


Device-Independent Quantum Secure Direct Communication with Single-Photon Sources

Lan Zhou,¹ Bao-Wen Xu,^{1,2} Wei Zhong,³ and Yu-Bo Sheng^{2,3,*}

¹College of Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

²College of Electronic and Optical Engineering, & College of Flexible Electronics (Future Technology), Nanjing University of Posts and Telecommunications, Nanjing 210023, China

³Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

 (Received 14 June 2022; revised 22 August 2022; accepted 9 December 2022; published 11 January 2023)

Quantum secure direct communication (QSDC) can directly transmit secret messages through a quantum channel. Device-independent (DI) QSDC can guarantee the communication security relying only on the observation of the Bell-inequality violation, but not on any detailed description or trust of the inner workings of users' devices. In the paper, we propose a DI-QSDC protocol with practical highly efficient single-photon sources. The communication parties construct the entanglement channel from single photons by adopting the heralded architecture, which makes the message-leakage rate independent of the photon-transmission loss. The secure communication distance and the practical communication efficiency of the current DI-QSDC protocol are about 6 times and 600 times of those in the original DI-QSDC protocol. Combining with the entanglement purification, the parties can construct the nearly perfect entanglement channel and completely eliminate the message leakage. This DI-QSDC protocol may have useful applications in the future quantum communication field.

DOI: [10.1103/PhysRevApplied.19.014036](https://doi.org/10.1103/PhysRevApplied.19.014036)

I. INTRODUCTION

Quantum secure communication, based on intrinsic properties of quantum systems, can guarantee the absolute security of communication. Quantum key distribution and quantum secure direct communication (QSDC) are two branches of quantum secure communication. Quantum key distribution can distribute secure keys between the sender and the receiver, which was proposed in 1984 [1]. Quantum key distribution has been widely investigated in both theory and experiment [2–21]. QSDC allows the message sender to directly transmit secret messages to the receiver without keys [22–47]. The QSDC protocol was proposed firstly in 2000 [22]. Later, the typical entanglement-based two-step QSDC protocol and single-photon-based QSDC protocol were successively proposed [23,24], which were experimentally demonstrated in 2016 and 2017, respectively [26,27]. In 2020, the device-independent (DI) QSDC and measurement-device-independent QSDC protocols were put forward, which can guarantee QSDC's security under practical experimental condition [30,31]. In 2022, the one-step QSDC was put forward, which can simplify the operation and reduce the message loss [44]. In the last few years, QSDC has made great experimental progress. In

2021, a 15-user QSDC network with any two users being 40-km apart was demonstrated [39]. Recently, researchers achieved the QSDC over 100-km fiber with time-bin and phase quantum states [41].

Similar to DI quantum key distribution [48–55], DI-QSDC relaxes conventional assumptions on devices and allows users to transmit secret messages with unknown and uncharacterized devices. As long as some minimal assumptions (the quantum physics is correct and no unwanted signal can escape from the communication parties' laboratories) are satisfied, DI-QSDC can guarantee the communication security based solely on the observed data conclusively violating the Bell inequality [typically, the Clauser-Horne-Shimony-Holt (CHSH) inequality] [56–58]. The observation of the CHSH inequality violation should close the so-called detection loophole [56]. Although recent advances on single-photon detector have achieved the detection efficiency close to 1 [59,60], DI-QSDC still faces big challenges. On one hand, the original DI-QSDC protocol requires the entanglement photon source and constructs the entanglement channel by the long-distance entanglement distribution. The entanglement generation of practical entanglement source (spontaneous parametric down-conversion source) is probabilistic and the double-pair emission cannot be eliminated [61–63]. On the other hand, the experimental devices and

*shengyb@njupt.edu.cn

quantum channel are imperfect, which may cause photon loss. Photon loss occurring at the generation, transmission, and detection stages would deteriorate the nonlocal correlations between the photons. The above two features provide an opportunity for the eavesdropper (Eve) to steal some photons without being detected and largely reduce the secure communication distance.

Actually, comparing with the spontaneous parametric down-conversion source, the practical single-photon sources have already allowed for nearly on-demand [64], highly efficient [65] extraction of single photons (also in pulse trains [66,67] as well as at telecom wavelengths [68]). Current single-photon sources can maintain the purity and indistinguishability of the generated photons with the probability of above 99% [69,70]. In 2020, Long *et al.* reported an experimental implementation of free-space QSDC based on single-photon sources with the repetition rate of 16 MHz [33]. In 2022, a high-fidelity photonic quantum logic gate based on near-optimal Rydberg single-photon source was realized. The excitation frequencies of the 780- and 479-nm laser pulses reach $\Omega_{780}^e/2\pi \approx 6.4$ MHz and $\Omega_{479}^e/2\pi \approx 4.2$ MHz, respectively [71]. Soon later, a single-photon source at the telecom wavelength based on InAs/GaAs quantum dots was reported. This single-photon source has the bright single-photon emission with Purcell factor > 5 and count rates up to 10 MHz [72]. Meanwhile, the heralded architectures have been used to construct the entanglement channel, which can eliminate the influence from photon-transmission loss on the Bell (CHSH) violations [50]. In 2020, two DI quantum key distribution schemes were proposed, which realized the entanglement creation process with single-photon sources [55], and distributed keys at high rates over large distance. In this work, we propose a DI-QSDC protocol based on single-photon sources and the heralded Bell state measurement (BSM). Comparing with original DI-QSDC protocol, this current DI-QSDC protocol can efficiently increase the practical communication efficiency and communication distance.

The paper is organized as follows. In Sec. II, we introduce the heralded long-distance entanglement distribution based on single-photon sources. In Sec. III, we explain the DI-QSDC protocol in detail. In Sec. IV, we provide the security analysis and calculate the secrecy message capacity and practical communication efficiency of the DI-QSDC protocol against collective attacks. In Sec. V, we make a discussion and finally provide a conclusion.

II. HERALDED LONG-DISTANCE ENTANGLEMENT DISTRIBUTION BASED ON SINGLE-PHOTON SOURCES

We explain the construction of the long-distance entanglement channel based on the single-photon sources [73]. From Refs. [64–72], we can treat the single-photon sources

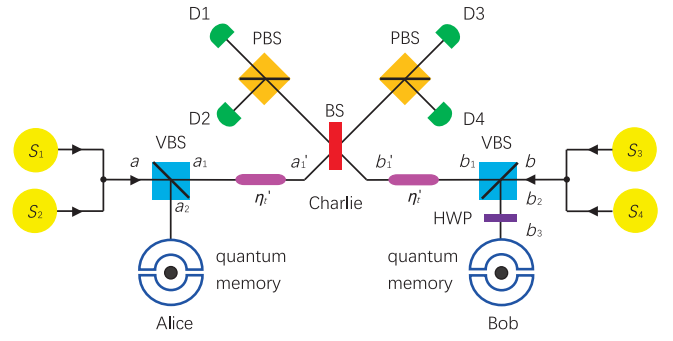


FIG. 1. The basic principle of constructing the long-distance entanglement channel between Alice and Bob with the help of the heralded architecture. Here, S_i ($i = 1, 2, 3, 4$) represents the single-photon source. The generated photons pass through a variable beam splitter (VBS). After the VBS, the photons in the transmitted port of the VBSs are sent to Charlie for the Bell-state measurement (BSM). η_i' represents the photon-transmission efficiency corresponding to the distance $L_{A(B)C}$ between Alice (Bob) and Charlie. BS and PBS represent the 50:50 beam splitter and polarization beam splitter, respectively. HWP represents the half-wave plate.

as the on-demand sources. In contrast, the practical spontaneous parametric down-conversion source adopted in the original DI-QSDC protocol [30] can generate the mixed state as [61]

$$\rho_0 \approx (1 - p - p^2)|\text{vac}\rangle\langle\text{vac}| + p|\phi\rangle\langle\phi| + p^2|\phi^{\otimes 2}\rangle\langle\phi^{\otimes 2}|, \quad (1)$$

where $|\text{vac}\rangle$ means the vacuum state, $|\phi\rangle = 1/\sqrt{2}(|HH\rangle + |VV\rangle)$. The desired entangled photon pair generates at the order of p ($p \sim 10^{-5} - 10^{-3}$) [63]. Meanwhile, the double pair emission is unavoidable.

