FRONTIERS OF PHYSICS

RESEARCH ARTICLE
Volume 18 / Issue 5 / 51301 / 2023

# A quantum secure direct communication scheme based on intermediate-basis

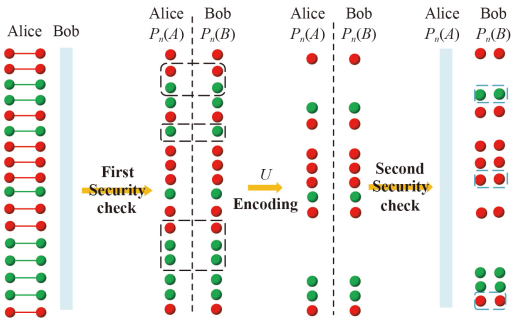
Kexin Liang[1,2], Zhengwen Cao[1,2,†], Xinlei Chen[1], Lei Wang[1], Geng Chai[1,‡], Jinye Peng[1]

1 Laboratory of Quantum Information & Technology (QIT), School of Information Science and Technology, Northwest University, Xi'an 710127, China
2 State Key Laboratory of Integrated Services Networks (Xidian University), Xi'an 710071, China
Corresponding authors. E-mail: †caozhw@nwu.edu.cn, ‡chai.geng@nwu.edu.cn
Received October 19, 2022; accepted February 23, 2023



## ABSTRACT

Quantum secure direct communication (QSDC) is a method of communication that transmits secret information directly through a quantum channel. This paper proposes a two-step QSDC scheme based on intermediate-basis, in which the intermediate-basis Einstein–Podolsky–Rosen (EPR) pairs can assist to detect channel security and help encode information. Specifically, the intermediate-basis EPR pairs reduce the probability of Eve choosing the correct measurement basis in the first step, enhancing the security of the system. Moreover, they encode information together with information EPR pairs to improve the transmission efficiency in the second step. We consider the security of the protocol under coherent attack when Eve takes different dimensions of the auxiliary system. The simulation results show that intermediate-basis EPR pairs can lower the upper limit of the amount of information that Eve can steal in both attack scenarios. Therefore, the proposed protocol can ensure that the legitimate parties get more confidential information and improve the transmission efficiency.




**Keywords** quantum secure direct communication, two-step, intermediate-basis

## 1 Introduction

Secure communication guarantees political and economic security and social well-being. However, fast-growing supercomputer technology and quantum computing [1] threaten traditional encryption methods (for example, RSA public key scheme [2]). Quantum communication is an emerging and vibrant alternative approach based on the uncertainty principle and no-cloning theorem of quantum mechanics, which can fulfill unconditional theoretical security. So far, it mainly includes quantum key distribution (QKD) [3, 4], quantum teleportation (QT) [5], and quantum secure direct communication (QSDC) [6].

QKD was first proposed in 1984 to establish a secure key before transmitting a message and has come a long way since then [7, 8]. QT can execute the transmission and reconstruction of the quantum state over arbitrary distance, and it will be a critical ingredient for a quantum computation network [9, 10]. QSDC is a milestone during the development of quantum communication, which can achieve the direct transmission of messages through a quantum channel [11]. There are two well-known protocols known as two-step protocol [12] and DL04 protocol [13], and the former uses Einstein–Podolsky–Rosen (EPR) pairs while the latter uses single photons. The security analyses [14–16] and experimental demonstrations [17, 18] enable the two protocols to become the

Higher Education Press

https://doi.org/10.1007/s11467-023-1284-4

mainstream of QSDC. Moreover, [19] reports the first practical QSDC experiment through the fiber transmission of 0.5 km, and quantum state fidelity of entanglement is 91%, which shows the potential of QSDC and supports its application on quantum communication networks. A QSDC scheme without quantum memory is proposed to solve one of the biggest obstacles to its practical applications [20]. In addition, the measurement-device-independent (MDI) QSDC [21, 22] and its security analysis [23] gradually become mature. The theories and researches on free space QSDC and its experiments are in progress [24, 25]. Another important QSDC scheme that has been studied in recent years is semi-quantum secure direct communication, which is proposed in [26]. And some further development has been done in [27–29]. Continuous variable QSDC is also being studied [30, 31]. Therefore, the research branch of QSDC is becoming more and more abundant.

