Quantum secure direct communication based on single-photon Bell-state measurement

Tao Li and Gui-Lu Long

1 School of Science, Nanjing University of Science and Technology, Nanjing 210094, People's Republic of China
2 State Key Laboratory of Low-Dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, People's Republic of China
3 Tsinghua National Laboratory of Information Science and Technology, Beijing 100084, People's Republic of China
4 Collaborative Innovation Center of Quantum Matter, Beijing 100084, People's Republic of China

E-mail: tao.li@njust.edu.cn and gllong@tsinghua.edu.cn

Keywords: quantum communication, single-photon Bell-state measurement, detector-side-channel attack, hyper-encoded photon, quantum secure direct communication

Abstract
Security loopholes exploiting the flaws of practical apparatus, especially non-ideal photon detectors, are pressing issues in practical quantum communication. We propose a simple quantum secure direct communication protocol based on single-photon Bell-state measurement and remove side-channel attacks on photon detectors. This quantum communication protocol in principle works in a deterministic way, and it does not require the two-photon interference of photons from independent sources. The single-photon Bell-state measurement with a unity efficiency can be constructed with only linear optics, which significantly simplifies its experimental implementation. Furthermore, we prove that our quantum secure direct communication protocol is immune to general detector-side-channel attacks.

1. Introduction
Security of communication between distant parties is an indispensable criteria for evaluating the performance of any communication network [1–3]. Quantum communication in principle provides unconditional security for exchanging sensitive information over public channels, since its security is based on the distinct characters of quantum mechanics, such as quantum entanglement and quantum no-cloning theorem [4]. Eavesdroppers cannot get any useful information during a quantum communication process without introducing perturbations that inevitably reveal their interception [5]. However, eavesdroppers can exploit security loopholes that are introduced by non-ideal apparatuses and/or channels to attack practical quantum communication [6, 7]. Quantum key distribution (QKD) is a useful quantum communication protocol that generates secure keys between separated parties in the presence of eavesdroppers [8]. Subsequently, these keys enable secure communication and authentication. Non-ideal apparatuses, especially single-photon detectors with imperfections, have been exploited to carry out side-channel attacks against practical QKD [9–19], although the QKD is unbreakable in theory.

So far, several approaches have been researched to eliminate these side-channel attacks to recover the security of QKD that is implemented with practical detectors. Device independent QKD, based on the violation of Bell inequality, is proved to be secure and removes all side-channel attacks [20–22], and it requires a loophole-free Bell test [23–25]. Measurement-device-independent QKD (MDI-QKD) is a relatively simple solution that is based on postselected entanglement to remove all side-channel attacks using practical measurement apparatuses [26–31]. It requires the interference of photons from independent single-photon sources that are spatially separated by a long distance. Moreover, the coincidence rate of two single-photon detectors, corresponding to the rate of entanglement generation, is at most 50% using linear optics [32]. Recently, detector-device-independent QKD (DDI-QKD) is introduced to avoid these
limitations of MDI-QKD by using single-photon Bell-state measurement (BSM) together with a relatively stringent security assumption on photon detectors [33–36]. In addition to all assumptions in MDI-QKD, DDI-QKD assumes that single-photon detectors are built by the legitimate parties and thus have never correlated with outside eavesdroppers [35, 36].

Quantum secure direct communication (QSDC) is another important quantum communication protocol that transmits private information directly between communication parties without producing secret keys in advance [37–40]. In general, QSDC can function as a deterministic QKD when the parties exchange random keys instead of private information. No basis reconciliation is involved in QSDC. Since the first two-step QSDC based on Einstein–Podolsky–Rosen (EPR) photon-pair block was proposed [37], much attention has been devoted to construct more QSDC protocols [41–52]. In 2016, Hu et al demonstrated the DLO4-QSDC protocol [41] using the frequency encoding of single photons [53]. Lum et al demonstrated a quantum enigma machine based on quantum data locking, which can transmit secure information directly [54]. The two-step QSDC protocols in references [37, 38] based on EPR photon pairs are experimentally demonstrated by using quantum memory [55], and using fiber entanglement source to perform a long-distance communication [56]. A practical QSDC for intra-city communication is experimentally demonstrated by using concatenation of low-density parity check codes very recently [57]. Security analysis of QSDC has been done [57, 58] by combining quantum mechanics with Wyner’s wiretap channel theory [59]. Recently, Shapiro et al presented a quantum low probability of intercept protocol, which in principle can transmit private information directly with a rate of gigabits per second [60]. The QSDC with a measurement-device-independent setting closes potential loopholes that might be exploited to perform a side-channel attack using practical measurement apparatus [61–63]. Meanwhile, it also requires the interference of photons from independent sources and has an upper bound efficiency 50% of the BSM using linear optics. Very recently, a device-independent QSDC protocol was proposed to remove all attacks on practical devices, based on the violation of Bell inequality [64].