As shown in Fig. 1, Alice (Bob) adopts two single-photon sources S_1 and S_2 (S_3 and S_4) to prepare two single photons with the horizontal polarization ($|H\rangle$) and the vertical polarization ($|V\rangle$), respectively.

Then, each of the two parties passes his photons through a variable beam splitter (VBS) with the transmittance of T , which makes the photon states in Alice's and Bob's locations evolve to

$$\begin{aligned} |\phi_1\rangle &= |H\rangle_a \otimes |V\rangle_a \\ &\rightarrow (\sqrt{T}|H\rangle_{a_1} + \sqrt{1-T}|H\rangle_{a_2}) \\ &\quad \otimes (\sqrt{T}|V\rangle_{a_1} + \sqrt{1-T}|V\rangle_{a_2}), \\ |\phi_2\rangle &= |H\rangle_b \otimes |V\rangle_b \\ &\rightarrow (\sqrt{T}|H\rangle_{b_1} + \sqrt{1-T}|H\rangle_{b_2}) \\ &\quad \otimes (\sqrt{T}|V\rangle_{b_1} + \sqrt{1-T}|V\rangle_{b_2}). \end{aligned} \quad (2)$$

Alice and Bob send the photon in a_1 and b_1 modes to a third party Charlie for the BSM. The BSM devices are totally

in linear optics, which can only distinguish $|\psi^\pm\rangle_{a'_1b'_1}$. In detail, a click in $D1D2$, or $D3D4$ indicates a projection into $|\psi^+\rangle_{a'_1b'_1}$, and a click in $D2D3$, or $D1D4$ projects the quantum state into $|\psi^-\rangle_{a'_1b'_1}$ [73]. Then, Bob passes the reflected photon in b_2 mode through the half-wave plate. Next, the photon in a_2 and b_3 modes are stored in the quantum memory devices. The experimental realizations of the quantum memory in the single-photon level with the electromagnetically induced transparency have been reported since 2013 [74,75]. It is noticeable that the quantum memory can herald the existence of the photon in the reflected port. Only when the BSM is successful and the quantum memory in each party's location responds, the distant parties can share the entangled state. Otherwise, the entanglement distribution will fail. In this way, only the case that one photon transmits the VBS and the other photon is reflected by the VBS in each party's location may lead to the success of the entanglement distribution. We define the photon-transmission efficiency $\eta'_t = 10^{-\alpha L_{A(B)C}/10}$ [76] corresponding to the distance $L_{A(B)C}$ between Alice (Bob) and Charlie, where $\alpha = 0.2$ dB/km. If the transmitted photons lose during the transmission process, the BSM cannot obtain the successful detector response. As a result, for obtaining the successful entanglement distribution, the state $|\phi_1\rangle \otimes |\phi_2\rangle$ will collapse to

$$\begin{aligned} |\Phi_1\rangle &= \sqrt{\eta'_t T(1-T)}(|HV\rangle_{a'_1a_2} + |VH\rangle_{a'_1a_2}) \\ &\quad \otimes \sqrt{\eta'_t T(1-T)}(|HV\rangle_{b'_1b_2} + |VH\rangle_{b'_1b_2}) \\ &= \eta'_t T(1-T)(|HH\rangle_{a'_1b'_1}|VV\rangle_{a_2b_2} + |VH\rangle_{a'_1b'_1}|HV\rangle_{a_2b_2} \\ &\quad + |HV\rangle_{a'_1b'_1}|VH\rangle_{a_2b_2} + |VV\rangle_{a'_1b'_1}|HH\rangle_{a_2b_2}) \\ &= \frac{\eta'_t T(1-T)}{\sqrt{2}}(|\phi^+\rangle_{a'_1b'_1}|\phi^+\rangle_{a_2b_2} - |\phi^-\rangle_{a'_1b'_1}|\phi^-\rangle_{a_2b_2} \\ &\quad + |\psi^+\rangle_{a'_1b'_1}|\psi^+\rangle_{a_2b_2} - |\psi^-\rangle_{a'_1b'_1}|\psi^-\rangle_{a_2b_2}), \quad (3) \end{aligned}$$

where $|\phi^\pm\rangle$ and $|\psi^\pm\rangle$ represent the polarization Bell states with the form of

$$\begin{aligned} |\phi^\pm\rangle &= \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle), \\ |\psi^\pm\rangle &= \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle). \quad (4) \end{aligned}$$

We define the total photon-transmission efficiency $\eta_t = \eta_t'^2 = 10^{-0.2L_{AB}/10}$ for simplicity.

As shown in Eq. (3), if the BSM result is $|\psi^+\rangle_{a'_1b'_1}$, $|\Phi_1\rangle$ will collapse to $|\psi^+\rangle_{a_2b_2}$, which can be transformed to $|\phi^+\rangle_{a_2b_3}$ after the photon in b_2 passing through the half-wave plate. If the BSM result is $|\psi^-\rangle_{a'_1b'_1}$, $|\Phi_1\rangle$ will collapse to $|\psi^-\rangle_{a_2b_2}$, which can be transformed to $|\phi^-\rangle_{a_2b_3}$ after the half-wave plate. $|\phi^-\rangle_{a_2b_3}$ can be further transformed to $|\phi^+\rangle_{a_2b_3}$ after the phase-flip operation. As a

result, when the BSM is successful and the quantum memory in each party's location responds, Alice and Bob can deterministically obtain the pure output quantum state $|\phi^+\rangle_{a_2b_3}$ and the photon-transmission loss case can be automatically eliminated. The probability of obtaining the successful entanglement distribution can be calculated as

$$P_1 = \eta_t'^2 T^2 (1-T)^2 = \eta_t T^2 (1-T)^2. \quad (5)$$

It can be easily found that P_1 can reach the maximal value of $\eta_t/8$ when $T = 0.5$.

III. THE DI-QSDC PROTOCOL WITH SINGLE-PHOTON SOURCES

The security of the current DI-QSDC protocol can be guaranteed by only two fundamental assumptions. First, the quantum physics is correct and Eve obeys the rules of quantum physics. Second, Alice's and Bob's physical locations are secure, say, no unwanted information can leak to the outside. The basic principle of the DI-QSDC protocol is shown in Fig. 2.

