PHOTONICS Research

Experimental free-space quantum secure direct communication and its security analysis

Dong Pan,[1,2,†] Zaisheng Lin,[2,3,4,5,†] Jiawei Wu,[1,2] Haoran Zhang,[1,2] Zhen Sun,[2,3] Dong Ruan,[1,2] Liuguo Yin,[2,3,4,5,6] and Gui Lu Long[1,2,3,4,5,7]

[1]State Key Laboratory of Low-dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, China
[2]Frontier Science Center for Quantum Information, Beijing 100084, China
[3]School of Information Science and Technology, Tsinghua University, Beijing 100084, China
[4]Beijing National Research Center for Information Science and Technology, Beijing 100084, China
[5]Beijing Academy of Quantum Information Sciences, Beijing 100193, China
[6]e-mail: yinlg@tsinghua.edu.cn
[7]e-mail: gllong@tsinghua.edu.cn

Received 22 January 2020; revised 10 June 2020; accepted 20 June 2020; posted 22 June 2020 (Doc. ID 388790); published 31 August 2020

We report an experimental implementation of free-space quantum secure direct communication based on single photons. The quantum communication scheme uses phase encoding, and the asymmetric Mach–Zehnder interferometer is optimized so as to automatically compensate phase drift of the photons during their transitions over the free-space medium. At a 16 MHz pulse repetition frequency, an information transmission rate of 500 bps over a 10 m free space with a mean quantum bit error rate of 0.49% ± 0.27% is achieved. The security is analyzed under the scenario that Eve performs the collective attack for single-photon state and the photon number splitting attack for multi-photon state in the depolarizing channel. Our results show that quantum secure direct communication is feasible in free space.

https://doi.org/10.1364/PRJ.388790

1. INTRODUCTION

Information security and data encryption [1,2] have risen to a pivotal position in the digital information era. The development of quantum communication provides us with new approaches for secure communication tasks, with the benefit of provable security provided by quantum mechanical laws. Quantum key distribution (QKD) protocol was proposed by Bennett and Brassard in 1984 (called BB84 QKD protocol) [3] to perform key exchanges between legitimate distant users. Hitherto, QKD has been well developed in optical fiber, laying the foundation for the establishment of quantum communication networks [4–6]. Compared with fiber, the free-space channel is also considered to be a befitting link for quantum communication. The atmosphere has several high transmission windows at particular wavelengths, which allows low-loss light transmission. Quantum communication can be established by using a free-space channel [7] for rough areas where optical fiber networks are not constructed. In addition, free-space quantum communication is valuable for long-distance quantum communication, combining earth-to-satellite and satellite-to-satellite communications. Due to nonbirefringence for the propagation of light in the atmosphere, the polarization of a single photon is maintained well, most free-space quantum communications are implemented using polarization encoding [8–12]. QKD ensures security through detection of eavesdropping on-site. Therefore QKD transmits random numbers first, and if it can assure no eavesdropping, the random numbers are adopted as keys for use to encrypt the message in a subsequent classical communication. But it cannot prevent the eavesdropper from obtaining the transmitted ciphertext.

In the past two decades, quantum secure direct communication (QSDC) was proposed and developed [13–16]. QSDC directly conveys safely secret messages over the quantum channel. Demonstration experiments have contributed the key technologies of QSDC, such as frequency coding [17], quantum memory [18], fiber entanglement source [19], and practical system for intra-city applications [20]. Up to now, this philosophy has been extended to numerous different theoretical proposals aimed to directly convey secret information over the quantum channel, which guarantees security by ensuring that the eavesdropper cannot simultaneously access the two parts of a correlated quantum state [13,14,16,21,22] or by encrypting information with the quantum state [15,23–25]. Recently, the measurement-device-independent (MDI) theories of QSDC have been established [26–28], MDI scheme for the single photon–based QSDC was given in Ref. [26], and that for the entanglement-based QSDC protocols in Refs. [13,14] is provided in Ref. [27]. The scheme that is secure against all defects in devices in QSDC, namely, the device-independent QSDC, was given in Ref. [29].

Against the aforementioned background, our main contributions are as follows. First, to the best of our knowledge, we report the first fully operational system for free-space QSDC with phase encoding. The transmitter and receiver modules are further developed by utilizing the most common fiber optical components. A round-trip optical architecture can also mitigate the problem of phase drift in the free-space channel so as to achieve a stable QSDC. Second, the security of the QSDC system is analyzed under the photon number splitting (PNS) attack for multi-photon components. The Gottesman-Lo-Lütkenhaus-Preskill (GLLP) theory [30] and decoy state [31–33] can be extended into our model to analyze security. One surprising result is that we can achieve secure information transmission by the two-photon component, which is consistent with the results of two-way QKD [34–36], a special case of the DL04 QSDC protocol [15]. This paper is arranged as follows. In Section 2, we review the details of the single photon–based QSDC protocol and show how we run it on a free-space experimental system with phase encoding. In Section 3, we present the experimental results. In Section 4, we analyze the security of the QSDC system. Finally, conclusions are given in Section 5.

2. EXPERIMENTAL IMPLEMENTATION

A. Protocol

The DL04 QSDC protocol [15] realized in this work has the following steps.

(1) Bob randomly chooses either the basis Z or X for preparing a sequence of single photons, which are subsequently transmitted to Alice. Each of the photons is in one of four quantum states: $\{|0\rangle, |1\rangle, |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\}$. One could implement this random selection using a quantum random number generator [37].

(2) After receiving the photons from Bob, Alice randomly chooses some photons as samples for detecting eavesdropping. For these selected photons, Alice measures each of them by using either the basis Z or X randomly and then announces the positions of the sample together with the measurement basis and outcomes. Alice and Bob obtained the detection bit error rate (DBER) through a classical authenticated channel.

(3) If the DBER is lower than a predetermined threshold, the information encoding process continues. Alice performs $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ or $Y = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$ on the remaining photons to encode the secret information bit 0 or 1 and then returns them to Bob. She will also encode some photons randomly for error-checking. Otherwise, the communication process is aborted.

(4) After receiving the photon sequence, Bob deterministically decodes the secret information. Bob obtains a quantum bit error rate (QBER) by discussing with Alice the checking bits.

There are two error rates in the DL04 QSDC protocol, the DBER and the QBER, which ensure the security of the first transmission and the reliability of the second transmission, respectively.

B. Phase Encoding

The schematic of our experimental setup is shown in Fig. 1. The system is comprised of two legitimate users' optical setups and a free-space channel between them. The apparatus of Alice and Bob all adopt fiber-optic components. Some low-absorption atmospheric spectral windows in the near-infrared, such as regions of $\lambda \sim 850$ nm and $\lambda \sim 1550$ nm, are usually considered for free-space quantum communications. Our system works at a wavelength of 1550 nm to take advantage of a

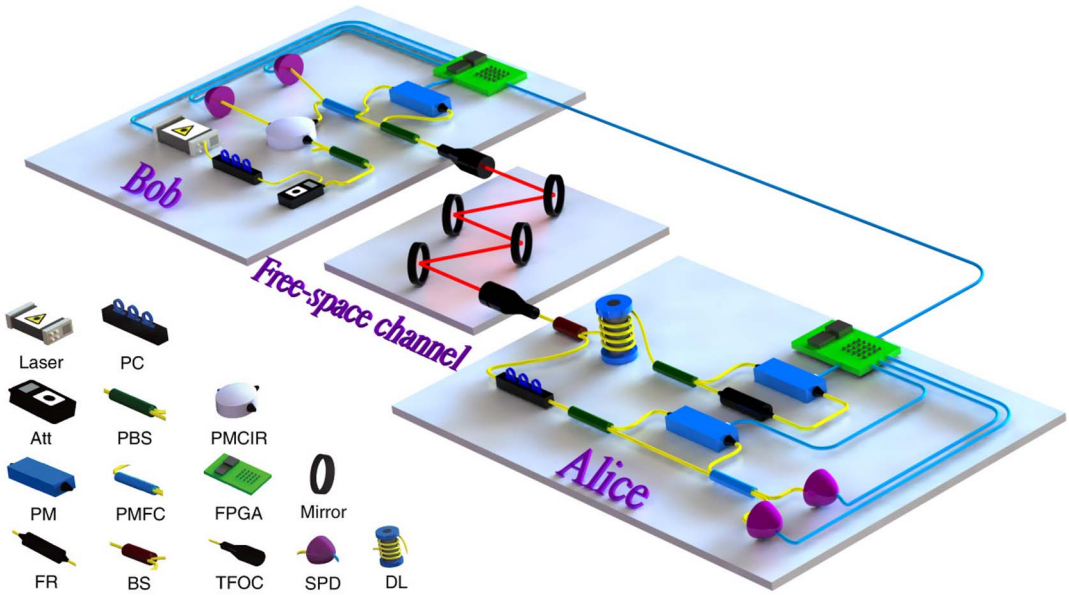

Fig. 1. Schematic diagram of free-space QSDC system. Att, attenuator; BS, beam splitter; DL, delay line; FPGA, field-programmable gate array; FR, Faraday rotator; PBS, polarization beam splitter; PC, polarization controller; PM, phase modulator; PMCIR, polarization-maintaining circulator; PMFC, polarization-maintaining fiber coupler; SPD, single-photon detector; TFOC, triplet fiber-optic collimator. Blue, yellow, and red lines are the electric line, optical fiber line, and free-space path, respectively.

