sigma|a_1b_1\rangle + \xi|a_2b_2\rangle). \tag{21}$$

By performing the heralded amplification, we can effectively increase the fidelity of the hyperentangled state to very close to 1 while keeping its spatial and polarization features unchanged. Moreover, this amplification protocol only requires the common linear-optical elements, so that it can be realized under current experimental condition.

Entanglement purification is a reliable method to distill high-quality entanglement from degraded low-quality entangled ensembles [59-70]. In recent years, some attractive hyperentanglement purification protocols (HEPPs) were proposed [71-75]. For example, in 2014, Ren et al. [72] proposed a two-step HEPP for the nonlocal polarization-spatial-mode hyperentangled state. By successfully performing the HEPP, the parties can increase the fidelity in each DOF when the initial fidelity in each DOF is higher than $\frac{1}{2}$. Moreover, the parties can repeat the HEPP to further increase the fidelity of the hyperentangled state.

Figure 5 shows the diagram of the modified one-step DI-QSDC protocol. In detail, once Bob sends a photon of a hyperentangled photon pair to Alice, Alice performs the heralded amplification protocol in ref. [58]. When the amplification protocol is successful, it indicates that the photon arrives at Alice's location. Alice announces Bob to keep the corresponding photon. Otherwise, if the amplification fails, it indicates that the photon is lost during the transmission. Alice announces Bob to discard his corresponding photon. In this way, the parties can nearly eliminate the influence of photon transmission loss. After that, the parties need to repeat the HEPP in ref. [72] to increase the fidelity of $|\phi^+_{\rm p}\rangle\otimes|\phi^+_{\rm sAB}\rangle$ to the expected value, i.e., above 0.99. In this way, if no eavesdropping exists, the CHSH polynomials $S'_{\rm p}$ and $S'_{\rm s}$ can be very close to $2\sqrt{2}\eta_1^2$ and the error rates $Q'_{\rm p1} + Q'_{\rm p2}$, $Q'_{\rm s1} + Q'_{\rm s2}$ will be close to $\frac{1}{2}(1-\eta_1^2)$. The message leakage rate can be effectively reduced to $I'_{\rm AE} \le h(\frac{1+\sqrt{(S'_{\rm s}/2)^2-1}}{2})$. Moreover, the message loss and message error caused by the photon transmission loss and the decoherence can be nearly eliminated and the communication distance can be largely extended. The secret message capacity of the modified one-step DI-QSDC protocol can be calculated as:

$$\begin{aligned} E_{\rm cm} \ge & P_{\rm am}P_{\rm hepp}2\Bigg[1 - h(2Q'_{\rm s1} + 2Q'_{\rm p1} - 6Q'_{\rm s1}Q'_{\rm p1}) \\ & - h\left(\frac{1+\sqrt{(S'_{\rm s}/2)^2-1}}{2}\right)\Bigg], \end{aligned} \tag{22}$$

where $P_{\rm am}$ and $P_{\rm hepp}$ are the total success probability of the heralded hyperentanglement amplification and the HEPP, respectively. For example, we control the initial fidelity in each DOF as 0.8 and the communication distance as 50 km. With the help of the heralded amplification and the HEPP, we can increase the photon transmission rate from 0.1 to 0.95 and fidelity in each DOF from 0.8 to be higher than 0.99. In this case, considering the photon source with the excitation repetition rate of 10 GHz [76], we can still obtain $E_{\rm cm} \approx 7$ bit/s.

5 Discussion

The original QSDC and DI-QSDC protocols all adopt local BSA, so that the encoded photon pairs should be sent to the message receiver by two rounds of photon transmission. After receiving the encoded photon pairs, the message receiver can read out the encoded messages by performing the local BSA without the additional classical communication. In the paper, we propose the first one-step DI-QSDC protocol, which only requires one round of polarization-spatial-mode hyperentanglement distribution in the quantum channel. The key element of this one-step DI-QSDC protocol is the non-