Step 1: Alice and Bob construct the entanglement channel based on the principle in Sec. II. In detail, Alice and Bob each prepare ordered N (N is large) photon pairs in the state of $|H\rangle \otimes |V\rangle$ from the on-demand single-photon sources. Each of them passes the photons through a VBS. The photons in the reflected ports construct the S_{A1} and S_{B1} sequences, and those in the transmitted ports construct the S_{A2} and S_{B2} sequences. As shown in Fig. 1, Alice and Bob send the photons in S_{A2} and S_{B2} sequences to Charlie for the BSM and store the photons in S_{A1} and S_{B1} sequences in the quantum memory devices. Only when the BSM is successful and each quantum memory responds, the photons in the S_{A1} and S_{B1} sequences can finally evolve to $|\phi^+\rangle$. Otherwise, Alice and Bob discard the photons in S_{A1} and S_{B1} sequences. In this way, Alice and Bob can deterministically construct the entanglement channel in $|\phi^+\rangle$ with N_1 entangled photon pairs, where $N_1 = P_1 N$ in theory.

Step 2: To ensure the security of the photon transmission, Alice randomly selects some photons in the S_{A1} sequence as the security checking photons and announces their positions to Bob through a public channel. They extract the security checking photons from the quantum memories to make the first round of DI security checking. In detail, for each security checking photon, Alice has four possible measurement bases $A_0 = \sigma_z$, $A_1 = (\sigma_z + \sigma_x)/\sqrt{2}$, $A_2 = (\sigma_z - \sigma_x)/\sqrt{2}$, and $A_3 = \sigma_x$, and Bob has two possible measurement bases $B_1 = A_0$ and $B_2 = A_3$ [53,54]. All the measurement results $a = \{a_0, a_1, a_2, a_3\}$ and $b = \{b_1, b_2\}$ have binary outcome “+1” or “-1.” Without loss of generality, we suppose that the marginal of all the measurements are random, such as $\langle a_i \rangle = \langle b_j \rangle = 0$ ($i \in \{0, 1, 2, 3\}, j \in \{1, 2\}$). If the parties obtain the inconclusive result (the photon detectors click no photon), the measurement result is set to be “+1” or “-1” randomly. After all

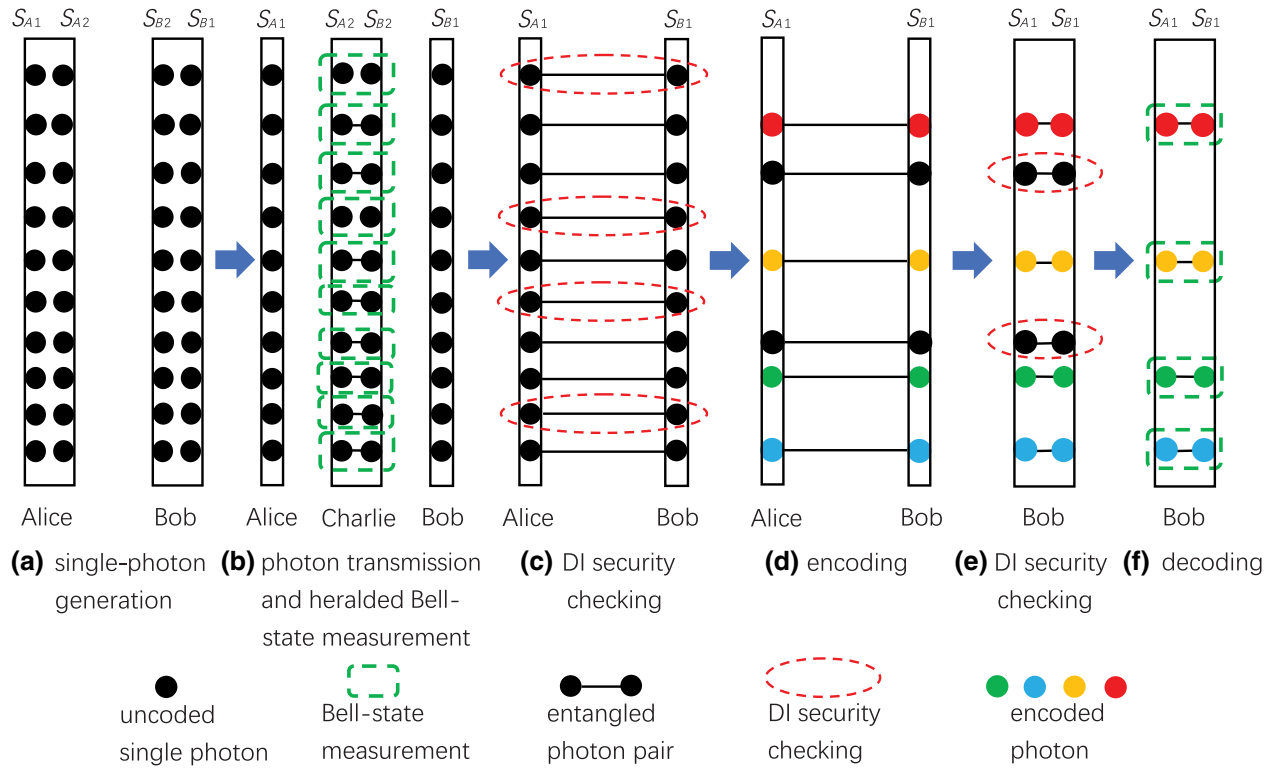


FIG. 2. Schematic principle of the DI-QSDC protocol. In the protocol, Alice and Bob prepare single-photon sequences with orthogonal polarizations $|H\rangle$ and $|V\rangle$, respectively. They construct the entanglement channels by the heralded architecture. Then, Alice encodes the messages by two unitary operations and sends the encoded photons to Bob. After the photon transmission, Bob performs the BSM on each photon pair and can finally read out the encoded secure messages. The security of both photon-transmission processes are guaranteed by the DI security checking.

the checking photon pairs have been measured, Alice and Bob announce their measurement bases and measurement results.

There are four different cases. In the first case, if Alice chooses A_1 or A_2 basis, their measurement results are used to estimate the CHSH polynomial as

$$S_1 = \langle a_1 b_1 \rangle + \langle a_1 b_2 \rangle + \langle a_2 b_1 \rangle - \langle a_2 b_2 \rangle, \quad (6)$$

where $\langle a_i b_j \rangle$ is defined as $P(a_i = b_j) - P(a_i \neq b_j)$ (the probability of $a_i = b_j$ minus the probability of $a_i \neq b_j$). In the second case, if Alice chooses A_0 and Bob chooses B_1 , their measurement results are used to estimate the quantum bit-flip error rate Q_{b1} as

$$Q_{b1} = P(a_0 \neq b_1). \quad (7)$$

Third, if Alice chooses A_3 and Bob chooses B_2 , their measurement results are used to estimate the quantum phase-flip error rate Q_{p1} as

$$Q_{p1} = P(a_3 \neq b_2). \quad (8)$$

In the last case, if Alice chooses A_0 and Bob chooses B_2 , or Alice chooses A_3 and Bob chooses B_1 , their measurement results should be discarded.

If $S_1 \leq 2$ (the CHSH inequality), the measurement results from Alice and Bob are classically correlated. Under this case, there exists a trivial attack for Eve to eavesdrop photons without being detected, so that the first photon-transmission process is not secure and the parties have to discard the communication. If $S_1 > 2$, Alice's and Bob's measurement results are non-locally correlated, and they can bound Eve's photon interception rate. If S_1 reaches the maximal value of $2\sqrt{2}$, Alice and Bob share the maximally entangled state $|\phi^+\rangle_{AB}$. In this case, Eve cannot intercept any photon without being detected. As a result, when $2 < S_1 \leq 2\sqrt{2}$, Alice and Bob ensure that the first photon-transmission process is secure and go on to the next step.

