Science Bulletin 67 (2022) 367–374

Contents lists available at ScienceDirect

Science Bulletin

journal homepage: www.elsevier.com/locate/scib

Science Bulletin www.scibull.com

Article

One-step quantum secure direct communication

Yu-Bo Sheng [a,g,*], Lan Zhou [b], Gui-Lu Long [c,d,e,f,*]

[a] College of Electronic and Optical Engineering & College of Microelectronics, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[b] School of Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[c] Department of Physics, Tsinghua University, Beijing 100084, China
[d] State Key Laboratory of Low-Dimensional Quantum Physics, Tsinghua University, Beijing 100084, China
[e] Beijing National Research Center for Information Science and Technology, Beijing 100084, China
[f] Beijing Academy of Quantum Information Sciences, Beijing 100193, China
[g] Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

ARTICLE INFO

Article history:
Received 6 September 2021
Received in revised form 13 October 2021
Accepted 26 October 2021
Available online 4 November 2021

Keywords:
Quantum secure direct communication
Hyperentanglement
Nonlocal Bell-state analysis

ABSTRACT

Quantum secure direct communication (QSDC) attracts much attention for it can transmit secret messages directly without sharing a key. In this article, we propose a one-step QSDC protocol, which only requires to distribute polarization-spatial-mode hyperentanglement for one round. In this QSDC protocol, the eavesdropper cannot obtain any message, so that this protocol is unconditionally secure in principle. This protocol is a two-way quantum communication and has high capacity for it can transmit two bits of secret messages with one pair of hyperentanglement. With entanglement fidelities of both polarization and spatial-mode degrees of freedom being 0.98, the maximal communication distance of this one-step QSDC can reach about 216 km. QSDC can also be used to generate the key. In this regard, the key generation rate is estimated about 2.5 times of that in the entanglement-based QKD with the communication distance of 150 km. With the help of future quantum repeaters, this QSDC protocol can provide unconditionally secure communication over arbitrarily long distance.

1. Introduction

Quantum communication can ensure the unconditional security of communication. Quantum communication began with quantum key distribution (QKD), which can distribute random key between two users [1]. With the help of entanglement purification [2] and quantum repeaters [3], QKD can be unconditionally secure in a noise channel over arbitrarily long distance [4–6]. Since Bennett and Brassard (BB84) [1] proposed the first QKD protocol in 1984, some other important QKD protocols based on entanglement [7,8] have also been proposed. In the past nearly 40 years, QKD has been widely investigated in both theory and experiment. In theory, the security of the QKD with realistic devices has been proved [9–11]. Using satellites, the space-to-ground quantum communication network has already been realized [12]. Meanwhile, the chip-based QKD system has also been constructed [13]. Nowadays, QKD becomes the most practical quantum technology.

Besides QKD, there are two other typical quantum communication modes. The first mode is the quantum teleportation (QT) [14], which can transmit an arbitrary unknown quantum state $\alpha|0\rangle + \beta|1\rangle$ $(|\alpha|^2 + |\beta|^2 = 1)$ without transmitting the encoded particle itself. QT has been widely investigated in long distance [15], multiple degrees of freedom (DOFs) [16,17] and high dimension [18,19]. The second important quantum communication mode is the two-step quantum secure direct communication (QSDC) [20,21]. QSDC can directly transmit secret message without sharing a key. QSDC protocols require to transmit photons for two rounds. In the first round, two users distribute the entanglement to set up the quantum channel. Then, the message sender encodes his message using the dense coding approach [22]. After encoding, one of the photons in each photon pair should be sent back to perform the Bell-state analysis (BSA) to read out the secret message. During recent few years, QSDC has achieved great progress in both theory and experiments [23–40]. In the theoretical aspect, the device-independent (DI) and measurement-device-independent (MDI) QSDC have been successively proposed in 2020 [32,33]. In 2021, Long and Zhang [39] adopted the masking (INCUM) technique to increase the capacity of QSDC. In the experimental aspect, in 2016, Hu et al. [26] experimentally demonstrated the QSDC with single photons in a noisy environment using frequency coding. In

[*] Corresponding authors.
E-mail addresses: shengyb@njupt.edu.cn (Y.-B. Sheng), gllong@tsinghua.edu.cn (G.-L. Long).

https://doi.org/10.1016/j.scib.2021.11.002
2095-9273/© 2021 Science China Press. Published by Elsevier B.V. and Science China Press. All rights reserved.

2017, Zhang et al. [27] demonstrated the entanglement-based QSDC experiment with quantum memory. In the same year, the first long-distance QSDC experiment in fiber was realized by the group of Zhu [28]. In 2021, a 15-user QSDC network has been realized, and the fidelity of the entangled state shared by any two users is $> 97\%$ [40].

Entanglement distribution is of great importance for QSDC realization. During the past few years, entanglement distribution via fibers, satellites, and drones have developed rapidly [41–44]. In 2017, the group of Pan [42] successfully demonstrated the satellite-based entanglement distribution to receiver stations separated by more than 1200 km. In 2020, the group of Zhu [43] realized the first mobile entanglement distribution based on drones. Later, using two drones, they achieved the entanglement distribution with Clauser-Horne-Shimony-Holt S parameter of 2.59 ± 0.11 at 1 km distance [44].

Hyperentanglement [45], which means the simultaneous entanglement in more than one DOF, has been widely investigated in increasing the channel capacity [46–48], entanglement purification [49–52], complete BSA [53,54], and teleportation in multiple DOFs [16,17]. In this paper, based on precious QSDC protocols [20,21], we propose a feasible one-step QSDC protocol in linear optics using hyperentanglement. Although some previous QSDC protocols have also adopted hyperentanglement to increase the message capacity or realize the bidirectional communication [55–59], our one-step QSDC protocol is quite different with them. Those QSDC protocols belong to the conventional two-step QSDC, which require to distribute the hyperentanglement in the quantum channels twice. The receiver needs to perform local BSA to decode the message. Our one-step QSDC protocol only requires to distribute hyperentanglement in the quantum channel once to construct the hyperentanglement channel. Then, the information sender encodes the message in polarization DOF using the dense coding approach. The encoded photons do not need to be sent back for local BSA. The spatial-mode entanglement can help to distinguish the polarization Bell states nonlocally. Finally, according to two parties' measurement results, the message receiver can completely distinguish the four Bell states in polarization DOF secretly and decode the secret message from the sender. Compared with entanglement-based QKD, this protocol can transmit 2 bits of secret message by distributing the hyperentanglement only one round, while QKD can only share 1 bit of key with 50% success probability.

2. One-step QSDC protocol

Our one-step QSDC protocol adopts the polarization-spatial-mode hyperentanglement with the form of

$$|\Phi^+\rangle = |\phi^+\rangle_{\rm P} \otimes |\phi^+\rangle_{\rm S}. \tag{1}$$

$|\phi^+\rangle_{\rm P}$ is one of the four Bell states in polarization DOF with the form of

$$\begin{aligned}|\phi^\pm\rangle_{\rm P} &= \frac{1}{\sqrt{2}}(|H\rangle|H\rangle \pm |V\rangle|V\rangle),\\ |\psi^\pm\rangle_{\rm P} &= \frac{1}{\sqrt{2}}(|H\rangle|V\rangle \pm |V\rangle|H\rangle).\end{aligned} \tag{2}$$

$|\phi^+\rangle_{\rm S}$ is one of the four Bell states in spatial-mode DOF, which can be described as

$$\begin{aligned}|\phi^\pm\rangle_{\rm S} &= \tfrac{1}{\sqrt{2}}(|a_1\rangle|b_1\rangle \pm |a_2\rangle|b_2\rangle),\\ |\psi^\pm\rangle_{\rm S} &= \tfrac{1}{\sqrt{2}}(|a_1\rangle|b_2\rangle \pm |a_2\rangle|b_1\rangle).\end{aligned} \tag{3}$$

Here, $|H\rangle$ and $|V\rangle$ denote horizontal and vertical polarization, respectively. a_1, b_1, a_2, and b_2 are different spatial modes.