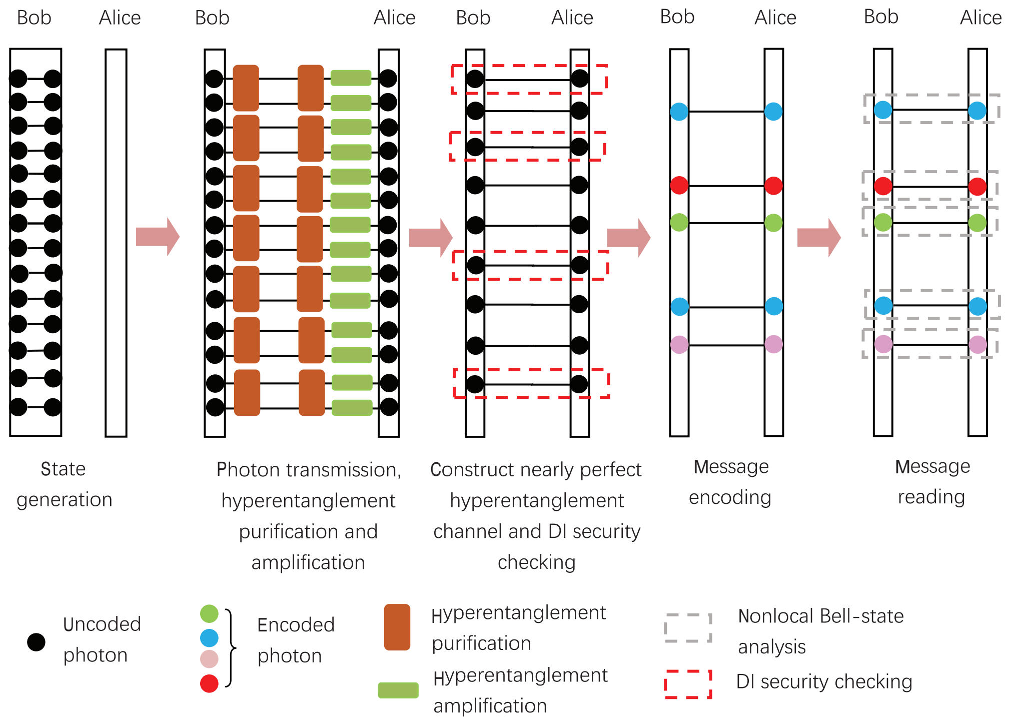
Bob
Alice
Bob
Alice
Bob
Alice
Bob
Alice
Bob
Alice
State generation
Photon transmission, hyperentanglement purification and amplification
Construct nearly perfect hyperentanglement channel and DI security checking
Message encoding
Message reading
Uncoded photon
Encoded photon
Hyperentanglement purification
Hyperentanglement amplification
Nonlocal Bell-state analysis
DI security checking

Figure 5 (Color online) The diagram of the modified one-step DI-QSDC protocol. After the photon transmission process, the parties perform the hyperentanglement heralded amplification [58] and the hyperentanglement purification [72] to solve the photon transmission loss and the decoherence problems, respectively. In this way, the parties can construct the near-perfect hyperentangled quantum channel.

local polarization BSA, which can completely distinguish all the four polarization Bell states assisted by the entanglement in the spatial-mode DOF and the one-way classical communication (Alice announces her measurement results). With the help of the nonlocal BSA, the encoded photons do not need to be sent back, which can effectively simplify the experimental operation.

Although the one-step DI-QSDC has a slightly higher error rate and a lower secrecy message capacity than the original two-step DI-QSDC protocol [33] and DI-QKD protocol [42, 43], it still has some attractive advantages in practical applications.

First, the DI-QKD can only distribute 1 bit of random key with a photon pair. For transmitting secret messages, it requires the extra one-time pad and the two-way classical communication (Alice and Bob announce their measurement bases). Moreover, the parties also require secure encryption, perfect key management, and secure decryption. In contrast, our one-step DI-QSDC protocol can directly transmit 2 bits of secret messages assisted with the one-way classical communication. Considering the classical communication time of t_c, the photon transmission time of t_q and neglecting the local operation time and security checking time, one round of the DI-QKD based communication consumes $t_q + 3t_c$, while one round of the one-step DI-QSDC only consumes $t_q + t_c$. Therefore, the practical communication efficiency C of the DI-QKD based communication and the one-step DI-QSDC can be respectively calculated as:

$$\begin{aligned} C_{\mathrm{QKD}} &= \frac{1}{t_q + 3t_c} R, \\ C_{\text{one-step QSDC}} &= \frac{1}{t_q + t_c} E_c. \end{aligned} \tag{23}$$

If we set $t_q = t_c$, it can be found that the one-step DI-QSDC has higher practical communication efficiency.

Second, for transmitting 2 bits of secret messages per entangled photon pair, the two-step DI-QSDC requires the local complete BSA. Actually, current local complete BSA protocols all require the nonlinear optical elements, i.e., the cross-Kerr medium [77, 78] and the artificial atoms [79-81]. The local BSA in linear optics can only distinguish two of the four polarization Bell states so that the two-step DI-QSDC protocol can only transmit 1 bit of message per photon pair in the practical experimental condition. However, the nonlocal complete polarization BSA adopted in the one-step DI-QSDC protocol is totally in linear optics and feasible under the current experimental condition.

Third, in the original two-step DI-QSDC protocol [33], the parties cannot perform the entanglement purification after the second photon transmission process. The reason is that the entanglement purification may change the polarization Bell states, thus destroying the encoded messages [33].

In this way, the two-step DI-QSDC protocol cannot eliminate the message error problem caused by the decoherence during the second photon transmission process, which is a big obstacle in practical applications. In particular, if one hopes to further extend DI-QSDC's communication distance, the quantum repeater is necessary. For the two-step DI-QSDC, the quantum repeater should be used in both rounds of photon transmission. However, it is difficult to implement the quantum repeater during the second photon transmission process without entanglement purification. In contrast, the one-step DI-QSDC protocol only requires one round of photon transmission. As long as the parties can construct the nearly perfect quantum channel with the help of the hyperentanglement heralded amplification and hyperentanglement purification, the one-step DI-QSDC can nearly eliminate the message loss and the message error caused by the channel noise. Moreover, the quantum repeater can also be implemented with the help of entanglement purification. Therefore, combined with the quantum repeater technology, it is possible to realize the one-step DI-QSDC with an arbitrarily long distance.