Step 3: Alice extracts the other stored photons in S_{A1} sequence from the quantum memory and encodes her message on them by performing two unitary operations U_0 or U_1 . The two unitary operations have the form of

$$\begin{aligned} U_0 &= \sigma_x = |V\rangle\langle H| + |H\rangle\langle V|, \\ U_1 &= i\sigma_y = |H\rangle\langle V| - |V\rangle\langle H|, \end{aligned} \quad (9)$$

which can transform $|\phi^+\rangle$ to $|\psi^+\rangle$ and $|\psi^-\rangle$, respectively. Alice can encode her messages "0" and "1" on the

photon pairs by performing U_0 and U_1 , respectively. Meanwhile, Alice randomly selects some photons as the security checking photons for the second photon-transmission round and does not perform any operation on them. For preventing Eve to precisely intercept the corresponding encoded photons during the second photon-transmission process according to her intercepted photons in the first photon-transmission process, Alice messes up her photons in sequence S_{A1} and records the position of each photon in the original sequence.

Step 4: Alice successively sends all the photons in S_{A1} sequence to Bob. After the photon transmission, Alice announces the position of each photon in the original S_{A1} sequence by a public channel. Bob stores all the photons into the quantum memory devices and recovers the original photon sequence. Next, Alice announces the positions of the security checking photons and Bob extracts the security checking photon pairs in S_{A1} and S_{B1} sequences to make the second round of DI security checking by himself. After the measurements, Bob can estimate the CHSH polynomial S_2 , the bit-flip error rate Q_{b2} , and the phase-flip error rate Q_{p2} . Similar as the first round of security checking, when $S_2 \leq 2$, the second photon-transmission process is not secure and the parties should discard the communication. When $2 < S_2 \leq 2\sqrt{2}$, they ensure that the second photon-transmission process is secure and go on to the next step.

Step 5: Bob extracts all the other photon pairs from the memory devices and makes the BSM on each of them. His BSM devices are the same as those in Charlie's location, which can distinguish only $|\psi^+\rangle$ and $|\psi^-\rangle$. After the measurement, Bob can read out the encoded messages by comparing his measurement results with the initial entangled state $|\phi^+\rangle$. For example, if the BSM result is $|\psi^+\rangle$, Bob can deduce that Alice performs U_0 operation, so that the encoded message is "0." If the BSM result is $|\psi^-\rangle$, Bob can obtain that Alice performs U_1 on the photon pair and the encoded message is "1."

IV. SECURITY AND COMMUNICATION QUALITY OF THE DI-QSDC PROTOCOL AGAINST COLLECTIVE ATTACKS

In the device-independent scenario, Eve is required only to obey the laws of quantum physics. In both two security checking processes, Alice and Bob can only use the observed correlations between the measurement basis (input) and the measurement result (outcome) to bound Eve's knowledge. We consider a general attack, namely, collective attack, where Eve applies the same attack on each system of Alice and Bob. As a result, after the photon transmission, all the photon pairs have the same form. We also assume that each party's measurement result is only a function of the current inputs.

We define that the secret message capacity C_s is the amount of transmitted correct and secure qubits divided by the total amount of the encoded photon pairs. Although we have specified a particular state in the DI-QSDC protocol to produce these correlations, we do not assume anything about the implementation of the correlations when computing the secret message capacity.

We first consider the ideal scenario, including the ideal devices and channels. If there is no eavesdropping, the CHSH polynomials in both security checking processes can reach the maximal value of $2\sqrt{2}$, and the bit-flip and phase-flip error rates are zero. In this case, any eavesdropping during the photon-transmission processes would reduce the CHSH polynomials and increase the error rates, so that the eavesdropping can be easily detected. As a result, in the ideal scenario, Eve cannot eavesdrop any photon without being detected. As each encoded photon pair can transmit 1 bit of message, the value of C_s equals 1.

Next, we consider the practical scenario, including the practical devices and noisy channels. For collective attacks, the secret message capacity from Alice to Bob is lower bounded by the Devetak-Winter rate [48,49] as

$$C_s \geq I_{AB} - I_{AE}, \quad (10)$$

where I_{AB} and I_{AE} represent the mutual information between Alice and Bob, and the mutual information between Alice and Eve, respectively. Since we assume uniform marginal, the mutual information between Alice and Bob is given by [48,49]

$$I_{AB} = 1 - H(Q_t), \quad (11)$$

where Q_t is the total error rate after two rounds of photon transmission, and $H(x)$ is the binary entropy with the form of

$$H(x) = -x\log_2 x - (1-x)\log_2(1-x). \quad (12)$$

In the practical scenario, we consider the photon loss and decoherence. The photon loss can be divided into two categories, say, the transmission loss and local loss. The transmission loss represents the photon loss occurring in the transmission process. We provide the photon-transmission efficiency $\eta_t = 10^{-0.2L_{AB}/10}$ in Sec. II. The local loss represents all the photon loss occurring within the users' laboratories [55]. As the DI-QSDC requires the quantum memory devices, we have to consider the finite photon-extraction efficiency of the quantum memory. In this way, we define the local efficiency η_l as the product of the coupling efficiency η_c between the photon and the fiber, the efficiency η_m of the quantum memory, and the detection efficiency of the photon detector η_d ($\eta_l = \eta_c\eta_m\eta_d$). To our knowledge, the known DI protocols all require a high local efficiency, i.e., above 90% [50,52,54]. According to Sec. II,

after the first round of photon transmission, the photon-transmission-loss case can be eliminated with the help of the heralded architecture, but the local loss and decoherence still exist, which may degrade the entanglement and increase the total error rate. The decoherence caused by the channel noise has been widely researched in the quantum system [77]. Here, we consider a general model, say, the white-noise model, in which the target state $|\phi^+\rangle$ may degrade to the other three Bell states in Eq. (4) with the same probability. After the first round of photon transmission, Alice and Bob can finally share N_1 pairs of mixed states as

$$\begin{aligned} \rho_1 = & \eta_l^2 F |\phi^+\rangle\langle\phi^+| + \eta_l^2 \frac{1-F}{3} (|\psi^+\rangle\langle\psi^+| + |\phi^-\rangle\langle\phi^-| \\ & + |\psi^-\rangle\langle\psi^-|) + 2\eta_l(1-\eta_l)(|H\rangle\langle H| + |V\rangle\langle V|) \\ & + (1-\eta_l)^2 |\text{vac}\rangle\langle\text{vac}|, \end{aligned} \quad (13)$$

where F is the fidelity of the target entangled state $|\phi^+\rangle$. If $|\phi^+\rangle$ transforms to the other state, Alice and Bob cannot deterministically construct the entanglement channel in $|\phi^+\rangle$ according to the BSM result. In theory, if there is no eavesdropping, the error rates and CHSH polynomial can be calculated as [48,49],

$$\begin{aligned} Q_{b1} + Q_{p1} &= \frac{1}{2}(1 - \eta_l^2) + \eta_l^2(1 - F) \\ &= \frac{1}{2} - \eta_l^2 \left(F - \frac{1}{2}\right), \\ S_1 &= 2\sqrt{2}\eta_l^2 F. \end{aligned} \quad (14)$$

