

One-step quantum dialogue

Peng-Hui Zhu(朱鹏辉), Wei Zhong(钟伟), Ming-Ming Du(杜明明), Xi-Yun Li(李喜云), Lan Zhou(周澜), and Yu-Bo Sheng(盛宇波)

Citation: Chin. Phys. B, 2024, 33 (**3**): 020302. DOI: 10.1088/1674-1056/ad1c5c

Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Compact generation scheme of path-frequency hyperentangled photons using 2D periodical nonlinear photonic crystal

Yang-He Chen(陈洋河), Bo Ji(季波), Nian-Qin Li(李念芹), Zhen Jiang(姜震), Wei Li(李维),Yu-Dong Li(李昱东), Liang-Sen Feng(冯梁森), Teng-Fei Wu(武腾飞), and Guang-Qiang He(何广强)

Chin. Phys. B, 2023, 32 (**12**): 120307. DOI: 10.1088/1674-1056/ad0625

Generation of hyperentangled photon pairs based on lithium niobate waveguide

Yang-He Chen(陈洋河), Zhen Jiang(姜震), and Guang-Qiang He(何广强)

Chin. Phys. B, 2023, 32 (**9**): 090306. DOI: 10.1088/1674-1056/acd5c4

Faithful and efficient hyperentanglement purification for spatial-polarization-time-bin photon system

Fang-Fang Du(杜芳芳), Gang Fan(樊钢), Yi-Ming Wu(吴一鸣), and Bao-Cang Ren(任宝藏)

Chin. Phys. B, 2023, 32 (**6**): 060304. DOI: 10.1088/1674-1056/aca395

Complete hyperentangled Greenberger-Horne-Zeilinger state analysis for polarization and time-bin hyperentanglement

Zhi Zeng(曾志)

Chin. Phys. B, 2023, 32 (**6**): 060301. DOI: 10.1088/1674-1056/ac9044

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

Jia-Wei Ying(应佳伟), Lan Zhou(周澜), Wei Zhong(钟伟), and Yu-Bo Sheng(盛宇波)

Chin. Phys. B, 2022, 31 (**12**): 120303. DOI: 10.1088/1674-1056/ac8f37

RAPID COMMUNICATION

One-step quantum dialogue

Peng-Hui Zhu(朱鹏辉)[1,2], Wei Zhong(钟伟)[3], Ming-Ming Du(杜明明)[2], Xi-Yun Li(李喜云)[1], Lan Zhou(周澜)[1,†], and Yu-Bo Sheng(盛宇波)[2,3,‡]

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

(Received 23 November 2023; revised manuscript received 29 December 2023; accepted manuscript online 9 January 2024)

Quantum dialogue (QD) enables two communication parties to directly exchange secret messages simultaneously. In conventional QD protocols, photons need to transmit in the quantum channel for two rounds. In this paper, we propose a one-step QD protocol based on the hyperentanglement. With the help of the non-local hyperentanglement-assisted Bell state measurement (BSM), the photons only need to transmit in the quantum channel once. We prove that our one-step QD protocol is secure in theory and numerically simulate its secret message capacity under practical experimental condition. Compared with previous QD protocols, the one-step QD protocol can effectively simplify the experiment operations and reduce the message loss caused by the photon transmission loss. Meanwhile, the non-local hyperentanglement-assisted BSM has a success probability of 100% and is feasible with linear optical elements. Moreover, combined with the hyperentanglement heralded amplification and purification, our protocol is possible to realize long-distance one-step QD.

Keywords: one-step quantum dialogue, hyperentanglement, hyperentanglement distribution, non-local Bell-state measurement

PACS: 03.67.Pp, 03.67.Hk, 03.65.Ud **DOI:** 10.1088/1674-1056/ad1c5c

1. Introduction

Quantum secure communication can protect the security of transmitted messages based on the basic principles of quantum mechanics. Quantum secure communication has unconditional security, which is its most attractive advantage comparing with classical communication. There are some important branches in the quantum secure communication field, such as quantum key distribution (QKD),[1–9] quantum secret sharing (QSS),[10–14] quantum secure direct communication (QSDC),[15–18] and quantum dialogue (QD).[19,20] QKD and QSS can generate secret keys between two distant parties and among multiple parties, respectively. QSDC does not require keys. It enables the message sender to directly transmit messages to the message receiver through the quantum channel. QSDC has developed rapidly in theoretical and experimental aspects during the last few years.[21–42] In theory, in 2020, researchers introduced device-independent (DI) and measurement-device-independent (MDI) techniques in QSDC to enhance QSDC's security under practical conditions.[22,23] Soon after, the masking (IN-CUM) technique was utilized in QSDC to increase its message capacity.[26] In 2023, the two-step QSDC scheme based on intermediate-basis was proposed, which used the intermediate-basis Einstein–Podolsky–Rosen (EPR) pairs to detect the channel security and help encode information.[32] Experimentally, the single-photon based QSDC experiment and entanglement-based QSDC experiment were realized in 2016 and 2017, respectively.[35,36] Recently, QSDC network experiment and a 100 km QSDC experiment were reported, which largely promoted the practicality of QSDC.[39,40] In 2023, the group of Paparelle realized the table-top experimental demonstration of a CV-QSDC system.[42]

QD, which will be detailed here, enables two distant communication parties to exchange messages through quantum channels.[43–51] In this way, QD can play the role of bidirectional QSDC. In 2004, Nguyen proposed the first QD protocol based on quantum entanglement.[19] In 2005, Man *et al.* pointed out the security loophole of the QD protocol in Ref. [19] and proposed a modified secure QD protocol.[20] In 2007, a quasi-secure single-photon-based QD protocol was proposed,[43] which can guarantee the confidentiality and control of the QD content, and has certain anti-attack capabilities. In 2009, Shi *et al.* utilized Bell state to realize a secure QD.[45] In 2010, they proposed a secure single-photon-based QD protocol combining the idea of QSDC and BB84 protocol.[46] In 2014, a two-step QD protocol evolved from the two-step QSDC protocol was proposed,[49] whose security is assured by the two-step QSDC protocol.[16] In the same year, the entanglement swapping technique was introduced into the QD protocol.[50] Later, Gong *et al.* utilized the continuous-variable GHZ states to realize the quantum network dialogue.[51]

The conventional QSDC and QD protocols all require two rounds of photon transmission. We take the entanglement-

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

© 2024 Chinese Physical Society and IOP Publishing Ltd

based QSDC and QD protocols as examples.[15,16,19,20,45,49] Firstly, two communication parties firstly construct the long-distance entanglement channel by distributing a photon of each entangled photon pair in the quantum channel. Then, the photons are encoded by the parties. The encoded photons should be sent to one party for the Bell state measurement (BSM). However, in the photon transmission processes, the channel noise may cause photon transmission loss and quantum state decoherence, which may cause message loss and message error. Worse still, utilizing the channel noise, the eavesdropper (Eve) can intercept some messages without being detected. In 2022, the one-step QSDC protocol based on the hyperentanglement was put forward,[28] which reduces the photon transmission rounds from two to one. Compared with conventional two-step QSDC protocols,[15,16] one-step QSDC protocol can effectively simplify the experimental operation and reduce the message loss caused by the photon transmission loss. Later, to further enhance one-step QSDC's security under practical imperfect conditions, researchers proposed DI and MDI one-step QSDC protocols.[29,30] Inspired by the one-step QSDC protocol, we propose the first one-step QD protocol. This one-step QD protocol first constructs the hyperentanglement channel between two distant communication parties. Then, the parties perform the hyperentanglement-assisted complete BSM with the probability of 100%. In this way, the encoded photons are not required to transmit to one party, which can effectively reduce the message loss. To evaluate the one-step QD protocol's performance under practical experimental conditions, we simulate its secret message capacity. Our one-step QD protocol has important applications in the quantum communication field.

The paper is organized as follows. In Section 2, we explain the one-step QD protocol based on hyperentanglement. In Section 3, an example of the one-step QD protocol is put forward. In Section 4, we analyze the theoretic security and the secret message capacity of the one-step QD protocol. In Section 5, we make some discussion and the summary elaboration.