Here we propose a simple QSDC protocol based on a single-photon BSM [65, 66]. This protocol enables legitimate parties to exchange private information directly by using practical single-photon detectors, without two-photon interference. The key point is the single-photon Bell-state measurement on one hyper-encoded photon of an EPR pair, which establishes a correlation between the sender and receiver. The sender encodes two bit values by performing different unitary operations that can be exclusively decoded by the receiver through the correlation in a deterministic way. Furthermore, we prove that the protocol, with reasonable assumptions, is secure even when practical detectors are exploited for two typical attacks: symmetric individual attacks and intercept-resend attacks. The intervention of any eavesdropper will be detected by the legitimate parties before any leakage of the private information, making our protocol useful for long-distance secure communication.

2. Protocol description

The diagram of our QSDC protocol is illustrated in figure 1. To send a private message to a receiver Bob, the sender Alice prepares a sequence of polarization-encoded EPR photon pairs and sends half of each photon pair to Bob that encodes a spatial-mode qubit by introducing a random phase \( \varphi \) in two conjugate bases. An exclusive correlation between Alice and Bob can be established by a single-photon BSM on the photon pair to Bob that encodes a spatial-mode qubit by introducing a random phase \( \varphi \). Then she takes one photon from each photon pair and arranges them into a photon sequence, such as \( S = (s_1, s_2, \ldots, s_j, \ldots, s_2) \). The other photon of the corresponding photon pair is arranged in the same order according to the subscribe \( j \), leading to a photon sequence \( T = (t_1, t_2, \ldots, t_j, \ldots, t_2) \). Alice sends photon sequence \( T \) to the receiver Bob and keeps the other photon sequence \( S \) in her node, referred to as stationary qubits below.

(2) Hyper-encoding: upon receiving the photon sequence \( T \), Bob randomly encodes one qubit information on the spatial-mode DoF of each photon, referred to as \( |\psi\rangle_r \), by sending each photon into a balanced beam splitter (BS) followed by a phase modulator (PM) in one output mode, such as \( l \) mode. The PM then introduces a phase \( \varphi \) in the \( l \) mode, which evolves each photon pair into a state
terminate their communication and restart the aforementioned phases. Remaining

Alice and Bob, can complete the teleportation of the spatial-mode DoF of each photon by performing measurement in the same basis as he used for hyper-encoding. At present, classical communication is much less costly than quantum-qubit transmissions, the procedure can be alternatively

\[ U_0 = |0\rangle\langle 0| + |1\rangle\langle 1| \]

a polarization beam splitter (PBS) transmits (reflects) a photon in the state \( |0\rangle (|1\rangle); \) a half-wave plate (HWP) performing a bit-flip operation on photons passing through it. PM is a phase modulator and introduces a phase shift in the set \( \{0, \pi/2, \pi, 3\pi/2\}. \)

**Table 1.** State of stationary qubit \( s_j \) after the quantum teleportation operation, according to the specific encoding of Bob and the result of single-photon BSM. Here

| \(|\psi\rangle_0\rangle | \langle\psi|_0\rangle | \langle\Psi^+|_0\rangle | \langle\Phi^+|_0\rangle |
|---|---|---|---|
| 0 | \(|\rangle +\rangle | \langle\rangle -\rangle | \langle\rangle +\rangle | \langle\rangle -\rangle |
| 0 | \(|\rangle +\rangle | \langle\rangle +\rangle | \langle\rangle -\rangle | \langle\rangle -\rangle |
| 0 | \(|\rangle -\rangle | \langle\rangle +\rangle | \langle\rangle -\rangle | \langle\rangle +\rangle |
| 0 | \(|\rangle -\rangle | \langle\rangle -\rangle | \langle\rangle +\rangle | \langle\rangle -\rangle |

\[ |\psi\rangle_0 = \frac{1}{\sqrt{2}} (|0\rangle_0 + |1\rangle_0), \]

\[ |\psi\rangle_0 = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle). \]

A simple BSM for a hyperencoded single photon can be deterministically constituted by linear optics and single-photon detectors, shown in figure 1. According to the result of BSM, the communication parties, Alice and Bob, can complete the teleportation of the spatial-mode DoF of each photon \( s_j \), and map its state to the corresponding stationary qubit \( s_j \) belonging to Alice, up to a single-qubit rotation. Now, the state of \( s_j \) could be \(|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}, |\pm\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}, |\pm\rangle = (|0\rangle - i|1\rangle)/\sqrt{2}, \)

\[ |\psi\rangle_0 = \frac{1}{\sqrt{2}} (|0\rangle_0 + |1\rangle_0). \]
identified by Bob and publishes the measurement results together with the operations and positions of $n_i$ test bits in $S$. Therefore, Bob can decode the information sent by Alice directly and ascertain the faith of the direct communication by comparing Alice’s measurement results with table 1: when they are the same, Alice’s information is bit 0, otherwise, Alice’s information is bit 1.