During the second photon-transmission process, the photon local loss, photon-transmission loss and decoherence all may reduce the CHSH polynomial and increase the error rates. After the photon transmission, all the security checking photon pairs have the form of

$$\rho_2 = \eta_l \eta_l' \rho_2' + (1 - \eta_l \eta_l') \rho_{\text{disturb}}, \quad (15)$$

where

$$\begin{aligned} \rho_2' = & F^2 |\phi^+\rangle\langle\phi^+| + \frac{1-F^2}{3} (|\psi^+\rangle\langle\psi^+| \\ & + |\phi^-\rangle\langle\phi^-| + |\psi^-\rangle\langle\psi^-|), \end{aligned} \quad (16)$$

and ρ_{disturb} includes the disturb items, such as the single-photon state and vacuum state. As a result, S_2 and $Q_{b2} + Q_{p2}$ can be written as

$$\begin{aligned} Q_{b2} + Q_{p2} &= \frac{1}{2}(1 - \eta_l \eta_l'^2) + \eta_l \eta_l'^2(1 - F^2) \\ &= \frac{1}{2} - \eta_l \eta_l'^2 \left(F^2 - \frac{1}{2}\right), \\ S_2 &= 2\sqrt{2}\eta_l \eta_l'^2 F^2. \end{aligned} \quad (17)$$

After two rounds of photon transmission, the total error rate $Q_t = Q_{b2} + Q_{p2}$. In this way, we can obtain

$$I_{AB} = 1 - H(Q_t) = 1 - H(Q_{b2} + Q_{p2}). \quad (18)$$

Then, we calculate I_{AE} . After the first and second photon-transmission rounds, when $S_1 > 2$ and $S_2 > 2$, we can estimate the Holevo quantity by

$$\begin{aligned} \chi(S_1) &\leq H\left(\frac{1 + \sqrt{(S_1/2)^2 - 1}}{2}\right), \\ \chi(S_2) &\leq H\left(\frac{1 + \sqrt{(S_2/2)^2 - 1}}{2}\right). \end{aligned} \quad (19)$$

The upper bound on the Holevo quantities in Eq. (19) has been well proved and Eve's photon interception rates in the first and second photon-transmission rounds equal to $\chi(S_1)$ and $\chi(S_2)$, respectively [48,49]. It is obvious that $S_2 < S_1$, so that we can obtain $\chi(S_1) < \chi(S_2)$. As Eve can read out the message only when she intercepts both photons of an encoded photon pair from Alice, we can bound the message leakage rate I_{AE} of the current DI-QSDC protocol by

$$I_{AE} \leq \chi(S_1). \quad (20)$$

I_{AE} reaches the maximum of $\chi(S_1)$ only when in the second photon-transmission round, Eve can intercept all the corresponding photons of her intercepted photons in the first photon-transmission process. However, as Alice messes up her photons in sequence S_{A1} before the second round of photon transmission, the probability that I_{AE} reaches $\chi(S_1)$ is quite close to 0 with a large number of transmitted photons. Meanwhile, as S_1 is independent with the photon-transmission efficiency η_l , the message-leakage rate I_{AE} is independent with the communication distance L_{AB} .

Based on above calculation, we provide the lower bound of C_s in Eq. (10) by

$$C_s \geq 1 - H(Q_{b2} + Q_{p2}) - \chi(S_1). \quad (21)$$

As Q_t increases with the growth of L_{AB} , C_s would decrease with L_{AB} . Different with quantum key distribution, as QSDC directly transmits secret messages, not the random keys, the parties cannot perform the post-error-correction method to correct the message error or message loss. We define the message loss rate (r_{loss}) as the amount of lost message qubits divided by the total amount of the message qubits, and the message error rate (r_{error}) as the amount of incorrect qubits read out by Bob divided by the total amount of the message qubits that Bob can read out. r_{loss}

and r_{error} can be calculated as

$$\begin{aligned} r_{\text{loss}} &= 1 - \eta_l^2 \eta_t, \\ r_{\text{error}} &= 1 - F^2. \end{aligned} \quad (22)$$

As the photon-transmission loss in the first photon-transmission process does not cause message loss, the current DI-QSDC protocol has lower r_{loss} than the original DI-QSDC protocol ($r_{\text{loss}0} = 1 - \eta_l^2 \eta_t^2$) [30].

In Fig. 3, we provide C_s of the current DI-QSDC protocol and C_{s0} of the original DI-QSDC protocol [30] as a function of the communication distance L_{AB} in the device-independent scenario. Here, we fix $F = 0.98$ and $\eta_l = 0.98$. It can be found that the maximal communication distance of the current DI-QSDC protocol can reach about 6.68 km, which is about 6 times of that in the original DI-QSDC protocol (about 1.18 km). Meanwhile, at the same communication distance, C_s is much higher than C_{s0} .

Meanwhile, we define the practical secure communication efficiency E_s as the amount of transmitted correct and secure qubits per second. Here, we suppose the repetition rate of the photon source as R_{rep} . After each round of photon transmission, we choose half the number of entangled photon pairs to make the DI security checking, so that only 1/4 of the amount of entangled photon pairs can be used to transmit messages. In this way, we can calculate E_s of the current DI-QSDC protocol and E_{s0} of the original DI-QSDC protocol as

$$\begin{aligned} E_s &= \frac{1}{4} R_{\text{rep}} P_1 C_s, \\ E_{s0} &= \frac{1}{4} R_{\text{rep}} C_{s0}, \end{aligned} \quad (23)$$

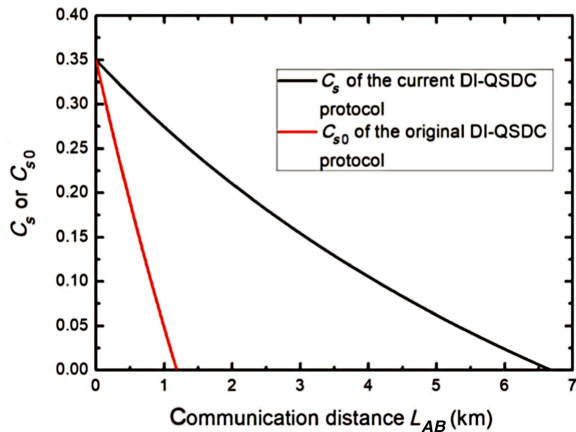


FIG. 3. The secret message capacity C_s of the current DI-QSDC protocol and C_{s0} of the original DI-QSDC protocol in Ref. [30] as a function of the communication distance L_{AB} in the device-independent scenario. Here, we control the local efficiency $\eta_l = 98\%$ and the fidelity $F = 0.98$.

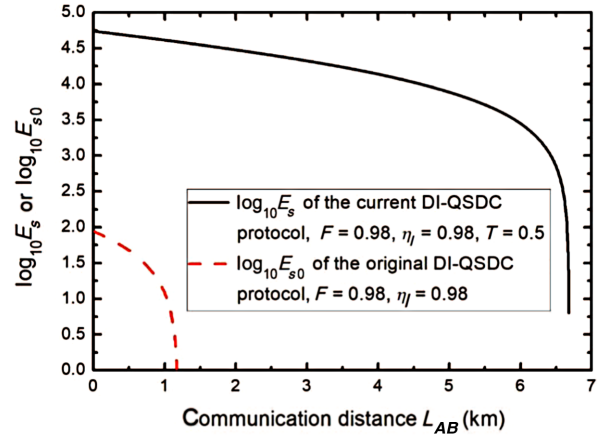


FIG. 4. The practical secure communication efficiency E_s of the current DI-QSDC protocol and E_{s0} of the original DI-QSDC protocol in Ref. [30] on a logarithmic (with subscript 10) versus the communication distance L_{AB} in the device-independent scenario. Here, we control the local efficiency $\eta_l = 0.98$ and the fidelity $F = 0.98$. We set the repetition rate R_{rep} of both the single-photon source and the spontaneous parametric down-conversion source to be 10 MHz. In the current DI-QSDC protocol, we consider the transmittance of the VBS as $T = 0.5$. In the original DI-QSDC protocol, we consider the practical spontaneous parametric down-conversion source generates a pair of two-photon entangled state with the fidelity of $p = 10^{-4}$.