2. One-step QD protocol

The one-step QD protocol utilizes the hyperentangled photon pairs as the sources. Hyperentanglement means entanglement in two or more DOFs of a system. Hyperentanglement has important applications in increasing the channel capacity,[52,53] realizing the high-efficient entanglement purification,[54–57] complete BSM,[58,59] and multi-DOF teleportation.[60,61] The generation of various hyperentanglement has been widely researched.[62–64] As shown in Fig. 1, the one-step QD protocol can be described as follows.

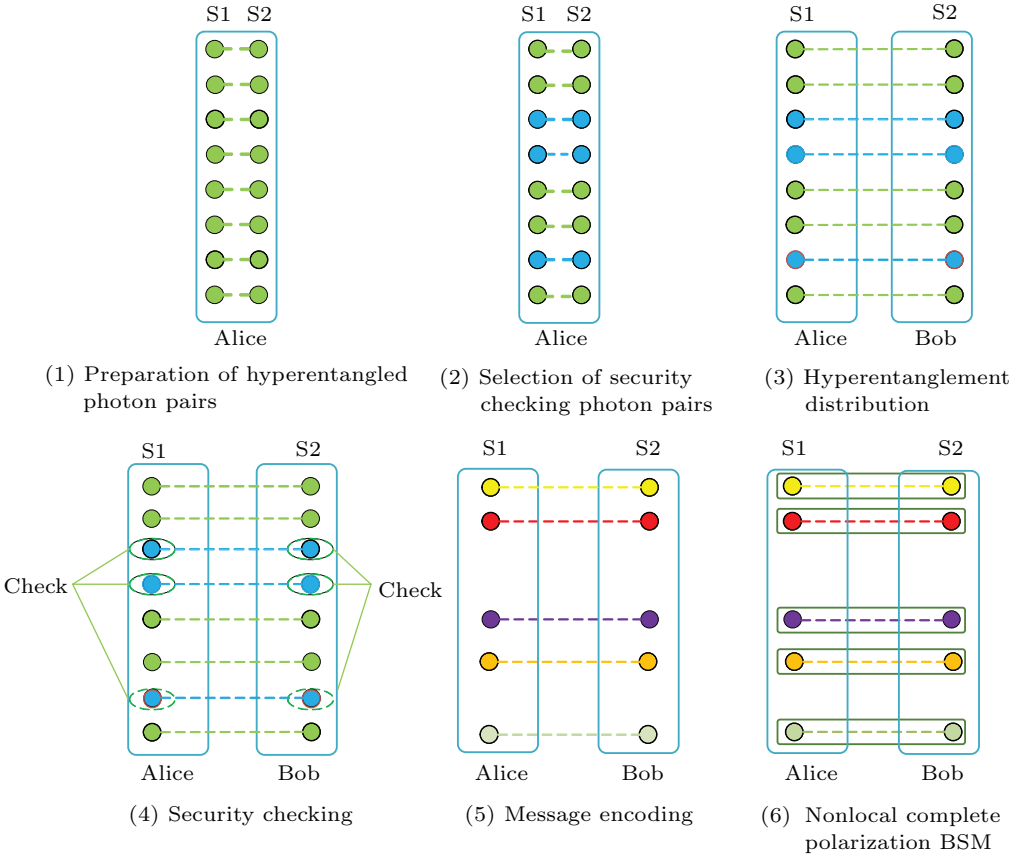


Fig. 1. The schematic diagram of the one-step QD protocol. The green circles linked by the dashed lines represent the initially prepared polarization-spatial-mode hyperentangled photon pairs in $|\phi^+\rangle_{\rm p}\otimes|\phi^+\rangle_{\rm s}$. The light blue circle pairs represent the randomly selected security checking photon pairs. The colorful circle pairs in steps (5) and (6) represent the encoded photon pairs. The light green rectangular box represents the non-local complete polarization Bell state measurement (BSM).

Step 1 The communication party Alice requires to generate N polarized-spatial-mode hyperentangled states in $|\phi^+\rangle_{\rm p}\otimes|\phi^+\rangle_{\rm s}$ (N is large). Here, we use $|H\rangle$ and $|V\rangle$ to represent the horizontal polarization and vertical polarization, respectively. The four polarization Bell states can be described as

$$|\phi^{\pm}\rangle_{\rm p}=\frac{1}{\sqrt{2}}\left(|H\rangle|H\rangle\pm|V\rangle|V\rangle\right),$$
$$|\psi^{\pm}\rangle_{\rm p}=\frac{1}{\sqrt{2}}\left(|H\rangle|V\rangle\pm|V\rangle|H\rangle\right). \quad (1)$$

In the spatial-mode DOF, a_1, a_2, a_1', a_2' represent different spatial modes in Alice's location. The four spatial-mode Bell states can be described as

$$|\phi^{\pm}\rangle_{\rm s}=\frac{1}{\sqrt{2}}\left(|a_1\rangle|a_1'\rangle\pm|a_2\rangle|a_2'\rangle\right),$$
$$|\psi^{\pm}\rangle_{\rm s}=\frac{1}{\sqrt{2}}\left(|a_1\rangle|a_2'\rangle\pm|a_2\rangle|a_1'\rangle\right). \quad (2)$$

We divide the N copies of photon pairs into two photon sequences S1 and S2.

Step 2 Alice randomly selects M photon pairs for subsequent security checking and records their positions (M is a large number and $M<N$).

Step 3 The photons in sequence S2 are sent from Alice to Bob through two quantum channels, and the photons in sequence S1 are stored in Alice's quantum memory (QM) devices. The spatial modes a_1' and a_2' in Alice's location correspond to the spatial modes b_1 and b_2 in Bob's location, respectively. Bob stores all the received photons in his QM devices.

Step 4 For each security checking photon, Alice randomly selects the rectilinear (Z) basis or diagonal (X) basis in each DOF. Then, Alice announces the position and measurement bases in both DOFs of each security checking photon pair through a classical channel. Alice and Bob extract the security checking photons from the QM devices and measure them in both DOFs with the announced bases. In Fig. 2, we show four linear optical apparatuses for Alice (Bob) measuring the photon in $X_{\rm s}Z_{\rm p}$, $X_{\rm s}X_{\rm p}$, $Z_{\rm s}X_{\rm p}$, $Z_{\rm s}Z_{\rm p}$ bases and the corresponding measurement results.[65] Then, Alice (Bob) announces her (his) measurement results through the classical channel. Under the case that they both choose Z basis in a DOF, if their measurement results are different, it indicates that a bit-flip error occurs in this DOF. Under the case that they both choose X basis in a DOF, if their measurement results are different, it indicates that a phase-flip error occurs. After the security checking, Alice and Bob estimate the bit-flip error rate ($e_{\rm B}$) and phase-flip error rate ($e_{\rm P}$) in both DOFs. If $e_{\rm B}$ or $e_{\rm P}$ in any DOF exceeds a tolerable threshold, Alice determines that the photon transmission is unsafe and aborts the communication. Only when both $e_{\rm B}$ and $e_{\rm P}$ in each DOF are lower than the tolerable thresholds, Alice and Bob continue the communication.