peak in the typical atmospheric transmission window and the low attenuation dip in fiber-optic components.

The laser pulses are emitted at Bob with a repetition frequency of 16 MHz and a pulse width of 200 ps. They are reduced to a specific attenuated level at the input of Bob's station. To be more specific, Bob modulates a random phase $\phi_1^B \in \{0, \pi/2, \pi, 3\pi/2\}$ on the pulse by using his phase modulator (PM) located in the long-path of the asymmetric Mach–Zehnder interferometer. It is equivalent to the preparation of four initial states in the DL04 QSDC protocol. The photons are transported to a triplet fiber-optic collimator (TFOC) where they are output to a free-space channel and then collected by Alice's collimator for coupling into the single-mode fiber. In our proof-of-principle experimental demonstration, Alice's and Bob's collimators are separated by 10 m with four mirror reflections. A 50/50 beam splitter (BS) in Alice's system randomly reflects or transmits the incoming photons to two different paths: the lower and upper paths in Fig. 1, one for detecting eavesdropping and the other for encoding secret information. For the lower path, Alice detects the photon with her interferometer by randomly applying phase modulation $\phi_1^A \in \{0, \pi/2\}$ to the pulse passing over the long-path, and then a DBER is obtained by public discussion between Alice and Bob. By contrast, in the upper path, an encoding operation I or Y is performed on the pulse (previously passing over the long-path at Bob) by adding a phase $\phi_2^A = 0$ or $\phi_2^A = \pi$ after it passes through the Faraday rotator (FR). Finally, by the time of the pulse arriving back to Bob's station, Bob applies phase modulation ϕ_2^B to the pulse for finishing measurement according to the initial phase modulation that he has imposed. To estimate the QBER, the measurement results of checking bits are compared with Alice's encoding. The photons are detected by InGaAs avalanche photodiodes gated in Geiger mode and cooled to −50°C, with a gate width of 1 ns and an efficiency of 5.57% as well as a dark count probability of 1×10^{-6} per gate.

In this setup, all pulses propagate over a loop with the FR and the PM to perform information encoding. The Faraday mirror in Muller's scheme [38] is replaced by the FR. All pulses only pass through the PM once compared with the Faraday mirror as a reflection terminal, so this loop has less attenuation than the original Muller's scheme. It will help to improve the repetition rate of our QSDC system. The pulses are delivered through the same optical path to convey information, the phase is very stable, and the light propagation with an FR automatically compensates for all polarization fluctuations in the optical links. Furthermore, this system has a low requirement on the PM, since the PM is consistent with the conventional one that only requires both its input and output fibers are polarization-maintaining fibers [39]. The polarization controller (PC) located at the Alice site is used to compensate polarization drift in the fiber so that the pulses are completely transmitted at the polarization beam splitter (PBS), guiding the short (long) path pulse which comes from Bob into Alice's long (short) path. This free-space QSDC system is controlled as well as synchronized by two field-programmable gate array (FPGA) devices, and specific computer software programs are developed at Alice's and Bob's terminal.

3. EXPERIMENTAL RESULTS

The experiment is conducted in a lab platform. Figure 2 shows the interference fringes. Both curves are coincident with a sinusoidal pattern. Interference visibility of single-trip (Bob-to-Alice) and round-trip (Bob-to-Alice-to-Bob) is 97.37% and 99.48%, respectively. Although the light is susceptible to scatter in free space, producing phase aberrations which perturb quantum bits, stable interference can still be observed in our experiment system.

To guarantee the reliable transmission of secret information, low-density parity-check code [20,40] is applied to our free-space QSDC system, and the compensation algorithm that aims to eliminate phase shift of a single photon in the free-space channel is equipped. A transmission rate of 500 bps is obtained, and consequently, files of reasonable sizes, such as text, picture, and audio, can be transmitted directly over the quantum channel by running our system. In the experiment test, Alice transmits an image of size 800 × 525 pixels (194 k) to Bob, and Fig. 3 shows the variation of DBER and QBER during the transmission time. The average of DBER and QBER during image transmission is 1.90% ± 0.32% and 0.49% ± 0.27%, respectively. High visibility of the interferometer is crucial to obtain a low error rate in our free-space QSDC system. The QBER through a round-trip optical path is obtained where phase drifts are auto-compensated by the modified Muller's scheme, while the DBER is detected through a single-trip optical path using phase compensation algorithm to mitigate phase shifts. This active compensation is not as efficient as the auto-compensation, and therefore DBER is higher than QBER, as shown in Fig. 3. The phenomenon of DBER higher than QBER is consistent with the result of Fig. 2, in which the interference visibility of the single-trip is lower than that of the round-trip, since the interference visibility has an important

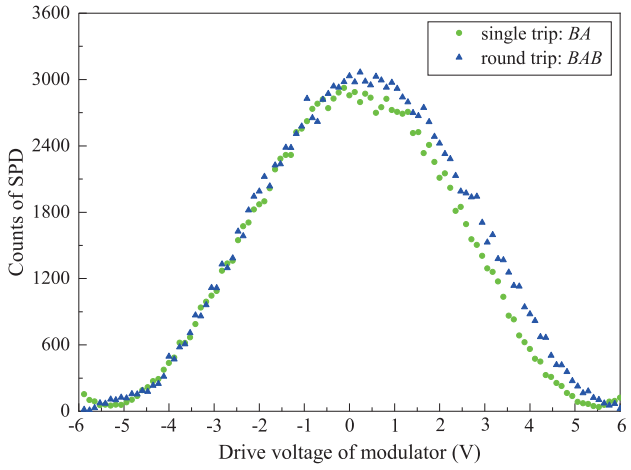

Fig. 2. Interference fringes. Driving voltage ranges from −6 V to +6 V with a half-wave voltage 4.8 V and a step of about 0.1 V. The interference fringe of a single-trip (photons transmitted from Bob-to-Alice) is obtained from Alice's detection. More specifically, the counts are recorded by Alice's SPD at each step when she drives the voltage of her PM. By contrast, when the photons are received by Bob (after their trip Bob-Alice-Bob), he drives the voltage of his PM and records counts by his SPD to obtain the interference fringe of the round-trip.