Although QSDC has made some progress, there is still a need to improve system performance. In this paper, we propose a novel two-step QSDC scheme with intermediate-basis [32]. Intermediate-basis EPR pairs, on one hand, enhance the system security by reducing the probability of Eve choosing the correct measurement basis, and they also participate in information encoding together with information EPR pairs, improving the transmission efficiency. Finally, the security analyses when Eve employs two different auxiliary systems to execute coherent attack are all considered. Results show that the intermediate-basis EPR pairs played a positive role in resisting these attacks.

The remainder of this paper is organized as follows. In Section 2, the proposed two-step QSDC protocol is described in detail. The security analyses of this protocol under coherent attack with two different auxiliary systems of Eve are proved in Section 3. The summary is given in Section 4.

## 2 The two-step QSDC scheme with intermediate-basis

In this section, we describe the proposed protocol as shown in Fig. 1, which includes two stages: security detection and message transmission. Alice employs block transmission technology, for arbitrary $i$-th block, $i \in [1, M]$ ($M$ is the number of all information blocks)

### Step 1: Preparation of entangled pairs

Alice prepares two kinds of entangled pairs, $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ represented by red balls in Fig. 1, and $\left|\psi_{\theta_i}^-\right\rangle = (\left|\theta_i\theta_i^\perp\right\rangle - \left|\theta_i^\perp\theta_i\right\rangle)/\sqrt{2}, (\theta_i \in (0, \frac{\pi}{4}))$ represented by green balls in Fig. 1. $\theta_i$ is the angle of intermediate-basis selected by legal parties when transmitting the $i$-th block (its range is shown in Fig. 2) and is represented as

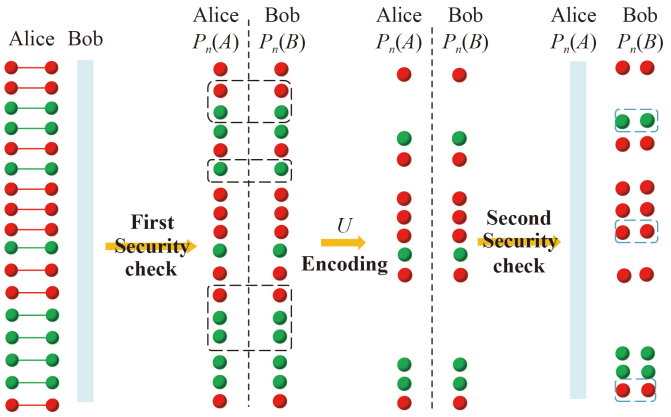



**Fig. 1** A QSDC scheme based on intermediate-basis. ($U$: A unitary operation for encoding. The red balls refer to information EPR pairs $|\psi^-\rangle$, and the green balls refer to intermediate-basis EPR pairs $\left|\psi_{\theta_i}^-\right\rangle$. Black dashed frame represents these particles are chosen for channel security detection and blue dashed frame represents these particles are used for channel secondary detection.)

$$\begin{aligned} |\theta_i\rangle &= \cos(\theta_i/2)\,|0\rangle + \sin(\theta_i/2)\,|1\rangle\,, \\ \left|\theta_i^\perp\right\rangle &= \sin(\theta_i/2)\,|0\rangle - \cos(\theta_i/2)\,|1\rangle\,. \end{aligned} \tag{1}$$

Alice randomly arranges two entangled pairs to form a new sequence and keeps one subsequence $\{P_n(A), n = 1, 2, ..., N\}$ by herself. Then she sends another subsequence $\{P_n(B), n = 1, 2, ..., N\}$ to Bob and announces $\theta_i$ ($N$ is the length of the two sequences).