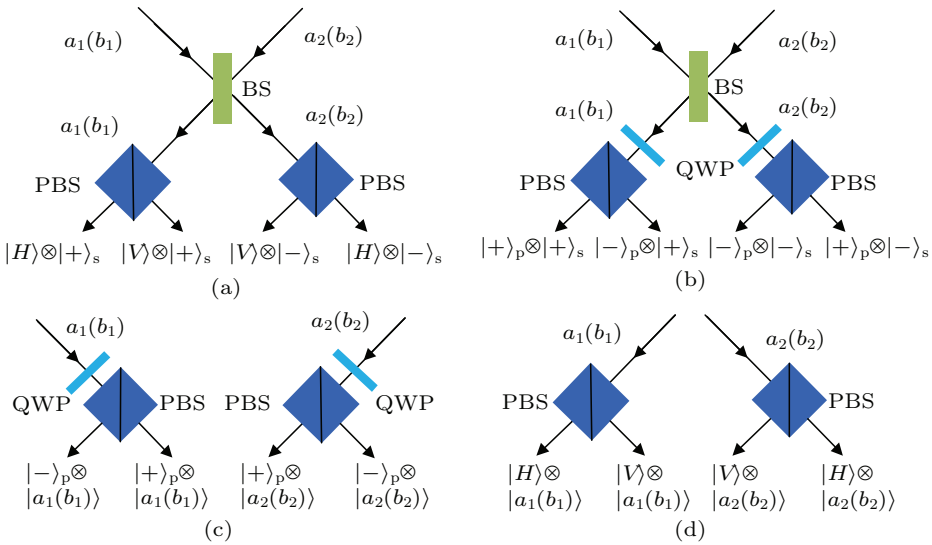


Fig. 2. Four linear optical apparatuses for the parties measuring the photons in (a) $X_{\rm s}Z_{\rm p}$, (b) $X_{\rm s}X_{\rm p}$, (c) $Z_{\rm s}X_{\rm p}$, (d) $Z_{\rm s}Z_{\rm p}$, and the corresponding measurement results.[65] PBS and BS represent the polarization beam splitter and 50:50 beam splitter, respectively. PBS can totally transmit the photon in $|H\rangle$ and totally reflect the photon in $|V\rangle$ photon. BS plays the role of the Hadamard (H) gate in the spatial-mode DOF, leading $|i_1\rangle\rightarrow\frac{1}{\sqrt{2}}(|i_1\rangle+|i_2\rangle)$ and $|i_2\rangle\rightarrow\frac{1}{\sqrt{2}}(|i_1\rangle-|i_2\rangle)$ $(i=a,b)$. The quarter wave plate (QWP) can be treated as the H gate in the polarization DOF, leading $|H\rangle\rightarrow\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)$ and $|V\rangle\rightarrow\frac{1}{\sqrt{2}}(|H\rangle-|V\rangle)$.

Step 5 Alice extracts the stored photons from the QM devices and encodes her messages on them by performing the unitary operations $I_{\rm p}=|H\rangle\langle H|+|V\rangle\langle V|$ and $\sigma_{\rm zp}=|H\rangle\langle H|-|V\rangle\langle V|$. She utilizes the operations $I_{\rm p}$ and $\sigma_{\rm zp}$ to represent the messages 0 and 1, respectively. Meanwhile, Bob extracts the remained photons in the S2 sequence and utilizes the unitary operations $I_{\rm p}$ and $\sigma_{\rm xp}=|H\rangle\langle V|+|V\rangle\langle H|$ to encode his messages on the photons in the S2 sequence, where $I_{\rm p}$ represents the classical message 0 and $\sigma_{\rm xp}$ represents the classical message 1. In addition, to prevent message leakage, Alice ran-

domly performs $I_{\rm p}$ or $\sigma_{x{\rm p}}$ operation on each photon in S1 sequence, and Bob randomly performs $I_{\rm p}$ or $\sigma_{z{\rm p}}$ operation on each photon in S2 sequence. We show the basic principle of the encoding in linear optics in Fig. 3. In detail, the half wave plate (HWP) can make $|H\rangle \leftrightarrow |V\rangle$. It has the function of $\sigma_{x{\rm p}}$ operation, which makes $|\phi^+\rangle_{\rm p} \to |\psi^+\rangle_{\rm p}$. The quarter wave plate (QWP) can make $|H\rangle \to \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ and $|V\rangle \to \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$. We use two QWPs combined with an HWP to perform the $\sigma_{z{\rm p}}$ operation on the photon pair. Suppose Alice passes her photon through two QWPs combined with an HWP. The formula derivation process can be written as

$$\begin{aligned}|\phi^+\rangle_{\rm p} &= \frac{1}{\sqrt{2}}(|H\rangle|H\rangle + |V\rangle|V\rangle)\\ &\xrightarrow{\rm QWP} \frac{1}{2}\left[(|H\rangle + |V\rangle)|H\rangle + (|H\rangle - |V\rangle)|V\rangle\right]\\ &\xrightarrow{\rm HWP} \frac{1}{2}\left[(|V\rangle + |H\rangle)|H\rangle + (|V\rangle - |H\rangle)|V\rangle\right]\\ &\xrightarrow{\rm QWP} \frac{1}{\sqrt{2}}(|H\rangle|H\rangle - |V\rangle|V\rangle) = |\phi^-\rangle_{\rm p}. \end{aligned} \tag{3}$$

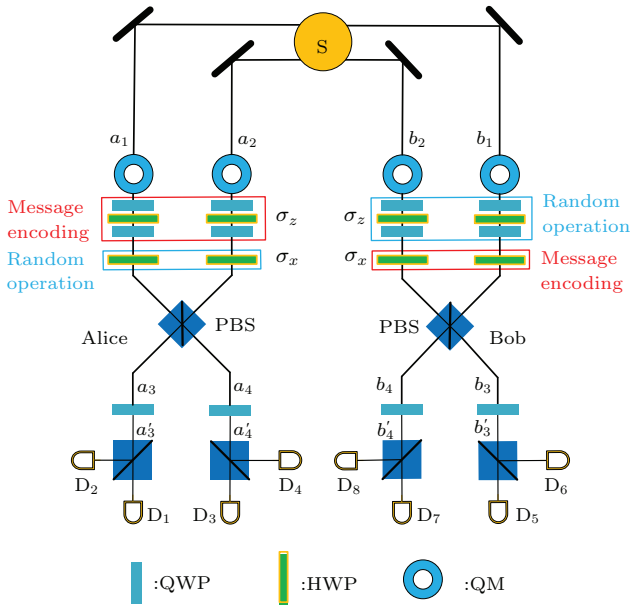


Fig. 3. Schematic principle of the encoding and non-local hyperentanglement-assisted polarization BSM in our one-step QD protocol. The parties can perform the $\sigma_{x{\rm p}}$ operation by passing the photon through the half wave plate (HWP). Combining two QWPs with an HWP, the parties can perform the $\sigma_{z{\rm p}}$ operation. After the encoding, the parties perform the non-local hyperentanglement-assisted polarization BSM.[28,58] Four polarization Bell states can be distinguished by the responses of eight photon detectors D_1–D_8.

Step 6 Both parties perform the non-local hyperentanglement-assisted polarization BSM, which is also shown in Fig. 3. After the measurement, both parties announce the detector responses through a classical channel. From the detector responses, both parties can deduce the encoded polarization Bell state. The detector responses and the corresponding polarization Bell states are shown in Table 1. Then, combined with the detector responses and their own random operations, they can deduce the encoded operations from each other and realize the bidirectional communication. As the random operations are private, anyone except the communication parties cannot read out the exchanged messages.

Table 1. The non-local complete polarization BSM results corresponding to the detector responses with the spatial Bell state being $|\phi^+\rangle_{\rm s}$. D_iD_j means both the photon detectors D_i and D_j response.

Polarization Bell state	Photon detector response			
$\|\phi^+\rangle_{\rm p}$	D_1D_5	D_2D_6	D_3D_7	D_4D_8
$\|\psi^+\rangle_{\rm p}$	D_1D_7	D_2D_8	D_3D_5	D_4D_6
$\|\phi^-\rangle_{\rm p}$	D_1D_6	D_2D_5	D_3D_8	D_4D_7
$\|\psi^-\rangle_{\rm p}$	D_1D_8	D_2D_7	D_3D_6	D_4D_5

It is worth noting that if the Bell state in the spatial-mode DOF degrades to one of the other three Bell states in Eq. (2), the parties will obtain wrong polarization BSM result from the detector responses. We list the polarization Bell states corresponding to the detector responses with the spatial-mode entanglement in $|\psi^+\rangle_{\rm s}$ in Table 2. We take a specific example. From Table 2, if the polarization is $|\phi^+\rangle_{\rm p}$, the detectors D_1D_7, D_2D_8, D_3D_5, or D_4D_6 will click. However, the parties deduce the polarization Bell state from Table 1, so that they will deduce that the encoded polarization Bell state is $|\psi^+\rangle_{\rm p}$.

Table 2. The non-local complete polarization BSM results corresponding to the detector responses with the spatial Bell state being $|\psi^+\rangle_{\rm s}$. D_iD_j means both the photon detectors D_i and D_j response.

