Passive decoy-state quantum secure direct communication with a heralded single-photon source

Jia-Wei Ying,[1,2] Peng Zhao,[1,2] Wei Zhong,[2] Ming-Ming Du,[1] Xi-Yun Li,[3] Shu-Ting Shen,[1] An-Lei Zhang,[3] Lan Zhou,[3,*] and Yu-Bo Sheng[1,2,†]

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

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

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

(Received 8 February 2024; revised 7 July 2024; accepted 26 July 2024; published 13 August 2024)

Quantum secure direct communications (QSDC) can directly transmit secret messages through a quantum channel without keys. The imperfect photon source is a major obstacle for QSDC's practical implementation. The unwanted vacuum state and multiphoton components emitted from imperfect photon source largely reduce QSDC's secrecy message capacity and even threaten its security. In the paper, we propose a high-efficient passive decoy-state QSDC protocol with the heralded single-photon source (HSPS). We adopt a spontaneous parametric down-conversion source to emit entangled photon pairs in two spatial modes. By detecting the photons in one of the two correlated spatial modes, we can infer the photon-number distribution of the other spatial mode. Meanwhile, our protocol allows a simple passive preparation of the signal states and decoy state. The HSPS can effectively reduce the probability of vacuum state and increase QSDC's secrecy message capacity. Meanwhile, the passive decoy-state method can simplify the experimental operations and enhance QSDC's robustness against the third-party side-channel attacks. Under the communication distance of 10 km, the secrecy message capacity of our QSDC protocol can achieve 81.85 times with average photon number of 0.1 and 12.79 times with average photon number of 0.01 of that in the original single-photon-based QSDC protocol without the HSPS. Our QSDC protocol has longer maximal communication distance about 17.975 km with average photon number of 0.01. Our work serves as a major step toward the further development of practical passive decoy-state QSDC systems.

DOI: 10.1103/PhysRevApplied.22.024040

I. INTRODUCTION

Quantum communication has emerged as a promising avenue, owing to its unconditional security guaranteed by the principles of quantum mechanics. The pioneering quantum communication protocol, known as quantum key distribution (QKD) [1,2], which can share random keys between two distant users. Over the past years, QKD has achieved significant advancements in both theoretical [3–9] and experimental aspects [10–13]. Another remarkable branch of quantum communication is the quantum secure direct communication (QSDC), which was first proposed by Long [14]. Unlike QKD, QSDC allows the direct transmission of secure messages without sharing keys in advance. In 2003 and 2004, entanglement-based (two-step QSDC) and single-photon-based (DL04) QSDC protocols were proposed [15,16]. The two-step QSDC protocol utilizes a dense coding method, which can transmit two bits of messages with one pair of entangled Bell state. The DL04 QSDC protocol can transmit one bit of message using a single photon. QSDC also has gained significant development in recent years [17–41]. The DL04 QSDC protocol and two-step QSDC protocol were realized in experiment in 2016 and 2017, respectively [18,19]. Later, some pivotal QSDC experiments have been reported, such as the QSDC network experiment [27], 100-km fiber QSDC experiment [29], and continuous-variable QSDC experiment [26,33,37]. In the theoretical aspect, the device-independent (DI) QSDC protocol and measurement-device-independent (MDI) QSDC protocol have been proposed to resist the potential attacks focusing on imperfect experimental equipment [21,22,35]. Recently, one-step QSDC based on polarization-spatial-mode hyperentanglement was proposed [28]. Compared to traditional two-step QSDC, the one-step QSDC protocol

*Contact author: zhoul@njupt.edu.cn
†Contact author: shengyb@njupt.edu.cn

requires only one round of photon transmission, which can simplify the experimental operation and significantly reduce the message loss caused by the photon transmission loss. Later, the DI one-step QSDC protocol [30] and MDI one-step QSDC protocol [31] were successively proposed, which can enhance one-step QSDC's security under practical experimental condition.

Single-photon source plays a role in both QKD and QSDC [1,16]. Unfortunately, ideal single-photon source is not available under current experimental conditions. The current available single-photon source is the phase-randomized weak coherent pulse (WCP) source, which can emit vacuum state, single-photon state, and multiphoton state with different probabilities. Imperfect single-photon source not only decreases the communication efficiency of quantum communication, but also introduces a security loophole. An alternative approach is to use the device-independent (DI) type protocols, i.e., DI-QKD protocols [3,42–44] and DI-QSDC protocols [21,30,34]. However, these protocols are limited by the short communication distance. Moreover, they are also hard to realize in experiment. DI-QKD has been experimentally demonstrated until 2022 [45–47] and DI-QSDC has not obtained experimental demonstration yet. Another alternative approach is to use the heralded single-photon source (HSPS) [48–54]. Suppose that a spontaneous parametric down-conversion (SPDC) source emits correlated photon pairs in two spatial modes. By detecting the photons in one of the two correlated spatial modes, it is possible to infer the photon-number statistics of the other spatial mode. This approach can significantly reduce the probability of the vacuum state occurrence. Furthermore, the multiphoton components in the WCP may provide the eavesdropper (Eve) an opportunity to exploit the photon-number-splitting (PNS) attack [55,56]. Fortunately, the PNS attack in QKD and QSDC can be effectively resisted by the decoy-state methods [57–61]. However, the decoy-state method necessitates active modulation of light intensity, which could potentially be exploited by Eve for a side-channel attack. Passive protocols are more resistant to side-channel attacks than active systems [62–69]. In the passive protocols, two phase-randomized WCPs interfere at a beam splitter (BS), which makes the photon-number statistics of the outcome signals classically correlated. By measuring one of the two outcome signals of the BS, we can passively obtain the conditional photon-number distribution of the other signal mode.

In this paper, we introduce the passive decoy-state method and the HSPS into the single-photon-based QSDC, and propose a passive decoy-state QSDC protocol with the HSPS. Comparing with the original DL04 QSDC protocol with the WCP source, this passive decoy-state QSDC protocol has two attractive advantages. First, using the passive decoy-state method, this QSDC protocol has strong robustness against the side-channel attack. Second, with HSPS, this protocol can largely reduce the influence from the vacuum state, and thus the secrecy message capacity and maximal communication distance can be increased. This paper is organized as follows. In Sec. II, we explain the passive decoy-state QSDC protocol with the HSPS in detail. In Sec. III, we analyze its secrecy message capacity under practical experimental conditions in theory and perform the numerical simulation. In Sec. IV, we provide a conclusion.

II. THE PASSIVE DECOY-STATE QSDC PROTOCOL WITH THE HSPS

In this section, we explain our passive decoy-state QSDC protocol with the HSPS. As shown in Fig. 1, the passive decoy-state QSDC protocol can be described as follows.

Step 1: The message receiver Bob passes a WCP in $|H\rangle$ to pump an SPDC crystal, splitting a single photon to two correlated photons in $|HH\rangle$ probabilistically. One photon is in the heralded path and the other photon is in the signal path. The photon in the heralded path passes through a $t:(1-t)$ BS and the output photon will be detected by two photon detectors D_1 and D_2. In this way, the responses of D_1 and D_2 will herald the existence of the photon in the signal path. In detail, when only D_1 or D_2 responds, the pulse in the signal path will be used as signal states. When D_1 and D_2 both respond, the pulse in the signal path will be used as the decoy state. When neither D_1 nor D_2 clicks, the pulse in the signal path would be discarded.

Step 2: Based on the detector responses, Bob performs the randomly encoding operation to generate one of the four polarization states, i.e., $|H\rangle$, $|V\rangle$, $|+\rangle$, $|-\rangle$. Here, $|H\rangle$ (horizontal polarization) and $|V\rangle$ (vertical polarization) belong to the rectilinear (Z) basis and $|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$ belong to the diagonal (X) basis. Bob sends the randomly encoded signal photons and decoy-state photons to the message sender Alice through the quantum channel. Simultaneously, Bob also sends an indication laser pulse to prompt Alice to perform the storage operation.

Step 3: Alice stores the signal states and decoy states in the quantum memory if she receives the indication laser pulse. Then, she performs the first round of security checking, which is similar as that of the decoy-state QKD protocols [57,58]. After the security checking, the communication parties calculate the quantum bit error rate $E1$. If $E1$ is below the tolerate threshold, the communication continues. Otherwise, the parties have to discard the communication.

Step 4: Alice extracts the remaining signal photons from the quantum memory and encodes her messages by performing I or Y operation on each photon, where $I = |H\rangle\langle H| + |V\rangle\langle V|$ and $Y = i\sigma_y = |H\rangle\langle V| - |V\rangle\langle H|$. I and Y represent the classical messages 0 and 1, respectively.

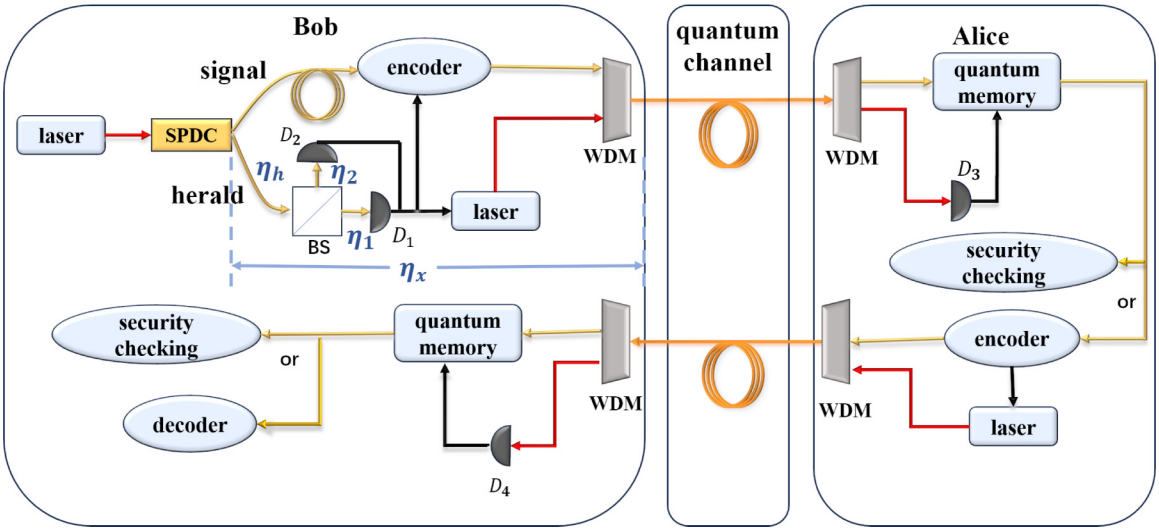

FIG. 1. The structure of the passive decoy-state QSDC protocol with the HSPS. In the diagram, the yellow lines represent the spatial paths of the photons, while the orange lines represent the quantum channels used for communication. The red lines indicate the input laser, which is used as a source to pump a nonlinear crystal or a calibration tool to assist Alice's and Bob's memory devices to store photons. The black lines represent the detector response signals, which prompt Alice or Bob to perform a series of operations, including encoding, decoding, storing, and sending the indication laser. Overall, this process involves two rounds of security checking to ensure the security and integrity of the transmitted messages.