Finally, we discuss the experimental realization. This one-step DI-QSDC protocol uses the polarization-spatial-mode hyperentanglement. The generation of hyperentanglement has been widely researched [82-86]. In 2004, Yabushita et al. [82] reported that photon pairs produced by the spontaneous parametric down conversion (SPDC) source can be hyperentangled in polarization and spatial-mode DOFs, polarization, spatial, energy, and time-bin DOFs, polarization and frequency DOFs. Soon later, the group of Barreiro [83] realized the first quantum system hyperentangled in polarization, spatial-mode, and time energy DOFs in the experiment. Recently, researchers also experimentally demonstrated the distribution of the polarization-time-bin hyperentanglement [87] and the polarization-spatial-mode hyperentanglement [88]. Meanwhile, the hyperentanglement storage in the path and the orbital angular momentum DOFs has also been realized in experiments [89]. Combined with the complete hyperentangled BSA [78] and hyperentanglement purification [72], the hyperentanglement swapping is also possible to realize. Based on the above attractive achievements, the one-step DI-QSDC with an arbitrarily long distance may be realized with the help of the hyperentanglement quantum repeaters.

6 Conclusion

In conclusion, QSDC can directly transmit secret messages between communication parties without keys. In the practical imperfect experimental condition, DI-QSDC can effectively enhance QSDC's security. In the paper, we propose the first one-step DI-QSDC protocol. In the protocol, the message receiver Bob generates a large amount of polarization-spatial-mode hyperentangled photon pairs and sends one photon of each photon pair to the information sender Alice. The parties guarantee the security of the photon transmission process by the observation of the data conclusively violating the CHSH inequality. Then, Alice encodes her messages on the photons in the polarization DOF by performing four unitary operations and Bob also randomly performs the unitary operations on his photons. The parties perform the nonlocal complete polarization BSA on each photon pair assisted with the entanglement in spatial-mode DOF and Bob can deduce Alice's encoded messages according to their measurement results combined with his unitary operations. This one-step DI-QSDC protocol is unconditionally secure in theory. The message sender can transmit 2 bits of secure messages to the receiver with one pair of hyperentangled states. In the practical noise channel condition, its message leakage rate equals the photon interception rate in the photon transmission process. This one-step DI-QSDC protocol has some attractive advantages. First, the encoded photons should not be sent back for the local BSA, which can simplify the experimental operation and reduce the message loss. Second, the nonlocal BSA only relies on linear optical elements, so that it is feasible under the current experimental condition. Third, with the help of the hyperentanglement heralded amplification and the HEPP, the parties can construct the near-perfect hyperentanglement channel and completely eliminate the message error and the message loss caused by the channel noise. In particular, it is possible to combine this one-step DI-QSDC protocol with the quantum repeater, which has the potential to realize the one-step DI-QSDC with an arbitrary distance. The one-step DI-QSDC protocol may have application potential in the future quantum communication field.

This work was supported by the National Natural Science Foundation of China (Grant Nos. 11974189, and 12175106).

1 C. H. Bennett, G. Brassard, in *Quantum cryptography: Public key distribution and coin tossing: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, 1984.

2 A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

3 R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, Nat. Phys. **3**, 481 (2007).

4 T. Sasaki, Y. Yamamoto, and M. Koashi, Nature **509**, 475 (2014).

5 S. Wang, Z. Q. Yin, W. Chen, D. Y. He, X. T. Song, H. W. Li, L. J. Zhang, Z. Zhou, G. C. Guo, and Z. F. Han, Nat. Photon. **9**, 832 (2015).

6 W. Liu, Z. Yin, X. Chen, Z. Peng, H. Song, P. Liu, X. Tong, and Y. Zhang, Sci. Bull. **63**, 1034 (2018).

7 Z. X. Cui, W. Zhong, L. Zhou, and Y. B. Sheng, Sci. China-Phys. Mech. Astron. **62**, 110311 (2019).

8 F. Xu, X. Ma, Q. Zhang, H. K. Lo, and J. W. Pan, Rev. Mod. Phys. **92**, 025002 (2020), arXiv: 1903.09051.

9 Y. A. Chen, Q. Zhang, T. Y. Chen, W. Q. Cai, S. K. Liao, J. Zhang, K. Chen, J. Yin, J. G. Ren, Z. Chen, S. L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M. S. Zhao, T. Y. Wang, X. Jiang, L. Zhang, W. Y. Liu, Y. Li, Q. Shen, Y. Cao, C. Y. Lu, R. Shu, J. Y. Wang, L. Li, N. L. Liu, F. Xu, X. B. Wang, C. Z. Peng, and J. W. Pan, Nature **589**, 214 (2021).