Polarization Bell state	Photon detector response			
$\|\phi^+\rangle_{\rm p}$	D_1D_7	D_2D_8	D_3D_5	D_4D_6
$\|\psi^+\rangle_{\rm p}$	D_1D_5	D_2D_6	D_3D_7	D_4D_8
$\|\phi^-\rangle_{\rm p}$	D_1D_8	D_2D_7	D_3D_6	D_4D_5
$\|\psi^-\rangle_{\rm p}$	D_1D_6	D_2D_5	D_3D_8	D_4D_7

3. A specific example of the one-step QD protocol

To enhance the understanding of the one-step QD protocol, we provide a specific example of this one-step QD protocol. After the hyperentanglement distribution, Alice and Bob share the initial hyperentangled state in $|\phi^+\rangle_{\rm p} \otimes |\phi^+\rangle_{\rm s}$. Suppose that Alice aims to transmit the message 1, and Bob aims to transmit the message 0. In this way, Alice performs $\sigma_{z{\rm p}}$ on the photon in S1 sequence, and Bob performs $I_{\rm p}$ on the corresponding photon in S2 sequence. In addition, Alice also performs $\sigma_{x{\rm p}}$ on her photon and Bob performs $\sigma_{z{\rm p}}$ on his photon. After the encoding, the initial state $|\phi^+\rangle_{\rm p}$ is converted to $|\psi^+\rangle_{\rm p}$, while the state $|\phi^+\rangle_{\rm s}$ is unchanged. The specific process is as follows:

$$\begin{aligned}\sigma_{z{\rm p}}|\phi^+\rangle_{\rm p} &= (|H\rangle\langle H| - |V\rangle\langle V|)\frac{1}{\sqrt{2}}(|H\rangle|H\rangle + |V\rangle|V\rangle)\\ &= |\phi^-\rangle_{\rm p},\\ \sigma_{x{\rm p}}|\phi^-\rangle_{\rm p} &= (|H\rangle\langle V| + |V\rangle\langle H|)\frac{1}{\sqrt{2}}(|H\rangle|H\rangle - |V\rangle|V\rangle)\\ &= |\psi^-\rangle_{\rm p},\\ I_{\rm p}|\psi^-\rangle_{\rm p} &= (|H\rangle\langle H| + |V\rangle\langle V|)\frac{1}{\sqrt{2}}(|H\rangle|V\rangle - |V\rangle|H\rangle)\end{aligned}$$

$$
\begin{aligned}
&= |\psi^-\rangle_{\rm p},\\
\sigma_{\rm zp}|\psi^-\rangle_{\rm p} &= (|H\rangle\langle H| - |V\rangle\langle V|)\frac{1}{\sqrt{2}}(|H\rangle|V\rangle - |V\rangle|H\rangle)\\
&= |\psi^+\rangle_{\rm p}. \qquad (4)
\end{aligned}
$$

Then, the communication parties perform the non-local complete polarization BSM. After the PBSs and QWP, the hyperentangled state $|\psi^+\rangle_{\rm p}\otimes|\phi^+\rangle_{\rm s}$ will evolve to

$$
\begin{aligned}
|\psi^+\rangle_{\rm p}\otimes|\phi^+\rangle_{\rm s} &= \frac{1}{\sqrt{2}}(|H\rangle|V\rangle + |V\rangle|H\rangle)\\
&\quad\otimes\frac{1}{\sqrt{2}}(|a_1\rangle|a_1'\rangle + |a_2\rangle|a_2'\rangle)\\
&= \frac{1}{2}(|H\rangle_{a_1}|V\rangle_{a_1'} + |H\rangle_{a_2}|V\rangle_{a_2'}\\
&\quad + |V\rangle_{a_1}|H\rangle_{a_1'} + |V\rangle_{a_2}|H\rangle_{a_2'})\\
&\longrightarrow \frac{1}{2}(|H\rangle_{a_1}|V\rangle_{b_1} + |H\rangle_{a_2}|V\rangle_{b_2}\\
&\quad + |V\rangle_{a_1}|H\rangle_{b_1} + |V\rangle_{a_2}|H\rangle_{b_2})\\
&\xrightarrow{\rm PBS} \frac{1}{2}(|H\rangle_{a_4}|V\rangle_{b_3} + |H\rangle_{a_3}|V\rangle_{b_4}\\
&\quad + |V\rangle_{a_3}|H\rangle_{b_4} + |V\rangle_{a_4}|H\rangle_{b_3})\\
&\xrightarrow{\rm QWP} \frac{1}{4}\big[(|H\rangle_{a_4'} + |V\rangle_{a_4'})(|H\rangle_{b_3'} - |V\rangle_{b_3'})\\
&\quad + (|H\rangle_{a_3'} + |V\rangle_{a_3'})(|H\rangle_{b_4'} - |V\rangle_{b_4'})\\
&\quad + (|H\rangle_{a_3'} - |V\rangle_{a_3'})(|H\rangle_{b_4'} + |V\rangle_{b_4'})\\
&\quad + (|H\rangle_{a_4'} - |V\rangle_{a_4'})(|H\rangle_{b_3'} + |V\rangle_{b_3'})\big]\\
&= \frac{1}{2}(|H\rangle_{a_4'}|H\rangle_{b_3'} - |V\rangle_{a_4'}|V\rangle_{b_3'}\\
&\quad + |H\rangle_{a_3'}|H\rangle_{b_4'} - |V\rangle_{a_3'}|V\rangle_{b_4'}), \qquad (5)
\end{aligned}
$$

which corresponds to the responses of D_1D_7, D_2D_8, D_3D_5, or D_4D_6. Based on the detector responses, the parties obtain the encoded polarization Bell state is $|\psi^+\rangle_{\rm p}$ from Table 1. Then, each party combined $|\psi^+\rangle_{\rm p}$ with his/her random operation. Alice can obtain that Bob's encoding operation is $I_{\rm p}$ corresponding to the transmitted message of 0. Bob can obtain that Alice's encoding operation is $\sigma_{\rm zp}$ corresponding to the message of 1.

4. Security analysis and the secret message capacity

We first analyze the theoretic security of our one-step QD protocol against the most common attack, say, the intercept-resend attack. During the photon transmission process, Eve can intercept some photons. To avoid being discovered, Eve prepares some new hyperentangled photon pairs in $|\phi^+\rangle_{\rm p}\otimes|\phi^+\rangle_{\rm s}$. He distributes one photon of each hyperentangled photon pair to Bob through a perfect quantum channel and randomly encodes the photons in his location. After the parties' encodings, Eve performs the non-local complete polarization BSM with the parties, respectively, and he can deduce Alice's and Bob's message according to the announced detector responses from Alice and Bob. Meanwhile, the parties can only obtain Eve's randomly encoded messages. However, this attack can be resisted by the security checking. As Alice randomly selects a large number of security checking photon pairs in the photon sequences. It is unavoidable for Eve to intercept some security checking photons. Eve's newly generated photons in Bob's location are not entangled with Alice's corresponding photons. As a result, their measurement results in each DOF may be different with a probability of 50%. In this way, Eve's intercept-resend attack can increase $e_{\rm B}$ and $e_{\rm P}$ in each DOF. Under ideal conditions, if there is no eavesdropping, $e_{\rm B}$ and $e_{\rm P}$ in each DOF are strictly equal to 0. If $e_{\rm B}$ or $e_{\rm P}$ in any DOF is higher than 0, Alice can detect the existence of Eve. Under practical noisy conditions, Alice sets the tolerable thresholds of $e_{\rm B}$ and $e_{\rm P}$ in both DOFs. If the any error rate exceeds the tolerable threshold, Alice ensures that the photon distribution is unsafe and discards the communication.

Actually, in the practical noisy channel condition, Eve can intercept a part of photons from the photon transmission process. The total error rates caused by Eve's interception can be concealed by that caused by the channel noise, so that Eve will not be detected by the parties. As a result, Eve can obtain a part of encoded messages. As each hyperentangled photon pair carries 2 bits of messages, the message leakage rate of our one-step QD protocol is twice the photon interception rate.