Meanwhile, Alice also randomly encodes a part of photons as the second round of security-checking photons. After encoding, Alice sends all the encoded photons to Bob through the quantum channel. Meanwhile, she sends another indication laser pulse to ask Bob to receive the signal states.

Step 5: After receiving the transmitted photons, Bob stores the photons in quantum memory and Alice announces the positions and encoding operations of the security-checking photons. Bob extracts the security-checking photons and measures them with the same basis as he prepared the initial photons. After the measurement, Bob calculates the quantum bit error rate $E2$ combined with Alice's announcement and his initial photon states. If $E2$ is below the threshold, the communication continues. Otherwise, the parties have to discard the communication.

Step 6: Bob extracts the remaining signal photons from the quantum memory and measures the photons with the same basis in which he prepared the initial photons. After the measurements, Bob can deduce Alice's operation by comparing the initial quantum state and the encoded quantum state, and thus obtain Alice's transmitted messages.

As shown in Fig. 1, in step 1, we suppose that the SPDC source emits two photon pulses in the signal path and heralded path with the probability of $P_\mu(k)$, which satisfies the Poisson distribution (μ is the average photon number) [70–72]. There are four possible combinations of detector responses after the photons in the heralded path passing through the $t:(1-t)$ BS. We note them as four events x_i $(i=1,2,3,4)$, where $x_1=\bar{D}_1\bar{D}_2$, $x_2=D_1\bar{D}_2$, $x_3=\bar{D}_1D_2$, $x_4=D_1D_2$. D_j represents the photon detector D_j has a response and $\bar{D}_j$ represents that the detector D_j has no response. We define $\gamma_{x_i}(k)$ as the probability of k photons in the heralded path leading to the event x_i. Hence, in the signal path, the photon-number distribution function $q_{x_i}(n)$ after the heralded generation is

$$\begin{aligned} q_{x_i}(n) &= \sum_{k=n}^{\infty} P_\mu(k)\gamma_{x_i}(k)S(k,n), \\ P_\mu(k) &= e^{-\mu}\frac{\mu^k}{k!}, \\ S(k,n) &= C_k^n \eta_x^n (1-\eta_x)^{k-n}. \end{aligned} \tag{1}$$

Here, $S(k,n)$ is the probability that the emitted k photons turn to n photons due to the photon loss with the transmission efficiency of η_x. This process can be understood as the source emits k photons, which are successfully detected in the heralded path. Then, after a series of losses, the photon number in the signal path is reduced to n.

$\gamma_{x_i}(k)$ $(i=1,2,3,4)$ varies depending on the responses of the detectors, which is shown as

$$\begin{aligned} \gamma_{x_1}(k) &= (1-d_1)(1-d_2)f^k, \\ \gamma_{x_2}(k) &= (1-d_2)f_1^k - \gamma_{x_1}(k), \\ \gamma_{x_3}(k) &= (1-d_1)f_2^k - \gamma_{x_1}(k), \\ \gamma_{x_4}(k) &= 1-\gamma_{x_1}(k)-\gamma_{x_2}(k)-\gamma_{x_3}(k). \end{aligned} \tag{2}$$

Here f, f_1, and f_2 represent the photon-loss probabilities in the heralded path, while d_1 (d_2) is the dark count rates of Alice's detector D_1 (D_2).

We define the coefficients η_h as the transmission efficiency in the heralded path, and define η_1 (η_2) as the detection efficiency of the detector D_1 (D_2). In this way, we can obtain f, f_1, and f_2 as

$$\begin{aligned} f &= \eta_h[t(1-\eta_1)+(1-t)(1-\eta_2)]+1-\eta_h, \\ f_1 &= \eta_h[1-(1-t)\eta_2]+1-\eta_h, \\ f_2 &= \eta_h(1-t\eta_1)+1-\eta_h. \end{aligned} \tag{3}$$

By substituting the parameters in Eqs. (2) and (3) into Eq. (1), we can further derive $q_{x_i}(n)$ $(i=1,2,3,4)$ as

$$\begin{aligned} q_{x_1}(n) &= (1-d_1)(1-d_2)\frac{(\mu\eta_x f)^n}{n!}e^{\mu[f(1-\eta_x)-1]}, \\ q_{x_2}(n) &= (1-d_2)\frac{(\mu\eta_x f_1)^n}{n!}e^{\mu[f_1(1-\eta_x)-1]}-q_{x_1}(n), \\ q_{x_3}(n) &= (1-d_1)\frac{(\mu\eta_x f_2)^n}{n!}e^{\mu[f_2(1-\eta_x)-1]}-q_{x_1}(n), \\ q_{x_4}(n) &= \frac{(\mu\eta_x)^n}{n!}e^{-\mu\eta_x}-q_{x_1}(n)-q_{x_2}(n)-q_{x_3}(n). \end{aligned} \tag{4}$$

Here, the detector response x_1 indicates the heralded failure. In this case, Bob will discard the photon pulse in the signal path, so that $q_{x_1}(n)$ should also be discarded. The detector responses x_2 and x_3 enable Bob to obtain two different distributed signal states $q_{x_2}(n)$ and $q_{x_3}(n)$ in the signal path. If the detector response x_4 is obtained, the pulse in the signal path is used as the decoy state. It can be found that by adopting the heralded generation method, the ratio corresponding to the vacuum state event in the signal path can be greatly reduced, which can effectively reduce the influence of the dark count on the photon-number distribution in the signal path.

III. SECURITY ANALYSIS

A. The theoretical secrecy message capacity of the single-photon-based QSDC

According to Wyner's wiretap channel theory [73], the secrecy message capacity of the single-photon-based QSDC can be calculated as

$$C_s = \max_{P_A}\{I(A:B)-I(A:E)\}, \tag{5}$$

where $I(A:B)$ is the mutual information between Alice and Bob, and $I(A:E)$ is the mutual information between Alice and Eve. We define P_A as the probability distribution of Alice's encoding operations. In general, we consider the case that the messages 0 and 1 sent by Alice are equally distributed, that is, $P(A0)=P(A1)=0.5$.

In the single-photon-based QSDC protocol, two rounds of quantum transmission are needed. We denote the photon transmission from Bob to Alice as BA, and the photon transmission from Bob to Alice and then back to Bob after Alice's encoding as BAB. $I(A:B)$ can be calculated as

$$I(A:B) = Q_\mu^{BAB}[1-h(E_\mu^{BAB})], \tag{6}$$

where Q_μ^{BAB} is the overall gain of a photon traveling from Bob to Alice and then back to Bob, and E_μ^{BAB} is the total QBER after two rounds of photon transmission. The function $h(x)$ is the binary Shannon entropy with the form of $h(x) = -x\log_2(x)-(1-x)\log_2(1-x)$.

The mutual information $I(A:E)$ between Alice and Eve can be considered as the message leakage rate through imperfect quantum channels and devices. Due to the inherent characteristics of QSDC, Eve can steal the encoded messages only when he can steal the corresponding photons in both photon-transmission processes. If Eve steals only some encoded photons in the second round of photon transmission, he is unable to decode the encoded messages without knowing the initial quantum states of the photons. Consequently, Eve's message interception rate is upper bounded by his photon interception rate in the first photon-transmission round.

For Eve, there are many strategies he can adopt to maximize his photon interception rate. We first consider the one-photon case, say, the signal pulse contains exactly one photon. Here, we consider a common approach, say, the collective attack, which has been considered in many works [60,74,75]. In the collective attack, Eve sets up an auxiliary quantum system and makes a joint operation on his intercepted photon and the auxiliary system. It is generally assumed that Eve can perform an optimal unitary operation to maximize the amount of messages he can steal. According to Holevo's theorem [76], we can deduce that the maximal photon interception rate that Eve can obtain from a single photon pulse is $h(e_X^{BA}+e_Z^{BA})$, where e_X^{BA} and e_Z^{BA} represent the error rates in the X basis and Z basis after the first photon-transmission process, respectively. From the analysis in Ref. [60], if the signal pulse contains two or more photons, Eve can perform the PNS attack and the collective attack. In detail, when the signal pulse contains two photons, Eve steals one photon with the PNS attack, and performs a collective attack on the other photon. The maximal message interception rate that Eve can obtain from the two photon pulse can be calculated as $\frac{1}{2}h(2e_2^{BA})+\frac{1}{2}$ with the Holevo bound. When the signal pulse contains three or more photons, the photons emitted by Bob can be unambiguously discriminated by Eve [77], and thus the encoded messages can be completely stolen. As a result, $I(A:E)$ can be calculated as

$$I(A:E) = \sum_{n=0}^{\infty} Q_{\mu,n}^{BAE} * H_n$$
$$= Q_{\mu,n=1}^{BAE} * h(2e_1^{BA}) + Q_{\mu,n=2}^{BAE} * \left[\frac{1}{2}h(2e_2^{BA}) + \frac{1}{2}\right]$$
$$+ Q_{\mu,n\geq 3}^{BAE} * 1, \quad (7)$$

where $Q_{\mu,n}^{BAE}$ is the gain of the n-photon event from Eve, and H_n is the contribution of the n-photon event to $I(A:E)$. The one-photon event's contribution for H_n is $h(e_X^{BA} + e_Z^{BA})$. Here, we assume that $e_X^{BA} = e_Z^{BA} = e_1^{BA}$. e_2^{BA} represents the total error rate after the first photon transmission caused by the two-photon event.