### Step 2: Channel security check

Entanglement is a resource that can resist interference [19], attenuation, and mutation from the channel. However, it is destroyed when Eve lurks in the channel, and the measurement results of Alice and Bob no longer conform to the EPR relationship. Therefore, an unreasonable quantum bit error rate (QBER) appears.

Here, we judge the security of the first step of trans-

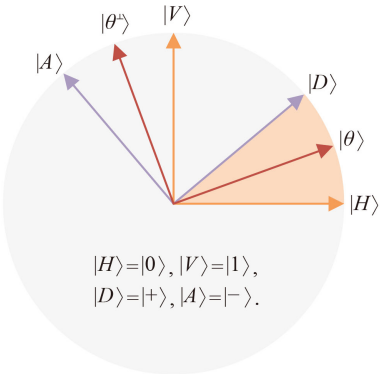



**Fig. 2** The relationship between intermediate basis and $X$ basis and $Z$ basis. ($|H\rangle = |0\rangle, |V\rangle = |1\rangle, |D\rangle = |+\rangle, |A\rangle = |-\rangle$, and the shaded part is the effective range of $\theta_i$.)

mission through the Clauser–Horne–Shimony–Holt (CHSH) inequality [33–35]. That is, when the CHSH inequality is violated, Eve cannot completely determine the measurement results of both communication parties. When the violation is greater, the weaker its correlation with Eve; When the violation reaches the maximum, the quantum state and Eve are completely separated, and the measurement results of both sides of the communication will not be leaked to Eve.

(2.a) Alice chooses randomly $\hat{Q}$ basis or $\hat{R}$ basis to measure the chosen photons in $P_n(A)$. (2.b) Bob chooses randomly $\hat{S}$ basis or $\hat{T}$ basis to measure the chosen photons in $P_n(B)$, where

$$\begin{aligned}
&\hat{Q} = \hat{Z},\\
&\hat{R} = \hat{X},\\
&\hat{S} = \frac{-\hat{Z}-\hat{X}}{\sqrt{2}},\\
&\hat{T} = \frac{\hat{Z}-\hat{X}}{\sqrt{2}}.
\end{aligned} \tag{2}$$

(2.c) After all the checking photon pairs have been measured, Alice and Bob reveal their measurement basis and results, then they can calculate the CHSH polynomial,

$$S_{CHSH} = \left\langle \hat{Q}\hat{S} \right\rangle + \left\langle \hat{R}\hat{S} \right\rangle + \left\langle \hat{R}\hat{T} \right\rangle - \left\langle \hat{Q}\hat{T} \right\rangle. \tag{3}$$

where $\langle\cdot\rangle$ represents mean value of measurement results.

According to the measurement reasults, if $S_{CHSH} \leq 2$, entanglement does not exist. At this time, the channel security detection fails and the communication process is abandoned. If $2 < S_{CHSH} \leq 2\sqrt{2}$, the measurement results are non-local correlated, at this time, the channel security detection passes. When $S_{CHSH} = 2\sqrt{2}$, this means Alice and Bob share the maximally entanglement. In specific experiments, this maximum value is generally difficult to reach due to the influence of the environment. The detection process of intermediate-basis EPR pairs is similar.