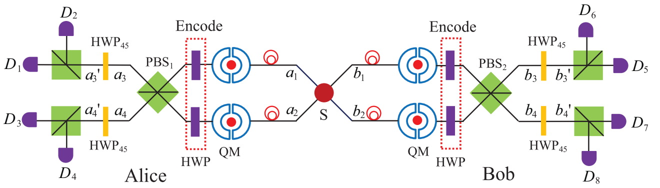

Fig. 1. (Color online) Schematic principle of the one-step QSDC protocol. HWP is the half-wave plate which can realize four single-qubit unitary operations to encode the messages. After encoding, Alice and Bob [53] perform the nonlocal complete polarization Bell-state analysis assisted with spatial-mode entanglement. PBS is the polarization beam splitter, which can transmit the $|H\rangle$ polarized photon and reflect the $|V\rangle$ polarized photon. QM represents the quantum memory. D_i $(i = 1, 2, 3, \cdots, 8)$ means the photon detector.

The basic principle of our one-step QSDC protocol is shown in Fig. 1. This one-step QSDC protocol can be described as follows.

(1) Alice prepares an ordered N pairs of polarization-spatial-mode hyperentangled states $|\Phi^+\rangle_i$ $(i = 1,\ 2,\ \cdots\ N)$ with the form of Eq. (1). These ordered N photon pairs construct the message sequence. She also prepares an ordered M pairs of hyperentangled states $|\Phi^+\rangle_j$ $(j = 1,\ 2,\ \cdots\ M)$ for security checking. The security checking photon pairs are randomly inserted into the message sequence. In this way, the message sequence includes $N + M$ hyperentangled photon pairs.

(2) For each hyperentangled photon pair in the message sequence, Alice retains the first photon and sends the second photon to Bob using the block transmission in Refs. [20,21]. After the photon transmission, Alice and Bob measure the security checking photons and store the other photons in the message sequence in quantum memories for waiting for the security checking.

(3) In the security checking sequence, Alice randomly chooses the basis $\{|H\rangle,\ |V\rangle\}$ or $\{|\pm\rangle_{\rm P} = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)\}$ in polarization DOF and $\{|a_1\rangle,\ |a_2\rangle\}$ or $\{|\pm\rangle_{\rm S} = \frac{1}{\sqrt{2}}(|a_1\rangle \pm |a_2\rangle)\}$ in spatial-mode DOF to measure the security checking photons. Then, Alice tells Bob the position and measurement basis she has chosen for each security checking photon. Bob uses the same measurement basis to measure the corresponding photon in his location. Finally, Alice and Bob compare their measurement results with classical communication. In ideal situation without eavesdropping, Alice and Bob always obtain the same results in both DOFs. If they obtain different measurement results in a DOF, it will cause a bit-flip error. If the bit-flip error rate (QBER) in any DOF exceeds the threshold, Alice and Bob should abort the communication. Otherwise, they ensure that the photon transmission process is secure. By the way, Alice and Bob can also use the Clauser-Horne-Shimony-Holt (CHSH) inequality like E91 protocol [7] in both polarization and spatial modes to perform the security checking.

(4) When the security of the photon transmission process is ensured, Alice distills the photons in the message sequence from the quantum memories and encodes her single photons with four single-qubit unitary operations. It is the "Encode" part in Fig. 1. The four unitary operations can be written as [22]

$$\begin{aligned}U_0 &= I = |H\rangle\langle H| + |V\rangle\langle V|,\\ U_1 &= \sigma_x = |H\rangle\langle V| + |V\rangle\langle H|,\\ U_2 &= \sigma_z = |H\rangle\langle H| - |V\rangle\langle V|,\\ U_3 &= i\sigma_y = |H\rangle\langle V| - |V\rangle\langle H|.\end{aligned} \tag{4}$$

The operation U_k $(k = 0,\ 1,\ 2,\ 3)$ can transform the state $|\phi^+\rangle_{\rm P}$ to $|\phi^+\rangle_{\rm P}$, $|\psi^+\rangle_{\rm P}$, $|\phi^-\rangle_{\rm P}$ and $|\psi^-\rangle_{\rm P}$, respectively. Here, these operations U_0, U_1, U_2, and U_3 are encoded as “00”, “01”, “10”, and “11”, respectively.

(5) For reading out the encoded message, Alice and Bob perform the nonlocal complete polarization BSA assisted with spatial-mode entanglement as shown in Fig. 1 [53]. The complete polarization BSA result depends on the output modes of Alice and Bob, as shown in Table 1.

(6) Alice publishes the positions and her measurement results of the message photons.

(7) According to the measurement results from Alice, Bob can decode the secret messages combined with his own measurement results. Certainly, this protocol can realize the two-way communication. After the successful security checking, Bob can also encode his secret messages similarly as Alice.

From above description, the key element of this one-step QSDC protocol is the nonlocal complete polarization BSA. It is known that in linear optics, only two of the four Bell states can be distinguished [60,61]. Interestingly, in hyperentanglement, with the help of the entanglement in other DOF, such as the spatial-mode, time-bin, orbital angular momentum (OAM), one can realize the complete polarization BSA [46,47,53,54].

Here, we give a specific example. As shown in Fig. 1, the initial state shared by Alice and Bob is a hyperentangled state in Eq. (1). After performing the security checking, if no eavesdropping exists, Alice encodes her secret messages using the “Encoder” module. If Alice wants to send “10”, she performs U_2 in the polarization DOF. The state $|\Phi^+\rangle$ becomes

$$\begin{aligned}|\Phi^-\rangle &= |\phi^-\rangle_{\mathrm{P}} \otimes |\phi^+\rangle_{\mathrm{S}} \\ &= \frac{1}{\sqrt{2}}(|H\rangle|H\rangle - |V\rangle|V\rangle) \otimes \frac{1}{\sqrt{2}}(|a_1\rangle|b_1\rangle + |a_2\rangle|b_2\rangle).\end{aligned} \tag{5}$$

After the photons passing through the polarizing beam splitters (PBSs) which can transmit the photon in $|H\rangle$ and reflect the photon in $|V\rangle$ and the HWPs (the HWPs can make $|H\rangle \rightarrow \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ and $|V\rangle \rightarrow \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$), successively, $|\Phi^-\rangle$ evolves as

$$\begin{aligned}|\Phi^-\rangle &\rightarrow \frac{1}{2}(|H\rangle_{a_4}|H\rangle_{b_4} + |H\rangle_{a_3}|H\rangle_{b_3} - |V\rangle_{a_4}|V\rangle_{b_4} - |V\rangle_{a_3}|V\rangle_{b_3}) \\ &\rightarrow \frac{1}{2}(|H\rangle_{a_{4'}}|V\rangle_{b_{4'}} + |V\rangle_{a_{3'}}|H\rangle_{b_{3'}} + |H\rangle_{a_{3'}}|V\rangle_{b_{3'}} + |V\rangle_{a_{4'}}|H\rangle_{b_{4'}}).\end{aligned} \tag{6}$$

The item $|H\rangle_{a_{4'}}|V\rangle_{b_{4'}}$ will make the photon detectors D_3D_8 click. Item $|V\rangle_{a_{3'}}|H\rangle_{b_{3'}}$ will make the two photon detectors D_2D_5 click. Item $|H\rangle_{a_{3'}}|V\rangle_{b_{3'}}$ will make D_1D_6 click and $|V\rangle_{a_{4'}}|H\rangle_{b_{4'}}$ will make D_4D_7 click. After Alice publishes her measurement result with 2 bits of classical message, i.e., one of the four single-photon detectors D_1, D_2, D_3, and D_4 registers the photon, Bob can distinguish the polarization Bell state $|\phi^-\rangle_{\mathrm{P}}$ deterministically combined with his measurement result. In this way, Bob can deduce that Alice performs U_2 on the photon corresponding to the message of “10”.