where P_1 is the success probability of the heralded BSM in Eq. (5). In Fig. 4, we show the $\log_{10} E_s$ of the current DI-QSDC protocol and $\log_{10} E_{s0}$ of the original DI-QSDC protocol [30] as a function of L_{AB} in the device-independent scenario. Here, we set $F = 0.98$ and $\eta_l = 0.98$. The current DI-QSDC protocol adopts the on-demand single photon source and suitable VBSs with $T = 0.5$. The original DI-QSDC protocol adopts the spontaneous parametric down-conversion source with the fidelity of $p = 10^{-4}$. The repetition rate of both kinds of sources are set to be 10 MHz. It can be found that by adopting the single-photon source and the heralded architecture, the practical secure communication efficiency of the current DI-QSDC protocol is about 600 times of that in the original DI-QSDC protocol.

V. DISCUSSION AND CONCLUSION

We propose a DI-QSDC protocol with single-photon sources. In the protocol, the communication parties generate single photons from single-photon sources and they can deterministically construct the entanglement channel with the help of the heralded BSM and the quantum memory. Then, Alice encodes the messages on her remaining photons and sends the encoded photons to Bob for the BSM. Bob can finally read out the secret messages by comparing the BSM results with the original Bell state. By performing the DI security checking, the parties can

guarantee the security of both photon-transmission processes. Comparing with original DI-QSDC protocol [30], the current DI-QSDC protocol has two advantages. First, the practical single-photon source is extremely close to the on-demand single-photon source, and the adoption of the single-photon source can increase the practical photon generation rate and eliminate the security loophole from the double-photon emission. Second, with the help of the heralded architecture, the parties can deterministically construct the entanglement channel from the single photons, and the message-leakage rate of the DI-QSDC protocol is independent from the communication distance. Both advantages enable the current DI-QSDC protocol to have much longer communication distance, much higher practical communication efficiency, and lower message-loss rate. It is noticeable that the DI quantum key distribution protocol in Ref. [55] also adopts the BSM to herald the construction of the entanglement channel. However, when two photons by one party are transmitted at the VBS and the other party has both photons reflected, the BSM may also obtain the successful measurement result but the parties cannot share the entanglement state. The probability that this happens scales exactly like P_1 even though $T \ll 1$. In this way, the DI quantum key distribution protocol in Ref. [55] cannot solve the double transmission interference problem, which may disturb the key generation. In our DI-QSDC protocol, the parties require to use quantum memory to store the reflected photons. Meanwhile, the quantum memory can also herald the existence of the reflected photon. As a result, the double transmission cases can be eliminated, which is actually an attractive advantage of our DI-QSDC protocol compared with the DI quantum key distribution in Ref. [55].

As shown in Sec. IV, the decoherence occurring in both photon-transmission processes may reduce C_s and increase message error. Meanwhile, the decoherence also provides an opportunity for Eve to intercept some photons in both photon-transmission processes without being detected. The entanglement purification is an effective method to resist the decoherence [63,78–80]. In this way, we can adopt the entanglement purification in the current DI-QSDC protocol to improve the quality of entanglement channel. In detail, after Alice and Bob construct the entanglement channel, they can perform the entanglement purification to increase the fidelity of $|\phi^+\rangle$. In theory, Alice and Bob can increase the fidelity of $|\phi^+\rangle$ to be quite close to 1 by repeating the entanglement purification. As a result, combined with the entanglement purification, Alice and Bob can construct nearly perfect entanglement channel and obtain $S_1 \rightarrow 2\sqrt{2}$. It means Eve cannot intercept any photon during the first photon-transmission process without being detected ($\chi(S_1) \rightarrow 0$). As the message-leakage rate $I_{AE} \leq \chi(S_1)$, I_{AE} can be reduced to 0 and the current DI-QSDC is absolutely secure. However, after the second transmission process,

Bob cannot perform the entanglement purification, for the entanglement purification may change the encoded message. By performing the entanglement purification after the first photon-transmission process, the total error rate of the current DI-QSDC protocol can be reduced from $Q_t = \frac{1}{2} - \eta_t \eta_t^2 (F^2 - \frac{1}{2})$ to $Q'_t = \frac{1}{2} - \eta_t \eta_t^2 (F - \frac{1}{2})$, and the lower bound of the secret message capacity can be increased to

$$C'_s \geq 1 - H(Q'_t). \quad (24)$$

Suppose Alice and Bob repeat the entanglement purification for N times to construct the nearly perfect quantum channel, the practical communication efficiency of the current DI-QSDC protocol can be written as

$$E_{sm} \geq \frac{1}{4} R_{\text{rep}} P_1 \frac{P_{EP_1} P_{EP_2} \cdots P_{EP_N}}{2^N} [1 - H(Q'_t)], \quad (25)$$

where P_{EP_i} ($i = 1, 2, \dots, N$) represents the success probability of the i th round of entanglement purification.

In conclusion, DI-QSDC can resist all possible attacks on the imperfect experimental devices thus guaranteeing QSDC's security under practical imperfect experimental condition. The original DI-QSDC protocol adopts the practical entanglement photon source to generate the entanglement probabilistically, where the double-photon-pair emission is unavoidable. During the entanglement distribution process, the photon-transmission loss largely deteriorates the entanglement. These two factors limit the secret message capacity and secure communication distance of the original DI-QSDC protocol. In the paper, we propose a DI-QSDC protocol with single-photon sources and heralded architecture. The practical single-photon source is extremely close to the on-demand single-photon source. The parties can deterministically construct the entanglement channel from the single photons heralded by the BSM and the quantum memory. The security of the DI-QSDC protocol is guaranteed by the observation of data conclusively violating the CHSH inequality, so that it is unconditionally secure in theory. The photon-transmission-loss case in the first photon-transmission process can be eliminated with the help of the heralded architecture, so that the message-leakage rate is independent from the communication distance. The above two features can efficiently increase DI-QSDC's secure communication distance and practical communication efficiency, and reduce the message-loss rate. We numerically simulate the secret message capacity and practical communication efficiency of our DI-QSDC protocol. Under the condition of $F = 0.98$, $T = 0.5$, and $\eta_t = 0.98$, the maximal communication distance of the current DI-QSDC protocol reaches about 6.68 km, which is about 6 times of that in the original DI-QSDC protocol. The practical communication efficiency of the current DI-QSDC protocol is about 600 times of that in the original DI-QSDC protocol. Moreover,

by performing the entanglement purification after the first photon-transmission process, the parties can construct the nearly perfect entanglement channel, so that they can completely eliminate the message leakage and reduce the total error rate. Based on above features, this DI-QSDC protocol may have useful application in the future quantum communication field.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China under Grants No. 11974189 and No. 12175106.