10 L. C. Kwek, L. Cao, W. Luo, Y. Wang, S. Sun, X. Wang, and A. Q. Liu, AAPPS Bull. **31**, 15 (2021).

11 Z. Q. Yin, F. Y. Lu, J. Teng, S. Wang, W. Chen, G. C. Guo, and Z. F. Han, Fundam. Res. **1**, 93 (2021).

12 H. Guo, Z. Li, S. Yu, and Y. Zhang, Fundam. Res. **1**, 96 (2021).

13 G. Z. Tang, C. Y. Li, and M. Wang, Quant. Eng. **3**, e79 (2021).

14 X. Wang, X. Sun, Y. Liu, W. Wang, B. Kan, P. Dong, and L. Zhao, Quant. Eng. **3**, e73 (2021).

15 G. L. Long, and X. S. Liu, Phys. Rev. A **65**, 032302 (2002), arXiv: quant-ph/0012056.

16 F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 042317 (2003), arXiv: quant-ph/0308173.

17 F. G. Deng, and G. L. Long, Phys. Rev. A **69**, 052319 (2004), arXiv: quant-ph/0405177.

18 C. Wang, F. G. Deng, Y. S. Li, X. S. Liu, and G. L. Long, Phys. Rev. A **71**, 044305 (2005).

19 M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999), arXiv: quant-ph/9806063.

20 L. Li, D. Qiu, and P. Mateus, J. Phys. A-Math. Theor. **46**, 045304 (2013).

21 R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009), arXiv: quant-ph/0702225.

22 J. Y. Hu, B. Yu, M. Y. Jing, L. T. Xiao, S. T. Jia, G. Q. Qin, and G. L. Long, Light Sci. Appl. **5**, e16144 (2016), arXiv: 1503.00451.

23 W. Zhang, D. S. Ding, Y. B. Sheng, L. Zhou, B. S. Shi, and G. C. Guo, Phys. Rev. Lett. **118**, 220501 (2017), arXiv: 1609.09184.

24 F. Zhu, W. Zhang, Y. Sheng, and Y. Huang, Sci. Bull. **62**, 1519 (2017), arXiv: 1710.07951.

25 Z. Sun, L. Song, Q. Huang, L. Yin, G. Long, J. Lu, and L. Hanzo, IEEE Trans. Commun. **68**, 5778 (2020).

26 D. Pan, Z. Lin, J. Wu, H. Zhang, Z. Sun, D. Ruan, L. Yin, and G. L. Long, Photon. Res. **8**, 1522 (2020).

27 Z. Qi, Y. Li, Y. Huang, J. Feng, Y. Zheng, and X. Chen, Light Sci. Appl. **10**, 183 (2021), arXiv: 2106.13509.

28 S. S. Chen, L. Zhou, W. Zhong, and Y. B. Sheng, Sci. China-Phys. Mech. Astron. **61**, 090312 (2018).

29 P. H. Niu, Z. R. Zhou, Z. S. Lin, Y. B. Sheng, L. G. Yin, and G. L. Long, Sci. Bull. **63**, 1345 (2018).

30 R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G. L. Long, Light Sci. Appl. **8**, 22 (2019), arXiv: 1810.11806.

31 J. Wu, Z. Lin, L. Yin, and G. L. Long, Quant. Eng. **1**, e26 (2019).

32 Z. Gao, T. Li, and Z. Li, Europhys. Lett. **125**, 40004 (2019).

33 L. Zhou, Y. B. Sheng, and G. L. Long, Sci. Bull. **65**, 12 (2020).

34 Z. R. Zhou, Y. B. Sheng, P. H. Niu, L. G. Yin, G. L. Long, and L. Hanzo, Sci. China-Phys. Mech. Astron. **63**, 230362 (2020), arXiv: 1805.07228.

35 L. Yang, J. W. Wu, Z. S. Lin, L. G. Yin, and G. L. Long, Sci. China-Phys. Mech. Astron. **63**, 110311 (2020).

36 T. Li, and G. L. Long, New J. Phys. **22**, 063017 (2020).

37 C. Wang, Fundam. Res. **1**, 91 (2021).

38 G. L. Long, and H. Zhang, Sci. Bull. **66**, 1267 (2021).

39 C. Y. Gao, P. L. Guo, and B. C. Ren, Quant. Eng. **3**, e83 (2021).

40 Y. B. Sheng, L. Zhou, and G. L. Long, Sci. Bull. **67**, 367 (2022).

41 A. Acín, S. Massar, and S. Pironio, New J. Phys. **8**, 126 (2006), arXiv: quant-ph/0605246.

42 A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007), arXiv: quant-ph/0702152.

43 S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009), arXiv: 0903.4460.

44 A. Máttar, and A. Acín, Phys. Scr. **91**, 043003 (2016), arXiv: 1603.02921.

45 R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Nat. Commun. **9**, 459 (2018).

46 V. Zapatero, and M. Curty, Sci. Rep. **9**, 17749 (2019), arXiv: 1905.03591.

47 J. Kołodyński, A. Máttar, P. Skrzypczyk, E. Woodhead, D. Cavalcanti, K. Banaszek, and A. Acín, Quantum **4**, 260 (2020).