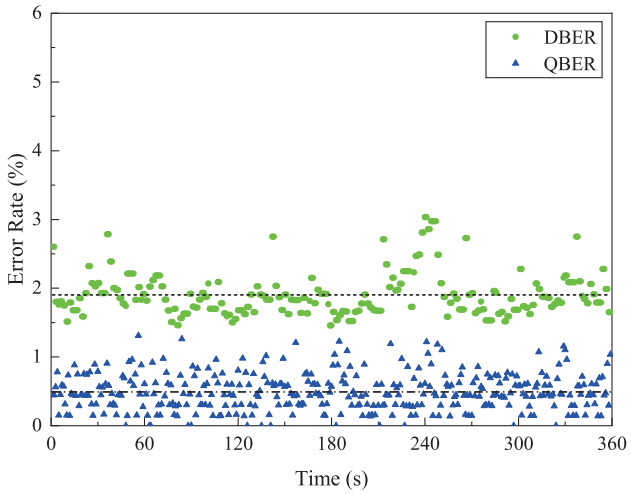

Fig. 3. Error rates during image file transmission. Dashed lines represent the mean values of DBER, and dash-dotted lines show the mean values of QBER. The definition of DBER and QBER is given in Section 2.A, while the experimental approach for accessing them is introduced in Section 2.B.

influence on the bit error rate of the phase-encoding scheme. The round-trip interferometer which has the same optical path for the two interfering pulses produces better interference than the single-trip where the two interfering pulses have only approximately the same optical path. Therefore, the interference visibility of round-trip is higher than that of single-trip. The interference visibility test is generally used to assess the performance of interferometer while the effect of the dark count of single-photon detectors is included. We maintain the detectors' maximum count of ~3000 by improving the light intensity during the interference visibility test of the round-trip. In this count rate, the influence of the dark count could be ignored. As a result, the count curves are given as Fig. 2.

4. SECURITY ANALYSIS

The secrecy capacity lower bound of the DL04 QSDC is given in Ref. [20] according to Wyner's wiretap channel theory [41], which can be written as

$$C_s = \max_{\{p_0\}}\{I(A{:}B) - I(A{:}E)\}, \tag{1}$$

where $I(A{:}B)$ is the mutual information between Alice and Bob, while $I(A{:}E)$ is the maximum information that Eve can steal, and p_0 is the probability that Alice performs operation I during her information encoding. Hence, C_s defines the asymptotic information rate at which Alice can convey to Bob over the quantum channel with the guarantee that Eve has negligible information about the transmitted secret information. Remarkably, the asymptotic regime cannot be met for practical implementation, which has been fully considered in QKD [42]. The finite size of a block in the practical implementation of block-transmission-based QSDC [13–15] is actually the finite-size regime, and the block size would affect the security of QSDC. However, the finite-size analysis of QKD cannot be directly invoked for QSDC, since negotiating random secret key bits is different from transmitting secret information bits. The finite-size effect of QSDC would be an interesting direction for future research.

A. Photon Number Splitting Attack

The general collective attacks on a single photon have been taken into account in many works [20,43–45]. However, practical quantum communication systems are usually implemented with weak coherent light sources. The pulse generated from such a light source can be written as a mixture of Fock states: $\rho = \int(1/2\pi)\mathrm{d}\theta|\sqrt{\mu}e^{i\theta}\rangle\langle\sqrt{\mu}e^{i\theta}| = \sum_n p(n,\mu)|n\rangle\langle n|$, in which the number of photons n follows the Poisson distribution $p(n,\mu) = e^{-\mu}\mu^n/n!$ with mean photon number μ and phase θ. It occasionally emits multiple photons. Unfortunately, the pulses containing multiple photons cannot be secure in some quantum communication protocols when they are under PNS attack [31], namely, Eve splits one of the photons from the pulse that contains two or more photons for measuring. Here, we suggest a photon number splitting attack according to the two-way characteristic of the DL04 QSDC, which combines the PNS attack as well as the collective attack. Hence, the security analysis of this system is given in the context of both the general collective attack on a single photon and the PNS attack on multiple photons.

The attack strategies of Eve are shown in Fig. 4. Eve has the ability to discern the number of photons in every pulse, and then the specific attack strategies performed by Eve would be divided into two types. On the one hand, if the pulse in the forward quantum channel contains only one photon ($n = 1$), Eve performs the collective attack on this photon [20,43]. To be more specific, Eve prepares ancilla states each of which interacts individually with the photons sent from Bob-to-Alice, and these ancilla states are stored in the quantum memory until the photons are returned from Alice after secret information has been encoded. Eve would perform the optimal measurement by combining her ancilla states and the encoded states in order to obtain the secret information. According to Ref. [20], the maximum information that Eve can obtain from

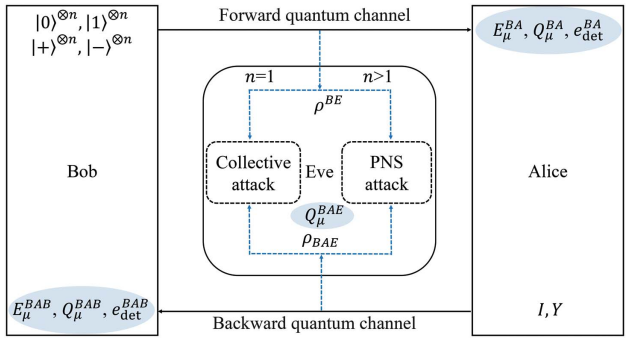

Fig. 4. Illustration of Eve's attack strategies. n, the number of photons in a pulse in the forward quantum channel; E_μ^{BA} is the error rate of the Bob-Alice channel, which is also called as DBER; Q_μ^{BA}, the overall signal gain of Alice; $e_{\mathrm{det}}^{\mathrm{BA}}$, the erroneous signal detection of Alice; ρ^{BE}, the joint state after Eve's attack in the forward quantum channel; Q_μ^{BAE}, the overall signal gain of Eve; ρ^{BAE}, the joint state after Alice's information encoding and Eve's attacks in the two quantum channels; E_μ^{BAB} is QBER; Q_μ^{BAB}, the overall signal gain of Bob; $e_{\mathrm{det}}^{\mathrm{BAB}}$ is the erroneous signal detection of Bob.

a single photon is $I(A{:}E)_{n=1} = h(2e_1^{\mathrm{BA}})$, in which we have assumed reasonably that Eve introduces equivalent error rate in the X and Z basis, and e_1^{BA} is the DBER originated from a single photon. On the other hand, if the pulse in the forward quantum channel is with photon number greater than 1 ($n > 1$), Eve can perform the PNS attack.

Let us start with case $n \geq 3$. The four linearly independent states ($\{|0\rangle^{\otimes n}, |1\rangle^{\otimes n}, |+\rangle^{\otimes n}, |-\rangle^{\otimes n}\}, n \geq 3$) could be unambiguously discriminated [46], hence there is a powerful attack that Eve can get all secret information for the pulse that contains multi-photon components ($n \geq 3$), and it goes as follows. Eve captures this pulse sent from Bob, and then a new photon in the right state that is based on her successful unambiguous discrimination would be prepared and transmitted to Alice. If Eve fails to discriminate the multi-photon state, she blocks it. After the secret information encoding is finished by Alice, Eve captures the pulse again and she can deterministically decode the secret information based on the known initial state. Consequently, the pulses with multiple photons ($n \geq 3$) referred to as multi-photon states cannot provide secrecy capacity in the DL04 QSDC protocol.

Indeed, $I(A{:}E)_{n\geq 3} = 1$, and we need to derive the secrecy capacity that two-photon components can achieve under the PNS attack. In the PNS attack, Eve splits one of the photons from the pulse that contains two photons in the forward quantum channel and retains it. As for the other photon, she applies the collective attack, as detailed above in the case of $n = 1$. What is unusual is that Eve can get two intercepted photons from each pulse, and these states will be combined with her ancillas for the optimal measurement. We assume that the initial state prepared by Bob is $\rho_B = (|00\rangle\langle 00| + |11\rangle\langle 11| + |++\rangle\langle ++| + |--\rangle\langle --|)/4$. Eve's quantum operation in the PNS attack can be represented as

$$\begin{aligned}
&U|0\rangle_B|0\rangle_B|E\rangle = |0\rangle_B|0\rangle_B|E_{0000}\rangle + |0\rangle_B|1\rangle_B|E_{0001}\rangle = |\varphi_1\rangle,\\
&U|1\rangle_B|1\rangle_B|E\rangle = |1\rangle_B|0\rangle_B|E_{1110}\rangle + |1\rangle_B|1\rangle_B|E_{1111}\rangle = |\varphi_2\rangle,\\
&U|+\rangle_B|+\rangle_B|E\rangle = |\varphi_3\rangle,\\
&U|-\rangle_B|-\rangle_B|E\rangle = |\varphi_4\rangle,
\end{aligned} \tag{2}$$

where U is an unitary operation performed on two particles, i.e., one photon of ρ_B together with $|E\rangle$ and $|E\rangle$ ($|E\rangle_{0000}$, $|E\rangle_{0001}$, $|E\rangle_{1110}$, and $|E\rangle_{1111}$) is the ancilla state before (after) attack. The effect of Alice's encoding unitary operation Y (single-particle operation) on the photons can be written as

$$\begin{aligned}
&YU|0\rangle_B|0\rangle_B|E\rangle = -|0\rangle_B|1\rangle_B|E_{0000}\rangle + |0\rangle_B|0\rangle_B|E_{0001}\rangle = |\varphi_5\rangle,\\
&YU|1\rangle_B|1\rangle_B|E\rangle = -|1\rangle_B|1\rangle_B|E_{1110}\rangle + |1\rangle_B|0\rangle_B|E_{1111}\rangle = |\varphi_6\rangle,\\
&YU|+\rangle_B|+\rangle_B|E\rangle = |\varphi_7\rangle,\\
&YU|-\rangle_B|-\rangle_B|E\rangle = |\varphi_8\rangle.
\end{aligned} \tag{3}$$