3. Security analysis and theoretical secrecy capacity of the one-step QSDC

In this section, we try to make a brief security analysis and provide the theoretical secrecy capacity of our one-step QSDC. The security checking method in both polarization and spatial-mode DOFs are analogy with that of the entanglement-based QKD [7,8]. In the hyperentanglement distribution process, if the eavesdropper (Eve) tries to intercept some photons and substitute his own prepared photons to Bob, such prepared photons are not entangled with the photons in Alice’s location. As a result, the intercept-resend eavesdropping may increase the QBER in each DOF. If the QBER in any DOF exceeds the threshold, the photon transmission process is not secure and the parties should abort the communication. Especially, Alice and Bob can judge whether there is an eavesdropper, even when the hyperentanglements come from the untrusted hyperentanglement source. Such security checking in each DOF depends on an appealing advantage of the hyperentanglement that the states in two DOFs can be operated independently. In practical noisy environment, Eve can intercept some photons without being detected by replacing the noise channel with a perfect channel. In this case, Alice and Eve perform the nonlocal complete polarization BSA, and Eve can obtain Alice’s encoded message according to Alice’s and his measurement results. In this way, the message leakage rate of our one-step QSDC protocol equals to Eve’s photon interception rate during the photon transmission process, which also equals to the key leakage rate of the entanglement-based QKD protocol.

Then, we estimate the secrecy message capacity (C_s) of the one-step QSDC protocol using a hyperentanglement source based on spontaneous parametric process. Suppose that the hyperentanglement source locates in the middle of Alice and Bob, and the hyperentangled photon pairs are sent to Alice and Bob through the quantum channels, respectively. Thanks to the nonlocal BSA with the success probability of 100%, the photons only require to distribute during the quantum channels once. In this way, the calculation of the secrecy message capacity C_s is quite similar to that of the key generation rate of the entanglement-based QKD [62,63]. It is noticed that as the QSDC transmits messages, not random keys, the parties cannot use error correction or private amplification. Meanwhile, each hyperentangled photon pair carries 2 bits of message. In this way, the C_s of our one-step QSDC is provided by [62,63]

$$C_s = 2C_{\mathrm{raw}}[1 - 2h(e_{\mathrm{QSDC}})], \tag{7}$$

where C_{raw}, e_{QSDC}, and h are the raw message capacity, error rate, and the binary entropy function, respectively.

Next, we estimate C_{raw} and e_{QSDC}. The initial two-photon hyperentangled photon states $|\Phi^+\rangle = |\phi^+\rangle_{\mathrm{P}} \otimes |\phi^+\rangle_{\mathrm{S}}$ are generated based on a spontaneous parametric process. The spontaneous parametric down-conversion source generates a photon pair with a probability of p ($p \sim 10^{-3}$) [51]. Here, we only consider the vacuum state, one-pair, two-pair, and three-pair emission and neglect the higher order term. The generated hyperentangled photon states can be written as

Table 1
The nonlocal complete BSA results in the polarization DOF according to the measurement results. It is similar to Ref. [53]. D_iD_j means both the photon detectors D_i and D_j detect photons.

State	Measurement results			
$\lvert\phi^+\rangle_{\mathrm{P}}$	D_1D_5	D_2D_6	D_3D_7	D_4D_8
$\lvert\psi^+\rangle_{\mathrm{P}}$	D_1D_7	D_3D_5	D_4D_6	D_2D_8
$\lvert\phi^-\rangle_{\mathrm{P}}$	D_1D_6	D_2D_5	D_3D_8	D_4D_7
$\lvert\psi^-\rangle_{\mathrm{P}}$	D_1D_8	D_2D_7	D_3D_6	D_4D_5

$$\rho = (1-p-p^2-p^3)|0\rangle\langle 0| + p|\Phi^+\rangle\langle\Phi^+| + p^2|\Phi^{+2}\rangle\langle\Phi^{+2}| + p^3|\Phi^{+3}\rangle\langle\Phi^{+3}|, \tag{8}$$

where $|\Phi^{+2}\rangle = |\Phi^+\rangle^{\otimes 2}$ and $|\Phi^{+3}\rangle = |\Phi^+\rangle^{\otimes 3}$, respectively.

After the photon transmission, Alice and Bob share the hyperentangled photon pairs and make the nonlocal BSA. There are totally eight photon detectors in the nonlocal BSA protocol. As shown in Table 1, each of the four polarization Bell states may lead to four kinds of detector responses with the same probability. We take $|\phi^+\rangle_P \otimes |\phi^+\rangle_S$ as an example, which may cause $D_1D_5,\ D_2D_6,\ D_3D_7$, or D_4D_8 to respond. In our protocol, we consider the practical photon detector which cannot distinguish the number of incident photons and has dark count. We denote D_j^k as the detection probability of the detector D_j $(j = 1,\ 2,\ \cdots,\ 8)$ when k photons are incident. Here, we define the collection efficiency α, which includes the coupling efficiency η_c between the nonlinear medium and the fiber, the photon transmission efficiency η_t, the quantum memory efficiency η_m, and the detection efficiency of the detector η_d $(\alpha = \eta_c\eta_t\eta_m\eta_d)$. The dark count probability of the photon detector is given by Y_0. When $\alpha,\ Y_0 \ll 1$, we can obtain D^k as

$$D^k = 1-\left(1-\frac{\alpha}{4}\right)^k + Y_0 \simeq \frac{k\alpha}{4} + Y_0. \tag{9}$$

Here, we define $\alpha' = \frac{\alpha}{4}$, so that we can obtain $D^k \simeq k\alpha' + Y_0$ for simplicity.

According to Eq. (8), the photon source can generate 0, 1, 2, and 3 hyperentangled photon pairs with different probabilities. In the first scenario, when the photon source generates the vacuum state with the probability of $1-p-p^2-p^3$, all the detector clicks are caused by the dark count. As a result, we can calculate C_{raw_1} as

$$\begin{aligned} C_{\mathrm{raw}_1} &= (1-p-p^2-p^3)(D_1^0+D_2^0+D_3^0+D_4^0)(D_5^0+D_6^0+D_7^0+D_8^0)\\ &= 16(1-p-p^2-p^3)Y_0^2. \end{aligned} \tag{10}$$

In the second scenario, the photon source generates one pair of hyperentangled photon pair. This photon pair can cause the detection at one of the four detector pairs, say $D_1D_5,\ D_2D_6,\ D_3D_7$, or D_4D_8 with the probability of $\alpha' + Y_0$. We take the case that this photon pair cause the detection at D_1D_5 for an example, and the other detector clicks are caused by the dark count. The number of combinations is $C_4^1 = 4$, where $C_m^n = \frac{m!}{n!(m-n)!}$. In this case, the C_{raw_2} can be written as

$$\begin{aligned} C_{\mathrm{raw}_2} &= C_4^1 p(D_1^1+D_2^0+D_3^0+D_4^0)(D_5^1+D_6^0+D_7^0+D_8^0)\\ &= 4p(\alpha'+4Y_0)(\alpha'+4Y_0)\\ &= 4p(\alpha'^2+16Y_0^2+8\alpha'Y_0). \end{aligned} \tag{11}$$