48 Y. M. Xie, B. H. Li, Y. S. Lu, X. Y. Cao, W. B. Liu, H. L. Yin, and Z. B. Chen, Opt. Lett. **46**, 1632 (2021), arXiv: 2103.17135.

49 J. S. Bell, Phys. Phys. Fizika **1**, 195 (1964).

50 J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

51 S. P. Walborn, S. Pádua, and C. H. Monken, Phys. Rev. A **68**, 042313 (2003), arXiv: quant-ph/0307212.

52 C. Schuck, G. Huber, C. Kurtsiefer, and H. Weinfurter, Phys. Rev. Lett. **96**, 190501 (2006).

53 J. T. Barreiro, T. C. Wei, and P. G. Kwiat, Nat. Phys. **4**, 282 (2008).

54 X. M. Hu, Y. Guo, B. H. Liu, Y. F. Huang, C. F. Li, and G. C. Guo, Sci. Adv. **4**, eaat9304 (2018), arXiv: 1807.10452.

55 B. S. Cirel'son, Lett. Math. Phys. **4**, 93 (1980).

56 I. Csiszar, and J. Korner, IEEE Trans. Inform. Theor. **24**, 339 (1978).

57 C. Simon, and J. W. Pan, Phys. Rev. Lett. **89**, 257901 (2002), arXiv: quant-ph/0108063.

58 G. Yang, Y. S. Zhang, Z. R. Yang, L. Zhou, and Y. B. Sheng, Quantum Inf. Process. **18**, 317 (2019).

59 J. W. Pan, C. Simon, C. Brukner, and A. Zeilinger, Nature **410**, 1067 (2001), arXiv: quant-ph/0012026.

60 G. Y. Wang, T. Li, Q. Ai, A. Alsaedi, T. Hayat, and F. G. Deng, Phys. Rev. Appl. **10**, 054058 (2018), arXiv: 1802.00111.

61 J. Miguel-Ramiro, and W. Dür, Phys. Rev. A **98**, 042309 (2018), arXiv: 1806.10162.

62 S. Krastanov, V. V. Albert, and L. Jiang, Quantum **3**, 123 (2019).

63 L. Zhou, W. Zhong, and Y. B. Sheng, Opt. Express **28**, 2291 (2020).

64 G. Y. Wang, and G. L. Long, Sci. China-Phys. Mech. Astron. **63**, 220311 (2020).

65 P. S. Yan, L. Zhou, W. Zhong, and Y. B. Sheng, Opt. Express **29**, 571 (2021).

66 P. S. Yan, L. Zhou, W. Zhong, and Y. B. Sheng, Opt. Express **29**, 9363 (2021).

67 X. M. Hu, C. X. Huang, Y. B. Sheng, L. Zhou, B. H. Liu, Y. Guo, C. Zhang, W. B. Xing, Y. F. Huang, C. F. Li, and G. C. Guo, Phys. Rev. Lett. **126**, 010503 (2021), arXiv: 2101.07441.

68 F. Riera-Sábat, P. Sekatski, A. Pirker, and W. Dür, Phys. Rev. Lett. **127**, 040502 (2021), arXiv: 2011.07078.

69 S. Ecker, P. Sohr, L. Bulla, M. Huber, M. Bohmann, and R. Ursin, Phys. Rev. Lett. **127**, 040506 (2021), arXiv: 2101.11503.

70 C. X. Huang, X. M. Hu, B. H. Liu, L. Zhou, Y. B. Sheng, C. F. Li, and G. C. Guo, Sci. Bull. **67**, 593 (2022).

71 B. C. Ren, and F. G. Deng, Laser Phys. Lett. **10**, 115201 (2013), arXiv: 1309.0168.

72 B. C. Ren, F. F. Du, and F. G. Deng, Phys. Rev. A **90**, 052309 (2014), arXiv: 1408.0048.

73 T. J. Wang, L. L. Liu, R. Zhang, C. Cao, and C. Wang, Opt. Express **23**, 9284 (2015).

74 T. J. Wang, S. C. Mi, and C. Wang, Opt. Express **25**, 2969 (2017).

75 F. F. Du, Y. T. Liu, Z. R. Shi, Y. X. Liang, J. Tang, and J. Liu, Opt. Express **27**, 27046 (2019).

76 Q. Zhang, X. Xie, H. Takesue, S. W. Nam, C. Langrock, M. M. Fejer, and Y. Yamamoto, Opt. Express **15**, 10288 (2007), arXiv: 0705.3875.

77 Y. B. Sheng, and F. G. Deng, Phys. Rev. A **81**, 032307 (2010), arXiv: 0912.0079.

78 Y. B. Sheng, F. G. Deng, and G. L. Long, Phys. Rev. A **82**, 032318 (2010), arXiv: 1103.0230.

79 B. C. Ren, H. R. Wei, M. Hua, T. Li, and F. G. Deng, Opt. Express **20**, 24664 (2012), arXiv: 1207.0168.

80 T. J. Wang, Y. Lu, and G. L. Long, Phys. Rev. A **86**, 042337 (2012).

81 G. Y. Wang, Q. Ai, B. C. Ren, T. Li, and F. G. Deng, Opt. Express **24**,

28444 (2016), arXiv: 1611.03352.