Hence, after Eve's attack, the joint state of two photons and Eve's ancilla in the forward quantum channel is $\rho_{\mathrm{BE}} = U(\rho_B \otimes |E\rangle\langle E|)U^\dagger$. During the information encoding, if Alice performs unitary operation I or Y with the probability of p_0 and p_1 on the photons, respectively, the joint state would become $\rho_{\mathrm{BE}}^0 = U(\rho_B \otimes |E\rangle\langle E|)U^\dagger$ or $\rho_{\mathrm{BE}}^1 = YU(\rho_B \otimes |E\rangle\langle E|)U^\dagger Y^\dagger$ with respective probabilities. Thus, the joint state that Eve can access in the backward quantum channel is

$$\begin{aligned}
\rho_{\mathrm{BEA}} &= p_0 \cdot \rho_{\mathrm{BE}}^0 + p_1 \cdot \rho_{\mathrm{BE}}^1\\
&= \frac{1}{4}(p_0|\varphi_1\rangle\langle\varphi_1| + p_0|\varphi_2\rangle\langle\varphi_2| + p_0|\varphi_3\rangle\langle\varphi_3|\\
&\quad + p_0|\varphi_4\rangle\langle\varphi_4| + p_1|\varphi_5\rangle\langle\varphi_5| + p_1|\varphi_6\rangle\langle\varphi_6|\\
&\quad + p_1|\varphi_7\rangle\langle\varphi_7| + p_1|\varphi_8\rangle\langle\varphi_8|),
\end{aligned} \tag{4}$$

where $p_0 + p_1 = 1$.

The maximum information that Eve can steal $I(A{:}E)$ is given by the Holevo bound χ [45,47], that is,

$$I(A{:}E) \leq \chi = \max_{\{U\}}\{S(\rho_{\mathrm{BEA}}) - p_0 \cdot S(\rho_{\mathrm{BE}}^0) - p_1 \cdot S(\rho_{\mathrm{BE}}^1)\}, \tag{5}$$

where $S(\rho) = -\mathrm{Tr}(\rho \log_2 \rho)$ represents the von Neumann entropy. On the one hand, since the density operators ρ_{BE}^0 and ρ_{BE}^1 are only different in unitary operation from $\rho_B \otimes |E\rangle\langle E|$, we can conclude that $S(\rho_{\mathrm{BE}}^0) = S(\rho_{\mathrm{BE}}^1) = S(\rho_B \otimes |E\rangle\langle E|) = 3/2$. On the other hand, we must obtain the eigenvalues of the joint state ρ_{BEA} in order to calculate the von Neumann entropy $S(\rho_{\mathrm{BEA}})$. We can simplify the process of calculating eigenvalues by using the Gram matrix representation, which is proved to have the same eigenvalues with its corresponding density operator [48]. For the joint state ρ_{BEA}, its Gram matrix is given by

$$G = \frac{1}{4}\begin{bmatrix}
p_0\langle\varphi_1|\varphi_1\rangle & p_0\langle\varphi_1|\varphi_2\rangle & \cdots & \sqrt{p_0p_1}\langle\varphi_1|\varphi_8\rangle\\
p_0\langle\varphi_2|\varphi_1\rangle & p_0\langle\varphi_2|\varphi_2\rangle & \cdots & \sqrt{p_0p_1}\langle\varphi_2|\varphi_8\rangle\\
\vdots & \vdots & & \vdots\\
\sqrt{p_0p_1}\langle\varphi_8|\varphi_1\rangle & \sqrt{p_0p_1}\langle\varphi_8|\varphi_2\rangle & \cdots & p_1\langle\varphi_8|\varphi_8\rangle
\end{bmatrix}. \tag{6}$$

Note that the above analysis applies to the most general PNS attack. To illustrate the use of the above result, we assume that Eve's attack operator U is symmetric, which further means that her attack could be modeled as a depolarizing channel [49]. The depolarizing channel is a typical model invoked in the unconditional security proofs of some QKD protocols, as detailed in Refs. [44,50,51]. Hence, in addition to the conditions of orthonormality, $\langle E_{0000}|E_{0000}\rangle + \langle E_{0001}|E_{0001}\rangle = 1$ and $\langle E_{1110}|E_{1110}\rangle + \langle E_{1111}|E_{1111}\rangle = 1$, there are some equations of the depolarizing channel to calculate the specific values of Gram matrix's elements, which are given as follows [20,44]:

$$\begin{aligned}
&\langle E_{0000}|E_{1110}\rangle = \langle E_{0001}|E_{1111}\rangle = 0,\\
&\langle E_{0000}|E_{0001}\rangle = \langle E_{1110}|E_{1111}\rangle = 0,\\
&\langle E_{0001}|E_{1110}\rangle = 0,\\
&\langle E_{0000}|E_{1111}\rangle = 1 - 2e_2^{\mathrm{BA}},
\end{aligned} \tag{7}$$

where e_2^{BA} is the DBER caused by two photons from Bob-to-Alice. Furthermore, we assume that $p_0 = p_1 = 1/2$ [20]. After cumbersome calculations, we can get that the eigenvalues of ρ_{BEA} are $\lambda_{1,2}^{\mathrm{BEA}} = 0$, $\lambda_{3,4}^{\mathrm{BEA}} = 1/4$, $\lambda_{5,6}^{\mathrm{BEA}} = (1 - 2e_2^{\mathrm{BA}})/4$, and

$\lambda_{7,8}^{\mathrm{BEA}} = 2e_2^{\mathrm{BA}}/4$. Therefore, $S(\rho_{\mathrm{BEA}}) = -\mathrm{Tr}(\rho_{\mathrm{BEA}}\log_2\rho_{\mathrm{BEA}}) = -\sum_i \lambda_i^{\mathrm{BEA}}\log_2(\lambda_i^{\mathrm{BEA}}) = 2 + h(2e_2)/2$, where $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy. According to Eq. (5), the maximum information that Eve can steal via the pulse containing two photons is

$$I(A{:}E)_{n=2} = \frac{1}{2}h(2e_2^{\mathrm{BA}}) + \frac{1}{2}. \tag{8}$$

One important conclusion we can draw from Eq. (8) is that the DL04 QSDC protocol [15] has the ability to defend against the PNS attack in the case of two photons, since $I(A{:}E)_{n=2}$ could be below one. The basic physics is that no basis announcement is required in QSDC for information decoding, while basis comparison is necessary for establishing the common secret keys in the BB84 QKD [3].