3. Security analysis

The present QSDC protocol is based on the single-photon double encoding and the single-photon BSM. The nonorthogonal states, encoded by Bob for the information alignment, are teleported to Alice’s node by performing single-photon BSM on both the spatial-mode and polarization DoFs of photons that are sent to Bob. To read out Alice’s message that is encoded in the form of a sequence of unitary operations, Eve needs to know the states that Bob encoded and the measurement outcomes of the corresponding BSM, the combination of which leads to the leakage of the photon state just before Alice’s encoding process. Subsequently, a simple comparison between the measurement outcome in faithful decoding phase and the photon state that is eavesdropped by Eve reveals the unitary operation (the encoding bit information) that is applied by Alice. Therefore, Eve can focus her attack on acquiring Bob’s encoding information, the phase $\varphi$, by using two different general strategies: (I) symmetric individual attacks; (II) intercept-resend attacks. We will show below that both attacks cannot get any useful information for Eve without being detected by legitimated communication parties.

3.1. Symmetric individual attacks

During a symmetric individual attack, Eve prepares a probe and makes it interact with a qubit propagating from Alice to Bob; she then measures the probe after Alice has encoded her information and announced the outcomes of her measurement. In principle, Eve can freely choose the probe and let it interact with the qubit under any evolution that is subjected to the laws of quantum mechanics. However, the most general evolution of the qubit and the probe is unitary and can be specified as follows [6, 41, 42],

\[ |0\rangle_{t}\epsilon \rightarrow \sqrt{F}|0\rangle_{s}|\epsilon_{00}\rangle + \sqrt{D}|1\rangle_{s}|\epsilon_{01}\rangle, \]
\[ |1\rangle_{t}\epsilon \rightarrow \sqrt{D}|0\rangle_{s}|\epsilon_{10}\rangle + \sqrt{F}|1\rangle_{s}|\epsilon_{11}\rangle. \]

Here the subscript $t$ represents a travelling qubit and $|\epsilon\rangle$ is the initial state of the probe; Eve’s effective Hilbert space is at most four dimensions and is spanned by four ancillary states $|\epsilon_{ij}\rangle$ that are nonorthogonal but normalized with $\langle \epsilon_{ij}|\epsilon_{ij}\rangle = 1$. The parameter $F$ is proportional to the probability that Eve learns the state of a travelling qubit without being detected; $D$ is proportional to a similar probability, except that Eve will be detected. Both $F$ and $D$ are supposed to be positive real numbers, since the relative phase involved in the unitary transformation can be absorbed into the states $|\epsilon_{ij}\rangle$. Therefore, the orthonormality of the two states in equation (2) can be equivalent to the constraints $F + D = 1$ and $\langle \epsilon_{s0}|\epsilon_{10}\rangle + \langle \epsilon_{s1}|\epsilon_{11}\rangle = 0$. Furthermore, without loss of generality, we may assume that $\langle \epsilon_{0}\epsilon_{1}\rangle = \langle \epsilon_{ji}\epsilon_{ij}\rangle = 0$ for $j = 1 - j$, $\cos \alpha = \langle \epsilon_{i0}|\epsilon_{i1}\rangle$, and $\cos \beta = \langle \epsilon_{0j}|\epsilon_{1j}\rangle$, $\alpha, \beta \in [0, \pi/2]$.

For a photon pair in the state $|\varphi^+\rangle$, Eve introduces a probe in the state $|\epsilon\rangle$ and makes it interact with the travelling photon $t_i$. The composite system consisting of Eve’s probe and particles belonging to Alice and Bob evolves into a new state

\[ |\Psi_1\rangle = \frac{1}{\sqrt{2}} \left( \sqrt{F}|0\rangle_{s}|1\rangle_{s}|\epsilon_{11}\rangle + \sqrt{D}|0\rangle_{s}|0\rangle_{s}|\epsilon_{10}\rangle + \sqrt{F}|1\rangle_{s}|0\rangle_{s}|\epsilon_{00}\rangle + \sqrt{D}|1\rangle_{s}|1\rangle_{s}|\epsilon_{01}\rangle \right), \]

where the subscripts ($s$, $t$) are used as the shorthand for a general qubit pair ($s_i$, $t_i$). After photons $t_i$ passing through Bob’s encoding circuit that introduces a random phase $\varphi \in \{0, \pi/2, \pi, 3\pi/2\}$ in the lower mode $i_l$, a polarization-flip operation is applied on photons in the upper mode $u$. Subsequently, the photon $t_i$ in either the lower or upper mode is emitted by the BS in the single-photon BSM setup, which evolves the composite system into