82 A. Yabushita, and T. Kobayashi, Phys. Rev. A **69**, 013806 (2004), arXiv: quant-ph/0306154.

83 J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, Phys. Rev. Lett. **95**, 260501 (2005), arXiv: quant-ph/0507128.

84 G. Vallone, R. Ceccarelli, F. De Martini, and P. Mataloni, Phys. Rev. A **79**, 030301 (2009), arXiv: 0810.4461.

85 K. Liu, J. Guo, C. Cai, S. Guo, and J. Gao, Phys. Rev. Lett. **113**, 170501 (2014).

86 P. Vergyris, F. Mazeas, E. Gouzien, L. Labonté, O. Alibart, S. Tanzilli, and F. Kaiser, Quantum Sci. Technol. **4**, 045007 (2019), arXiv: 1807.04498.

87 F. Steinlechner, S. Ecker, M. Fink, B. Liu, J. Bavaresco, M. Huber, T. Scheidl, and R. Ursin, Nat. Commun. **8**, 15971 (2017), arXiv: 1612.00751.

88 X. M. Hu, W. B. Xing, B. H. Liu, D. Y. He, H. Cao, Y. Guo, C. Zhang, H. Zhang, Y. F. Huang, C. F. Li, and G. C. Guo, Optica **7**, 738 (2020).

89 W. Zhang, D. S. Ding, M. X. Dong, S. Shi, K. Wang, S. L. Liu, Y. Li, Z. Y. Zhou, B. S. Shi, and G. C. Guo, Nat. Commun. **7**, 13514 (2016).

Appendix

A1 The nonlocal complete polarization BSA

In this section, we provide the detailed formula derivation of the nonlocal complete polarization BSA assisted with the entanglement in the spatial-mode DOF. As shown in Figure 2, this BSA protocol only requires some linear optical elements, including the PBSs, the QWPs, and the single photon detectors (D_1-D_8).

Suppose that the parties share a maximally hyperentangled state as:

$$|\phi_{\mathrm{p}}^{+}\rangle\otimes|\phi_{\mathrm{sAB}}^{+}\rangle=\frac{1}{\sqrt{2}}(|HH\rangle+|VV\rangle)\otimes\frac{1}{\sqrt{2}}(|a_1b_1\rangle+|a_2b_2\rangle). \quad \text{(a1)}$$

After the parties' operations in the polarization DOF, the polarization state may transform to four Bell states. In the first case, the polarization state does not change, so that the hyperentangled state is $|\phi_{\mathrm{p}}^{+}\rangle\otimes|\phi_{\mathrm{sAB}}^{+}\rangle$. By passing the photons in a_1a_2 and b_1b_2 through the PBSs, which can totally transmit the photon in $|H\rangle$ and reflect the photon in $|V\rangle$, $|\phi_{\mathrm{p}}^{+}\rangle\otimes|\phi_{\mathrm{sAB}}^{+}\rangle$ evolves to

$$\frac{1}{2}(|HH\rangle+|VV\rangle)\otimes(|a_3b_3\rangle+|a_4b_4\rangle). \quad \text{(a2)}$$

Then, the photons in a_3a_4 and b_3b_4 modes pass through the QWPs, which make $|H\rangle\rightarrow\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)$, and $|V\rangle\rightarrow\frac{1}{\sqrt{2}}(|H\rangle-|V\rangle)$. In this way, the state in eq. (a2) becomes

$$\frac{1}{2}(|HH\rangle+|VV\rangle)\otimes(|a_5b_5\rangle+|a_6b_6\rangle). \quad \text{(a3)}$$

Finally, the parties pass the photons in a_5a_6 and b_5b_6 modes through the PBSs and detect the output photons by the single photon detectors. It can be found that the initial hyperentangled state $|\phi_{\mathrm{p}}^{+}\rangle\otimes|\phi_{\mathrm{sAB}}^{+}\rangle$ can make the detectors D_1D_5, D_2D_6, D_3D_7, or D_4D_8 each register one photon.

In the second case, the polarization state changes to $|\phi_{\mathrm{p}}^{-}\rangle$, and the whole hyperentangled state is $|\phi_{\mathrm{p}}^{-}\rangle\otimes|\phi_{\mathrm{sAB}}^{+}\rangle=\frac{1}{\sqrt{2}}(|HH\rangle-|VV\rangle)\otimes\frac{1}{\sqrt{2}}(|a_1b_1\rangle+|a_2b_2\rangle)$. After the PBSs, it evolves to

$$\frac{1}{2}(|HH\rangle-|VV\rangle)\otimes(|a_3b_3\rangle+|a_4b_4\rangle). \quad \text{(a4)}$$

Then, by passing the photons through the QWPs, the parties can obtain

$$\frac{1}{2}(|HV\rangle+|VH\rangle)\otimes(|a_5b_5\rangle+|a_6b_6\rangle), \quad \text{(a5)}$$

which can make the detectors D_1D_6, D_2D_5, D_3D_8, or D_4D_7 each register one photon.