In this way, we can obtain the secrecy message capacity as

$$C_s = Q_{\mu}^{BAB}[1 - h(E_{\mu}^{BAB})] - \left\{Q_{\mu,n=1}^{BAE} * h(2e_1^{BA})\right.$$
$$\left. + Q_{\mu,n=2}^{BAE} * \left[\frac{1}{2}h(2e_2^{BA}) + \frac{1}{2}\right] + Q_{\mu,n\geq 3}^{BAE} * 1\right\}. \quad (8)$$

B. System model

In order to analyze the secrecy message capacity of our passive decoy-state QSDC protocol with the HSPS, we establish a QSDC system simulation model, including the source, channel, detector, and yield.

As shown in Sec. II, Eq. (4) provides the photon-number distributions of two signal sources (q_{x_2} and q_{x_3}) and a decoy-state source (q_{x_4}). The channel transmission efficiency is shown as

$$t^{\text{chan}} = 10^{-\frac{\alpha^{\text{chan}}}{10}}, \quad (9)$$

where α^{chan} is the loss of quantum channel and chan $\in \{BA, BAB\}$.

In this situation, the overall transmission efficiency η^{chan} of the signal state and decoy state can be expressed as

$$\eta^{\text{chan}} = t^{\text{chan}} \eta_{\text{opt}}^{\text{chan}} \eta_d^{\text{par}}, \quad (10)$$

where $\eta_{\text{opt}}^{\text{chan}}$ is the intrinsic optical efficiency of the device, and η_d^{par} is the detection efficiency of Alice or Bob (par $\in \{A, B\}$).

In order to calculate the secrecy message capacity, we need to obtain the yield and gain of the channel. Let Y_n^A and Y_n^B denote the yields of the n-photon signal at Alice's and Bob's locations, respectively. They can be calculated as

$$Y_n^{\text{par}} = 1 - (1 - Y_0^{\text{par}})(1 - \eta^{\text{chan}})^n, \quad (11)$$

where Y_0^{par} is the background detection rate. The item $(1 - Y_0^{\text{par}})(1 - \eta^{\text{chan}})^n$ can be understood as the probability that no background detection event occurs and all the n photons are lost in the quantum channel.

Through the system model described above, we can estimate both the overall gain and the error rate. The formula of the overall gain can be written as

$$Q_{x_i}^{\text{chan}} = \sum_{n=0}^{\infty} Q_{x_i,n}^{\text{chan}} = \frac{1}{P_{x_i}} \sum_{n=0}^{\infty} q_{x_i}(n) Y_n^{\text{par}}, \quad (12)$$

where P_{x_i} is the total probability of event x_i and $P_{x_i} = \sum_{n=0}^{\infty} q_{x_i}(n)$. We can further derive $Q_{x_1}^{\text{chan}}$ as

$$Q_{x_1}^{\text{chan}} = \sum_{n=0}^{\infty} Q_{x_1,n}^{\text{chan}} = \frac{1}{P_{x_1}} \sum_{n=0}^{\infty} q_{x_1}(n) Y_n^{\text{par}}$$
$$= \frac{1}{P_{x_1}} \sum_{n=0}^{\infty} q_{x_1}(n)[1 - (1 - Y_0^{\text{par}})(1 - \eta^{\text{chan}})^n]$$
$$= \frac{1}{P_{x_1}} \sum_{n=0}^{\infty} q_{x_1}(n) - \frac{1}{P_{x_1}} \sum_{n=0}^{\infty} q_{x_1}(n)(1 - Y_0^{\text{par}})(1 - \eta^{\text{chan}})^n$$
$$= 1 - \frac{1}{P_{x_1}} \sum_{n=0}^{\infty} (1 - d_1)(1 - d_2) \frac{(\mu \eta_x f)^n}{n!} e^{\mu[f(1-\eta_x)-1]} (1 - Y_0^{\text{par}})(1 - \eta^{\text{chan}})^n$$
$$= 1 - \frac{1}{P_{x_1}} \sum_{n=0}^{\infty} (1 - d_1)(1 - d_2) \frac{[\mu \eta_x f (1 - \eta^{\text{chan}})]^n}{n!} e^{-\mu \eta_x f (1-\eta^{\text{chan}})} e^{\mu[f(1-\eta_x)-1] + \mu \eta_x f (1-\eta^{\text{chan}})} (1 - Y_0^{\text{par}})$$
$$= 1 - \frac{1}{P_{x_1}} (1 - Y_0^{\text{par}})(1 - d_1)(1 - d_2) e^{-\mu \eta_x f \eta^{\text{chan}} + \mu f - \mu}. \quad (13)$$

For simplicity, we rewrite

$$Q_{x_1}^{\text{chan}} = 1 - \frac{1}{P_{x_1}}(1 - Y_0^{\text{par}})(1 - d_1)(1 - d_2)g(f\,), \quad (14)$$

$$g(f) = e^{-\mu f\,\eta_x \eta^{\text{chan}} + \mu f\,-\mu}, \quad (15)$$

where $g(f\,)$ is a substitute function for aesthetics. In addition, note that $Q_{x_1}^{\text{chan}}$ here is only a computational example, and we do not need to calculate $Q_{x_1}^{\text{chan}}$ in practical experiment or simulations. Similarly, we can obtain the overall signal gains of the three kinds of heralded states (two signal states and one decoy state) as

$$\begin{aligned}
Q_{x_2}^{\text{chan}} &= 1 - \frac{1}{P_{x_2}}(1 - Y_0^{\text{par}})(1 - d_2)[g(f_1) - (1 - d_1)g(f)],\\
Q_{x_3}^{\text{chan}} &= 1 - \frac{1}{P_{x_3}}(1 - Y_0^{\text{par}})(1 - d_1)[g(f_2) - (1 - d_2)g(f)],\\
Q_{x_4}^{\text{chan}} &= 1 - \frac{1}{P_{x_4}}(1 - Y_0^{\text{par}})[g(1) - (1 - d_1)g(f_2)\\
&\quad - (1 - d_2)g(f_1) + (1 - d_1)(1 - d_2)g(f\,)]. \quad (16)
\end{aligned}$$

According to Ref. [60], the overall signal gain of Eve can be calculated as

$$\begin{aligned}
Q_{x_i}^{BAE} &= \sum_{n=0}^{\infty} Q_{x_i,n}^{BAE}\\
&\le \sum_{n=0}^{\infty}\left[Q_{x_i,n}^{BA} - \frac{q_{x_i}(n)}{P_{x_i}} Y_0^A\right]\max\left\{1, \frac{\gamma^E}{\gamma^A}\right\}, \quad (17)
\end{aligned}$$

where γ^E is the overall transmission efficiency of Eve after Alice encodes her receiving photons, and γ^A is the overall transmission efficiency for photons received and then measured by Alice.

Similarly, we can also calculate the total error rate of our QSDC protocol as

$$E_{x_i}^{\text{chan}} = \frac{\sum_{n=0}^{\infty} q_{x_i}(n) e_n Y_n^{\text{par}}}{Q_{x_i}^{\text{chan}} P_{x_i}}. \quad (18)$$

Here, we construct the error model $e_n Y_n^{\text{par}}$ as

$$e_n Y_n^{\text{par}} = e_0^{\text{par}} Y_0^{\text{par}} + e_d^{\text{par}}[1 - (1 - \eta)^n], \quad (19)$$

where e_d^{par} is detector error rate and e_0^{par} is the error rate caused by the dark count. e_0^{par} is equal to 0.5, which means when no photon arrives, the dark count from one of the two detectors may cause the error with the probability of 0.5.

Here, we also take the calculation of the total error rate $E_{x_1}^{\text{chan}}$ as an example. In detail, we can obtain

$$\begin{aligned}
E_{x_1}^{\text{chan}} &= \frac{\sum_{n=0}^{\infty} q_{x_1}(n) e_n Y_n^{\text{par}}}{Q_{x_1}^{\text{chan}} P_{x_1}}\\
&= \frac{1}{Q_{x_1}^{\text{chan}} P_{x_1}} \sum_{n=0}^{\infty} q_{x_1}(n)\{e_0^{\text{par}} Y_0^{\text{par}} + e_d^{\text{par}}[1 - (1 - \eta)^n]\}\\
&= \frac{1}{Q_{x_1}^{\text{chan}} P_{x_1}}\left[\sum_{n=0}^{\infty} q_{x_1}(n)(e_0^{\text{par}} Y_0^{\text{par}} + e_d^{\text{par}})\right.\\
&\qquad \left. - \sum_{n=0}^{\infty} q_{x_1}(n) e_d^{\text{par}}(1 - \eta)^n\right]\\
&= \frac{e_0^{\text{par}} Y_0^{\text{par}} + e_d^{\text{par}}}{Q_{x_1}^{\text{chan}}} - \frac{e_d^{\text{par}}}{Q_{x_1}^{\text{chan}} P_{x_1}}(1 - d_1)(1 - d_2)g(f). \quad (20)
\end{aligned}$$

Similarly, we can calculate the total error rate of the two signal states and one decoy state as

$$\begin{aligned}
E_{x_2}^{\text{chan}} &= \frac{1}{Q_{x_2}^{\text{chan}}}(e_0^{\text{par}} Y_0^{\text{par}} + e_d^{\text{par}})\\
&\quad - \frac{e_d^{\text{par}}}{Q_{x_2}^{\text{chan}} P_{x_2}}(1 - d_2)[g(f_1) - (1 - d_1)g(f\,)],\\
E_{x_3}^{\text{chan}} &= \frac{1}{Q_{x_3}^{\text{chan}}}(e_0^{\text{par}} Y_0^{\text{par}} + e_d^{\text{par}})\\
&\quad - \frac{e_d^{\text{par}}}{Q_{x_3}^{\text{chan}} P_{x_3}}(1 - d_1)[g(f_2) - (1 - d_2)g(f\,)],\\
E_{x_4}^{\text{chan}} &= \frac{1}{Q_{x_4}^{\text{chan}}}(e_0^{\text{par}} Y_0^{\text{par}} + e_d^{\text{par}})\\
&\quad - \frac{e_d^{\text{par}}}{Q_{x_4}^{\text{chan}} P_{x_4}}[g(1) - (1 - d_1)g(f_2)\\
&\quad - (1 - d_2)g(f_1) + (1 - d_1)(1 - d_2)g(f\,)]. \quad (21)
\end{aligned}$$

In this way, we can estimate $I(A:B)$ based on Eqs. (16) and (21).