\[ |\Psi_2\rangle = \frac{1}{2\sqrt{2}} \left( |0_u\rangle \left( \sqrt{D} e^{i\varphi}|0\rangle_{s}|\epsilon_{10}\rangle + \sqrt{F} e^{i\varphi}|1\rangle_{s}|\epsilon_{00}\rangle + \sqrt{F}|0\rangle_{s}|\epsilon_{11}\rangle + \sqrt{D}|1\rangle_{s}|\epsilon_{01}\rangle \right) + |1_u\rangle \right) \]
\[ \times \left( \sqrt{F} e^{i\varphi}|0\rangle_{s}|\epsilon_{11}\rangle + \sqrt{D}|0\rangle_{s}|\epsilon_{10}\rangle + \sqrt{F}|1\rangle_{s}|\epsilon_{00}\rangle + \sqrt{D} e^{i\varphi}|1\rangle_{s}|\epsilon_{01}\rangle \right), \]
\[ \times \left( \sqrt{F}|0\rangle_{s}|\epsilon_{11}\rangle - \sqrt{D} e^{i\varphi}|0\rangle_{s}|\epsilon_{10}\rangle - \sqrt{F} e^{i\varphi}|1\rangle_{s}|\epsilon_{00}\rangle + \sqrt{D}|1\rangle_{s}|\epsilon_{01}\rangle + |1_l\rangle \right), \]
\[ \times \left( \sqrt{D}|0\rangle_{s}|\epsilon_{10}\rangle - \sqrt{F} e^{i\varphi}|0\rangle_{s}|\epsilon_{11}\rangle + \sqrt{F}|1\rangle_{s}|\epsilon_{00}\rangle - \sqrt{D} e^{i\varphi}|1\rangle_{s}|\epsilon_{01}\rangle \right). \]
Here $|0_u\rangle$, $|1_u\rangle$, $|0_l\rangle$, and $|1_l\rangle$ correspond to four single-photon BSM outcomes of $|\Psi^+\rangle$, $|\Phi^+\rangle$, $|\Psi^-\rangle$, and $|\Phi^-\rangle$, respectively. Upon the click of any single-photon detector that measures the photon $t_i$, Alice’s stationary qubit and Eve’s probe collapse into a superposition state. To give out the probability that Eve is detected by Alice and Bob through the sampling process, Alice’s photon state is redescribed in the basis that Bob has used to encode his qubit, i.e., Bob encodes a phase $\varphi = 0, \pi$ in the basis $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. The state $|\Psi_2^{(0)}\rangle$ for the case $\varphi = 0$ can be redescribed as,

$$
|\Psi_2^{(0)}\rangle = \frac{1}{4} \left\{ (|0_u\rangle + |1_u\rangle) \left[ |\mp\rangle (\sqrt{F(\epsilon_{11})} + \sqrt{D(\epsilon_{10})} + \sqrt{F(\epsilon_{00})} + \sqrt{D(\epsilon_{10})}) + |\pm\rangle (\sqrt{F(\epsilon_{11})} + \sqrt{D(\epsilon_{10})})
- \sqrt{H(\epsilon_{00})} + \sqrt{D(\epsilon_{01})}) \right] + (|0_l\rangle - |1_l\rangle) \left[ |\mp\rangle (\sqrt{F(\epsilon_{11})} - \sqrt{D(\epsilon_{10})} - \sqrt{F(\epsilon_{00})} + \sqrt{D(\epsilon_{10})}) + |\pm\rangle (\sqrt{F(\epsilon_{11})} - \sqrt{D(\epsilon_{10})})
\times \left( \sqrt{H(\epsilon_{00})} - \sqrt{D(\epsilon_{01})} + \sqrt{F(\epsilon_{00})} - \sqrt{D(\epsilon_{01})} \right) \right] \right\}.
$$

(5)

Therefore, no matter in which state the photon $t_i$ is, the system consisting of Alice’s stationary qubit and Eve’s probe is collapsed into a superposition state that is isomorphic to each other, due to the specific character of ancillary states $|\epsilon_i\rangle$.