For evaluating the performance of our one-step QD protocol in the practical scenario, we numerically simulate its secret message capacity ($C_{\rm s}$). Similar to QSDC, we define the secret message capacity of QD as the ratio of the total exchanged secure and correct qubits to the overall number of encoded photon pairs. Here, we consider the symmetric scenario, where the hyperentanglement source is at the midpoint between the communication parties. Under this circumstance, the generated photon pairs hyperentangled in two DOFs pass through a quantum channel with the transmission distance of L to reach both parties, and the communication distance $d = 2L$. Consequently, this configuration allows Eve to intercept photons intended for each party. According to Wyner's wiretap channel theory,[66] we can calculate $C_{\rm s}$ as[38,67,68]

$$
C_{\rm s} = I(A:B) + I(B:A) - I(A:E) - I(B:E). \qquad (6)
$$

Here, $I(A:B)$ ($I(B:A)$) represents the message capacity from Alice to Bob (Bob to Alice). Similarly, $I(B:E)$ ($I(A:E)$) denotes the mutual message capacity between Bob and Eve (Alice and Eve). Theoretically, for a hyperentangled photon pair, Alice and Bob can exchange two bits of messages in total. With this framework, we can obtain the sum of $I(A:B)$ and $I(B:A)$ as

$$
I(A:B) + I(B:A) = 2C_{\rm raw}[1 - H(e_{\rm QD})], \qquad (7)
$$

where $H(x)$ represents the binary Shannon entropy as $H(x) = -x\log_2 x-(1-x)\log_2(1-x)$ and $C_{\rm raw}$ denotes the raw message capacity. $e_{\rm QD}$ represents the total error rate of the protocol.

Referring to the principles of the entanglement-based QKD and one-step QSDC protocols,[28,69,70] on can obtain the sum of $I(A:E)$ and $I(B:E)$ as

$$I(A:E)+I(B:E)=2C_{\rm raw}H(e_{\rm QD}). \tag{8}$$

Thus, $C_{\rm s}$ of the one-step QD protocol can be calculated as

$$C_{\rm s}=2C_{\rm raw}[1-2H(e_{\rm QD})]. \tag{9}$$

Next, we estimate the values of $C_{\rm raw}$ and $e_{\rm QD}$. We utilize the spontaneous parametric down-conversion (SPDC) source to generate the original two-photon hyperentangled states. The SPDC source can generate a hyperentangled photon pair with a probability of P (where $P\sim 10^{-3}$).[57] Given $P\ll 1$, our protocol only focuses on the vacuum state, one-pair, two-pair and three-pair emissions, while ignores the higher-order terms. Consequently, the practical photon state ρ generated by the SPDC source can be expressed as

$$\begin{aligned}\rho &= (1-P-P^2-P^3)|0\rangle\langle 0|+P|\Phi^+\rangle\langle\Phi^+|\\ &\quad +P^2|\Phi^+\rangle^{\otimes 2}\langle\Phi^+|^{\otimes 2}+P^3|\Phi^+\rangle^{\otimes 3}\langle\Phi^+|^{\otimes 3}.\end{aligned} \tag{10}$$

Following the hyperentanglement distribution, the communication parties perform the non-local complete polarization BSM. The non-local polarization BSM protocol requires eight photon detectors $\rm D_1$–$\rm D_8$, four in Alice's location and four in Bob's location. As illustrated in Table 1, there are four kinds of detector responses corresponding to each polarized Bell state, each with an equal probability. In this simulation, we account for the practical photon detector, which is unable to distinguish the number of incident photons. Meanwhile, the photon detector has a dark count rate denoted as Y_0. The detection probability of detector $\rm D_j$ $(j=1,2,\ldots,8)$ when k photons are incident is represented as D_j^k. Here, we introduce the concept of collection efficiency α, encompassing the coupling efficiency $\eta_{\rm c}$ between the photon source and fiber, the quantum memory efficiency $\eta_{\rm m}$, the photon transmission efficiency $\eta_{\rm t}=10^{-0.2L/10}$, and the detection efficiency of the detector $\eta_{\rm d}$ $(\alpha=\eta_{\rm c}\eta_{\rm m}\eta_{\rm t}\eta_{\rm d})$. As α and Y_0 are far less than 1, D_j^k can be written as

$$D_j^k=1-(1-\frac{\alpha}{4})^k+Y_0\simeq\frac{k\alpha}{4}+Y_0. \tag{11}$$

Here, we introduce a simplification by defining $\alpha'=\alpha/4$, enabling us to express $D_j^k\simeq k\alpha'+Y_0$.

The calculation of $C_{\rm raw}$ in our one-step QD protocol is similar as that in the one-step QSDC protocol.[28] First, we consider the vacuum state with the probability of $1-P-P^2-P^3$, the clicks of all detectors are attributed to dark counts. Consequently, $C_{\rm raw1}$ can be calculated as

$$\begin{aligned}C_{\rm raw1} &= (1-P-P^2-P^3)(D_1^0+D_2^0+D_3^0+D_4^0)\\ &\quad\times(D_5^0+D_6^0+D_7^0+D_8^0)\\ &= 16(1-P-P^2-P^3)Y_0^2.\end{aligned} \tag{12}$$

Second, we focus on the one hyperentangled-photon-pair component in Eq. (10) with a probability of P. After the non-local BSM, this photon pair can cause the click of one detector pair, while the clicks of the other detector pairs are due to dark counts. Here, we suppose the encoded hyperentangled state to be $|\Phi^+\rangle=|\phi^+\rangle_{\rm p}\otimes|\phi^+\rangle_{\rm s}$. It may lead the response of $\rm D_1D_5$, $\rm D_2D_6$, $\rm D_3D_7$, or $\rm D_4D_8$. In this case, $C_{\rm raw2}$ can be calculated as

$$\begin{aligned}C_{\rm raw2} &= C_4^1P(D_1^1+D_2^0+D_3^0+D_4^0)(D_5^1+D_6^0+D_7^0+D_8^0)\\ &= 4P(\alpha'^2+16Y_0^2+8\alpha'Y_0).\end{aligned} \tag{13}$$

Third, we consider the two hyperentangled-photon-pair components in Eq. (10) with a probability of P^2. The detection results can be categorized into the following two scenarios. First, only one detector pair clicks by the incident of the two photon pairs, such as $\rm D_1D_5$. Secondly, two detector pairs click by the incident of the two photon pairs, such as $\rm D_1D_5$ and $\rm D_2D_6$. Combining the two categories, we can obtain

$$\begin{aligned}C_{\rm raw3} &= 4P^2(D_1^2+D_2^0+D_3^0+D_4^0)(D_5^2+D_6^0+D_7^0+D_8^0)\\ &\quad+12P^2(D_1^1+D_2^1+D_3^0+D_4^0)(D_5^1+D_6^1+D_7^0+D_8^0)\\ &= 16P^2(4\alpha'^2+16Y_0^2+16\alpha'Y_0).\end{aligned} \tag{14}$$

Fourth, we focus on the three hyperentangled-photon-pair components with a probability of P^3. This situation can be classified into three categories, say, the incident of three photon pairs may cause the clicks of one detector pair, two detector pairs, and three detector pairs, respectively. In all the three categories, we can calculate $D_1+D_2+D_3+D_4=D_5+D_6+D_7+D_8=3\alpha'+4Y_0$. As a result, we can obtain $C_{\rm raw4}$ as

$$\begin{aligned}C_{\rm raw4} &= (4+36+24)P^3(3\alpha'+4Y_0)(3\alpha'+4Y_0)\\ &= 64P^3(9\alpha'^2+16Y_0^2+24\alpha'Y_0).\end{aligned} \tag{15}$$

Finally, we can calculate the overall raw message capacity $C_{\rm rawt}$ as

$$C_{\rm rawt}=C_{\rm raw1}+C_{\rm raw2}+C_{\rm raw3}+C_{\rm raw4}. \tag{16}$$

On the other hand, we have to consider the multiple coincidences, say, three or more photon pairs click simultaneously at any one party's side. It is obvious that the multiple coincidence will cause the failure of the non-local BSM. As the probability of four or more detectors clicking simultaneously is significantly lower than that of the threefold click, we only focus on the threefold click case. Referring to the calculations

in Ref. [28], the threefold coincidence rate in the above four cases can be calculated as

$$\begin{aligned} T_1 &= 56(1-P-P^2-P^3)Y_0^3, \\ T_2 &= P(24\alpha'^2 Y_0 + 168\alpha' Y_0^2 + 224 Y_0^3), \\ T_3 &= P^2(48\alpha'^3 + 528\alpha'^2 Y_0 + 1344\alpha' Y_0^2 + 896 Y_0^3), \\ T_4 &= P^3(912\alpha'^3 + 4032\alpha'^2 Y_0 + 6336\alpha' Y_0^2 + 3008 Y_0^3). \end{aligned} \tag{17}$$