B. System Model

In order to analyze the practical QSDC experiment system, let us calculate $I(A{:}B)$ and $I(A{:}E)$ under the frame of Eve performing the general collective attack on a single photon and the PNS attack on multi-photons, considering the device and channel losses. Assume that α^{BA} and α^{BAB} are the channel attenuation of different paths BA and BAB, respectively. As can be seen in Fig. 4, Eve performs her eavesdropping after Alice finishes information encoding, which indicates $\alpha^{\mathrm{BAB}} = 2\alpha^{\mathrm{BA}}$. Thus, we have the channel transmissions as follows:

$$\begin{aligned} t^{\mathrm{BA}} &= 10^{-\left(\frac{\alpha^{\mathrm{BA}}}{10}\right)}, \\ t^{\mathrm{BAB}} &= 10^{-\left(\frac{\alpha^{\mathrm{BAB}}}{10}\right)}, \end{aligned} \tag{9}$$

and then the concomitant overall transmissions are given by

$$\begin{aligned} \eta^{\mathrm{BA}} &= t^{\mathrm{BA}}\eta_{\mathrm{opt}}^{\mathrm{BA}}\eta_D^A, \\ \eta^{\mathrm{BAB}} &= t^{\mathrm{BAB}}\eta_{\mathrm{opt}}^{\mathrm{BAB}}\eta_D^B, \end{aligned} \tag{10}$$

where $\eta_{\mathrm{opt}}^{\mathrm{BA}}$ and $\eta_{\mathrm{opt}}^{\mathrm{BAB}}$ are the specific devices' intrinsic optical losses, while η_D^A and η_D^B are the detection efficiency of Alice and Bob, respectively. The transmittances of n-photon state through different paths are $\eta_n^{\mathrm{BA}} = 1-(1-\eta^{\mathrm{BA}})^n$ and $\eta_n^{\mathrm{BAB}} = 1-(1-\eta^{\mathrm{BAB}})^n$. With Y_0^A and Y_0^B as background detection events of different parties, the yields become $Y_n^A = Y_0^A + \eta_n^{\mathrm{BA}} - \eta_n^{\mathrm{BA}}Y_0^A \approx Y_0^A + \eta_n^{\mathrm{BA}}$ and $Y_n^B \approx Y_0^B + \eta_n^{\mathrm{BAB}}$, and the overall signal gains and the error rates are given by [52]

$$\begin{aligned} Q_\mu^{\mathrm{BA}} &= \sum_{n=0}^{\infty} Q_{\mu,n}^{\mathrm{BA}} = \sum_{n=0}^{\infty} p(n,\mu)Y_n^A = Y_0^A + 1 - e^{-\eta^{\mathrm{BA}}\mu}, \\ Q_\mu^{\mathrm{BAE}} &= \sum_{n=0}^{\infty} Q_{\mu,n}^{\mathrm{BAE}} \le \sum_{n=0}^{\infty}\left[Q_{\mu,n}^{\mathrm{BA}} - p(n,\mu)Y_0^A\right]\max\left\{1, \frac{\gamma^E}{\gamma^A}\right\}, \\ Q_\mu^{\mathrm{BAB}} &= \sum_{n=0}^{\infty} Q_{\mu,n}^{\mathrm{BAB}} = \sum_{n=0}^{\infty} p(n,\mu)Y_n^B = Y_0^B + 1 - e^{-\eta^{\mathrm{BAB}}\mu}, \end{aligned} \tag{11}$$

and

$$\begin{aligned} E_\mu^{\mathrm{BA}} &= \frac{e_0 Y_0^A + e_{\mathrm{det}}^{\mathrm{BA}}(1-e^{-\eta^{\mathrm{BA}}\mu})}{Q_\mu^{\mathrm{BA}}}, \\ E_\mu^{\mathrm{BAB}} &= \frac{e_0 Y_0^B + e_{\mathrm{det}}^{\mathrm{BAB}}(1-e^{-\eta^{\mathrm{BAB}}\mu})}{Q_\mu^{\mathrm{BAB}}}, \end{aligned} \tag{12}$$

where $e_0 = 1/2$ is the error rate of background, $Q_{\mu,n}^{\mathrm{BA}}$ ($Q_{\mu,n}^{\mathrm{BAE}}$ and $Q_{\mu,n}^{\mathrm{BAB}}$) is the n-photon signal gain at Alice (Eve and Bob), and $e_{\mathrm{det}}^{\mathrm{BA}}$ and $e_{\mathrm{det}}^{\mathrm{BAB}}$ are intrinsic detector error rates which can be calculated by the visibilities V of the detection system: $e_{\mathrm{det}}^{\mathrm{BA}} = (1-V^{\mathrm{BA}})/2$ and $e_{\mathrm{det}}^{\mathrm{BAB}} = (1-V^{\mathrm{BAB}})/2$ [53]. The derivation of $Q_{\mu,n}^{\mathrm{BAE}}$ is given in Appendix A.

According to the theory of binary symmetric channel and binary erasure channel [54], the mutual information between Alice and Bob can be calculated as

$$I(A{:}B) = Q_\mu^{\mathrm{BAB}}[1 - h(E_\mu^{\mathrm{BAB}})], \tag{13}$$

where Q_μ^{BAB} is the overall signal gain of Bob after a round-trip BAB, and E_μ^{BAB} is the QBER. The secret information that Eve can obtain from a single photon by using the collective attack is [20,43]

$$I(A{:}E)_{n=1} = Q_{\mu,n=1}^{\mathrm{BAE}}h(2e_1^{\mathrm{BA}}), \tag{14}$$

where e_1^{BA} is the DBER caused by the single photon. Given the above, the lower bound of secrecy capacity is

$$\begin{aligned} C_s = {} & Q_\mu^{\mathrm{BAB}}[1 - h(E_\mu^{\mathrm{BAB}})] - Q_{\mu,n=1}^{\mathrm{BAE}}h(2e_1^{\mathrm{BA}}) \\ & - Q_{\mu,n=2}^{\mathrm{BAE}}\left[\frac{1}{2}h(2e_2^{\mathrm{BA}}) + \frac{1}{2}\right] - Q_{\mu,n\ge 3}^{\mathrm{BAE}}\cdot 1. \end{aligned} \tag{15}$$

Obviously, now we need to discuss how to evaluate the DBERs in Eq. (15) caused by single-photon (e_1^{BA}) states and two-photon (e_2^{BA}) states.

C. GLLP Theory

There is a pessimistic assumption in the GLLP theory [30]: all multi-photon signals could be detected by Alice and all errors originate from a single photon. Hence, the upper bound of e_1^{BA} is evaluated by

$$e_1^{\mathrm{BA}} = \frac{E_\mu^{\mathrm{BA}}}{1 - \frac{p(n\ge 2,\mu)}{Q_\mu^{\mathrm{BA}}}}, \tag{16}$$

where E_μ^{BA} is the DBER, and Q_μ^{BA} is the overall signal gain at Alice's terminal after the BA path. However, the GLLP theory cannot give us a real value of e_2^{BA}, in other words, $e_2^{\mathrm{BA}} = 0$ with its assumption. In this case, $I(A{:}E)_{n=2} = Q_{\mu,n=2}^{\mathrm{BAE}}\cdot(1/2)$ according to Eqs. (8) and (15), which means Eve can obtain a part of the secret information from the two-photon state by zero-DBER eavesdropping. Actually, it is a special case of our PNS attack. Eve intercepts one photon in the forward quantum channel but does nothing for the other and forwards it directly (no error rate here, $e_2^{\mathrm{BA}} = 0$). After Alice finishes secret information encoding, Eve intercepts the encoded photon and combines the intercepted two photons to read the secret information. Note that the PNS attack needs to be combined with the unambiguous state discrimination (USD) attack [55], namely, Eve obtains information by discriminating the states before and after Alice's encoding operation, since there

is no basis reconciliation in the DL04 QSDC protocol [15]. The upper bound on the maximum probability to discriminate two mixed states is 1/2 [56], which matches the above-mentioned result $I(A{:}E)_{n=2} = Q^{\mathrm{BAE}}_{\mu,n=2} \cdot (1/2)$ we have obtained under the PNS attack, in which the secret information Eve may steal from the two-photon state is 1/2 without considering her reception rate $Q^{\mathrm{BAE}}_{\mu,n=2}$. Based on the assumption of GLLP, the value of $Q^{\mathrm{BAE}}_{\mu,n=1} = Q^{\mathrm{BA}}_{\mu} - p(n \geq 2,\mu) - p(0,\mu)Y^A_0 - p(1,\mu)Y^A_0$, $Q^{\mathrm{BAE}}_{\mu,n=2} = p(2,\mu) - p(2,\mu)Y^A_0$, and $Q^{\mathrm{BAE}}_{\mu,n\geq 3} = p(n \geq 3,\mu) - p(n \geq 3,\mu)Y^A_0$ in GLLP can be estimated by combining the Eq. (A5) and the constraint of the first formula of Eq. (11) for maximizing $I(A{:}E)$.