The probability of detecting Eve is proportional to $P_0 = (1 - F \cos \alpha - D \cos \beta)/2$ for $\varphi = 0$. Similarly, for the cases $\varphi = \pi, \varphi = \pi/2$, and $\varphi = 3\pi/2$, the system consisting of Alice’s stationary qubit and Eve’s probe is also collapsed into an isomorphic superposition state that is independent of the state of the photon $t_i$. The corresponding probabilities of detecting Eve are $P_\pi = (1 - F \cos \alpha - D \cos \beta)/2$, $P_{\pi/2} = (1 - F \cos \alpha + D \cos \beta)/2$, and $P_{3\pi/2} = P_{\pi/2}$, respectively. The average probability of detecting Eve, when it is averaged over all input states and all results of single-photon BSMS, can be described as

$$
P = \frac{1 - F \cos \alpha}{2},
$$

(6)

which is independent of $\cos \beta$ when Bob encodes his qubit in both bases with an equal probability. Now, the minimum of the detecting probability is

$$
P_m = \frac{1 - \cos \alpha}{2}.
$$

(7)

This is achieved for $F = 1$, since $F \in [0, 1]$, as shown in equation (2).

After the security check process, if Alice wants to transmit a bit value ‘$k$’ through the qubit $s_i$, she performs the $U_k$ operation on this qubit. After this, she measures the qubit $s_i$ by using the same basis that Bob has used to encode his qubit. She then announces her measurement outcome through a public channel. During this process, Eve wants to learn the information as much as she can, while keeping the detecting probability $P_m$ as low as she can. Since the different outcomes of a single-photon BSM project Alice’s stationary qubit and Eve’s probe into an isomorphic state, we can analyse the case with the BSM outcome $|\Psi^+\rangle$, denoted as $|b_u\rangle$, to calculate the correlation between the legitimated parties and the eavesdropper Eve.

When the outcome of single-photon BSM is $|\Psi^+\rangle$, the system consisting of Alice’s stationary qubit and Eve’s probe is collapsed into

$$
|\Psi_3\rangle = \frac{1}{\sqrt{2}} \left( \sqrt{F(\epsilon_{11})} |0\rangle_{s_i} \right| \epsilon_{11} \rangle + \sqrt{D(\epsilon_{10})} |0\rangle_{s_i} \right| \epsilon_{10} \rangle + \sqrt{F(\epsilon_{00})} |0\rangle_{s_i} \right| \epsilon_{00} \rangle + \sqrt{D(\epsilon_{10})} |1\rangle_{s_i} \right| \epsilon_{00} \rangle \right),
$$

(8)

which can be redescribed in different bases of Alice’s qubit i.e., $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ and $|\pm \rangle = (|0\rangle \pm |\bar{1}\rangle)/\sqrt{2}$ as follows:

$$
|\Psi_3^{(0)}\rangle = \frac{1}{2} \left[ |\pm\rangle (\sqrt{F(\epsilon_{11})} + \sqrt{D(\epsilon_{10})} + \sqrt{F(\epsilon_{00})} + \sqrt{D(\epsilon_{01})}) + |\pm\rangle (\sqrt{F(\epsilon_{11})} + \sqrt{D(\epsilon_{10})})
\times \left( \sqrt{F(\epsilon_{11})} + \sqrt{D(\epsilon_{10})} - \sqrt{F(\epsilon_{00})} - \sqrt{D(\epsilon_{01})} \right) \right],
$$

$$
|\Psi_3^{(\pm)}\rangle = \frac{1}{2} \left[ |\mp\rangle (\sqrt{F(\epsilon_{11})} + \sqrt{D(\epsilon_{10})} + \sqrt{F(\epsilon_{00})} + \sqrt{D(\epsilon_{01})}) + |\pm\rangle (\sqrt{F(\epsilon_{11})} + \sqrt{D(\epsilon_{10})})
\times \left( \sqrt{F(\epsilon_{11})} + \sqrt{D(\epsilon_{10})} - \sqrt{F(\epsilon_{00})} + \sqrt{D(\epsilon_{01})} \right) \right].
$$

(9)

when Bob encodes his qubit in the basis $|\pm\rangle$, Alice’s qubit will be collapsed into $|\mp\rangle \ (|\pm\rangle)$ for $\varphi = 0 \ (\varphi = \pi)$ in the ideal situation. However, this ideal situation is changed due to the presence of any eavesdropper Eve, shown in equation (9). We can give out the bit information derived by Bob and Eve for different conditions: Bob encodes the phase $\varphi = 0, \pi$, Alice encodes a bit value ‘$k$’ by performing a unitary operation $U_k$ for $k = 0, 1$; Alice announces her outcome $|\pm\rangle$, or $|\mp\rangle$, shown in table 2.
Table 2. Bit information obtained by Bob and Eve for different conditions.