In the third case, the polarization state changes to $|\psi_{\mathrm{p}}^{+}\rangle$, thus the whole hyperentangled state is $|\psi_{\mathrm{p}}^{+}\rangle\otimes|\phi_{\mathrm{sAB}}^{+}\rangle=\frac{1}{\sqrt{2}}(|HV\rangle+|VH\rangle)\otimes\frac{1}{\sqrt{2}}(|a_1b_1\rangle+|a_2b_2\rangle)$. After all the operations, the state $|\psi_{\mathrm{p}}^{+}\rangle\otimes|\phi_{\mathrm{sAB}}^{+}\rangle$ evolves to

$$\frac{1}{2}(|HH\rangle-|VV\rangle)\otimes(|a_5b_6\rangle+|a_6b_5\rangle), \quad \text{(a6)}$$

and can be finally detected by D_1D_7, D_2D_8, D_3D_5, or D_4D_6.

In the last case, the polarization state changes to $|\psi_{\mathrm{p}}^{-}\rangle$, thus the whole hyperentangled state is $|\psi_{\mathrm{p}}^{-}\rangle\otimes|\phi_{\mathrm{sAB}}^{+}\rangle=\frac{1}{\sqrt{2}}(|HV\rangle-|VH\rangle)\otimes\frac{1}{\sqrt{2}}(|a_1b_1\rangle+|a_2b_2\rangle)$. After the BSA operations, it becomes

$$\frac{1}{2}(|HV\rangle-|VH\rangle)\otimes(|a_5b_6\rangle+|a_6b_5\rangle), \quad \text{(a7)}$$

and can be detected by D_1D_8, D_2D_7, D_3D_6, or D_4D_5.

Therefore, when Alice announces her measurement results through the classical channel, Bob can obtain the BSA results based on their measurement results, and read out Alice's encoded messages combined with his unitary operations.

A2 The nonlocal complete polarization BSA when the same kind of errors occur in both DOFs

In this section, we prove that when the same kind of errors happens in both DOFs, Bob can still obtain the correct encoded messages from their measurement results. Here, we suppose Bob's unitary operation is $U_{2\mathrm{p}}$. We first consider that the bit-flip error occurs in both DOFs, so that the initial hyperentangled state degrades to $|\psi_{\mathrm{p}}^{+}\rangle\otimes|\psi_{\mathrm{sAB}}^{+}\rangle=\frac{1}{\sqrt{2}}(|HV\rangle+|VH\rangle)\otimes\frac{1}{\sqrt{2}}(|a_1b_2\rangle+|a_2b_1\rangle)$.

In the first case, Alice performs $U_{0\mathrm{p}}$ on the T photon. Combined with Bob's operation, the initial state changes to $|\phi_{\mathrm{p}}^{+}\rangle\otimes|\psi_{\mathrm{sAB}}^{+}\rangle=\frac{1}{\sqrt{2}}(|HH\rangle+|VV\rangle)\otimes\frac{1}{\sqrt{2}}(|a_1b_2\rangle+|a_2b_1\rangle)$. After the nonlocal BSA operations, it evolves to

$$\frac{1}{2}(|HH\rangle+|VV\rangle)\otimes(|a_6b_5\rangle+|a_5b_6\rangle). \quad \text{(a8)}$$

The state in eq. (a8) can be detected by D_1D_7, D_2D_8, D_3D_5, or D_4D_6. According to Table 1, Bob can deduce that the encoded polarization Bell state is $|\psi_{\rm p}^+\rangle$. Combined with his own operation, he can further obtain that after Alice's encoding, the polarization state is $|\phi_{\rm p}^+\rangle$, so that Alice's operation is $U_{0\rm p}$ and her encoded messages are 00.

In the second case, Alice performs $U_{1\rm p}$ on the T photon. After Bob's operation, the initial state changes to $|\phi_{\rm p}^-\rangle \otimes |\psi_{\rm sAB}^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle - |VV\rangle) \otimes \frac{1}{\sqrt{2}}(|a_1b_2\rangle + |a_2b_1\rangle)$. By performing the nonlocal BSA operations, $|\phi_{\rm p}^-\rangle \otimes |\psi_{\rm sAB}^+\rangle$ is converted to

$$\frac{1}{2}(|HV\rangle + |VH\rangle) \otimes (|a_6b_5\rangle + |a_5b_6\rangle), \tag{a9}$$

and can be detected by D_1D_8, D_2D_7, D_3D_6, or D_4D_5. In this way, Bob can obtain that the encoded polarization Bell state is $|\psi_{\rm p}^-\rangle$. Combined with his own operation, he can further obtain that the polarization state after Alice's encoding is $|\phi_{\rm p}^-\rangle$, so that Alice's encoded messages are 01.