D. Decoy-State Method

One way to beat the PNS attack in QKD is by utilizing decoy-state method [31–33]. This method also can be integrated into the DL04 QSDC [15], and we consider the decoy state here only for detecting the PNS attack, leaving the problem of whether it can be used to transmit secret information for future work. More importantly, the decoy state can provide a better estimation of the DBER. Bob randomly uses the signal source or the decoy source to prepare the initial states and sends them to Alice. Once these states are received by Alice, she randomly chooses some of them to publicly discuss with Bob for eavesdropping detection that is the same as Step (2) in Section 2.A. Bob announces where the decoy states are and then their transmission properties would be tested by Alice. It is impossible for Eve to discriminate which ones are the decoy states; in this way, if Eve still performs the PNS attack in the forward quantum channel, the counting rate of the system in path of BA will be inevitably disturbed. If Alice and Bob confirm that the forward quantum channel has not been tapped, Alice will use the remaining signal states for information encoding.

Much of the decoy-state research in the Scarani-Acin-Ribordy-Gisin 2004 (SARG 04) QKD protocol [57–60] has shown how the decoy-state method can be used to estimate the error rate caused by two photons. Inspired by these previous works, we use four decoy states: one vacuum state and three weak decoy states (ν_1, ν_2, and ν_3) to estimate our e^{BA}_2, so that the background rate can be estimated by the vacuum state, i.e., $Y^A_0 = Q^{\mathrm{BA}}_{\mathrm{vac}}$ and $e_0 = E^{\mathrm{BA}}_{\mathrm{vac}} = 1/2$. The upper bounds of single-photon DBER and two-photon DBER are, respectively, given by [60]

$$e^{\mathrm{BA},U}_1 = \frac{E^{\mathrm{BA}}_{\nu_3} Q^{\mathrm{BA}}_{\nu_3} e^{\nu_3} - e_0 Y^A_0}{Y^{A,L}_1 \nu_3}, \tag{17}$$

and

$$e^{\mathrm{BA},U}_2 = \frac{2\left(E^{\mathrm{BA}}_{\nu_2} Q^{\mathrm{BA}}_{\nu_2} e^{\nu_2} - \frac{\nu_2}{\nu_3} E^{\mathrm{BA}}_{\nu_3} Q^{\mathrm{BA}}_{\nu_3} e^{\nu_3} + \frac{\nu_2-\nu_3}{\nu_3} e_0 Y^A_0\right)}{Y^{A,L}_2 \nu_2(\nu_2 - \nu_3)}, \tag{18}$$

where

$$Y^{A,L}_1 = \frac{\mu^2(Q^{\mathrm{BA}}_{\nu_2} e^{\nu_2} - Q^{\mathrm{BA}}_{\nu_3} e^{\nu_3}) - (\nu_2^2 - \nu_3^2)(Q^{\mathrm{BA}}_{\mu} e^{\mu} - Y^A_0)}{\mu(\nu_2 - \nu_3)(\mu - \nu_2 - \nu_3)}, \tag{19}$$

and

$$Y^{A,L}_2 = \frac{2\mu(Q^{\mathrm{BA}}_{\nu_1} e^{\nu_1} - Q^{\mathrm{BA}}_{\nu_2} e^{\nu_2}) - 2(\nu_1 - \nu_2)(Q^{\mathrm{BA}}_{\mu} e^{\mu} - Y^A_0)}{\mu(\nu_1 - \nu_2)(\nu_1 + \nu_2 - \mu)}. \tag{20}$$

Furthermore, the above mean photon numbers μ, ν_1, ν_2, and ν_3 meet the following conditions:

$$\begin{aligned} &0 < \nu_3 < \nu_2 \leq \frac{2}{3}\mu < \nu_1 \leq \frac{3}{4}\mu, \\ &\nu_1 + \nu_2 > \mu, \\ &\nu_2 + \nu_3 < \mu, \\ &\nu_1 - \nu_2 - \frac{\nu_1^3 - \nu_2^3}{\mu^2} = 0. \end{aligned} \tag{21}$$

Results with explicit examples obtained from Eq. (15) are given in Fig. 6.

E. Performance Analysis

The devices' intrinsic optical losses are measured from our experimental setup. There is an altogether loss of 4.3 dB from PBS and PM. The attenuation of the short-arm optical link of the Mach–Zehnder interferometer is 2.3 dB. Suppose Eve's detection efficiency is $\eta^E_D = 100\%$ and without background detection events, while Alice and Bob utilize the superconducting single-photon detector with detection efficiency $\eta^A_D = \eta^B_D = 70\%$ and background detection events $Y^A_0 = Y^B_0 = 8 \times 10^{-8}$. $\gamma^A = (1-k) \times 10^{-2.3/10} \times 70\%$ and $\gamma^E = k \times 10^{-4.3/10} \times k \times 100\%$, where k originates from a $(1{-}k){:}k$ BS. Then, the overall device intrinsic optical losses of Alice and Bob are given by $\eta^{\mathrm{BA}}_{\mathrm{opt}} = (1-k) \times 10^{-2.3/10}$ and $\eta^{\mathrm{BAE}}_{\mathrm{opt}} = k^2 \times 10^{-6.6/10}$, respectively. The intrinsic detector error rates $e^{\mathrm{BA}}_{\mathrm{det}} = 1.31\%$ and $e^{\mathrm{BAB}}_{\mathrm{det}} = 0.26\%$ are deduced from system visibilities. Furthermore, the value of k is fixed by $\gamma^A = \gamma^E$. We then performed a numerical simulation to estimate the secrecy capacity under Eve's attacks with this setup in terms of maximum optical link attention.

Figure 5 shows the secrecy capacity of the free-space QSDC system with different mean photon numbers given by the GLLP theory. There is a trade-off between the secrecy capacity and the maximum tolerable attenuation. The maximum tolerable attenuation would be very small with the large mean photon numbers due to the high multi-photon probability in pulse, and it is susceptible to the PNS attack. However, it is infeasible to improve the maximum tolerable attenuation by reducing the mean photon numbers drastically on account of the decrease in the secrecy capacity. Hence, we choose the mean photon number $\mu = 0.01$ as the near-optimal value to highlight performance, as this is its preferable performance both in the secrecy capacity and in the maximum tolerable attenuation. Consequently, as shown in Fig. 5, the channel attenuation of secure communication against the collective attack as well as the PNS and USD attack for the QSDC system with realistic devices is less than 5.8 dB.

By contrast, as shown in Fig. 6, the secrecy capacity and the maximum tolerable attenuation can be greatly increased by using a decoy-state method. To be more specific, the maximum tolerable attenuation of decoy state method is 3.9 times that of GLLP. The results show that the decoy state can accu-

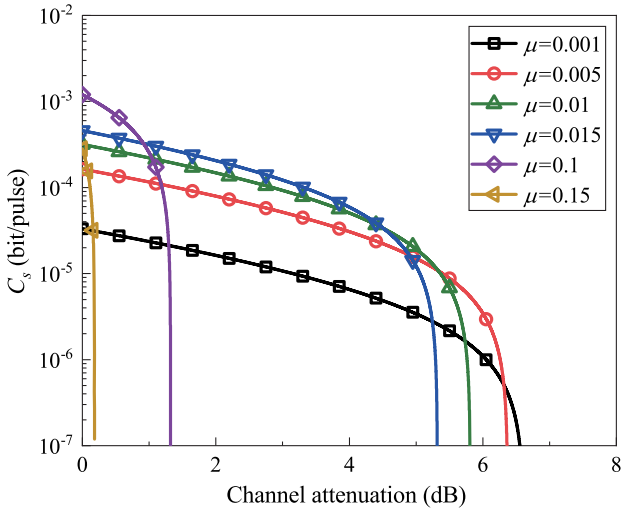

Fig. 5. Secrecy capacities versus the attenuation given the collective attack as well as the PNS and USD attack under the framework of GLLP analysis. The curves labeled by different markers represent the data with different mean photon numbers.