Bob encodes a qubit by $\varphi_B$; Alice sends a bit value $i$ by performing $U_i$ on her qubit and then announces the outcome $M_i$ of the measurement of the qubit; Eve and Bob get the probe state $M_E$ and the bit value $M_B$ with corresponding probabilities $p_{\pm} = (1 \pm \cos \alpha)/4$.

| $\varphi_B$ | $U_i$ | $M_i$ | $M_E$ | $M_B$ | $p_+$ |
|-------------|-------|-------|-------|-------|-------|
| 0           | 0     | $|$+ $|$ | 0     | 0     | $p_+$ |
| 0           | 0     | $|$− $|$ | 1     | 0     | $p_-$ |
| 0           | 1     | $|$+ $|$ | 0     | 1     | $p_+$ |
| 0           | 1     | $|$− $|$ | 1     | 1     | $p_-$ |
| $\pi$       | 0     | $|$+ $|$ | 1     | 0     | $p_+$ |
| $\pi$       | 0     | $|$− $|$ | 0     | 1     | $p_-$ |
| $\pi$       | 1     | $|$+ $|$ | 1     | 0     | $p_+$ |
| $\pi$       | 1     | $|$− $|$ | 0     | 1     | $p_-$ |

![Figure 2](image-url)  
**Figure 2.** Mutual information $I(A : B)$ and $I(A : E)$, and detecting probability $P_m$ versus the nonorthogonal value $\cos \alpha$.

When Bob encodes his qubit in the basis $|\pm i\rangle$, we can also give out the bit information that can be derived by Bob and Eve for different conditions, which is similar to the case that Bob encodes his qubit in $|\pm\rangle$. The degree of correlation between Alice and Bob, referred to as the mutual information between two parties, can be written as

$$I(A : B) = \frac{1}{2} \left( (1 - \cos \alpha) \log (1 - \cos \alpha) + (1 + \cos \alpha) \log (1 + \cos \alpha) \right).$$

(10)

However, the mutual information between Alice and Eve is vanish with $I(A : E) = 0$ and the mutual information between Bob and Eve is also vanish with $I(B : E) = 0$.

The symmetric individual attacks cannot provide the eavesdropper Eve with any useful information when Eve attacks the system with the minimum detecting probability $P_m$ of different nonorthogonal probe states. However, the presence of Eve decreases the mutual information $I(A : B)$ between the communication parties Alice and Bob. In figure 2, the minimum detecting probability $P_m$ and the mutual information $I(A : B)$ are presented as a function of $\cos \alpha$. Clearly, Alice and Bob share perfect correlation with the mutual information $I(A : B) = 1$ when $P_m = 0$; Alice and Bob share vanish correlation with the mutual information $I(A : B) = 0$ when $P_m = 1/2$.

3.2. Intercept-resend attacks

A direct intercept-resend attack that is performed by one eavesdropper Eve can be carried out as follows: Eve intercepts each photon $t_i$, measures it in a randomly chosen basis $|\pm\rangle$ or $|\pm i\rangle$, and then sends Bob a photon in the same state as her measurement outcome. Eve can easily obtain the bit information encoded by Alice’s unitary operations if Eve can hide from Alice and Bob. Fortunately, this type of intercept-resend attack will be detected by Alice and Bob during the sampling process in step (4). Then, Alice stops her encoding before the leakage of any private information.

Suppose Eve uses the basis $|\pm\rangle$ to measure the photon $t_i$ of a photon pair that are in the state $|\varphi^+\rangle$. Eve gets two possible outcomes $|+\rangle$ and $|−\rangle$, and sends Bob a photon $t'_i$ that is in the same state as her measurement outcome. After passing through Bob’s encoding circuit, the photon $t'_i$ in the upper mode flips its polarization and combines again with that in the lower mode at a BS. When the photon $t'_i$ entering into
Bob’s encoding circuit is in the state $|+\rangle$ or $|-\rangle$, its state evolves as follows,

$$|\psi_{+}\rangle = \frac{1}{2\sqrt{2}} \left[ (1 + e^{i\varphi}) (|0_u\rangle + |1_u\rangle) + (1 - e^{i\varphi}) (|0_l\rangle + |1_l\rangle) \right],$$ (11)

$$|\psi_{-}\rangle = \frac{1}{2\sqrt{2}} \left[ (1 - e^{i\varphi}) (|1_u\rangle - |0_u\rangle) + (1 + e^{i\varphi}) (|1_l\rangle - |0_l\rangle) \right],$$ (12)

where the subscript $u(l)$ labels a photon that clicks one of the two upper (lower) single-photon detectors and $\varphi \in \{0, \pi/2, \pi, 3\pi/2\}$.