In the third scenario, the photon source generates two hyperentangled photon pairs with the probability of p^2. This situation can be divided into two cases. In the first case, the two photon pairs cause the click of one pair of photon detectors, i.e., D_1D_5 with the probability of $2\alpha' + Y_0$. The number of combinations is also $C_4^1 = 4$. In this case, the raw information capacity is

$$\begin{aligned} C_{\mathrm{raw}_{30}} &= 4p^2(D_1^2+D_2^0+D_3^0+D_4^0)(D_5^2+D_6^0+D_7^0+D_8^0)\\ &= 4p^2(2\alpha'+4Y_0)(2\alpha'+4Y_0)\\ &= 4p^2(4\alpha'^2+16Y_0^2+16\alpha'Y_0). \end{aligned} \tag{12}$$

In the second case, the two photon pairs cause the click of two pairs of detectors, i.e., D_1D_5 and D_2D_6. The number of combinations is $C_2^1C_4^2 = 12$. In this case, the raw information capacity is

$$\begin{aligned} C_{\mathrm{raw}_{31}} &= 12p^2(D_1^1+D_2^1+D_3^0+D_4^0)(D_5^1+D_6^1+D_7^0+D_8^0)\\ &= 12p^2(2\alpha'+4Y_0)(2\alpha'+4Y_0)\\ &= 12p^2(4\alpha'^2+16Y_0^2+16\alpha'Y_0). \end{aligned} \tag{13}$$

As a result, we can calculate the total raw information capacity in the third scenario as

$$C_{\mathrm{raw}_3} = C_{\mathrm{raw}_{30}} + C_{\mathrm{raw}_{31}} = 16p^2(4\alpha'^2+16Y_0^2+16\alpha'Y_0). \tag{14}$$

In the forth scenario, the photon source generates three hyperentangled photon pairs with the probability of p^3. This scenario includes three cases. In the first case, three photon pairs cause the click of one detector pair with the probability of $3\alpha' + Y_0$ (i.e., D_1D_5) and the number of combinations of $C_4^1 = 4$. In the second case, three photon pairs cause the response of two pairs of photon detectors (i.e., D_1D_5 and D_2D_6) with the combination number of $C_3^2C_4^1C_3^1 = 36$. In the third case, three photon pairs cause the click of three pairs of photon detectors with the combination number of $C_3^1C_2^1C_4^3 = 24$. In all the three cases, we can obtain $D_1+D_2+D_3+D_4 = D_5+D_6+D_7+D_8 = 3\alpha'+4Y_0$. As a result, we can simplify the calculation and directly obtain the total raw information capacity of the forth scenario as

$$\begin{aligned} C_{\mathrm{raw}_4} &= (4+36+24)p^3(3\alpha'+4Y_0)(3\alpha'+4Y_0)\\ &= 64p^3(9\alpha'^2+16Y_0^2+24\alpha'Y_0). \end{aligned} \tag{15}$$

Therefore, the total raw information capacity C_{rawt} can be calculated as

$$C_{\mathrm{rawt}} = C_{\mathrm{raw}_1} + C_{\mathrm{raw}_2} + C_{\mathrm{raw}_3} + C_{\mathrm{raw}_4}. \tag{16}$$

Then, we consider the case of multiple coincidences, which gives multiple clicks either at Alice's or Bob's side. Here, we only consider the threefold click and neglect the events where more than three detectors click simultaneously, for they have much lower probability than the threefold click. According to above calculations, we can derive the threefold coincidence rate $(T_i,\ i = 1,\ 2,\ 3,\ 4)$ in above four scenarios as

$$\begin{aligned} T_1 &= (1-p-p^2-p^3)C_8^3Y_0^3 = 56(1-p-p^2-p^3)Y_0^3,\\ T_2 &= pC_4^1[C_6^1(\alpha'+Y_0)^2Y_0 + 2C_6^2(\alpha'+Y_0)Y_0^2 + C_6^3Y_0^3]\\ &= p(24\alpha'^2Y_0 + 168\alpha'Y_0^2 + 224Y_0^3),\\ T_3 &= p^2C_4^1[C_6^1(2\alpha'+Y_0)^2Y_0 + 2C_6^2(2\alpha'+Y_0)Y_0^2 + C_6^3Y_0^3]\\ &\quad + p^2C_2^1C_4^2[C_4^3(\alpha'+Y_0)^3 + C_4^2(\alpha'+Y_0)^2C_4^1Y_0 + C_4^1(\alpha'+Y_0)C_4^2Y_0^2 + C_4^3Y_0^3]\\ &= p^2(48\alpha'^3 + 528\alpha'^2Y_0 + 1344\alpha'Y_0^2 + 896Y_0^3),\\ T_4 &= p^3C_4^1[C_6^1(3\alpha'+Y_0)^2Y_0 + 2C_6^2(3\alpha'+Y_0)Y_0^2 + C_6^3Y_0^3]\\ &\quad + C_3^2p^3C_4^1C_3^1[2(2\alpha'+Y_0)^2(\alpha'+Y_0) + 2(2\alpha'+Y_0)(\alpha'+Y_0)^2\\ &\quad + 4(2\alpha'+Y_0)^2Y_0 + 4(\alpha'+Y_0)^2Y_0 + 2C_4^2(2\alpha'+Y_0)Y_0^2\\ &\quad + 2C_4^2(\alpha'+Y_0)Y_0^2 + C_4^3Y_0^3] + C_3^1C_2^1p^3C_4^1[C_6^3(\alpha'+Y_0)^3\\ &\quad + 2C_6^2(\alpha'+Y_0)^2Y_0 + C_6^1(\alpha'+Y_0)Y_0^2]\\ &= p^3(912\alpha'^3 + 4032\alpha'^2Y_0 + 6336\alpha'Y_0^2 + 3008Y_0^3). \end{aligned} \tag{17}$$

In this way, the total threefold coincidence rate can be written as

$$T_t = T_1 + T_2 + T_3 + T_4. \tag{18}$$

In practical operation, the threefold click cases are discarded, so that we can obtain the raw information capacity C_{raw} in Eq. (7) as

$$C_{\mathrm{raw}} = C_{\mathrm{rawt}} - T_t. \tag{19}$$

Next, we calculate the error rate e_{QSDC} in Eq. (7). For a specific hyperentangled state, i.e., $|\phi^+\rangle_P \otimes |\phi^+\rangle_S$, only the simultaneous clicks on $D_1D_5,\ D_2D_6,\ D_3D_7$, or D_4D_8 correspond to the correct BSA result, the other items in $(D_1+D_2+D_3+D_4)(D_5+D_6+D_7+D_8)$ would cause error. In this way, we can calculate the correct message capacity C_{correct_i} in above four scenarios as

$$
\begin{aligned}
C_{\mathrm{correct}_1} &= (1-p-p^2-p^3)4Y_0^2,\\
C_{\mathrm{correct}_2} &= pC_4^1[(\alpha'+Y_0)^2+3Y_0^2]\\
&= 4p(\alpha'^2+2\alpha'Y_0+4Y_0^2),\\
C_{\mathrm{correct}_3} &= p^2C_4^1[(2\alpha'+Y_0)^2+3Y_0^2]+C_2^1p^2C_4^2[2(\alpha'+Y_0)^2+2Y_0^2]\\
&= p^2(40\alpha'^2+64\alpha'Y_0+64Y_0^2),\\
C_{\mathrm{correct}_4} &= p^3C_4^1[(3\alpha'+Y_0)^2+3Y_0^2]\\
&\quad +C_3^2p^3C_4^1C_3^1[(2\alpha'+Y_0)^2+(\alpha'+Y_0)^2+2Y_0^2]\\
&\quad +C_3^1C_2^1p^3C_4^1[3(\alpha'+Y_0)^2+Y_0^2]\\
&= p^3(288\alpha'^2+384\alpha'Y_0+256Y_0^2).
\end{aligned}
\tag{20}
$$