According to Eq. (7), for estimating $I(A:E)$, we need to estimate the single-photon error rate e_1^{BA} and two-photon bit error rate e_2^{BA}. Here, we adopt the decoy-state method to estimate e_1^{BA} and e_2^{BA}. In Sec. II, we generate three types of heralded states through the heralded operation. After Alice receives the transmitted photons, Bob announces the type of each photon pulse, and selects a part of pulses for security checking. If Eve performs the PNS attack during the photon transmission, he will inevitably change the photon distribution, and thus be detected by the parties. After the

first round of security checking, we have

$$\begin{aligned} P_{x_2}Q^{BA}_{x_2} &= q^0_2 Y^A_0 + q^1_2 Y^A_1 + q^2_2 Y^A_2 + \sum_{n=3}^{\infty} q^n_2 Y^A_n, \\ P_{x_3}Q^{BA}_{x_3} &= q^0_3 Y^A_0 + q^1_3 Y^A_1 + q^2_3 Y^A_2 + \sum_{n=3}^{\infty} q^n_3 Y^A_n, \\ P_{x_4}Q^{BA}_{x_4} &= q^0_4 Y^A_0 + q^1_4 Y^A_1 + q^2_4 Y^A_2 + \sum_{n=3}^{\infty} q^n_4 Y^A_n, \end{aligned} \tag{22}$$

$$\begin{aligned} P_{x_2}Q^{BA}_{x_2}E^{BA}_{x_2} &= q^0_2 e_0 Y^A_0 + q^1_2 e_1 Y^A_1 + q^2_2 e_2 Y^A_2 + q^3_2 e_3 Y^A_3 \\ &\quad + \sum_{n=4}^{\infty} q^n_2 e_n Y^A_n, \\ P_{x_3}Q^{BA}_{x_3}E^{BA}_{x_3} &= q^0_3 e_0 Y^A_0 + q^1_3 e_1 Y^A_1 + q^2_3 e_2 Y^A_2 + q^3_3 e_3 Y^A_3 \\ &\quad + \sum_{n=4}^{\infty} q^n_3 e_n Y^A_n, \\ P_{x_4}Q^{BA}_{x_4}E^{BA}_{x_4} &= q^0_4 e_0 Y^A_0 + q^1_4 e_1 Y^A_1 + q^2_4 e_2 Y^A_2 + q^3_4 e_3 Y^A_3 \\ &\quad + \sum_{n=4}^{\infty} q^n_4 e_n Y^A_n, \end{aligned} \tag{23}$$

where q^n_i is the short for $q_{x_i}(n)$. Note that the parameters used in the parameter estimation are all from the first round of photon transmission, and we have omitted the superscript BA of Q and E below.

Here, Y^A_0 is the background detection rate, which we consider as an inherent property of the detector. Then, based on Eq. (22), we can calculate Y^A_1 as

$$\begin{aligned} Y^A_1 = &\frac{q^2_i P_{x_j} Q_{x_j} - q^2_j P_{x_i} Q_{x_i} - (q^2_i q^0_j - q^2_j q^0_i) Y^A_0}{q^2_i q^1_j - q^2_j q^1_i} \\ &- \frac{\sum_{n=3}^{\infty} (q^2_i q^n_j - q^2_j q^n_i) Y^A_n}{q^2_i q^1_j - q^2_j q^1_i}. \end{aligned} \tag{24}$$

According to Ref. [54], we have

$$\frac{q^n_4}{q^n_3} \geq \frac{q^2_4}{q^2_3} \geq \frac{q^1_4}{q^1_3}, \quad \frac{q^n_3}{q^n_2} \geq \frac{q^2_3}{q^2_2} \geq \frac{q^1_3}{q^1_2}. \tag{25}$$

Equation (25) can be further rewritten as

$$\frac{q^n_i}{q^n_j} \geq \frac{q^2_i}{q^2_j} \geq \frac{q^1_i}{q^1_j}, \quad i \geq j, \ \ i,j \in \{2,3,4\}. \tag{26}$$

According to Eq. (26), we have

$$\frac{(q^2_i q^n_j - q^2_j q^n_i)}{q^2_i q^1_j - q^2_j q^1_i} \leq 0. \tag{27}$$

As a result, we have the lower bound (Y^l_1) of Y^A_1 as

$$\begin{aligned} Y^A_1 &\geq \frac{q^2_i P_{x_j} Q_{x_j} - q^2_j P_{x_i} Q_{x_i} - (q^2_i q^0_j - q^2_j q^0_i) Y^A_0}{q^2_i q^1_j - q^2_j q^1_i}, \\ Y^l_1 &= \max_{\substack{i \geq j \,\&\, i,j \\ \in \{2,3,4\}}} \left\{ \frac{q^2_i P_{x_j} Q_{x_j} - q^2_j P_{x_i} Q_{x_i} - (q^2_i q^0_j - q^2_j q^0_i) Y^A_0}{q^2_i q^1_j - q^2_j q^1_i} \right\}, \end{aligned} \tag{28}$$

where the superscript l means the lower bound.

Similarly, Y^A_2 can be calculated as

$$\begin{aligned} Y^A_2 = &\frac{q^1_i P_{x_j} Q_{x_j} - q^1_j P_{x_i} Q_{x_i} - (q^1_i q^0_j - q^1_j q^0_i) Y^A_0}{q^1_i q^2_j - q^1_j q^2_i} \\ &- \frac{\sum_{n=3}^{\infty} (q^1_i q^n_j - q^1_j q^n_i) Y^A_n}{q^1_i q^2_j - q^1_j q^2_i}. \end{aligned} \tag{29}$$

According to Eq. (26), we have

$$\frac{(q^1_i q^n_j - q^1_j q^n_i)}{q^1_i q^2_j - q^1_j q^2_i} \leq 0. \tag{30}$$

In this way, the lower bound (Y^l_2) of Y^A_2 is shown as

$$\begin{aligned} Y^A_2 &\geq \frac{q^1_i P_{x_j} Q_{x_j} - q^1_j P_{x_i} Q_{x_i} - (q^1_i q^0_j - q^1_j q^0_i) Y^A_0}{q^1_i q^2_j - q^1_j q^2_i}, \\ Y^l_2 &= \max_{\substack{i \geq j \,\&\, i,j \\ \in \{2,3,4\}}} \left\{ \frac{q^1_i P_{x_j} Q_{x_j} - q^1_j P_{x_i} Q_{x_i} - (q^1_i q^0_j - q^1_j q^0_i) Y^A_0}{q^1_i q^2_j - q^1_j q^2_i} \right\}. \end{aligned} \tag{31}$$

According to Eq. (23), we can estimate e^{BA}_1 and e^{BA}_2 as

$$
\begin{aligned}
e_1^{BA} &= \frac{(q_4^3q_3^2 - q_3^3q_4^2)P_{x_2}Q_{x_2}E_{x_2} + (q_2^3q_4^2 - q_4^3q_2^2)P_{x_3}Q_{x_3}E_{x_3} + (q_3^3q_2^2 - q_2^3q_3^2)P_{x_4}Q_{x_4}E_{x_4} - \sum_{n=4}^{\infty} f_{q1}(n)e_n Y_n^A}{\{q_4^3(q_3^2q_2^1 - q_2^2q_3^1) + q_2^3(q_4^2q_3^1 - q_3^2q_4^1) + q_3^3(q_2^2q_4^1 - q_4^2q_2^1)\}Y_1^A} \\
&\quad - \frac{\{q_4^3(q_3^2q_2^0 - q_2^2q_3^0) + q_2^3(q_4^2q_3^0 - q_3^2q_4^0) + q_3^3(q_2^2q_4^0 - q_4^2q_2^0)\}e_0 Y_0^A}{\{q_4^3(q_3^2q_2^1 - q_2^2q_3^1) + q_2^3(q_4^2q_3^1 - q_3^2q_4^1) + q_3^3(q_2^2q_4^1 - q_4^2q_2^1)\}Y_1^A} \\
&\le \frac{(q_4^3q_3^2 - q_3^3q_4^2)P_{x_2}Q_{x_2}E_{x_2} + (q_2^3q_4^2 - q_4^3q_2^2)P_{x_3}Q_{x_3}E_{x_3} + (q_3^3q_2^2 - q_2^3q_3^2)P_{x_4}Q_{x_4}E_{x_4}}{\{q_4^3(q_3^2q_2^1 - q_2^2q_3^1) + q_2^3(q_4^2q_3^1 - q_3^2q_4^1) + q_3^3(q_2^2q_4^1 - q_4^2q_2^1)\}Y_1^l} \\
&\quad - \frac{\{q_4^3(q_3^2q_2^0 - q_2^2q_3^0) + q_2^3(q_4^2q_3^0 - q_3^2q_4^0) + q_3^3(q_2^2q_4^0 - q_4^2q_2^0)\}e_0 Y_0^A}{\{q_4^3(q_3^2q_2^1 - q_2^2q_3^1) + q_2^3(q_4^2q_3^1 - q_3^2q_4^1) + q_3^3(q_2^2q_4^1 - q_4^2q_2^1)\}Y_1^l} \\
&= e_1^u, \qquad (32)
\end{aligned}
$$