In this way, the raw message capacity $C_{\rm raw}$ of our one-step QD protocol can be calculated as

$$C_{\rm raw} = C_{\rm rawt} - T_1 - T_2 - T_3 - T_4. \tag{18}$$

Then, we focus on the total error rate $e_{\rm QD}$. The error may be caused by both the imperfect experimental devices and the decoherence during the photon transmission. We first consider the error caused by the imperfect experimental devices. We also take $|\Phi^+\rangle = |\phi^+\rangle_{\rm p} \otimes |\phi^+\rangle_{\rm s}$ as an example. Only the clicks from D_1D_5, D_2D_6, D_3D_7, or D_4D_8 are correct BSM results, while other types of clicks caused by dark counts would lead to error. Therefore, the correct message capacity corresponding to the vacuum state, one hyperentangled photon pair, two hyperentangled photon pairs, and three hyperentangled photon pairs can be calculated as

$$\begin{aligned} C_{\rm correct_1} &= (1-p-p^2-p^3)4Y_0^2, \\ C_{\rm correct_2} &= pC_4^1[(\alpha'+Y_0)^2 + 3Y_0^2] \\ &= 4p(\alpha'^2 + 2\alpha' Y_0 + 4Y_0^2), \\ C_{\rm correct_3} &= p^2 C_4^1[(2\alpha'+Y_0)^2 + 3Y_0^2] \\ &\quad + C_2^1 p^2 C_4^2[2(\alpha'+Y_0)^2 + 2Y_0^2] \\ &= p^2(40\alpha'^2 + 64\alpha' Y_0 + 64 Y_0^2), \\ C_{\rm correct_4} &= p^3 C_4^1[(3\alpha'+Y_0)^2 + 3Y_0^2] \\ &\quad + C_3^2 p^3 C_4^1 C_3^1[(2\alpha'+Y_0)^2 + (\alpha'+Y_0)^2 + 2Y_0^2] \\ &\quad + C_3^1 C_2^1 p^3 C_4^1[3(\alpha'+Y_0)^2 + Y_0^2] \\ &= p^3(288\alpha'^2 + 384\alpha' Y_0 + 256 Y_0^2). \end{aligned} \tag{19}$$

Next, we consider the influence of decoherence. Here, we suppose the white noise mode in each DOF. After the hyperentanglement distribution, the form of quantum state in two DOFs can be written as

$$\begin{aligned} \rho_{\rm p} &= F_{\rm p}|\phi^+\rangle_{\rm pp}\langle\phi^+| + \frac{1-F_{\rm p}}{3}(|\phi^-\rangle_{\rm pp}\langle\phi^-| \\ &\quad + |\psi^+\rangle_{\rm pp}\langle\psi^+| + |\psi^-\rangle_{\rm pp}\langle\psi^-|), \\ \rho_{\rm s} &= F_{\rm s}|\phi^+\rangle_{\rm ss}\langle\phi^+| + \frac{1-F_{\rm s}}{3}(|\phi^-\rangle_{\rm ss}\langle\phi^-| \\ &\quad + |\psi^+\rangle_{\rm ss}\langle\psi^+| + |\psi^-\rangle_{\rm ss}\langle\psi^-|). \end{aligned} \tag{20}$$

In the above expression, $F_{\rm p}$ ($F_{\rm s}$) represents the fidelity of target state in the polarization (spatial-mode) DOF. Decoherence may affect the non-local BSM results and cause errors, which may make Alice and Bob deduce incorrect messages. It is important to note that if the same kind of error occurs in both DOFs, the BSM can still obtain the right detector response. We take the case that the bit-flip error occurs in both DOFs as an example. In this case, the initial hyperentangled state will be converted to $|\psi^+\rangle_{\rm p} \otimes |\psi^+\rangle_{\rm s}$. Suppose that Alice aims to transmit the message 1 and Bob aims to transmit the message 0, and their random operations are both $I_{\rm p}$. After encoding, the hyperentangled state will evolve to $|\phi^+\rangle_{\rm p} \otimes |\psi^+\rangle_{\rm s}$. The BSM process can be written as

$$\begin{aligned} |\phi^+\rangle_{\rm p} \otimes |\psi^+\rangle_{\rm s} &= \frac{1}{\sqrt{2}}(|H\rangle|H\rangle + |V\rangle|V\rangle) \\ &\quad \otimes \frac{1}{\sqrt{2}}(|a_1\rangle|a_2'\rangle + |a_2\rangle|a_1'\rangle) \\ &= \frac{1}{2}(|H\rangle_{a_1}|H\rangle_{a_2'} + |H\rangle_{a_2}|H\rangle_{a_1'} \\ &\quad + |V\rangle_{a_1}|V\rangle_{a_2'} + |V\rangle_{a_2}|V\rangle_{a_1'}) \\ &\longrightarrow \frac{1}{2}(|H\rangle_{a_1}|H\rangle_{b_2} + |H\rangle_{a_2}|H\rangle_{b_1} \\ &\quad + |V\rangle_{a_1}|V\rangle_{b_2} + |V\rangle_{a_2}|V\rangle_{b_1}) \\ &\xrightarrow{\rm PBS} \frac{1}{2}(|H\rangle_{a_4}|H\rangle_{b_3} + |H\rangle_{a_3}|H\rangle_{b_4} \\ &\quad + |V\rangle_{a_3}|V\rangle_{b_4} + |V\rangle_{a_4}|V\rangle_{b_3}) \\ &\xrightarrow{\rm QWP} \frac{1}{4}\big[(|H\rangle_{a_4'} + |V\rangle_{a_4'})(|H\rangle_{b_3'} + |V\rangle_{b_3'}) \\ &\quad + (|H\rangle_{a_3'} + |V\rangle_{a_3'})(|H\rangle_{b_4'} + |V\rangle_{b_4'}) \\ &\quad + (|H\rangle_{a_3'} - |V\rangle_{a_3'})(|H\rangle_{b_4'} - |V\rangle_{b_4'}) \\ &\quad + (|H\rangle_{a_4'} - |V\rangle_{a_4'})(|H\rangle_{b_3'} - |V\rangle_{b_3'})\big] \\ &= \frac{1}{2}(|H\rangle_{a_4'}|H\rangle_{b_3'} + |V\rangle_{a_4'}|V\rangle_{b_3'} \\ &\quad + |H\rangle_{a_3'}|H\rangle_{b_4'} + |V\rangle_{a_3'}|V\rangle_{b_4'}). \end{aligned} \tag{21}$$

As a result, the output photons will be detected by D_3D_5, D_4D_6, D_1D_7, or D_2D_8. From Table 1, Alice and Bob can infer the encoded polarization Bell state to be $|\psi^+\rangle_{\rm p}$, and thus can exchange correct messages 1 and 0. Similarly, if the phase-flip error or bit-phase-flip error occurs in both DOFs, Alice and Bob can also obtain the correct polarization BSM results from the detector responses. Therefore, if the same kind of error occurs in both DOFs, the parties can still exchange correct messages based on the BSM results.

Thus, the total correct rate $C_{\rm correct_t}$ is

$$\begin{aligned} C_{\rm correct_t} &= \left[F_{\rm p}F_{\rm s} + \frac{(1-F_{\rm p})(1-F_{\rm s})}{3}\right] \\ &\quad \times (C_{\rm correct_1} + C_{\rm correct_2} + C_{\rm correct_3} + C_{\rm correct_4}). \end{aligned} \tag{22}$$

In this way, the total error rate $e_{\rm QD}$ can be calculated as

$$e_{\rm QD} = \frac{C_{\rm raw} - C_{\rm correct_t}}{C_{\rm raw}}. \tag{23}$$

Taking the values of $C_{\rm raw}$ and $e_{\rm QD}$ in Eqs. (18) and (23) into Eq. (9), we calculate the value of $C_{\rm s}$. In Fig. 4, we show

C_s of the one-step QD protocol altered with the communication distance d between the communication parties. We fix $Y_0 = 6.02 \times 10^{-6}$, $\eta_m = \eta_c = 0.95$, $\eta_d = 0.9$. For calculating η_t, we choose $\alpha = 0.2$ dB/km. The parameters F_p and F_s are adjusted to be 1, 0.98, 0.96, respectively. It can be seen that when $F_p = F_s = 0.98$, the maximum communication distance achieves approximately 211 km. With the repetition rate of the SPDC source being 10 GHz[71] and $F_p = F_s = 0.98$, C_s is around 1435 bit/s at a communication distance of 100 km.