In Eq. (20), we only consider the influence from the imperfect photon source and the photon detector on the secrecy message capacity. Actually, during the photon transmission in practical channel and storage in quantum memory, the decoherence in both DOFs is unavoidable. Here, we suppose that the entanglement in each DOF degrades to a Werner state with the form of

$$
\begin{aligned}
\rho_{\mathrm{P}} = & \; F_{\mathrm{P}}|\phi^+\rangle_{\mathrm{P}}\langle\phi^+|+\tfrac{1-F_{\mathrm{P}}}{3}(|\phi^-\rangle_{\mathrm{P}}\langle\phi^-|+|\psi^+\rangle_{\mathrm{P}}\langle\psi^+|+|\psi^-\rangle_{\mathrm{P}}\langle\psi^-|),\\
\rho_{\mathrm{S}} = & \; F_{\mathrm{S}}|\phi^+\rangle_{\mathrm{S}}\langle\phi^+|+\tfrac{1-F_{\mathrm{S}}}{3}(|\phi^-\rangle_{\mathrm{S}}\langle\phi^-|+|\psi^+\rangle_{\mathrm{S}}\langle\psi^+|+|\psi^-\rangle_{\mathrm{S}}\langle\psi^-|).
\end{aligned}
\tag{21}
$$

The decoherence would make the nonlocal BSA obtain wrong results, so that Bob may read out incorrect messages. It is noticed that when the entanglement in both DOFs suffers from the same error, say, both bit-flip error or both phase-flip error, Bob can still read out the correct messages from the nonlocal BSA results. The specific derivation process is shown in Appendix. As a result, we can obtain the total practical correct message capacity C_{correct_t} as

$$
C_{\mathrm{correct}_t} = [F_{\mathrm{P}}F_{\mathrm{S}}+\frac{(1-F_{\mathrm{P}})(1-F_{\mathrm{S}})}{3}](C_{\mathrm{correct}_1}+C_{\mathrm{correct}_2}+C_{\mathrm{correct}_3}+C_{\mathrm{correct}_4}).
\tag{22}
$$

Therefore, the error rate e_{QSDC} can be written as

$$
e_{\mathrm{QSDC}} = \frac{C_{\mathrm{raw}}-C_{\mathrm{correct}_t}}{C_{\mathrm{raw}}}.
\tag{23}
$$

Taking Eqs. (19) and (23) in Eq. (7), we can finally obtain the value of C_s.

It is interesting to compare the secrecy message capacity of our one-step QSDC with the key generation rate of the entanglement-based QKD. Here, we take the simple entanglement-based QKD protocol as an example [62]. Briefly speaking, Alice and Bob share a large number of entangled states in the polarization DOF with the form of $\frac{1}{\sqrt{2}}(|HH\rangle+|VV\rangle)$. Here, we neglect the security checking process for simplicity. Alice and Bob randomly choose the bases $\{|H\rangle,\ |V\rangle\}$ or $\{|\pm\rangle_P = \frac{1}{\sqrt{2}}(|H\rangle\ \pm|V\rangle)\}$ to measure the photons in their hands. For an entangled photon pair, if they choose the same basis with the probability of 50%, their measurement results are correlated and can be used to generate 1 bit of key. Otherwise, if they choose the different bases with the probability of 50%, their measurement results are uncorrelated and should be abandoned. In this way, according to Refs. [62,63], we can obtain the secure key generation rate of this entanglement-based QKD protocol as

$$
R = R_{\mathrm{sift}}[1-(1+f(e_{\mathrm{QKD}}))h(e_{\mathrm{QKD}})],
\tag{24}
$$

where $R_{\mathrm{sift}},\ e_{\mathrm{QKD}}$, and $f(e_{\mathrm{QKD}})$ are the sifted key rate, error rate and efficiency of the error correcting code, respectively.

Here, for comparing the entanglement-based QKD with our one-step QSDC protocol, we choose the same experimental parameters, such as the SPDC source with $p\sim 10^{-3}$, the photon detector with detection efficiency of η_d and dark count probability of Y_0. Here, the detailed formula derivation processes of R_{sift} and e_{QKD} are quite similar as those in Refs. [62,63]. With R_{sift} and e_{QKD}, we can finally obtain the value of R.

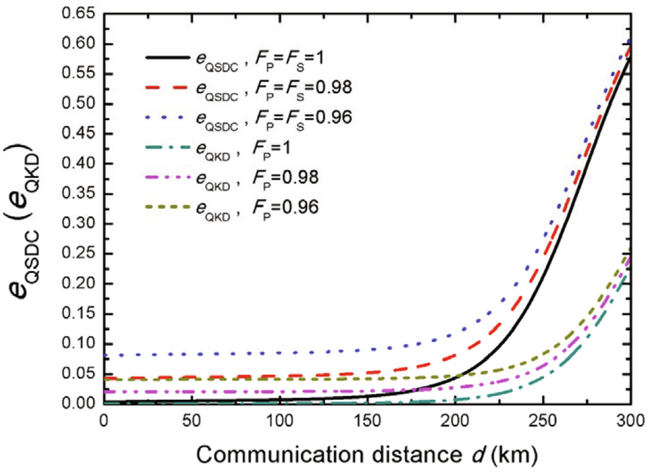

Fig. 2. (Color online) The error rates of our one-step QSDC protocol (e_{QSDC}) and the entanglement-based QKD (e_{QKD}) as a function of the communication distance d between Alice and Bob. Here, we consider the ideal quantum memory with $\eta_m = 100\%$. In QSDC and QKD, the error is caused by the practical SPDC source ($p\sim 10^{-3}$), imperfect photon detectors, photon transmission loss, and decoherence (white noise mode). We suppose $\eta_c = 0.95,\ \eta_d = 0.9$, and the fibre loss of 0.2 dB/km. In the one-step QSDC, we control $F_{\mathrm{P}} = F_{\mathrm{S}} = 1,\ 0.98,\ 0.96$, respectively. In the entanglement-based QKD, we suppose $F_{\mathrm{P}} = 1,\ 0.98,\ 0.96$, respectively.

In Fig. 2, we provide the error rate of our one-step QSDC protocol (e_{QSDC}) and the entanglement-based QKD (e_{QKD}) as a function of the communication distance d between Alice and Bob. It can be found that in both QSDC and QKD, within the relatively short communication distance, i.e., $d < 150$ km, the error rate increases quite slightly with the growth of d. With the further growth of d, the error rate increases rapidly. The error rate of our one-step QSDC is higher than that of the QKD, especially at long communication distance. The error is caused by two aspects. The first one is the imperfect experimental devices, i.e., imperfect entanglement source and photon detectors, and the second one is the noisy quantum channel. First, the imperfect entanglement source and detectors may cause accidental coincidences. Especially, the black solid line and the dark cyan dash dot line represent the error rates caused only by the first aspect in QSDC and QKD, respectively. The detector responses of the one-step QSDC (four successful detection results corresponding to a polarization Bell state) are more complex than those of QKD (two successful detection results). Considering the practical photon sources and imperfect photon detectors, it is natural that the more complex detector response may lead to the higher error rate. Second, the QKD only uses the entanglement in the polarization DOF and the one-step QSDC uses the entanglement in two DOFs. The decoherence effect in any DOF may cause error, so that the decoherence effect has a more serious influence on the one-step QSDC than QKD.