For the case that Eve uses the basis $|\pm\rangle$ to measure the photon $n_i$, she sends Bob a photon in the state $|+\rangle$ or $|-\rangle$ that evolves as follows

$$|\psi_{+i}\rangle = \frac{1}{2\sqrt{2}} \left[ (1 + i e^{i\varphi}) (|1_u\rangle + i|0_u\rangle) + (1 - i e^{i\varphi}) (|1_l\rangle + i|0_l\rangle) \right],$$ (13)

$$|\psi_{-i}\rangle = \frac{1}{2\sqrt{2}} \left[ (1 - i e^{i\varphi}) (|1_u\rangle - i|0_u\rangle) + (1 + i e^{i\varphi}) (|1_l\rangle - i|0_l\rangle) \right],$$ (14)

The probability $P_d$ of detecting Eve is identical for all cases that Eve sends Bob a photon in the state $|+\rangle$, $|-\rangle$, $|+\rangle$, or $|-\rangle$; the detecting probability for each single sampling process is $P_d = 1/4$, when Alice and Bob compare their practical outcomes of the BSM with that are obtained under ideal condition. For a sampling process of $n_1 = 25$ bits, Eve’s intervention in principle will be detected with a probability of $P_d(25) = 99.9\%$, before Alice encodes her bit information by performing unitary operations. The legitimate parties Alice and Bob restart the communication process and then securely exchange private message without being eavesdropped by any adversary.

An alternative intercept-resend attack follows the idea of two eavesdroppers before and after Bob’s encoding circuit [36]. The two eavesdroppers Eve and Fred work cooperatively as follows: Eve intercepts each photon $n_i$, measures it in a randomly chosen basis $|\pm\rangle$ or $|\pm\rangle$, and then sends $n_i$ photons to Bob with each photon in the same state as her measurement outcome. After these photons pass through Bob’s encoding circuit, they evolve into a product state with each photon evolves into a new state that reveals Bob’s encoding information $\varphi$. Fred can first perform nondestructive measurement of these photons to read out $n_i$, if the number of photons $n_i$ reveals the basis and outcome of Eve’s measurement; subsequently, Fred can get Bob’s encoding information $\varphi$ by unambiguous state discrimination measurement of the new state [68]. By comparing Eve’s measurement outcome with Bob’s encoding choice, Fred determines to announce a BSM outcome that consists with the ideal output shown in table 1.

For example, when Eve gets a measurement outcome $|-\rangle$ and Bob encodes a phase $\varphi = 0$ ($\varphi = \pi$), Fred can announce the outcome of the BSM as $|\Psi^-\rangle$ or $|\Phi^-\rangle$ ($|\Psi^+\rangle$ or $|\Phi^+\rangle$). In contrast, Fred announces the BSM as inconclusive, when Eve’s measurement outcome and Bob’s encoding choice are inconsistent, because any BSM outcome in this case leads to an error of 50% that can be detected by Alice and Bob during the sampling process. This inconclusive process can be absorbed into channel loss, when Eve substitutes a practical channel with a better channel of a lower loss rate. The security of our protocol is limited by a practical channel of the loss rate up to 50%. This limitation can be removed by inserting a filter before Bob’s encoding circuit, which decreases the number of photons $n_i$ [69–76]. Subsequently, this disturbs the correlation between Eve’s measurement outcome and $n_i$, and prevents Fred from learning about Bob’s encoding choice. Therefore, the security of our protocol can be improved to that achieved with direct intercept-resend attack when single-photon filter is available.

4. Discussion

In previous sections, the security of our protocol against two typical attacks are presented under ideal circumstance. For MDI quantum communication protocols [26–31, 61–63], their security is guaranteed by postselecting entanglement that is introduced by two-photon interference. However, the security of our protocol exploits the exclusive correlation that is introduced by an entanglement distribution together with a single-photon BSM, and removes side-channel attacks on photon detectors when they are built by the legitimate parties. We require no two-photon interference and thus eliminate the corresponding limitation, such as the identical character of two independent photons, time of arrival, frequency, and so on.

When the sender’s node is kept isolated from quantum nondestructive measurement applied by Eve, our protocol could be modified to implement a simplified QSDC protocol [46], in which the encoding basis in the receiver node is fixed to $\{|+\rangle, |\rangle\}$ and the sender can perform the measurement just after loading her private information on stationary qubit. Our protocol in practice can be used to perform a deterministic QKD [42], in which Alice encodes a random string of symbols rather than her private information before
performing random sampling. In addition, the single-photon BSM also enables a nondeterministic QKD by using single photons in nonorthogonal states: one party encodes a random spatial qubit to the received photon and performs single-photon BSM on it. Then it introduces exclusive correlation between two parties only when their bases are the same, which allows for the generation of a random key [33–36].