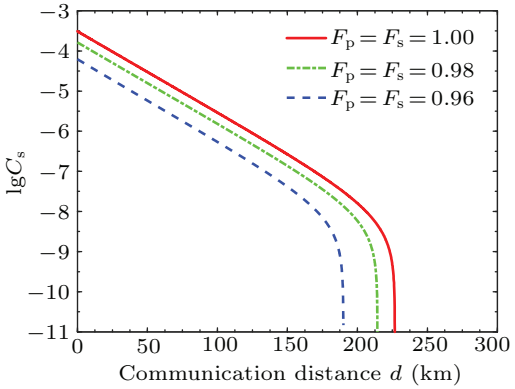


Fig. 4. The secret message capacity C_s alters with the communication distance d between the communication parties. Here, we fix $Y_0 = 6.02 \times 10^{-6}$, $\eta_m = \eta_c = 0.95$, $\eta_d = 0.9$, and adjust $F_p = F_s = 1, 0.98, 0.96$, respectively.

5. Discussion and conclusion

QD enables two communication parties to directly exchange secret messages simultaneously, realizing real-time secure bidirectional communication. Similar to conventional QSDC protocols,[15–18] previous QD protocols require to transmit photons in the quantum channel twice.[19,20,43–47] The channel noise may cause photon transmission loss and quantum state decoherence in each photon transmission process. The photon transmission loss and quantum state decoherence can largely limit the maximal secure communication distance and reduce the secret message capacity. Worse still, they may cause message loss and message error, which makes the transmitted messages incomplete and incorrect. In our QD protocol, the parties only require to distribute photons in the quantum channel once, which can simplify the experimental operation and reduce the photon transmission loss. Most entanglement-based QD requires the complete BSM.[19,20,45,49] However, the linear-optical BSM only has a success probability of 50%. The complete BSM often relies on nonlinear optical elements,[72–76] which are difficult to realize under current experimental conditions. In contrast, our one-step QD protocol adopts the hyperentanglement-assisted non-local complete polarization BSM with a probability of 100%, which is feasible with current linear optical devices.

QM is an important element of our one-step QD protocol. In the protocol, the parties should store the photons in the quantum memory until they ensure the photon transmission being secure. During recent few years, QM has achieved great experimental progresses.[77–83] In 2017, a high-fidelity nanophotonic QM with $> 95\%$ spin polarization for efficient initialization of the atomic frequency comb memory and time bin-selective readout was experimentally demonstrated.[78] In 2018, Hsiao *et al.* achieved a storage efficiency of 92.0% for a coherent optical memory based on the electromagnetically induced transparency (EIT) scheme in optically dense cold atomic media.[79] In 2019, a high-performance atomic Raman memory in ^{87}Rb vapor with the memory efficiency of above 82.0% for 6 ns–20 ns optical pulses and the unconditional fidelity of up to 98.0% was achieved.[80] Later, the coherent storage of light in an atomic frequency comb memory over 1 hour was realized by the group of Ma.[82] Recently, Zhang *et al.* reported their achievement on the fiber-integrated multimode quantum storage of single photon at telecom band with 330 temporal modes on a laser-written chip.[83] Based on these attractive progresses, our one-step QD protocol may be experimentally realized in the near future.

From the security analysis, the channel noise makes it possible for Eve to intercept some photons without being detected, and increases message loss rate and message error rate. Similar to QSDC, in QD, the communication parties cannot perform the post-processing technique to resist message loss and message errors. In this way, the message loss and message error are two big obstacles in the practicality of QD. Actually, we can adopt the polarization-spatial-mode hyperentanglement purification and heralded amplification to modify our one-step QD protocol. In detail, Bob can perform the hyperentanglement amplification to herald the arrival of each transmitted photon.[84] After that, both parties can repeat the hyperentanglement purification[85] to improve the fidelity of the hyperentanglement channel. In theory, Alice and Bob can construct the nearly perfect hyperentanglement channel, where the parties can detect any eavesdropping behavior from Eve. As a result, the message leakage loophole can be eliminated. Meanwhile, the message loss and message error can be also nearly eliminated, thus guaranteeing the correctness and integrity of the transmitted messages. In contrast, in the previous entanglement-based QD protocols,[19,20] the parties cannot perform the EPP after the second photon transmission round, for the EPP may change the encoded messages. As a result, the decoherence caused by the second photon transmission round cannot be eliminated, which can bring security loophole and message errors. Moreover, our one-step QD can be combined with the quantum repeater and drone to construct the long-distance hyperentanglement channel, and thus realize the long-distance one-step QD.

In summary, we propose the first one-step QD protocol with the help of hyperentanglement and non-local com-

plete BSM. In the protocol, two communication parties first construct the hyperentanglement channel. After checking the security of the photon transmission process, they encode their messages in the polarization DOF of each hyperentangled photon pair. Then, by performing the non-local hyperentanglement-assisted complete polarization BSM, they can finally obtain the exchanged messages. This one-step QD protocol is theoretically secure and two parties can exchange 2 bits of messages by using a hyperentangled photon pair. The secret message capacity of the one-step QD protocol is numerically simulated. We obtain that with the fidelities in both DOFs of $F_{\rm p} = F_{\rm s} = 0.98$, the one-step QD protocol can achieve the maximal communication distance of about 211 km. Compared with previous QD protocols, our one-step QD protocol has some attractive advantages. First, photons only need to transmit in the quantum channel once, which can simplify the experiment operations and reduce the photon transmission loss. Second, the non-local complete polarization BSM can completely distinguish four polarization Bell states and is feasible with current technique. Third, combined with the heralded amplification and purification, the nearly perfect hyperentanglement channel can be constructed between two parties, which can nearly eliminate the message leakage loophole, the message loss and message error. Moreover, combined with quantum repeater and drone, our one-step QD is possible to realize long-distance QD. In this way, our one-step QD protocol is an important development of QD and will have important applications in future quantum communication field.

Acknowledgement

Project supported by the National Natural Science Foundation of China (Grant Nos. 12175106 and 92365110).