In Fig. 3, we show the secrecy message capacity C_s of our one-step QSDC and the key generation rate R of the entanglement-based QKD. These values are plotted on a logarithmic scale as a function of the communication distance d between Alice and Bob. First, as the error rate of the one-step QSDC is higher than that of the entanglement-based QKD, the maximal communication distance of the one-step QSDC is lower than that of the entanglement-based QKD. With $F_{\mathrm{P}} = F_{\mathrm{S}} = 0.98$, the maximal communication distance of the one-step QSDC is about 216 km, while that of the entanglement-based QKD is about 265 km. Second, as the decoherence causes more serious influence on the one-step QSDC, the one-step QSDC has higher fidelity requirement than the entanglement-based QKD. In detail, the fidelity threshold of the one-step QSDC is $F_{\mathrm{P}}(F_{\mathrm{S}}) = 0.945$, while that of the entanglement-based QKD is $F_{\mathrm{P}} = 0.903$. However, within the scale of maximal communication

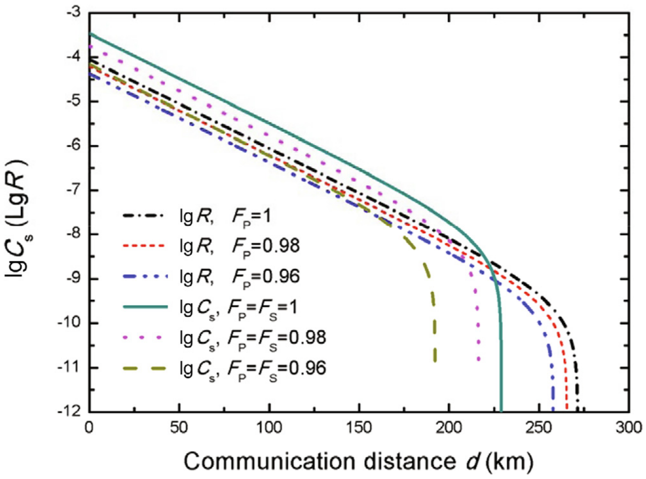

Fig. 3. (Color online) The secrecy capacity ($\lg C_s$) of our one-step QSDC protocol and the secure key generation rate ($\lg R$) of the entanglement-based QKD in Ref. [62] on a logarithmic scale as a function of the communication distance d between Alice and Bob. Here, we consider the ideal quantum memory with $\eta_m = 100\%$. We suppose $\eta_c = 0.95,\ \eta_d = 0.9$, the fibre loss of 0.2 dB/km. In the one-step QSDC, we let $F_P = F_S = 1,\ 0.98,\ 0.96$, respectively. In the entanglement-based QKD protocol, we suppose $f(e) = 1.16$ [64] and $F_P = 1,\ 0.98,\ 0.96$, respectively.

distance, C_s of the one-step QSDC is higher than R of the entanglement-based QKD. The main reason is that in the entanglement-based QKD, one pair of entangled photons can generate 1 bit of key with the probability of 50%, while in our one-step QSDC protocol, one pair of hyperentangled photons can deterministically transmit 2 bits of message. For example, considering the photon sources exciting with a repetition rate of 10 GHz [65], the value of R is about 614 bit/s at the distance of 150 km under $F_P = 0.98$ while C_s can reach about 1530 bit/s under $F_P = F_S = 0.98$, which is about 2.5 times of R. On the other hand, the entanglement-based QKD requires one round of photon transmission in quantum channel and two rounds of classical communication (Alice and Bob announce their measurement bases). QKD cannot transmit secret message directly. In order to transmit secret message, QKD requires extra one-time pad and a one-way classical communication. If we set the classical communication time as t_c, the photon transmission time is t_q and neglect the local operation time, one round of communication based on the QKD requires the time of $t_q + 3t_c$. On the contrary, our one-step QSDC protocol requires one round of photon transmission in quantum channel and one round of classical communication (Alice announces her measurement result) and can directly transmit secure messages between Alice and Bob. In this way, the one-step QSDC only requires the time of $t_q + t_c$. As a result, their practical message transmission efficiency Ec can be respectively written as

$$\begin{aligned} Ec_{\mathrm{QKD}} &= \frac{1}{t_q + 3t_c} R_{\mathrm{sift}}[1 - (1 + f(e_{\mathrm{QKD}}))h(e_{\mathrm{QKD}})], \\ Ec_{\mathrm{QSDC}} &= \frac{1}{t_q + t_c} 2C_{\mathrm{raw}}[1 - 2h(e_{\mathrm{QSDC}})]. \end{aligned} \tag{25}$$

According to Fig. 3, if we set $t_q = t_c$, it can be found that at the distance of 150 km, Ec_{QSDC} with $F_P = F_S = 0.98$ is about 5 times of Ec_{QKD} with $F_P = 0.98$.

4. Discussion

So far, we propose a feasible one-step QSDC protocol in linear optics based on the polarization-spatial-mode hyperentanglement. With the help of the nonlocal complete BSA in the polarization DOF assisted with the spatial-mode entanglement, the users only require to transmit hyperentangled photon pairs in the quantum channel once. After the BSA, only Alice announces her measurement results in the public channel, and Bob can completely distinguish the Bell states in polarization DOF secretly according to Alice's and his measurement results and decode the secret message from Alice.

It is interesting to compare this one-step QSDC protocol with existing typical quantum communication protocols, such as entanglement-based QKD [7,8], QT [14], and two-step entanglement-based QSDC [20,21]. In entanglement-based QKD, such as BBM92 [8], by transmitting one photon or sharing one pair of entangled state, Alice and Bob can obtain 1 bit of random key with 50% success probability combined with a two-way classical communication to pick up the same basis. QKD cannot transmit secret message directly. In order to transmit secret message, QKD requires extra one-time pad and a one-way classical communication. Moreover, it also requires perfect key management, and the encryption and decryption process should also be secure. Our one-step QSDC requires to distribute one pair of hyperentangled state and a one-way classical communication. It can directly transmit 2 bits of secret messages without sharing a key, whose channel capacity is four times of that in the entanglement-based QKD [7,8]. QT can transmit an unknown quantum state without transmitting the encoded photon. It can also be used to transmit classical secret messages. However, it requires not only a pair of entanglement, but also a single photon. With complete BSM, QT can transmit 1 bit of classical information. However, such complete BSM cannot be realized in linear optics. Two-step QSDC can also transmit secret messages without sharing a key [20,21]. After performing the security checking, one of the parties encodes the secret message using the single-qubit operation U_k. Then, one of the photons should be sent back for local BSA. In this one-step QSDC protocol, the encoded photons do not need to be sent back for local BSA, the spatial-mode entanglement can help to distinguish the polarization Bell states nonlocally [53]. Such operation will greatly simplify the two-step QSDC protocols and reduce the message error. In this way, this one-step QSDC protocol is more feasible in practical application. Compared with the QSDC protocol which requires to prepare, distribute and measure the two-photon three-dimensional hyperentangled states in two DOFs [25], this one-step QSDC protocol is feasible in existing technology. Without quantum memory, Ref. [66] also proposed the deterministic QKD using the approach in Ref. [53]. However, deterministic QKD cannot transmit the secure message directly.