-
- [1] C. H. Bennett and G. Brassard, Quantum cryptography: public key distribution and coin tossing, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, (India IEEE, New York, 1984), p. 175.
- [2] A. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [3] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, *Phys. Rev. Lett.* **85**, 441 (2000).
- [4] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Omer, M. Furst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, Entanglement-based quantum communication over 144 km, *Nat. Phys.* **3**, 481 (2007).
- [5] T. Sasaki, Y. Yamamoto, and M. Koashi, Practical quantum key distribution protocol without monitoring signal disturbance, *Nature* **509**, 475 (2014).
- [6] S. Wang, Z. Q. Yin, W. Chen, D. Y. He, X. T. Song, H. W. Li, L. J. Zhang, Z. Zhou, G. C. Guo, and Z. F. Han, Experimental demonstration of a quantum key distribution without signal disturbance monitoring, *Nat. Photon.* **9**, 832 (2015).
- [7] 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).
- [8] S. Zhao, P. Zeng, W. F. Cao, X. Y. Xu, Y. Z. Zhen, X. F. Ma, L. Li, N. L. Liu, and K. Chen, Phase-Matching Quantum Cryptographic Conferencing, *Phys. Rev. Appl.* **14**, 024010 (2020).
- [9] A. R. Jin, P. Zeng, R. V. Penty, and X. F. Ma, Reference-Frame-Independent Design of Phase-Matching Quantum Key Distribution, *Phys. Rev. Appl.* **16**, 034017 (2021).
- [10] Y. A. Chen, Q. Zhang, T. Y. Chen, W. Q. Cai, S. K. Liao, J. Zhang, K. Chen, J. Yin, J. G. Ren, and Z. Chen, *et al.*, An integrated space-to-ground quantum communication network over 4,600 kilometres, *Nature* **589**, 214 (2021).
- [11] W. B. Liu, C. L. Li, Y. M. Xie, C. X. Weng, J. Gu, X. Y. Cao, Y. S. Lu, B. H. Li, H. L. Yin, and Z. B. Chen, Homodyne Detection Quadrature Phase Shift Keying Continuous-Variable Quantum Key Distribution with High Excess Noise Tolerance, *PRX Quantum* **2**, 040334 (2021).
- [12] Z. Q. Yin, F. Y. Lu, J. Teng, S. Wang, W. Chen, G. C. Guo, and Z. F. Han, Twin-field protocols: towards inter-city quantum key distribution without quantum repeaters, *Funda. Res.* **1**, 93 (2021).
- [13] L. C. Kwek, L. Cao, W. Luo, Y. X. Wang, S. H. Sun, X. B. Wang, and A. Q. Liu, Chip-based quantum key distribution, *AAPPS Bull.* **31**, 15 (2021).
- [14] H. Guo, Z. Y. Li, S. Yu, and Y. C. Zhang, Toward practical quantum key distribution using telecom components, *Founda. Res.* **1**, 96 (2021).
- [15] G. Z. Tang, C. Y. Li, and M. Wang, Polarization discriminated time-bin phase-encoding measurement-device-independent quantum key distribution, *Quantum Eng.* **3**, e79 (2021).
- [16] X. F. Wang, X. J. Sun, Y. X. Liu, W. Wang, B. X. Kan, P. Dong, and L. L. Zhao, Transmission of photonic polarization states from geosynchronous earth orbit satellite to the ground, *Quantum Eng.* **3**, e73 (2021).
- [17] C. Y. Zhang and Z. J. Zheng, Entanglement-based quantum key distribution with untrusted third party, *Quantum Inform. Process.* **20**, 146 (2021).
- [18] W. Zhao, R. H. Shi, X. C. Ruan, Y. Guo, Y. Y. Mao, and Y. Y. Feng, Monte Carlo-based security analysis for multi-mode continuous-variable quantum key distribution over underwater channel, *Quantum Inform. Process.* **21**, 186 (2022).
- [19] C. Zhou, X. Y. Wang, Z. G. Zhang, S. Yu, Z. Y. Chen, and H. Guo, Rate compatible reconciliation for continuous-variable quantum key distribution using raptor-like LDPC codes, *Sci. China Phys. Mech. Astron.* **64**, 260311 (2022).
- [20] 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).
- [21] 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).
- [22] G. L. Long and X. S. Liu, Theoretically efficient high-capacity quantum-key-distribution scheme, arXiv:preprint [ArXiv:quant-ph/0012056](https://arxiv.org/abs/0012056), (2000) [*Phys. Rev. A* **65**, 032302 (2002)].
- [23] 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).
- [24] F. G. Deng and G. L. Long, Secure direct communication with a quantum one-time pad, *Phys. Rev. A* **69**, 052319 (2004).
- [25] 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).
- [26] 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).

- [27] 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).
- [28] F. Zhu, W. Zhang, Y. B. Sheng, and Y. D. Huang, Experimental long-distance quantum secure direct communication, *Sci. Bull.* **62**, 1519 (2017).
- [29] 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).
- [30] L. Zhou, Y. B. Sheng, and G. L. Long, Device-independent quantum secure direct communication against collective attacks, *Sci. Bull.* **65**, 12 (2020).
- [31] 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).
- [32] Z. Sun, L. Y. Song, Q. Huang, L. G. Yin, G. L. Long, J. H. Lu, and L. Hanzo, Toward practical quantum secure direct communication: A quantum-memory-free protocol and code design, *IEEE Trans. Commun.* **68**, 5778 (2020).
- [33] 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, *Photon. Res.* **8**, 1522 (2020).
- [34] L. Yang, J. W. Wu, Z. S. Lin, L. G. Yin, and G. L. Long, Quantum secure direct communication with entanglement source and single-photon measurement, *Sci. China Phys. Mech. Astron.* **63**, 110311 (2020).
- [35] T. Li and G. L. Long, Quantum secure direct communication based on single-photon Bell-state measurement, *New J. Phys.* **22**, 063017 (2020).
- [36] G. L. Long and H. R. Zhang, Drastic increase of channel capacity in quantum secure direct communication using masking, *Sci. Bull.* **66**, 1267 (2021).
- [37] 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).
- [38] 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).
- [39] Z. T. Qi, Y. H. Li, Y. W. Huang, J. Feng, Y. L. Zheng, and X. F. Chen, A 15-user quantum secure direct communication network, *Light Sci. Appl.* **10**, 183 (2021).
- [40] Z. M. Huang, Z. B. Rong, X. F. Zou, and Z. M. He, Semi-quantum secure direct communication in the curved spacetime, *Quantum Inform. Process.* **20**, 375 (2021).
- [41] 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).
- [42] L. Liu, B. Lu, J. Y. Song, and C. Wang, Secure communications based on sending-or-not-sending strategy, *Quantum Inform. Process.* **21**, 250 (2022).
- [43] N. Das and G. Paul, Measurement device-independent quantum secure direct communication with user authentication, *Quantum Inform. Process.* **21**, 260 (2022).
- [44] Y. B. Sheng, L. Zhou, and G. L. Long, One-step quantum secure direct communication, *Sci. Bull.* **67**, 367 (2022).
- [45] L. Zhou and Y. B. Sheng, One-step device-independent quantum secure direct communication, *Sci. China Phys. Mech. Astron.* **65**, 250311 (2022).
- [46] 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).
- [47] G. L. Long, D. Pan, Y. B. Sheng, Q. K. Xue, J. H. Lu, and L. Hanzo, An evolutionary pathway for the quantum internet relying on secure classical repeaters, *IEEE Netw.* **36**, 82 (2022).
- [48] 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).
- [49] 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).
- [50] N. Gisin, S. Pironio, and N. Sangouard, Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier, *Phys. Rev. Lett.* **105**, 070501 (2010).
- [51] C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin, Device-Independent Quantum Key Distribution with Local Bell Test, *Phys. Rev. X* **3**, 031006 (2013).
- [52] K. P. Seshadreesan, M. Takeoka, and M. Sasaki, Progress towards practical device-independent quantum key distribution with spontaneous parametric down-conversion sources, on-off photodetectors, and entanglement swapping, *Phys. Rev. A* **93**, 042328 (2016).
- [53] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Practical device-independent quantum cryptography via entropy accumulation, *Nat. Commun.* **9**, 459 (2018).
- [54] V. Zapatero and M. Curty, Long-distance device-independent quantum key distribution, *Sci. Rep.* **9**, 17749 (2019).
- [55] 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).
- [56] J. S. Bell, On the Einstein-Podolsky-Rosen paradox, *Physics* **1**, 195 (1964).
- [57] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, *Rev. Mod. Phys.* **86**, 419 (2014).
- [58] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, *Phys. Rev. Lett.* **23**, 880 (1969).
- [59] W. J. Zhang, L. X. You, H. Li, J. Huang, C. L. Lv, L. Zhang, X. Y. Liu, J. J. Wu, Z. Wang, and X. M. Xie, NbN superconducting nanowire single photon detector with efficiency over 90% at 1550 nm wavelength operational at compact cryocooler temperature, *Sci. China Phys. Mech. Astron.* **60**, 120314 (2017).
- [60] X. Y. Lu, Q. Li, D. A. Westly, G. Moille, A. Singh, V. Anant, and K. Srinivasan, Chip-integrated visible-telecom entangled photon pair source for quantum communication, *Nat. Phys.* **15**, 373 (2019).