In practice, there are several sources of noise that may be encountered, such as the noisy preparation of an EPR pair, the channel noise, the imprecise operation involved in the encoding, and the decoherence of a stationary qubit [77]. All these sources of noise decrease the fidelity of practical EPR pairs shared by the legitimate parties, and prevent them from sharing perfect correlation shown in table 1. Then it increases the bit-error rate, which equals zero under idealized circumstance, in random sampling. Fortunately, the legitimate parties, in principle, can use entanglement purification to create EPR pairs with a sufficiently high fidelity from the practical ones with a fidelity larger than a threshold value, such as a fidelity of 0.5 for a depolarizing channel [78]. It is an interesting future topic to study the tolerable bit-error rate. However, the error-rate threshold 5.7% for the DL04-QSDC protocol using four nonorthogonal states in reference [58] is a good estimate of the upper bound. In practical implementation of this protocol, forward error correction [79] might be more practical and easier, and explicit correction codes should be constructed, like those in references [57, 80].

The stationary qubit in our protocol can be implemented by quantum memory or optical delay line [53, 55–57]. The sender Alice prepares n EPR pairs, and stores half of each EPR pair in n quantum memories that are referred to as stationary qubits. In practice, a stationary qubit should hold on its state for an appreciable length of time $T_2$ to enable Alice and Bob perform classical communication and eavesdropping diagnostics. The decoherence of the stationary qubit changes a pure state into a mixed one, and it introduces an additional bit-error rate with the lower bound of $p_e = (1 - \exp(-2L/cT_2))/2 \sim L/cT_2 \ll 1$, which constraints the communicating distance $L$ for a given $T_2$ and the light speed $c$. The two-step QSDC with quantum memory was demonstrated with a fidelity of 0.9 [55]. Very recently, the entanglement between two quantum memories over dozens of kilometres was realized [81]. Their quantum memory setup can be modified to implement our protocol directly. A more practical way to circumvent the difficulty of quantum memory is to use a dynamic coding scheme to dispense with the quantum memory in the so-called quantum memory-free QSDC protocol [67].

5. Summary

The security of our protocol against symmetric-individual [6, 42] and intercept-resend attacks [35, 36] are demonstrated. For the symmetric-individual attack, the eavesdropper Eve cannot acquire any useful information when she uses a strategy that reveals her intervention with the lowest probability. However, her intervention decreases the mutual information between two legitimate communication parties. For the intercept-resend attack, the eavesdropper Eve is detected by an average probability of 1/4 for each single sampling process, and can be detected deterministically by a larger sampling subset. For a lossy channel, the security of our protocol against the intercept-resend attack is proved by inserting a filter before Bob’s encoding circuit [69–76].

In summary, we presented a simple quantum secure direct communication protocol based on single-photon BSM by using linear optics and practical single-photon detectors. It closes the potential security loopholes exploiting the flaws of detectors in practical quantum communication. Furthermore, it removes the limitation of two-photon interference, making it simple and efficient for practical communication.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grants No. 11904171, No. 11974205, No. 11474181, No. 11175094, and No. 91221205), the Natural Science Foundation of Jiangsu Province (Grant No. BK20180461), and the National key Research and Development Program of China (Grants No. 2017YFA0303700 and No. 2015CB921001); G L acknowledges support from Beijing Advanced Innovation Center for future Chip (ICFC).

ORCID iDs

Tao Li https://orcid.org/0000-0003-3353-4618
Gui-Lu Long https://orcid.org/0000-0002-9023-1579
[69] Birnbaum K M, Boca A, Miller R, Boozer A D, Northup T E and Kimble H J 2005 Nature 436 87–90
[70] Huang R, Miranowicz A, Liao J Q, Nori F and Jing H 2018 Phys. Rev. Lett. 121 153601
[71] Xia K, Lu G, Lin G, Cheng Y, Niu Y, Gong S and Twamley J 2014 Phys. Rev. A 90 043802
[72] Xia K, Nori F and Xiao M 2018 Phys. Rev. Lett. 121 203602
[73] Zhou L, Yang I. P, Li Y and Sun C P 2013 Phys. Rev. Lett. 111 103604
[74] Lu J, Zhou L, Kuang L M and Nori F 2014 Phys. Rev. A 89 013805
[75] Cao C, Duan Y W, Chen X, Zhang R, Wang T J and Wang C 2017 Opt. Express 25 16931–46
[76] De Santis I et al 2017 Nat. Nanotechnol. 12 663
[77] Lo H K and Chau H F 1999 Science 283 2050–6
[78] Bennett C H, Brassard G, Popescu S, Schumacher B, Smolin J A and Wootters W K 1996 Phys. Rev. Lett. 76 722
[79] Sadlier R J and Humble T S 2016 Quantum Meas. Quantum Metrol. 3 1–8
[80] Massa F, Mojarad A, Baumeler A, Del Santo F, Kettlewell J A, Dakić B and Walther P 2019 Adv. Quantum Technol. 2 1900050
[81] Yu Y et al 2020 Nature 578 240–5