In QKD, using the entanglement purification [2,51,67], one can obtain high quality entanglement from large number of low quality entanglements. With purified high-quality entanglement, quantum cryptography can be proved unconditionally secure [4–6]. In this one-step QSDC protocol, the parties are required to distribute the maximally hyperentangled states. The noise will degrade the hyperentanglement in both polarization and spatial-mode DOFs, which will increase the error rate and reduce the information capacity. We can use the hyperentanglement purification to distill the high quality hyperentangled states in both polarization and spatial-mode DOFs [68,69]. With the high quality hyperentanglement, we can effectively reduce the error rate of this one-step QSDC protocol. Quantum repeater provides us a powerful approach to realize arbitrary long-distance quantum communication [3]. Quantum repeaters can also be extended to hyperentanglement. Recently, the hyperentanglememnt distribution in polarization and time-bin DOFs [70], polarization and spatial-mode DOFs [71] were reported in experiments. The hyperentanglement storage in path (K-vector) and OAM have also been realized in experiments [72]. Moreover, the hyperentanglement swapping based on complete hyperentangled BSA [16] and hyperentanglement purification [68,69] were also proposed. Therefore, it is possible to realize this one-step QSDC over arbitrarily long distance with the hyperentanglement quantum repeaters. Another alternative approaches to realize long-distance one-step QSDC are to use the satellite and drones. Recently, the entanglement-based QKD over 1120 km was realized with satellite [73] and the entanglement distribution using drones was also reported [44]. If using hyperentanglement source, it is possible to distribute hyperentanglement and this long-distance one-step QSDC also can be realized.

5. Conclusion

In conclusion, we propose a one-step QSDC protocol in which the secret messages can be directly transmitted from the sender to the receiver. The communication parties should distribute the polarization-spatial-mode hyperentangled state. Without sharing a key, the message sender encodes 2 bits of message using a pair of hyperentangled state and the receiver could decode it if no eavesdropper was present. With the help of the nonlocal BSA in polarization DOF, the parties should not send the encoded photons back through the quantum channel, which can greatly simplify the implementation and reduce the message error. In ideal scenario, our one-step QSDC protocol is unconditionally secure. With the help of security checking, any futile attempt at eavesdropping would be detected by two legitimate users. In the practical noisy environment, the secrecy message capacity in the communication distance of 150 km with $F_P = F_S = 0.98$ is about 2.5 times of the key generation rate of the entanglement-based QKD with $F_P = 0.98$. Moreover, the one-step QSDC can effectively save the communication time. Considering the communication time, the practical message transmission efficiency of the one-step QSDC is about 5 times of the quantum communication based on the QKD. This protocol is general and can be effectively extended to other DOFs of photons, such as the polarization-time-bin, polarization-frequency, and polarization-OAM hyperentangled states. Moreover, this protocol is totally in linear optics, which can be experimentally realized under current condition. Based on above features, this one-step QSDC protocol may have important application in current and future quantum communication field.

Conflict of interest

The authors declare that they have no conflict of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (11974189, 11974205, and 12175106), the Key Area Research and Development Program of Guangdong Province (2018B030325002), and the National Key Research and Development Program of China (2017YFA0303700).

Author contributions

Yu-Bo Sheng and Gui-Lu Long conceived the one-step QSDC idea and designed the protocol. Lan Zhou analyzed its security and made the numerical simulation. Yu-Bo Sheng wrote the first draft and all authors contributed to the final version of the manuscript.

Appendix A. Supplementary materials

Supplementary materials to this article can be found online at https://doi.org/10.1016/j.scib.2021.11.002.

References

[1] Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. p. 175–9.

[2] Bennett CH, Brassard G, Popescu S, et al. Purification of noisy entanglement and faithful teleportation via noisy channels. Phys Rev Lett 1996;76:722.

[3] Briegel HJ, Dür W, Cirac JI, et al. Quantum repeaters: the role of imperfect local operations in quantum communication. Phys Rev Lett 1998;81:5932.

[4] Deutsch D, Ekert A, Jozsa R, et al. Quantum privacy amplification and the security of quantum cryptography over noisy channels. Phys Rev Lett 1996;77:2818.

[5] Lo HK, Chau HF. Unconditional security of quantum key distribution over arbitrarily long distances. Science 1999;283:2050–6.

[6] Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett 2000;85:441–4.

[7] Ekert AK. Quantum cryptography based on Bell's theorem. Phys Rev Lett 1991;67:661.

[8] Bennett CH, Brassard G, Mermin ND. Quantum cryptography without Bell's theorem. Phys Rev Lett 1992;68:557.

[9] Xu FH, Ma XF, Zhang Q, et al. Secure quantum key distribution with realistic devices. Rev Mod Phys 2020;92:025002.

[10] Wang XB. Beating the photon-number-splitting attack in practical quantum cryptography. Phys Rev Lett 2005;94:230503.

[11] Lo HK, Ma XF, Chen K. Decoy state quantum key distribution. Phys Rev Lett 2005;94:230504.

[12] Chen YA, Zhang Q, Chen TY, et al. An integrated space-to-ground quantum communication network over 4600 kilometres. Nature 2021;589:214–9.

[13] Kwek LC, Cao L, Luo W, et al. Chip-based quantum key distribution. AAPPS Bull 2021;31:15.

[14] Bennett CH, Brassard G, Crépeau C, et al. Teleporting an unknown quantum state via dual classic and Einstein-Podolsky-Rosen channels. Phys Rev Lett 1993;70:1895.

[15] Ren JG, Xu P, Yong HL, et al. Ground-to-satellite quantum teleportation. Nature 2017;549:70–3.

[16] Sheng YB, Deng FG, Long GL. Complete hyperentangled-Bell-state analysis for quantum communication. Phys Rev A 2010;82:032318.

[17] Wang XL, Cai XD, Su ZE, et al. Quantum teleportation of multiple degrees of freedom of a single photon. Nature 2015;518:516–9.

[18] Hu XM, Zhang C, Liu BH, et al. Experimental high-dimensional quantum teleportation. Phys Rev Lett 2020;125:230501.

[19] Luo YH, Zhong HS, Erhard M, et al. Quantum teleportation in high dimensions. Phys Rev Lett 2019;123:070505.

[20] Long GL, Liu XS. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A 2002;65:032302.

[21] Deng FG, Long GL, Liu XS. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A 2003;68:042317.

[22] Bennett CH, Wiesner SJ. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys Rev Lett 1992;69:2881.

[23] Deng FG, Long GL. Secure direct communication with a quantum one-time pad. Phys Rev A 2004;69:052319.

[24] Wang C, Deng FG, Li YS, et al. Quantum secure direct communication with high-dimension quantum superdense coding. Phys Rev A 2005;71:044305.

[25] Shi J, Gong YX, Xu P, et al. Quantum secure direct communication by using three-dimensional hyperentanglement. Commun Theor Phys 2011;56:831.

[26] Hu JY, Yu B, Jing MY, et al. Experimental quantum secure direct communication with single photons. Light Sci Appl 2016;5:e16144.

[27] Zhang W, Ding DS, Sheng YB, et al. Quantum secure direct communication with quantum memory. Phys Rev Lett 2017;118:220501.

[28] Zhu F, Zhang W, Sheng YB, et al. Experimental long-distance quantum secure direct communication. Sci Bull 2017;62:1519–24.

[29] Chen SS, Zhou L, Zhong W, et al. Three-step three-party quantum secure direct communication. Sci China Phys Mech Astron 2018;61:090312.