- [61] P. G. Kwiat, K. Mattle, H. Weinfurter, and A. Zeilinger, New High-Intensity Source of Polarization-Entangled Photon Pairs, *Phys. Rev. Lett.* **116**, 213601 (2016).
- [62] L. K. Chen, H. L. Yong, P. Xu, X. C. Yao, T. Xiang, Z. D. Li, C. Liu, H. Lu, N. L. Liu, L. Li, T. Yang, C. Z. Peng, B. Zhao, Y. A. Chen, and J. W. Pan, Experimental nested purification for a linear optical quantum repeater, *Nat. Photon.* **11**, 695 (2017).
- [63] X. M. Hu, C. X. Huang, Y. B. Sheng, L. Zhou, B. H. Liu, Y. Guo, C. Zhang, W. B. Xing, Y. F. Huang, C. F. Li, and G. C. Guo, Long-Distance Entanglement Purification for Quantum Communication, *Phys. Rev. Lett.* **126**, 010503 (2021).
- [64] M. Müller, S. Bounouar, K. D. Jöns, M. Glässl, and P. Michler, On-demand generation of indistinguishable polarization-entangled photon pairs, *Nat. Photon.* **8**, 224 (2014).
- [65] J. Claudon, J. Bleuse, N. S. Malik, M. Bazin, P. Jaffrennou, N. Gregersen, C. Sauvan, P. Lalanne, and J. M. Gerard, A highly efficient single-photon source based on a quantum dot in a photonic nanowire, *Nat. Photon.* **4**, 174 (2010).
- [66] J. C. Loredo, N. A. Zakaria, N. Somaschi, C. Anton, L. de Santis, V. Giesz, T. Grange, M. A. Broome, O. Gazzano, G. Coppola, I. Sagnes, A. Lemaitre, A. Auffèves, P. Senellart, M. P. Almeida, and A. G. White, Scalable performance in solid-state single-photon sources, *Optica* **3**, 433 (2016).
- [67] H. Wang, Z. C. Duan, Y. H. Li, S. Chen, J. P. Li, Y. M. He, M. C. Chen, Y. He, X. Ding, C. Z. Peng, C. Schneider, M. Kamp, S. Höfling, C. Y. Lu, and J. W. Pan, Near-Transform-Limited Single Photons from an Efficient Solid-State Quantum Emitter, *Phys. Rev. Lett.* **116**, 213601 (2016).
- [68] J. H. Kim, T. Cai, C. J. K. Richardson, R. P. Leavitt, and E. Waks, Two-photon interference from a bright single-photon source at telecom wavelengths, *Optica* **3**, 577 (2016).
- [69] N. Somaschi, V. Giesz, L. De Santis, J. C. Loredo, M. P. Almeida, G. Hornecker, S. L. Portalupi, T. Grange, C. Anton, J. Demory, C. Gomez, I. Sagnes, N. D. Lanzillotti-Kimura, A. Lemaitre, A. Auffèves, A. G. White, L. Lanco, and P. Senellart, Near-optimal single-photon sources in the solid state, *Nat. Photon.* **10**, 340 (2016).
- [70] X. Ding, Y. He, Z. C. Duan, N. Gregersen, M. C. Chen, S. Unsleber, S. Maier, C. Schneider, M. Kamp, S. Höfling, C. Y. Lu, and J. W. Pan, On-Demand Single Photons with High Extraction Efficiency and Near-Unity Indistinguishability from a Resonantly Driven Quantum Dot in a Micropillar, *Phys. Rev. Lett.* **116**, 020401 (2016).
- [71] S. Shi, B. Xu, K. Zhang, G. S. Ye, D. S. Xiang, Y. B. Liu, J. Z. Wang, D. Q. Su, and L. Li, High-fidelity photonic quantum logic gate based on near-optimal Rydberg single-photon source, *Nat. Commun.* **13**, 4454 (2022).
- [72] A. Barbiero, J. Huwer, J. Skiba-Szymanska, D. J. P. Ellis, R. M. Stevenson, T. Müller, G. Shooter, L. E. Goff, D. A. Ritchie, and A. J. Shields, High-performance single-photon sources at telecom wavelength based on broadband hybrid circular Bragg gratings, *ACS Photon.* **9**, 3060-3066 (2022).
- [73] M. Lasota, C. Radzewicz, K. Banaszek, and R. Thew, Linear optics schemes for entanglement distribution with realistic single-photon sources, *Phys. Rev. A* **90**, 033836 (2014).
- [74] D. S. Ding, Z. Y. Zhou, B. S. Shi, and G. C. Guo, Single-photon-level quantum image memory based on cold atomic ensembles, *Nat. Commun.* **4**, 2527 (2013).
- [75] E. Distante, P. Farrera, A. Padró-Brito, D. Paredes-Barato, G. Heinze, and H. de Riedmatten, Storing single photons emitted by a quantum memory on a highly excited Rydberg state, *Nat. Commun.* **8**, 14072 (2017).
- [76] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, The security of practical quantum key distribution, *Rev. Mod. Phys.* **81**, 1301 (2009).
- [77] B. X. Wang, M. J. Tao, Q. Ai, T. Xin, N. Lambert, D. Ruan, Y. C. Cheng, F. Nori, F. G. Deng, and G. L. Long, Efficient quantum simulation of photosynthetic light harvesting, *npj Quantum Inf.* **4**, 52 (2018).
- [78] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels, *Phys. Rev. Lett.* **76**, 722 (1996).
- [79] J. W. Pan, C. Simon, C. Brukner, and A. Zeilinger, Entanglement purification for quantum communication, *Nature* **410**, 1067 (2001).
- [80] C. X. Huang, X. M. Hu, B. H. Liu, L. Zhou, Y. B. Sheng, C. F. Li, and G. C. Guo, Experimental one-step deterministic polarization entanglement purification, *Sci. Bull.* **67**, 593 (2022).