In the third case, Alice performs $U_{2\rm p}$ on the T photon. In this case, the initial state changes to $|\psi_{\rm p}^+\rangle \otimes |\psi_{\rm sAB}^+\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle) \otimes \frac{1}{\sqrt{2}}(|a_1b_2\rangle + |a_2b_1\rangle)$. After the BSA operation, $|\psi_{\rm p}^+\rangle \otimes |\psi_{\rm sAB}^+\rangle$ evolves to

$$\frac{1}{2}(|HH\rangle - |VV\rangle) \otimes (|a_6b_6\rangle + |a_5b_5\rangle), \tag{a10}$$

so that the output photons can be detected by D_1D_5, D_2D_6, D_3D_7, or D_4D_8. According to Table 1, Bob can deduce the polarization state is $|\phi_{\rm p}^+\rangle$. Then, he can deduce that before his operation, the polarization state is $|\psi_{\rm p}^+\rangle$ and Alice's encoded messages are 10.

In the last case, Alice performs $U_{3\rm p}$ on the T photon, which makes the initial state evolve to $|\psi_{\rm p}^-\rangle \otimes |\psi_{\rm sAB}^+\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) \otimes \frac{1}{\sqrt{2}}(|a_1b_2\rangle + |a_2b_1\rangle)$. After the BSA operation, the parties can finally obtain

$$\frac{1}{2}(|HV\rangle - |VH\rangle) \otimes (|a_6b_6\rangle + |a_5b_5\rangle), \tag{a11}$$

which can be detected by D_1D_6, D_2D_5, D_3D_8, or D_4D_7. As a result, Bob can deduce the polarization state is $|\phi_{\rm p}^-\rangle$. He can obtain that the polarization state before his operation is $|\psi_{\rm p}^-\rangle$ and Alice's encoded message are 11.

Similarly, if the initial state is $|\phi_{\rm p}^-\rangle \otimes |\phi_{\rm sAB}^-\rangle$, Bob can also deduce the encoded messages from Alice based on their detector responses. We also suppose that Bob's operation is $U_{2\rm p}$.

In the first case, Alice performs $U_{0\rm p}$ on the T photon, and the above initial state changes to $|\psi_{\rm p}^-\rangle \otimes |\phi_{\rm sAB}^-\rangle$. After the BSA operations, the whole state evolves to

$$\frac{1}{2}(|HH\rangle - |VV\rangle) \otimes (|a_6b_5\rangle - |a_5b_6\rangle), \tag{a12}$$

which can be detected by D_1D_7, D_2D_8, D_3D_5, or D_4D_6. From Table 1, Bob can obtain the polarization state is $|\psi_{\rm p}^+\rangle$. Combined with his operation $U_{2\rm p}$, he can finally deduce that Alice's encoded messages are 00.

In the second case, Alice performs $U_{1\rm p}$ on the T photon, causing the hyperentangled state to become $|\psi_{\rm p}^+\rangle \otimes |\phi_{\rm sAB}^-\rangle$. After the BSA operation, the state evolves to

$$\frac{1}{2}(|HV\rangle - |VH\rangle) \otimes (|a_5b_6\rangle - |a_6b_5\rangle), \tag{a13}$$

which can be detected by D_1D_8, D_2D_7, D_3D_6, or D_4D_5. As a result, Bob can read out the polarization state as $|\psi_{\rm p}^-\rangle$. Combined with his operation $U_{2\rm p}$, Bob can obtain Alice's encoded messages of 01.

In the third case, Alice performs $U_{2\rm p}$ on the T photon, the initial state will evolve to $|\phi_{\rm p}^-\rangle \otimes |\phi_{\rm sAB}^-\rangle$. After the BSA, it evolves to

$$\frac{1}{2}(|HH\rangle + |VV\rangle) \otimes (|a_6b_6\rangle - |a_5b_5\rangle), \tag{a14}$$

which can make D_1D_5, D_2D_6, D_3D_7, or D_4D_8 each register one photon. Bob can read out the polarization state as $|\phi_{\rm p}^+\rangle$ and deduce Alice's encoded messages as 10.

In the last case, Alice performs $U_{3\rm p}$ on the T photon, causing the hyperentangled state to become $|\phi_{\rm p}^+\rangle \otimes |\phi_{\rm sAB}^-\rangle$. After the BSA, the state evolves to

$$\frac{1}{2}(|HV\rangle + |VH\rangle) \otimes (|a_6b_6\rangle - |a_5b_5\rangle), \tag{a15}$$

which can make D_1D_6, D_2D_5, D_3D_8, or D_4D_7 each register one photon. Based on Table 1, Bob can read out the polarization state is $|\phi_{\rm p}^-\rangle$. Considering his operation $U_{2\rm p}$, he can obtain Alice's encoded messages as 11.

Similarly, if the initial state is $|\psi_{\rm p}^-\rangle \otimes |\psi_{\rm sAB}^-\rangle$, we can also obtain the same results. In conclusion, as long as the same kind of errors occurs in both DOFs, this one-step QDC protocol can still transmit correct messages.