[30] Gao ZK, Li T, Li Z. Long-distance measurement-device-independent quantum secure direct communication. EPL 2019;125:40004.

[31] Qi RY, Sun Z, Lin ZS, et al. Implementation and security analysis of practical quantum secure direct communication. Light Sci Appl 2019;8:22.

[32] Zhou L, Sheng YB, Long GL. Device-independent quantum secure direct communication against collective attacks. Sci Bull 2020;65:12–20.

[33] Zhou ZR, Sheng YB, Niu PH, et al. Measurement-device-independent quantum secure direct communication. Sci China Phys Mech Astron 2020;63:230362.

[34] Sun Z, Song LY, Huang Q, et al. Toward practical quantum secure direct communication: a quantum-momery-free protocol and code design. IEEE Tran Commun 2020;68:5778–92.

[35] Pan D, Lin ZS, Wu JW, et al. Experimental free-space quantum secure direct communication and its security analysis. Photon Res 2020;8:1522–31.

[36] Yang L, Wu JW, Lin ZS, et al. Quantum secure direct communication with entanglement source and single-photon measurement. Sci China Phys Mech Astron 2020;63:110311.

[37] Li T, Long GL. Quantum secure direct communication based on single-photon bell-state measurement. New J Phys 2020;22:063017.

[38] Wang C. Quantum secure direct communication: intersection of communication and cryptography. Funda Res 2021;1:91–2.

[39] Long GL, Zhang HR. Drastic increase of channel capacity in quantum secure direct communication using masking. Sci Bull 2021;66:1267–9.

[40] Qi ZT, Li YH, Huang YW, et al. A 15-user quantum secure direct communication network. Light Sci Appl 2021;10:183.

[41] Inagaki T, Matsuda N, Tadanaga O, et al. Entanglement distribution over 300 km of fiber. Opt Express 2013;21:23241–9.

[42] Yin J, Cao Y, Li YH, et al. Satellite-based entanglement distribution over 1200 kilometers. Science 2017;356:1140–4.

[43] Liu HY, Tian XH, Gu CS, et al. Drone-based entanglement distribution towards mobile quantum networks. Nat Sci Rev 2020;7:921–8.

[44] Liu HY, Tian XH, Gu CS, et al. Optical-relayed entanglement distribution using drones as mobile nodes. Phys Rev Lett 2021;126:020503.

[45] Barreiro JT, Langford NK, Peters NA, et al. Generation of hyperentangled photon pairs. Phys Rev Lett 2005;95:260501.

[46] Barreiro JT, Wei TC, Kwiat PG. Beating the channel capacity limit for linear photonic superdense coding. Nat Phys 2008;4:282–6.

[47] Hu XM, Guo Y, Liu BH, et al. Beating the channel capacity limit for superdense coding with entangled ququarts. Sci Adv 2018;4:eaat9304.

[48] Chapman JC, Graham TM, Zeitler CK, et al. Time-bin and polarization superdense teleportation for space applications. Phys Rev Appl 2020;14:014044.

[49] Simon C, Pan JW. Polarization entanglement purification using spatial entanglement. Phys Rev Lett 2002;89:257901.

[50] Sheng YB, Deng FG. One-step deterministic polarization-entanglement purification using spatial entanglement. Phys Rev A 2010;82:044305.

[51] Hu XM, Huang CX, Sheng YB, et al. Long-distance entanglement purification for quantum communication. Phys Rev Lett 2021;126:010503.

[52] Ecker S, Sohr P, Bulla L, et al. Experimental single-copy entanglement distillation. Phys Rev Lett 2021;127:040506.

[53] Walborn SP, Pádua S, Monken CH. Hyperentanglement-assisted Bell-state analysis. Phys Rev A 2003;68:042313.

[54] Schuck C, Huber G, Kurtsiefer C, et al. Complete deterministic linear optics Bell state analysis. Phys Rev Lett 2006;96:190501.

[55] Gu B, Huang YG, Fang X, et al. Bidirectional quantum secure direct communication network protocol with hyperentanglement. Commun Theor Phys 2011;56:659.

[56] Gu B, Huang YG, Fang X, et al. A two-step quantum secure direct communication network protocol with hyperentanglement. Chin Phys B 2011;20:100309.

[57] Wang TJ, Li T, Du FF, et al. High-capacity quantum secure direct communication based on quantum hyperdence coding with hyperentanglement. Chin Phys Lett 2011;28:040305.

[58] Hong CH, Heo J, Lim JI, et al. Quantum secure direct communication network with hyperentanglement. Chin Phys B 2014;23:090309.

[59] Cai JR, Pan ZW, Wang TJ, et al. High-capacity quantum secure direct communication using hyper-entanglement of photonic qubits. Int J Quan Inf 2016;14:1650043.

[60] Vaidman L, Yoran N. Methods for reliable teleportation. Phys Rev A 1999;59:116.

[61] Lütkenhaus N, Calsamiglia J, Suominen KA. Bell measurements for teleportation. Phys Rev A 1999;59:3295.

[62] Ma XF, Fung CHF, Lo HK. Quantum key distribution with entangled photon sources. Phys Rev A 2007;76:012307.

[63] Takesue H, Harada K, Tamaki K, et al. Long-distance entanglement-based quantum key distribution experiment using practical detectors. Opt Express 2010;18:16777.

[64] Waks E, Zeevi A, Yamamoto Y. Security of quantum key distribution with entangled photons against individual attacks. Phys Rev A 2002;65:052310.

[65] Zhang Q, Xie XP, Takesue H, et al. Correlated photon-pair generation in reverse-proton-exchange PPLN waveguides with integrated mode demultiplexer at 10 GHz clock. Opt Express 2007;15:10288.

[66] Walborn SP, Almeida MP, Ribeiro PHS, et al. Quantum information processing with hyperentangled photon states. Quant Inf Comput 2006;6:336–50.

[67] Pan JW, Gasparoni S, Ursin R, et al. Experimental entanglement purification of arbitrary unknown states. Nature 2003;423:417–22.

[68] Ren BC, Du FF, Deng FG. Two-step hyperentanglement purification with the quantum-state-joining method. Phys Rev A 2014;90:052309.

[69] Wang GY, Liu Q, Deng FG. Hyperentanglement purification for two-photon six-qubit quantum systems. Phys Rev A 2016;94:032319.

[70] Steinlechner F, Ecker S, Fink M, et al. Distribution of high-dimensional entanglement via an intra-city free-space link. Nat Commun 2017;8:15971.

[71] Hu XM, Xing WB, Liu BH, et al. Efficient distribution of high-dimensional entanglement through 11 km fiber. Optica 2020;7:738–43.

[72] Zhang W, Ding DS, Dong MX, et al. Experimental realization of entanglement in multiple degrees of freedom between two quantum memories. Nat Commun 2016;7:13514.

[73] Yin J, Li YH, Liao SK, et al. Entanglement-based secure quantum cryptography over 1120 kilometres. Nature 2020;582:501–5.

Yu-Bo Sheng is a professor at Nanjing University of Posts and Telecommunications. He received his Ph.D. degree from Beijing Normal University in 2009 and engaged in postdoctoral research in Tsinghua University from 2009 to 2011. His research interest includes quantum secure communication, quantum repeater, quantum purification, and quantum computation.

Gui-Lu Long is a professor at Tsinghua University. He received his B.Sc. degree from Shandong University in 1982, and Ph.D. degree from Tsinghua University in 1987 respectively. His research interest includes quantum communication and computation, and optical microcavity.