$$
\begin{aligned}
e_2^{BA} &= \frac{(q_4^3q_3^1 - q_3^3q_4^1)P_{x_2}Q_{x_2}E_{x_2} + (q_2^3q_4^1 - q_4^3q_2^1)P_{x_3}Q_{x_3}E_{x_3} + (q_3^3q_2^1 - q_2^3q_3^1)P_{x_4}Q_{x_4}E_{x_4} - \sum_{n=4}^{\infty} f_{q2}(n)e_n Y_n^A}{\{q_4^3(q_3^1q_2^2 - q_2^1q_3^2) + q_2^3(q_4^1q_3^2 - q_3^1q_4^2) + q_3^3(q_2^1q_4^2 - q_4^1q_2^2)\}Y_2^A} \\
&\quad - \frac{\{q_4^3(q_3^1q_2^0 - q_2^1q_3^0) + q_2^3(q_4^1q_3^0 - q_3^1q_4^0) + q_3^3(q_2^1q_4^0 - q_4^1q_2^0)\}e_0 Y_0^A}{\{q_4^3(q_3^1q_2^2 - q_2^1q_3^2) + q_2^3(q_4^1q_3^2 - q_3^1q_4^2) + q_3^3(q_2^1q_4^2 - q_4^1q_2^2)\}Y_2^A} \\
&\le \frac{(q_4^3q_3^1 - q_3^3q_4^1)P_{x_2}Q_{x_2}E_{x_2} + (q_2^3q_4^1 - q_4^3q_2^1)P_{x_3}Q_{x_3}E_{x_3} + (q_3^3q_2^1 - q_2^3q_3^1)P_{x_4}Q_{x_4}E_{x_4}}{\{q_4^3(q_3^1q_2^2 - q_2^1q_3^2) + q_2^3(q_4^1q_3^2 - q_3^1q_4^2) + q_3^3(q_2^1q_4^2 - q_4^1q_2^2)\}Y_2^l} \\
&\quad - \frac{\{q_4^3(q_3^1q_2^0 - q_2^1q_3^0) + q_2^3(q_4^1q_3^0 - q_3^1q_4^0) + q_3^3(q_2^1q_4^0 - q_4^1q_2^0)\}e_0 Y_0^A}{\{q_4^3(q_3^1q_2^2 - q_2^1q_3^2) + q_2^3(q_4^1q_3^2 - q_3^1q_4^2) + q_3^3(q_2^1q_4^2 - q_4^1q_2^2)\}Y_2^l} \\
&= e_2^u. \qquad (33)
\end{aligned}
$$

Here, $f_{q1}(n)$ ($f_{q2}(n)$) is a coefficient of order n, and its value is proved to be positive [54]. By eliminating the positive term through scaling, we can estimate the upper bound of e_1^{BA} and e_2^{BA} as e_1^u and e_2^u, respectively.

C. Numerical simulation

In our QSDC protocol, we utilize the HSPS to generate three types of sources with the photon-number distributions of $q_{x_2}(n)$, $q_{x_3}(n)$, and $q_{x_4}(n)$, corresponding to three response events x_2, x_3, and x_4, respectively. Each of these three photon-number distributions as a function of the photon number n is depicted in Fig. 2. The parameters used in the numerical simulation are shown in Table I. Meanwhile, we also show the photon-number distribution of the WCP, which follows the Poisson distribution. It can be found that the vacuum state accounts for a large proportion (90.4%) in the WCP, while the single-photon state accounts only for 9.0%. In contrast, by adopting the HSPS, the proportions of vacuum state in $q_{x_2}(n)$ and $q_{x_3}(n)$ largely reduce to about 19.3% and 19.1%, and the proportions of the single-photon state increase to about 77.8% and 77.3%, respectively, which will greatly benefit the gain. Although the proportions of multiphoton events slightly increase in $q_{x_2}(n)$ and $q_{x_3}(n)$, their contribution can be negligible compared to the amplified single-photon component. The photon-number distribution $q_{x_4}(n)$ does not meet the ideal standard since the two-photon event accounts for a high proportion (about 60%). However, we use only $q_{x_2}(n)$ and $q_{x_3}(n)$ to transmit messages, but use $q_{x_4}(n)$ for the decoy state.

Therefore, the secrecy message capacity of our passive decoy-state QSDC protocol with the HSPS is written as

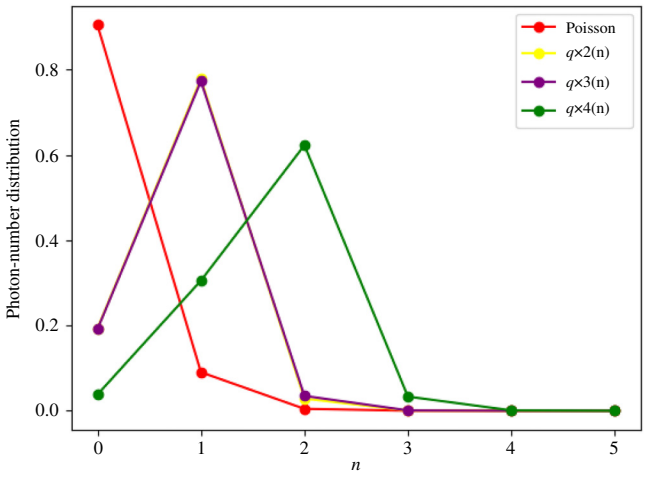

FIG. 2. Comparison between the photon distribution of the HSPS and the Poisson distribution, where $\mu = 0.1$ and the other parameters are shown in Table I. Notice that the curves $q_{x_2}(n)$ and $q_{x_3}(n)$ almost overlap.

TABLE I. Parameters used in the numerical simulation. $\eta_1, \eta_2, \eta_h, \eta_x, t$ are the parameters that we model for the HSPS distribution, and the other parameters are from Pan's experiments [60].

η_x	η_1	η_2	η_h	$\eta_d^{A(B)}$	t
0.8	0.6	0.8	0.9	0.7	0.4
$d_{1(2)}$	$Y_0^{A(B)}$	η_{opt}^{BA}	η_{opt}^{BAB}	e_d^A	e_d^B
8×10^{-8}	8×10^{-8}	0.21	0.088	0.0131	0.0026

$$
\begin{aligned}
C_s &= C_{sq_{x_2}} + C_{sq_{x_3}} \\
&= Q_{x_2}^{BAB}[1 - h(E_{x_2}^{BAB})] - \left\{ Q_{x_2,n=1}^{BAE} * h(2e_1^{BA}) \right. \\
&\quad \left. + Q_{x_2,n=2}^{BAE} * \left[\frac{1}{2} h(2e_2^{BA}) + \frac{1}{2} \right] + Q_{x_2,n\geq 3}^{BAE} * 1 \right\} \\
&\quad + Q_{x_3}^{BAB}[1 - h(E_{x_3}^{BAB})] - \left\{ Q_{x_3,n=1}^{BAE} * h(2e_1^{BA}) \right. \\
&\quad \left. + Q_{x_3,n=2}^{BAE} * \left[\frac{1}{2} h(2e_2^{BA}) + \frac{1}{2} \right] + Q_{x_3,n\geq 3}^{BAE} * 1 \right\}.
\end{aligned} \tag{34}
$$

Figure 3 illustrates the secrecy message capacity versus the channel attenuation under the collective attack as well as the PNS attack in the framework of decoy-state analysis. Consistent with traditional GLLP [78] and decoy-state theories [57,58], the maximum communication distances (channel attenuation) of our protocols decrease with the growth of the average photon number μ, due to the increased susceptibility to PNS attacks. Meanwhile, this multiphoton event caused by a high average photon number can also reduce the secrecy message capacity. In detail, as shown in Eq. (5), the secrecy message capacity is composed of the difference between $I(A:B)$ and $I(A:E)$. The adoption of HSPS can largely reduce the proportion of vacuum state and increase the proportion of single-photon state in the signal state laser pulses, which can effectively increase $I(A:B)$. However, the adoption of HSPS cannot reduce the proportion of the multiphoton component. With the growth of the average photon number, the proportion of the multiphoton component increases significantly, which gives Eve more opportunities to steal information and thus increase $I(A:E)$. As a result, our passive QSDC protocol performs better by using the HSPS with low average photon number, in terms of both secrecy message capacity and maximum communication distance. From Fig. 3, the HSPS with the average photon number $\mu = 0.001$ is optimal for our passive QSDC protocol.

In Fig. 4, we optimize the DL04 QSDC with the WCP source and decoy-state method (black line) to find the optimal pulse intensity for obtaining the maximal secrecy message capacity at each channel attenuation and compare it with that of our passive decoy-state QSDC protocol with the HSPS (red line, $\mu = 0.001$). It is evident that the secrecy message capacity of our QSDC protocol is always higher than that of the DL04 QSDC, especially in the case of large channel attenuation. In detail, at the channel attenuation of 4 dB, C_s of our QSDC protocol is about 14.92 times greater than that of the DL04 QSDC. At the channel attenuation of 7 dB, C_s of our passive QSDC protocol increases to about 186.83 times greater than that of the DL04 QSDC protocol.

Figure 5 illustrates C_s of our passive QSDC protocol with the HSPS and the DL04 QSDC protocol without the HSPS [60] under the average photon numbers $\mu = 0.1$ and 0.01, respectively. Comparing with the DL04 QSDC protocol without the HSPS, at a fixed channel attenuation of

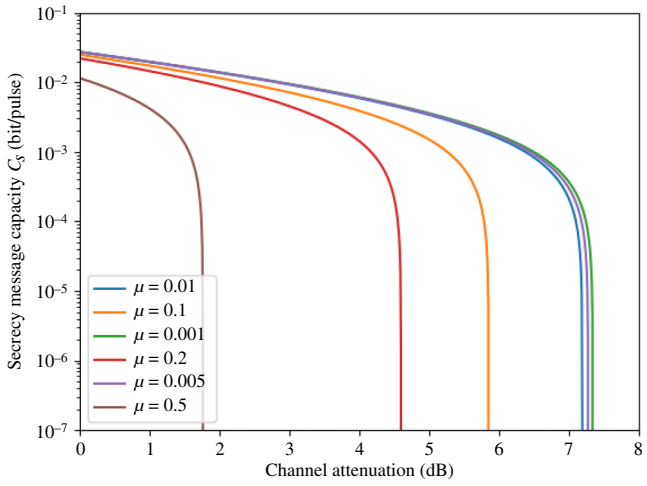

FIG. 3. Secrecy message capacity versus the channel attenuation given the collective attack as well as the PNS attack under the framework of decoy-state analysis.