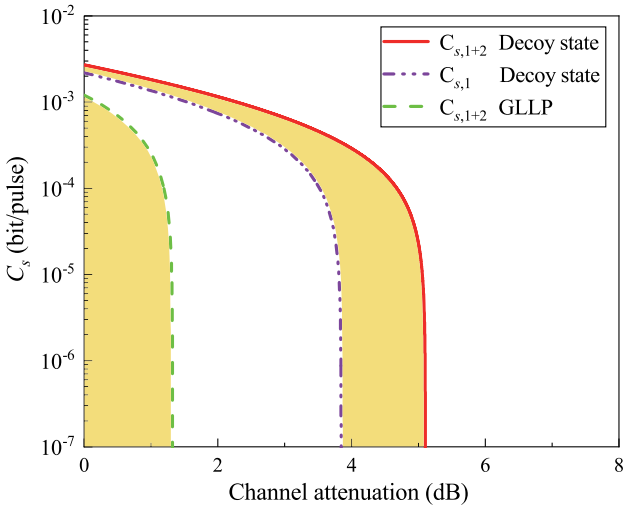

Fig. 6. Comparison of the secrecy capacities calculated by the GLLP theory and the decoy-state method. Simulations in the decoy-state method using $\mu = 0.1$, $\nu_1 = 0.07$, $\nu_2 = 0.0445$, and $\nu_3 = 0.03$ and in the GLLP theory using $\mu = 0.1$ are performed. In the secrecy capacity $C_{s,1+2}$, we have considered the contribution both from single-photon states and two-photon states, while $C_{s,1}$ has not considered the contribution from two-photon states. The two yellow areas represent the contribution of two-photon states to the secrecy capacity.

rately estimate the DBER caused by a single- and two-photon state in which it plays a positive role in improving communication performance, rather than the GLLP theory that gives a poor estimation. As seen in Fig. 6, the contribution of a two-photon state to the secrecy capacity cannot be completely disregarded, especially when the system is operated with a comparatively higher mean photon number. For GLLP, there is even no secrecy capacity at μ = 0.1 if the contribution of two-photon components has not been considered.

In clear weather conditions, when the typical atmosphere attenuation is 0.5–2 dB/km [61,62], it is feasible to exchange secret information by free-space QSDC based on phase encoding for two users over more than 1 km without using a decoy state, which is a typical distance between two terminals in a secure area. If the decoy-state method is applied, this secure communication distance could be further improved. One typical usage scenario would be applied in indoor environments for wireless communication, known as the quantum Li-Fi system [63].

5. CONCLUSIONS

We have constructed a free-space QSDC system based on phase encoding. The asymmetric Mach–Zehnder interferometers serve as transmitter and receiver with convincing fringe visibilities. The system can be operated to transmit text, picture, and audio, with a low average QBER of 0.49% ± 0.27%. This indicates the feasibility of phase encoding–based QSDC over a free-space channel. The security analysis of free-space QSDC has been given under the general collective attack on a single photon and the PNS attack on multi-photons, making a beneficial step to calculate the secrecy capacity of the QSDC system using a practical light source. Furthermore, the PNS attack is a general strategy that is applicable in explaining the previous PNS plus USD attack [56]. Our results show that the DL04 QSDC protocol is robust against the PNS attack in the depolarizing channel, and the secrecy capacity is increased significantly after considering the security of two-photon components, especially under the framework of a decoy state. As for future investigation, the effects of background light noise need to be considered in the free-space QSDC system. Decreasing the intrinsic loss of optical setups and optimizing the decoy-state method will be beneficial for long-distance transmission of QSDC over a free-space channel. It is worth mentioning that the phase drift of the photon must be carefully handled by the free-space QSDC system with phase encoding. Hence, the maximum communication distance of free-space QSDC with phase-encoding needs to be further investigated.

APPENDIX A

We can estimate $Q_{\mu,n}^{\mathrm{BAE}}$ from the value of $Q_{\mu,n}^{\mathrm{BA}}$, since they are related to the number of photons received by Alice. For n photons emitted by Bob, Alice actually receives m photons at her port BS after the forward quantum channel. The photon number distribution is $f_n = (m, \mu)$, which is no longer a Poissonian distribution under the PNS attack. The yields of Alice and Eve for these photons, are, respectively, given by

$$Y_n^A - Y_0^A = \sum_{m=0}^{\infty} f_n(m,\mu)\left\{1-\left(1-\gamma^A\right)^m - \left[1-\left(1-\gamma^A\right)^m\right] Y_0^A\right\}$$

$$\approx \sum_{m=0}^{\infty} f_n(m,\mu)\left[1-\left(1-\gamma^A\right)^m\right] \quad \textbf{(A1)}$$

and

$$Y_n^E = \sum_{m=0}^{\infty} f_n(m,\mu)\left\{1-\left(1-\gamma^E\right)^m - \left[1-\left(1-\gamma^E\right)^m\right]Y_0^E\right\} + Y_0^E$$
$$\approx \sum_{m=0}^{\infty} f_n(m,\mu)\left[1-\left(1-\gamma^E\right)^m\right], \quad \textbf{(A2)}$$

where γ^A is the overall transmission for photons received and then measured by Alice, γ^E is the overall transmission of Eve after Alice encodes her receiving photons, and $Y_0^E = 0$. Combining Eq. (A1) and Eq. (A2), the yield of Eve Y_n^E becomes

$$Y_n^E = (Y_n^A - Y_0^A)\frac{\sum_{m=0}^{\infty} f_n(m,\mu)\left[1-\left(1-\gamma^E\right)^m\right]}{\sum_{m=0}^{\infty} f_n(m,\mu)\left[1-\left(1-\gamma^A\right)^m\right]}$$
$$\le (Y_n^A - Y_0^A)\max\left\{1, \frac{\gamma^E}{\gamma^A}\right\}, \quad \textbf{(A3)}$$

where we have utilized the following mathematical property

$$\begin{cases} \dfrac{\sum_{m=0}^{\infty} f_n(m,\mu)\left[1-\left(1-\gamma^E\right)^m\right]}{\sum_{m=0}^{\infty} f_n(m,\mu)\left[1-\left(1-\gamma^A\right)^m\right]} \le 1 & \text{if } \gamma^A \ge \gamma^E, \\ \dfrac{\sum_{m=0}^{\infty} f_n(m,\mu)\left[1-\left(1-\gamma^E\right)^m\right]}{\sum_{m=0}^{\infty} f_n(m,\mu)\left[1-\left(1-\gamma^A\right)^m\right]} \le \dfrac{\gamma^E}{\gamma^A} & \text{if } \gamma^A < \gamma^E. \end{cases} \quad \textbf{(A4)}$$

The gains of the n-photon state of Alice and Eve are $Q_{\mu,n}^{\mathrm{BA}} = p(n,\mu)Y_n^A$ and $Q_{\mu,n}^{\mathrm{BAE}} = p(n,\mu)Y_n^E$, respectively. Hence, we have

$$Q_{\mu,n}^{\mathrm{BAE}} = p(n,\mu)Y_n^E \le \left[Q_{\mu,n}^{\mathrm{BA}} - p(n,\mu)Y_n^A\right]\max\left\{1, \frac{\gamma^E}{\gamma^A}\right\}. \quad \textbf{(A5)}$$

Funding. Government of Guangdong Province (2018B030325002); National Natural Science Foundation of China (11974205); Ministry of Science and Technology of the People's Republic of China (2017YFA0303700); Beijing Innovation Center for Future Chip.

Disclosures. The authors declare no conflicts of interest.

†These authors contributed equally to this paper.