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] Ursin R, Tiefenbacher F, Schmitt-Manderbach T, Weier H, Scheidl T and Lindenthal M B B 2007 *Nat. Phys.* **3** 481
[4] Sasaki T, Yamamoto Y and Koashi M 2014 *Nature* **509** 475
[5] Xu F H, Ma X F, Zhang Q, Lo H K and Pan J W 2020 *Rev. Mod. Phys.* **92** 025002
[6] Ren M, Zhou L and Yuan Z 2023 *Sci China: Inf. Sci.* **66** 180503
[7] Ma L, Yang J, Zhang T, *et al*. 2023 *Sci China: Inf. Sci.* **66** 180507
[8] Wu L X, Feng Y Y and Zhou J 2023 *Chin. Phys. B* **32** 070310
[9] Zhang X X, Lu Y F, Wang Y, Jiang M S, Li H W, Zhou C, Zhou Y and Bao W S 2023 *Chin. Phys. B* **32** 050308
[10] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[11] Fu Y, Yin H L, Chen T Y, Y and Chen Z B 2015 *Phys. Rev. Lett.* **114** 090501
[12] Ju X X, Zhong W, Sheng Y B and Zhou L 2022 *Chin. Phys. B* **31** 100302
[13] Shen A, Cao X Y, Wang Y, Fu Y, *et al*. 2023 *Sci. China Phys. Mech. Astron.* **66** 260311
[14] Xing D, Wang Y F, Dou Z, Li J, Chen X B and Li L X 2023 *Chin. Phys. B* **32** 070308
[15] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[16] Deng F G, Long G L and Liu X S 2003 *Phys. Rev. A* **68** 042317
[17] Deng F G and Long G L 2004 *Phys. Rev. A* **69** 052319
[18] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev. A* **71** 044305
[19] Nguyen B A 2004 *Phys. Lett. A* **328** 6
[20] Man Z X, Zhang Z J and Liu Y 2005 *Chin. Phys. Lett.* **22** 22
[21] Qi R Y, Sun Z, Lin Z S, *et al*. 2019 *Light Sci. Appl.* **8** 22
[22] Zhou L, Sheng Y B and Long G L 2020 *Sci. Bull.* **65** 12
[23] Zhou Z R, Sheng Y B, Niu P H, Yin L G, Long G L and Hanzo L 2020 *Sci. China Phys. Mech. Astron.* **63** 230362
[24] Sun Z, Song L Y, Huang Q, *et al*. 2020 *IEEE Trans. Commun.* **68** 5778
[25] Li T and Long G L 2020 *New J. Phys.* **22** 063017
[26] Long G L and Zhang H R 2021 *Sci. Bull.* **66** 1267
[27] Cao Z W, Wang L, Liang K X, Chai G and Peng J Y 2021 *Phys. Rev. Appl.* **16** 024012
[28] Sheng Y B, Zhou L and Long G L 2022 *Sci. Bull.* **67** 367
[29] Zhou L and Sheng Y B 2022 *Sci. China Phys. Mech. Astron.* **65** 250311
[30] Ying J W, Zhou L, Zhong W and Sheng Y B 2022 *Chin. Phys. B* **31** 120303
[31] Zhou L, Xu B W, Zhong W and Sheng Y B 2023 *Phys. Rev. Appl.* **19** 014036
[32] Liang K X, Cao Z W, Chen X L, Wang L, Chai G and Peng J Y 2023 *Front. Phys.* **18** 51301
[33] Zeng H, Du M M, Zhong W, Zhou L and Sheng Y B 2023 *Funda. Res.*
[34] Zhang Q, Du M M, Zhong W, Sheng Y B and Zhou L 2023 *Ann. Phys. Berlin*
[35] 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
[36] Zhang W, Ding D S, Sheng Y B, Zhou L, Shi B S and Guo G C 2017 *Phys. Rev. Lett.* **118** 220501
[37] Zhu F, Zhang W, Sheng Y B and Huang Y D 2017 *Sci. Bull.* **62** 1519
[38] Pan D, Lin Z S, Yin L G, Wu J W, Sun Z, Ruan D and Long G L 2020 *Photon. Res.* **8** 1522
[39] Qi Z T, Li Y H, Huang Y W, Feng J, Zheng Y L, Chen X F 2021 *Light Sci. Appl.* **10** 183
[40] Zhang H R, Sun Z, Qi R Y, Yin L G, Long G L and Lu J H 2022 *Light Sci. Appl.* **11** 83
[41] Long G L, Pan D, Sheng Y B, Xue Q K, Lu J H and Hanzo L 2022 *IEEE Network* **36** 82
[42] Paparelle I, Mousavi F, Scazza F, Bassi A, Paris M and Zavatta A 2023 arXiv:2306.14322
[43] Yang Y G and Wen Q Y 2007 *Sci. China Ser. G-Phys. Mech. Astron.* **50** 558
[44] Gao F, Guo F Z, Wen Q Y and Zhu F C 2008 *Sci. China Ser. G-Phys. Mech. Astron.* **51** 559
[45] Shi G F, Xi X Q, Tian X L, *et al*. 2009 *Opt. Commun.* **282** 2460
[46] Shi G F, Xi X Q, Hu M L, *et al*. 2010 *Opt. Commun.* **283** 1984
[47] Gao G 2010 *Opt. Commun.* **283** 2288
[48] Ye T Y 2014 *Commun. Theor. Phys.* **62** 338
[49] Zheng C and Long G F 2014 *Sci. China Phys. Mech. Astron.* **57** 1238
[50] Ye T Y and Jiang L Z 2014 *Phys. Scr.* **89** 015103
[51] Gong L H, Tian C, Li J F and Zou X F 2018 *Quant. Inf. Process.* **17** 331
[52] Barreiro J T, Wei T C and Kwiat P G 2008 *Nat. Phys.* **4** 282
[53] Hu X M, Guo Y, Liu B H, Huang Y F, Li C F and Guo G C 2018 *Sci. Adv.* **4** eaat9304
[54] Simon C and Pan J W 2002 *Phys. Rev. Lett.* **89** 257901
[55] Sheng Y B and Deng F G 2010 *Phys. Rev. A* **82** 044305
[56] Ecker S, Sohr P, Bulla L, Huber M and Bohmann M 2021 *Phys. Rev. Lett.* **127** 040506
[57] Hu X M, Huang C X, Sheng Y B, *et al*. 2021 *Phys. Rev. Lett.* **126** 010503
[58] Walborn S P, Pádua S and Monken C H 2003 *Phys. Rev. A* **68** 042313
[59] Schuck C, Huber G, Kurtsiefer C and Weinfurter H 2006 *Phys. Rev. Lett.* **96** 190501
[60] Wang X L, Cai X D, Su Z E, *et al*. 2015 *Nature* **518** 516
[61] Chapman J C, Graham T M, Zeitler C K, Bernstein H J and Kwiat P G 2020 *Phys. Rev. Appl.* **14** 014044
[62] Chen Y, Ecker S, Wengerowsky S, Bulla L, Joshi S K, Steinlechner F and Ursin R 2018 *Phys. Rev. Lett.* **121** 200502
[63] Hu X M, Xing W B, Liu B H, He D Y, Cao H, Guo Y, Zhang C, Zhang H, Huang Y F, Li C F and Guo G C 2020 *Optica* **7** 738

[64] Zhao P, Yang M Y, Zhu S, Zhou L, Zhong W, Du M M and Sheng Y B 2023 *Sci. China Phys. Mech. Astron.* **66** 100311
[65] Chen Z B, Pan J W, Zhang Y D, Brukner C and Zeilinger A 2003 *Phys. Rev. Lett.* **90** 160408
[66] Wyner A D 1975 *Bell Syst. Tech. J.* **54** 1355
[67] Wu J W, Lin Z S, Yin L G and Long G L 2019 *Quant. Engin.* **1** e26
[68] Liu X, Li Z, Luo D, *et al*. 2021 *Sci. China Phys. Mech. Astron.* **64** 120311
[69] Ma X F, Fung C H F and Lo H K 2007 *Phys. Rev. A* **76** 012307
[70] Takesue H, Harada K, Tamaki K, *et al*. 2010 *Opt. Express* **18** 16777
[71] Zhang Q, Xie X P, Takesue H, *et al*. 2007 *Opt. Express* **15** 10288
[72] Sheng Y B and Deng F G 2010 *Phys. Rev. A* **81** 032307
[73] Sheng Y B, Deng F G and Long G L 2010 *Phys. Rev. A* **82** 032318
[74] Ren B C, Wei H R, Hua M, *et al*. 2012 *Opt. Express* **20** 24664
[75] Wang T J, Lu Y and Long G L 2012 *Phys. Rev. A* **86** 042337
[76] Wang G Y, Ai Q, Ren B C, *et al*. 2016 *Opt. Express* **24** 28444
[77] Yang S J, Wang X J, Bao X H and Pan J W 2016 *Nat. Photon.* **10** 381
[78] Zhong T, Kindem J M, Bartholomew J G, Rochman J, Craiciu I, *et al.* 2017 *Science* **357** 1392
[79] Hsiao Y F, Tsai P J, Chen H S, *et al*. 2018 *Phys. Rev. Lett.* **120** 183602
[80] Guo J X, Feng X T, Yang P Y, Yu Z F, Chen L Q, Yuan C H and Zhang W P 2019 *Nat. Commun.* **10** 148
[81] Wang Y F, Li J F, Zhang S C, Su K Y, Zhou Y R, Liao K Y, Du S W, Yan H and Zhu S L 2019 *Nat. Photon.* **13** 346
[82] Ma Y, Ma Y Z, Zhou Z Q, Li C F and Guo G C 2021 *Nat. Commun.* **12** 2381
[83] Zhang X Y, Zhang B, Wei S H, Li H, Liao J Y, Li C, Deng G W, Wang Y, Song H Z and You L X 2023 *Sci. Adv.* **9** eadf4587
[84] Yang G, Zhang Y S, Yang Z R, *et al*. 2019 *Quant. Inf. Process.* **18** 1
[85] Ren B C, Du F F and Deng F G 2014 *Phys. Rev. A* **90** 052309