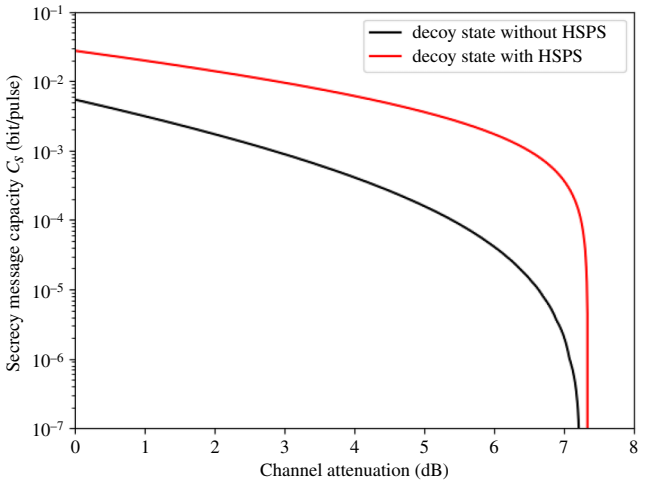

FIG. 4. Comparison of our passive decoy-state QSDC protocol ($\mu = 0.001$) with the DL04 QSDC protocol with the WCP source at the optimal intensities.

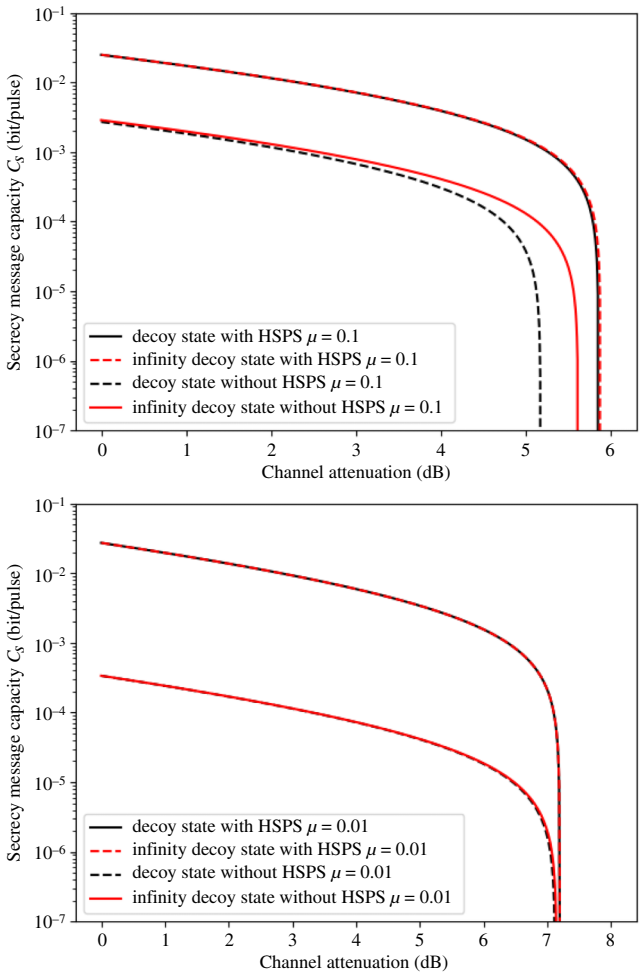

FIG. 5. The secrecy message capacity of our passive decoy-state QSDC protocol with the HSPS and the DL04 QSDC protocol without HSPS [60]. The parameters used in our QSDC protocol is also shown in Table I. The black and red lines represent the cases of finite and infinite decoy state, respectively.

4 dB (communication distance of about 10 km), C_s of our passive QSDC protocol with the HSPS can be increased to 81.85 times at $\mu = 0.1$ and 12.79 times at $\mu = 0.01$. Meanwhile, the maximal communication distance of our passive QSDC protocol with HSPS is also superior to that of the DL04 QSDC protocol without HSPS. When $\mu = 0.01$ (low average photon number), the maximal communication distance of our QSDC protocol can achieve 17.975 km (channel attenuation 7.19 dB), which is slightly longer than that of the DL04 QSDC (17.8 km, channel attenuation 7.12 dB). When $\mu = 0.1$ (high average photon number), our QSDC protocol can achieve the maximal communication distance of about 14.6 km (channel attenuation 5.84 dB), while the DL04 QSDC protocol without the HSPS can only achieve the maximal communication distance of 12.9 km (channel attenuation 5.16 dB). In Fig. 5, we also compare the secrecy message capacity of our passive QSDC protocol and the DL04 QSDC protocol with infinite decoy state (red lines) and finite decoy state (black lines), respectively. The infinite decoy-state method can lead to the ideal yields and error rates. The simulation results show that our simulated yields and error rates with the finite decoy state are very close to the ideal case with the infinite decoy state. Moreover, under the same average photon-number condition, our passive QSDC protocol is superior to the DL04 QSDC protocol without HSPS with infinite decoy states in terms of the communication distance and secrecy message capacity.

IV. DISCUSSION AND CONCLUSION

In QSDC, quantum memory plays a key role for they should ensure that the quantum channel is secure before transmitting secret messages. Therefore, some photons should be used for security checking and the other photons which are used to encode messages should be stored in quantum memory until the security checking is successful. In previous QSDC experiments, the ^{85}Rb atoms trapped in a two-dimensional magneto-optical trap (MOT) are used as the quantum memory [19]. The fiber delay can also act as the role of quantum memory [18,20]. Moreover, in future multihop quantum communication or quantum network, the quantum repeaters are required. The quantum memory is also indispensable [52]. Quantum memory research has been conducted across various physical systems, including atoms [79–82], defects in solids [83], hot atomic vapor [82], superconducting quantum memory [84], and so on. In practical experiment, the bandwidth mismatch between SPDC source and quantum memory may be an obstacle. Fortunately, many efforts have been made to couple high-bandwidth SPDC sources with quantum memory [85–88]. For example, Wei *et al.* achieved a spectrotemporally multiplexed quantum memory in cooled erbium-doped silica fiber with bandwidth up to 10 GHz [88]. They utilized dense wavelength division multiplexers to filter out heralded photons with a bandwidth of 100 GHz. Then five spectral channels were modulated using optical frequency combs with frequency spacing of 15 GHz. Each channel has a bandwidth of 10 GHz and a separation of 5 GHz. Finally coupled to a multiplexed quantum memory, it can store up to 1650 modes of heralded single photons.

Moreover, there have been some efforts to integrate quantum communication with memory, such as memory-enhanced quantum communication [89–91]. The development of these experiments and applications drives the experimental realization of our protocol. The imperfect quantum memory will affect communication distance and secrecy message capacity of our QSDC protocol. Considering the practical quantum memory in Ref. [85], our protocol can perform about 29.5% at a channel attenuation of 2 dB (declining from 1.37×10^{-2} bit/pulse to 4.05×10^{-3} bit/pulse) with the average photon number

of $\mu = 0.01$. The maximum communication attenuation will also be reduced to 3.82 dB, which is about 53.1% of that with the perfect quantum memory. In addition, the quantum-memory-free protocol [92], coupled with classical cryptography, introduces an alternative approach for implementing our QSDC protocol. With the classic ciphertext safeguarding the system, even in the absence of quantum memory, Eve can only pilfer the code words, not the meaningful messages, leading to prompt detection of any breach. This approach has been further expanded to entanglement-based two-step protocols [93] and the MDI protocol [94]. In this way, our passive decoy-state QSDC protocol is hopeful to be demonstrated experimentally in the near future.

In conclusion, we propose a high-efficient passive decoy-state QSDC protocol with the HSPS. Heralded by the detector responses in the HSPS, the input photon pulse can be passively divided as two kinds of high-quality signal single-photon sources, and a decoy-state source. When neither of the two detectors respond, the input photon pulse in the signal path should be discarded. In this way, the probability of the vacuum state in the signal state and decoy state can be largely reduced. In the security analysis, we consider that Eve performs the PNS attack combined with the collective attack and calculate the theoretical secrecy message capacity. The simulation results show that our passive decoy-state QSDC protocol with the HSPS is superior to the original DL04 QSDC protocol with WCP source in both secrecy message capacity and maximal communication distance. For a fixed channel attenuation of 4 dB (communication distance of about 10 km), C_s of our QSDC protocol can achieve 81.85 times ($\mu = 0.1$) and 12.79 times ($\mu = 0.01$) of the corresponding values in the original DL04 QSDC protocol with the WCP source. In the high average photon-number condition ($\mu = 0.1$), our passive decoy-state QSDC protocol can achieve the maximal communication distance of about 14.6 km, about 1.7 km longer than that of the original DL04 QSDC protocol, while in the low average photon-number condition ($\mu = 0.01$), the maximal communication distance can reach 17.975 km. We also optimize our QSDC protocol and the original DL04 QSDC protocol with the WCP source. Our QSDC protocol is always superior to the DL04 protocol at the optimal intensity. At the channel attenuation of 7 dB, the maximal secrecy message capacity of our QSDC protocol increases to about 186.83 times greater than that of the DL04 QSDC protocol. Based on the above features, benefiting from the HSPS and passive decoy-state method, our QSDC protocol shows significant advantages in both maximum communication distance and secrecy message capacity and has strong robustness against the side-channel attack. Our passive decoy-state QSDC protocol is conducive to the realization of high-capacity and long-distance QSDC in the future.