REFERENCES

1. H. Sun, S. Liu, W. Lin, K. Y. Zhang, W. Lv, X. Huang, F. Huo, H. Yang, G. Jenkins, Q. Zhao, and W. Huang, "Smart responsive phosphorescent materials for data recording and security protection," Nat. Commun. **5**, 3601 (2014).
2. S. Cai, H. Shi, J. Li, L. Gu, Y. Ni, Z. Cheng, S. Wang, W.-W. Xiong, L. Li, Z. An, and W. Huang, "Visible-light-excited ultralong organic phosphorescence by manipulating intermolecular interactions," Adv. Mater. **29**, 1701244 (2017).
3. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, 1984), pp. 175–179.
4. S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, D.-J. Huang, L.-J. Zhang, F.-Y. Li, D. Liu, Y.-G. Wang, G.-C. Guo, and Z.-F. Han, "Field test of wavelength-saving quantum key distribution network," Opt. Lett. **35**, 2454–2456 (2010).
5. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD network," Opt. Express **19**, 10387–10409 (2011).
6. S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, "Field and long-term demonstration of a wide area quantum key distribution network," Opt. Express **22**, 21739–21756 (2014).
7. H.-Y. Liu, X.-H. Tian, C. Gu, P. Fan, X. Ni, R. Yang, J.-N. Zhang, M. Hu, J. Guo, X. Cao, X. Hu, G. Zhao, Y.-Q. Lu, Y.-X. Gong, Z. Xie, and S.-N. Zhu, "Drone-based entanglement distribution towards mobile quantum networks," Natl. Sci. Rev. **7**, 921–928 (2020).
8. W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Practical free-space quantum key distribution over 1 km," Phys. Rev. Lett. **81**, 3283–3286 (1998).
9. J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, C. J. Williams, E. W. Hagley, and J. Wen, "Quantum key distribution with 1.25 Gbps clock synchronization," Opt. Express **12**, 2011–2016 (2004).
10. T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," Phys. Rev. Lett. **98**, 010504 (2007).
11. R. Tannous, Z. Ye, J. Jin, K. B. Kuntz, N. Lütkenhaus, and T. Jennewein, "Demonstration of a 6 state-4 state reference frame independent channel for quantum key distribution," Appl. Phys. Lett. **115**, 211103 (2019).
12. S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," Nature **549**, 43–47 (2017).
13. G.-L. Long and X.-S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," Phys. Rev. A **65**, 032302 (2002).
14. 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).
15. F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," Phys. Rev. A **69**, 052319 (2004).
16. 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).
17. 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).
18. 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).
19. F. Zhu, W. Zhang, Y. Sheng, and Y. Huang, "Experimental long-distance quantum secure direct communication," Sci. Bull. **62**, 1519–1524 (2017).
20. R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G.-L. Long, "Implementation and security analysis of practical quantum secure direct communication," Light Sci. Appl. **8**, 22 (2019).
21. A. M. Marino and C. Stroud, Jr., "Deterministic secure communications using two-mode squeezed states," Phys. Rev. A **74**, 022315 (2006).
22. J. H. Shapiro, Z. Zhang, and F. N. Wong, "Secure communication via quantum illumination," Quantum Inf. Process. **13**, 2171–2193 (2014).
23. S. Pirandola, S. L. Braunstein, S. Mancini, and S. Lloyd, "Quantum direct communication with continuous variables," Europhys. Lett. **84**, 20013 (2008).

24. S. Pirandola, S. L. Braunstein, S. Lloyd, and S. Mancini, "Confidential direct communications: a quantum approach using continuous variables," IEEE J. Sel. Top. Quantum Electron. **15**, 1570–1580 (2009).
25. D. J. Lum, J. C. Howell, M. S. Allman, T. Gerrits, V. B. Verma, S. W. Nam, C. Lupo, and S. Lloyd, "Quantum enigma machine: experimentally demonstrating quantum data locking," Phys. Rev. A **94**, 022315 (2016).
26. 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).
27. 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**, 1345–1350 (2018).
28. Z. Gao, T. Li, and Z. Li, "Long-distance measurement-device-independent quantum secure direct communication," Europhys. Lett. **125**, 40004 (2019).
29. L. Zhou, Y.-B. Sheng, and G.-L. Long, "Device-independent quantum secure direct communication against collective attacks," Sci. Bull. **65**, 12–20 (2019).
30. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quantum Inf. Comput. **4**, 325–360 (2004).
31. W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," Phys. Rev. Lett. **91**, 057901 (2003).
32. X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).
33. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
34. F.-G. Deng and G. L. Long, "Bidirectional quantum key distribution protocol with practical faint laser pulses," Phys. Rev. A **70**, 012311 (2004).
35. M. Lucamarini and S. Mancini, "Secure deterministic communication without entanglement," Phys. Rev. Lett. **94**, 140501 (2005).
36. H. Lu, "Ambiguous discrimination among linearly dependent quantum states and its application to two-way deterministic quantum key distribution," J. Opt. Soc. Am. B **36**, B26–B30 (2019).
37. Q. Zhou, R. Valivarthi, C. John, and W. Tittel, "Practical quantum random-number generation based on sampling vacuum fluctuations," Quantum Eng. **1**, e8 (2019).
38. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "'Plug and play' systems for quantum cryptography," Appl. Phys. Lett. **70**, 793–795 (1997).
39. S. Wang, W. Chen, Z.-Q. Yin, D.-Y. He, C. Hui, P.-L. Hao, G.-J. Fan-Yuan, C. Wang, L.-J. Zhang, J. Kuang, S.-F. Liu, Z. Zhou, Y.-G. Wang, G.-C. Guo, and Z.-F. Han, "Practical gigahertz quantum key distribution robust against channel disturbance," Opt. Lett. **43**, 2030–2033 (2018).
40. A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," IEEE Trans. Inf. Theory **53**, 2933–2945 (2007).
41. A. D. Wyner, "The wire-tap channel," Bell System Tech. J. **54**, 1355–1387 (1975).
42. M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," Nat. Commun. **3**, 634 (2012).
43. H. Lu, C.-H. F. Fung, X. Ma, and Q.-Y. Cai, "Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel," Phys. Rev. A **84**, 042344 (2011).
44. C. I. Henao and R. M. Serra, "Practical security analysis of two-way quantum-key-distribution protocols based on nonorthogonal states," Phys. Rev. A **92**, 052317 (2015).
45. J. Wu, Z. Lin, L. Yin, and G.-L. Long, "Security of quantum secure direct communication based on Wyner's wiretap channel theory," Quantum Eng. **1**, e26 (2019).
46. Y. Feng, R. Duan, and M. Ying, "Unambiguous discrimination between mixed quantum states," Phys. Rev. A **70**, 012308 (2004).
47. A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," Probl. Inf. Trans. **9**, 177–183 (1973).
48. R. Jozsa and J. Schlienz, "Distinguishability of states and von Neumann entropy," Phys. Rev. A **62**, 012301 (2000).
49. W. O. Krawec, "Quantum key distribution with mismatched measurements over arbitrary channels," Quantum Inf. Comput. **17**, 209–241 (2017).
50. M. Christandl, R. Renner, and A. Ekert, "A generic security proof for quantum key distribution," arXiv:quant-ph/0402131 (2004).
51. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301–1350 (2009).
52. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**, 012326 (2005).
53. X. Ma and H.-K. Lo, "Quantum key distribution with triggering parametric down-conversion sources," New J. Phys. **10**, 073018 (2008).
54. D. J. C. MacKay, *Information Theory, Inference and Learning Algorithms* (Cambridge University, 2003).
55. S. Zhang and M. Ying, "Set discrimination of quantum states," Phys. Rev. A **65**, 062322 (2002).
56. S. Lin, Q.-Y. Wen, F. Gao, and F.-C. Zhu, "Eavesdropping on secure deterministic communication with qubits through photon-number-splitting attacks," Phys. Rev. A **79**, 054303 (2009).
57. V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," Phys. Rev. Lett. **92**, 057901 (2004).
58. C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance of two quantum-key-distribution protocols," Phys. Rev. A **73**, 012337 (2006).
59. S. L. Zhang, X. Zou, K. Li, C. Jin, and G. C. Guo, "Limitation of decoy-state Scarani-Acin-Ribordy-Gisin quantum-key-distribution protocols with a heralded single-photon source," Phys. Rev. A **76**, 044304 (2007).
60. J.-B. Li and X.-M. Fang, "Nonorthogonal decoy-state quantum key distribution," Chin. Phys. Lett. **23**, 768–775 (2006).
61. I. I. Kim and E. J. Korevaar, "Availability of free-space optics (FSO) and hybrid FSO/RF systems," Proc. SPIE **4530**, 84–95 (2001).
62. A. Carrasco-Casado, N. Denisenko, and V. Fernandez, "Correction of beam wander for a free-space quantum key distribution system operating in urban environment," Opt. Eng. **53**, 084112 (2014).
63. O. Elmabrok and M. Razavi, "Wireless quantum key distribution in indoor environments," J. Opt. Soc. Am. B **35**, 197–207 (2018).