ACKNOWLEDGMENTS

We would like to thank Dong Pan for his generous providing of the comparison data in Fig. 5 and Professors Xiao-Min Hu and Qiang Zhou for helpful discussions. This work is supported by the National Natural Science Foundation of China under Grants No. 12175106 and No. 92365110, the Postgraduate Research & Practice Innovation Program of Jiangsu Province under Grant No. KYCX22-0963, and the Key R&D Program of Guangdong Province under Grant No. 2018B030325002.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175.

[2] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-independent security of quantum cryptography against collective attacks, Phys. Rev. Lett. **98**, 230501 (2007).

[4] H. K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[5] F. H. Xu, X. F. Ma, Q. Zhang, H. K. Lo, and J. W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[6] P. Ye, W. Chen, G. W. Zhang, F. Y. Lu, F. X. Wang, G. Z. Huang, S. Wang, D. Y. He, Z. Q. Yin, G. C. Guo, and Z. F. Han, Induced-photorefraction attack against quantum key distribution, Phys. Rev. Appl. **19**, 054052 (2023).

[7] D. Tupkary and N. Lütkenhaus, Using cascade in quantum key distribution, Phys. Rev. Appl. **20**, 064040 (2023).

[8] B. Liu, S. Xia, D. Xiao, W. Huang, B. J. Xu, and Y. Li, Decoy-state method for quantum-key-distribution-based quantum private query, Sci. China Phys. Mech. & Astron. **65**, 240312 (2022).

[9] Y. M. Xie, Y. S. Lu, C. X. Weng, X. Y. Cao, Z. Y. Jia, Y. Bao, Y. Wang, Y. Fu, H. L. Yin, and Z. B. Chen, Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference, PRX Quantum **3**, 020315 (2022).

[10] S. Wang, Z. Q. Yin, D. Y. He, W. Chen, R. Q. Wang, P. Ye, Y. Zhou, G. J. Fan-Yuan, F. X. Wang, W. Chen, Y. G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G. C. Guo, and Z. F. Han, Twin-field quantum key distribution over 830-km fibre, Nat. Photonics **16**, 2 (2022).

[11] Z. Q. Yin, F. Y. Lu, J. Teng, S. Wang, W. Chen, G. C. Guo, and Z. F. Han, Twin-field protocols: Towards intercity quantum key distribution without quantum repeaters, Fundam. Res. **1**, 93 (2021).

[12] Y. A. Chen, *et al.*, An integrated space-to-ground quantum communication network over 4,600 kilometres, Nature **589**, 214 (2021).

[13] W. Li, L. K. Zhang, Y. C. Lu, Z. P. Li, C. Jiang, Y. Liu, J. Huang, H. Li, Z. Wang, X. B. Wang, Q. Zhang, L. X. You, F. H. Xu, and J. W. Pan, Twin-field quantum key

distribution without phase locking, Phys. Rev. Lett. **130**, 250802 (2023).
[14] G. L. Long and X. S. Liu, Theoretically efficient high-capacity quantum-key-distribution scheme, Phys. Rev. A **65**, 032302 (2002).
[15] F. G. Deng, G. L. Long, and X. S. Liu, Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block, Phys. Rev. A **68**, 042317 (2003).
[16] F. G. Deng and G. L. Long, Secure direct communication with a quantum one-time pad, Phys. Rev. A **69**, 052319 (2004).
[17] C. Wang, F. G. Deng, Y. S. Li, X. S. Liu, and G. L. Long, Quantum secure direct communication with high-dimension quantum superdense coding, Phys. Rev. A **71**, 044305 (2005).
[18] J. Y. Hu, B. Yu, M. Y. Jing, L. T. Xiao, S. T. Jia, G. Q. Qin, and G. L. Long, Experimental quantum secure direct communication with single photons, Light: Sci. & Appl. **5**, e16144 (2016).
[19] W. Zhang, D. S. Ding, Y. B. Sheng, L. Zhou, B. S. Shi, and G. C. Guo, Quantum secure direct communication with quantum memory, Phys. Rev. Lett. **118**, 220501 (2017).
[20] F. Zhu, W. Zhang, Y. B. Sheng, and Y. D. Huang, Experimental long-distance quantum secure direct communication, Sci. Bull. **10**, 1519 (2017).
[21] L. Zhou, Y. B. Sheng, and G. L. Long, Device-independent quantum secure direct communication against collective attacks, Sci. Bull. **65**, 12 (2020).
[22] Z. R. Zhou, Y. B. Sheng, P. H. Niu, L. G. Yin, G. L. Long, and L. Hanzo, Measurement-device-independent quantum secure direct communication, Sci. China: Phys. Mech. & Astron. **63**, 230362 (2020).
[23] P. H. Niu, Z. R. Zhou, Z. S. Lin, Y. B. Sheng, L. G. Yin, and G. L. Long, Measurement-device-independent quantum communication without encryption, Sci. Bull. **63**, 1345 (2018).
[24] T. Li and G. L. Long, Quantum secure direct communication based on single-photon Bell-state measurement, New J. Phys. **22**, 063017 (2020).
[25] G. L. Long and H. Zhang, Drastic increase of channel capacity in quantum secure direct communication using masking, Sci. Bull. **66**, 1267 (2021).
[26] Z. W. Cao, L. Wang, K. X. Liang, G. Chai, and J. Y. Peng, Continuous-variable quantum secure direct communication based on Gaussian mapping, Phys. Rev. Appl. **16**, 024012 (2021).
[27] Z. T. Qi, Y. H. Li, W. Y. Huang, J. Feng, Y. L. Zheng, and X. F. Chen, A 15-user quantum secure direct communication network, Light: Sci. & Appl. **10**, 183 (2021).
[28] Y. B. Sheng, L. Zhou, and G. L. Long, One-step quantum secure direct communication, Sci. Bull. **67**, 367 (2022).
[29] H. R. Zhang, Z. Sun, R. Y. Qi, L. G. Yin, G. L. Long, and J. H. Lu, Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states, Light: Sci. & Appl. **11**, 83 (2022).
[30] L. Zhou and Y. B. Sheng, One-step device-independent quantum secure direct communication, Sci. China: Phys. Mech. & Astron. **65**, 250311 (2022).
[31] J. W. Ying, L. Zhou, W. Zhong, and Y. B. Sheng, Measurement-device-independent one-step quantum secure direct communication, Chin. Phys. B **31**, 120303 (2022).
[32] J. W. Wu, G. L. Long, and M. Hayashi, Quantum secure direct communication with private dense coding using a general preshared quantum state, Phys. Rev. Appl. **17**, 064011 (2022).
[33] I. Paparelle, F. Mousavi, F. Scazza, A. Bassi, M. Paris, and A. Zavatta, Practical quantum secure direct communication with squeezed states, arXiv:2306.14322.
[34] L. Zhou, B. W. Xu, W. Zhong, and Y. B. Sheng, Device-independent quantum secure direct communication with single-photon sources, Phys. Rev. Appl. **19**, 014036 (2023).
[35] Y. P. Hong, L. Zhou, W. Zhong, and Y. B. Sheng, Measurement-device-independent three-party quantum secure direct communication, Quantum Inf. Process. **22**, 111 (2023).
[36] Y. X. Xiao, L. Zhou, W. Zhong, M. M. Du, and Y. B. Sheng, The hyperentanglement-based quantum secure direct communication protocol with single-photon measurement, Quantum Inf. Process. **22**, 339 (2023).
[37] Z. W. Cao, Y. Lu, G. Chai, H. Yu, K. X. Liang, and L. Wang, Realization of quantum secure direct communication with continuous variable, Research **6**, 0193 (2023).
[38] H. Zeng, M. M. Du, W. Zhong, L. Zhou, and Y. B. Sheng, High-capacity device-independent quantum secure direct communication based on hyper-encoding, Fundam. Res. **4**, 852 (2024).
[39] Q. Zhang, M. M. Du, W. Zhong, Y. B. Sheng, and L. Zhou, Single-photon based three-party quantum secure direct communication with identity authentication, Ann. Phys. (Berlin, Ger.) **536**, 3 (2024).
[40] D. Pan, G. L. Long, L. G. Yin, Y. B Sheng, D. Ruan, S. X. Ng, J. H. Lu, and L. Hanzo, The Evolution of Quantum Secure Direct Communication: On the Road to the Qinternet, IEEE Commun. Surv. Tutor. (2024).
[41] J. Liu, X. Zou, X. Wang, Y. Chen, Z. Rong, Z. Huang, S. Zheng, X. Liang, and J. Wu, Applying a class of general maximally entangled states in measurement-device-independent quantum secure direct communication, Phys. Rev. Appl. **21**, 044010 (2024).
[42] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, Device-independent quantum key distribution secure against collective attacks, New J. Phys. **11**, 045021 (2009).
[43] J. KołodyŃski, A. Máttar, P. Skrzypczyk, E. Woodhead, D. Cavalcanti, K. Banaszek, and A. Acín, Device-independent quantum key distribution with single-photon sources, Quantum **4**, 260 (2020).
[44] Q. Zeng, H. Wang, H. Yuan, Y. Fan, L. Zhou, Y. Gao, H. Ma, and Z. Yuan, Controlled entanglement source for quantum cryptography, Phys. Rev. Appl. **19**, 054048 (2023).
[45] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, and E. Z. Tan, Experimental quantum key distribution certified by Bell's theorem, Nature **607**, 682 (2022).
[46] W. Zhang, T. V. Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, and C. C. W. Lim, A device-independent quantum key distribution system for distant users, Nature **607**, 687 (2022).

[47] W. Z. Liu, Y. Z. Zhang, Y. Z. Zhen, M. H. Li, Y. Liu, J. Y. Fan, F. H. Xu, Q. Zhang, and J. W. Pan, Toward a photonic demonstration of device-independent quantum key distribution, Phys. Rev. Lett. **129**, 050502 (2022).
[48] S. A. Castelletto and R. E. Scholten, Heralded single photon sources: A route towards quantum communication technology and photon standards, Eur. Phys. J. Appl. Phys. **41**, 181 (2008).
[49] X. Cao, M. Zopf, and F. Ding, Telecom wavelength single photon sources, J. Semicond. **40**, 071901 (2019).
[50] S. Signorini and L. Pavesi, On-chip heralded single photon sources, AVS Quantum Sci. **2**, 041701 (2020).
[51] C. Zhang, Y. F. Huang, B. H. Liu, C. F. Li, and G. C. Guo, Spontaneous parametric down-conversion sources for multiphoton experiments, Adv. Quantum Technol. **4**, 2000132 (2021).
[52] S. H. Wei, B. Jing, X. Y. Zhang, J. Y. Liao, C. Z. Yuan, B. Y. Fan, C. Lyu, D. L. Zhou, Y. Wang, G. W. Deng, H. Z. Song, D. Oblak, G. C. Guo, and Q. Zhou, Towards real-world quantum networks: A review, Laser Photonics Rev. **16**, 2100219 (2022).
[53] X. H. Zhan, S. Wang, Z. Q. Zhong, Z. Q. Yin, W. Chen, D. Y. He, G. C. Guo, and Z. F. Han, Quantum key distribution with a continuous-wave-pumped spontaneous-parametric-down-conversion heralded single-photon source, Phys. Rev. Appl. **19**, 034027 (2023).
[54] Q. Wang, C. H. Zhang, and X. B. Wang, Scheme for realizing passive quantum key distribution with heralded single-photon sources, Phys. Rev. A **93**, 032312 (2016).
[55] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent states, Phys. Rev. A **51**, 1863 (1995).
[56] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on practical quantum cryptography, Phys. Rev. Lett. **85**, 1330 (2000).
[57] W. Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, Phys. Rev. Lett. **91**, 057901 (2003).
[58] H. K. Lo, X. F. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).
[59] X. F. Ma, B. Qi, Y. Zhao, and H. K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).
[60] D. Pan, Z. S. Lin, J. W. Wu, H. R. Zhang, Z. Sun, D. Ruan, L. G. Yin, and G. L. Long, Experimental free-space quantum secure direct communication and its security analysis, Photonics Res. **8**, 1522 (2020).
[61] X. Liu, Z. J. Li, D. Luo, C. F. Huang, D. Ma, M. M. Geng, J. W. Wang, Z. R. Zhang, and K. J. Wei, Practical decoy-state quantum secure direct communication, Sci. China: Phys. Mech. & Astron. **64**, 120311 (2021).
[62] M. Curty, T. Moroder, X. F. Ma, and N. Lütkenhaus, Non Poissonian statistics from Poissonian light sources with application to passive decoy state quantum key distribution, Opt. Lett. **34**, 3238 (2009).
[63] M. Curty, X. F. Ma, B. Qi, and T. Moroder, Passive decoy-state quantum key distribution with practical light sources, Phys. Rev. A **81**, 022310 (2010).
[64] W. Y. Wang, R. Wang, C. Q. Hu, V. Zapatero, L. Qian, B. Qi, M. Curty, and H. K. Lo, Fully passive quantum key distribution, Phys. Rev. Lett. **130**, 220801 (2023).
[65] F. Y. Lu, Z. H. Wang, V. Zapatero, J. L. Chen, S. Wang, Z. Q. Yin, M. Curty, D. Y. He, R. Wang, W. Chen, G. J. Fan-Yuan, G. C. Guo, and Z. F. Han, Experimental demonstration of fully passive quantum key distribution, Phys. Rev. Lett. **131**, 110802 (2023).
[66] V. Zapatero, W. Wang, and M. Curty, A fully passive transmitter for decoy-state quantum key distribution, Quantum Sci. Technol. **8**, 025014 (2023).
[67] V. Zapatero and M. Curty, Finite-key security of passive quantum key distribution, Phys. Rev. Appl. **21**, 014018 (2024).
[68] J. J. Li, W. Y. Wang, and H. K. Lo, Fully passive measurement-device-independent quantum key distribution, Phys. Rev. Appl. **21**, 064056 (2024).
[69] X. Wang, F. Y. Lu, Z. H. Wang, Z. Q. Yin, S. Wang, J. Q. Geng, W. Chen, D. Y. He, G. C. Guo, and Z. F. Han, Fully passive measurement-device-independent quantum key distribution, Phys. Rev. Appl. **21**, 064067 (2024).
[70] H. D. Riedmatten, V. Scarani, I. Marcikic, A. Acín, W. Tittel, H. Zbinden, and N. Gisin, Two independent photon pairs versus four-photon entangled states in parametric down conversion, J. Mod. Opt. **51**, 1637 (2004).
[71] B. Blauensteiner, I. Herbauts, S. Bettelli, A. Poppe, and H. Hubel, Photon bunching in parametric down-conversion with continuous-wave excitation, Phys. Rev. A **79**, 063846 (2009).
[72] W. Mauerer, M. Avenhaus, W. Helwig, and C. Silberhorn, How colors influence numbers: Photon statistics of parametric down-conversion, Phys. Rev. A **80**, 053815 (2009).
[73] A. D. Wyner, The wire-tap channel, Bell Syst. Tech. J. **54**, 1355 (1975).
[74] R. Y. Qi, Z. Sun, Z. S. Lin, P. H. Niu, W. T. Hao, L. Y. Song, Q. Huang, J. C. Gao, L. G. Yin, and G. L. Long, Implementation and security analysis of practical quantum secure direct communication, Light Sci. Appl. **8**, 22 (2019).
[75] J. W. Wu, Z. S. Lin, L. G. Yin, and G. L. Long, Security of quantum secure direct communication based on Wyner's wiretap channel theory, Quant. Eng. **1**, e26 (2019).
[76] A. S. Holevo, Bounds for the quantity of information transmitted by a quantum communication channel, Probl. Inf. Trans. **9**, 177 (1973).
[77] Y. Feng, R. Duan, and M. Ying, Unambiguous discrimination between mixed quantum states, Phys. Rev. A **70**, 012308 (2004).
[78] D. Gottesman, H. K. Lo, N. Lutkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Quantum Inf. Comput. **4**, 325 (2004).
[79] O. Davidson, O. Yogev, E. Poem, and O. Firstenberg, Single-photon synchronization with a room-temperature atomic quantum memory, Phys. Rev. Lett. **131**, 033601 (2023).
[80] X. Bao, A. Reingruber, P. Dietrich, J. Rui, A. Dück, T. Strassel, L. Li, N. Liu, B. Zhao, and J. Pan, Efficient and long-lived quantum memory with cold atoms inside a ring cavity, Nat. Phys. **8**, 517 (2012).
[81] Y. W. Cho, G. T. Campbell, J. L. Everett, J. Bernu, D. B. Higginbottom, M. T. Cao, J. Geng, N. P. Robins, P. K. Lam, and B. C. Buchler, Highly efficient optical quantum memory with long coherence time in cold atoms, Optica **3**, 100 (2016).

[82] G. Buser, R. Mottola, B. Cotting, J. Wolters, and P. Treutlein, Single-photon storage in a ground-state vapor cell quantum memory, PRX Quantum **3**, 020349 (2022).

[83] D. D. Sukachev, A. Sipahigil, C. T. Nguyen, M. K. Bhaskar, R. E. Evans, F. Jelezko, and M. D. Lukin, The silicon-vacancy spin qubit in diamond: Quantum memory exceeding ten milliseconds and single-shot state readout, Phys. Rev. Lett. **119**, 223602 (2017).

[84] Z. Bao, Z. Wang, Y. Wu, Y. Li, C. Ma, Y. Song, H. Zhang, and L. Duan, On-demand storage and retrieval of microwave photons using a superconducting multi-resonator quantum memory, Phys. Rev. Lett. **127**, 010503 (2021).

[85] Y. F. Wang, J. F. Li, S. C. Zhang, K. Y. Su, Y. R. Zhou, K. Y. Liao, S. W. Du, H. Yan, and S. L. Zhu, Efficient quantum memory for single photon polarization qubits, Nat. Photonics **13**, 346 (2019).

[86] X. Liu, J. Hu, Z. F. Li, X. Li, P. Y. Li, P. J. Liang, Z. Q. Zhou, C. F. Li, and G. C. Guo, Heralded entanglement distribution between two absorptive quantum memories, Nature **594**, 41 (2021).

[87] X. Y. Zhang, B. Zhang, S. H. Wei, H. Li, J. Y Liao, C. Li, G. W. Deng, Y. Wang, H. Z. Song, L. X. You, B. Jing, F. Chen, G. C. Guo, and Q. Zhou, Telecom-band-integrated multimode photonic quantum memory, Sci. Adv. **9**, 28 (2023).

[88] S. H. Wei, B. Jing, X. Y. Zhang, J. Y. Liao, H. Li, L. X. You, Z. Wang, Y. Wang, G. W. Deng, H. Z. Song, D. Oblak, G. C. Guo, and Q. Zhou, Quantum storage of 1650 modes of single photons at telecom wavelength, npj Quantum Inf. **10**, 19 (2024).

[89] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin, Experimental demonstration of memory-enhanced quantum communication, Nature **580**, 60 (2020).

[90] F. Schmidt and P. van Loock, Memory-assisted long-distance phase-matching quantum key distribution, Phys. Rev. A **102**, 042614 (2020).

[91] M. S. Sun, C. H. Zhang, H. J. Ding, X. Y. Zhou, J. Li, and Q. Wang, Practical decoy-state memory-assisted measurement-device-independent quantum key distribution, Phys. Rev. Appl. **20**, 024029 (2023).

[92] Z. Sun, L. Song, Q. Huang, L. Yin, G. L. Long, J. Lu, and L. Hanzo, Toward practical quantum secure direct communication: A quantum-memory-free protocol and code design, IEEE Trans. Commun. **68**, 9 (2020).

[93] D. Pan, K. Li, D. Ruan, S. X. NG, and L. Hanzo, Single-photon-memory two-step quantum secure direct communication relying on Einstein-Podolsky-Rosen pairs, IEEE Access **8**, 121146 (2020).

[94] X. J. Li, D. Pan, G. L. Long, and L. Hanzo, Single-photon-memory measurement-device-independent quantum secure direct communication-Part II: A practical protocol and its secrecy capacity, IEEE Commun. Lett. **27**, 1060 (2023).