**Step 3: Encoding information**

Alice relies on four unitary operations to load information on the rest of the particles in $P_n(A)$, and the four unitary operations are represented as Eq. (4).

$$\begin{aligned}
&U_1 = I = |0\rangle\langle 0| + |1\rangle\langle 1|,\\
&U_2 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|,\\
&U_3 = \sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|,\\
&U_4 = \sigma_x\sigma_z = |0\rangle\langle 1| - |1\rangle\langle 0|.
\end{aligned} \tag{4}$$

Then the information EPR pairs $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ are transformed into $|\psi^-\rangle$, $|\psi^+\rangle$, $|\Phi^-\rangle$ and $|\Phi^+\rangle$, respectively. And the intermediate-basis EPR pairs $|\psi^-_{\theta_i}\rangle$ are transformed into $|\psi^-_{\theta_i}\rangle$, $|\psi^+_{\theta_i}\rangle$, $|\Phi^+_{\theta_i}\rangle$ and $|\Phi^-_{\theta_i}\rangle$, respectively.

$$\begin{aligned}
&|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right),\\
&|\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B\right),\\
&|\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B\right),\\
&|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right),\\
&|\psi^-_{\theta_i}\rangle = |\theta_i\rangle_A|\theta_i^\perp\rangle_B - |\theta_i^\perp\rangle_A|\theta_i\rangle_B,\\
&|\psi^+_{\theta_i}\rangle = |\theta_i\rangle_A\begin{pmatrix}-\cos(\frac{\theta_i}{2})\\ \sin(\frac{\theta_i}{2})\end{pmatrix}_B - |\theta_i^\perp\rangle_A\begin{pmatrix}\sin(\frac{\theta_i}{2})\\ \cos(\frac{\theta_i}{2})\end{pmatrix}_B,\\
&|\Phi^+_{\theta_i}\rangle = |\theta_i\rangle_A|\theta_i\rangle_B + |\theta_i^\perp\rangle_A|\theta_i^\perp\rangle_B,\\
&|\Phi^-_{\theta_i}\rangle = |\theta_i\rangle_A\begin{pmatrix}\sin(\frac{\theta_i}{2})\\ \cos(\frac{\theta_i}{2})\end{pmatrix}_B - |\theta_i^\perp\rangle_A\begin{pmatrix}\cos(\frac{\theta_i}{2})\\ -\sin(\frac{\theta_i}{2})\end{pmatrix}_B.
\end{aligned} \tag{5}$$

**Step 4: Decoding information**

After Bob receives these quantum states, Alice publishes the positions of these sampling pairs and the chosen unitary operations on them to Bob. Bob executes corresponding Bell-basis measurement on the two particles simultaneously. The result of comparing random numbers judges whether Eve cut the communication off. If the communication process is unbroken, Bob can obtain the secret information through Table 1.

It can be seen from Table 1 that due to the help of intermediate-basis EPR pair $|\psi^-_{\theta_i}\rangle$, the number of quantum states that can be used for encoding is increased from 4 to 8, and the information transmission rate is increased from 2 bit to 3 bit per operation.

## 3 Security analysis

### 3.1 Security analysis under coherent attack

A compound channel with an eavesdropper is called a compound wiretap channel, with the novel difference

**Table 1** Summary of Alice's encoding and Bob's decoding.

| Entangled pair | Alice's encoding | Information | Bob's decoding |
|---|---|---|---|
| $\|\psi^-\rangle$ | $U_1$ | 000 | $\|\psi^-\rangle$ |
| | $U_2$ | 001 | $\|\psi^+\rangle$ |
| | $U_3$ | 010 | $\|\Phi^-\rangle$ |
| | $U_4$ | 011 | $\|\Phi^+\rangle$ |
| $\|\psi^-_{\theta_i}\rangle$ | $U_1$ | 100 | $\|\psi^-_{\theta_i}\rangle$ |
| | $U_2$ | 101 | $\|\psi^+_{\theta_i}\rangle$ |
| | $U_3$ | 110 | $\|\Phi^+_{\theta_i}\rangle$ |
| | $U_4$ | 111 | $\|\Phi^-_{\theta_i}\rangle$ |

that one information rate is to be maximized and the other minimized. As a way to realize secure communication, wiretap channel provides a good model for realizing secure communication [36]. The security capacity $C_s$ is an important parameter which refers to the maximum transmission rate that can be reached when the eavesdropper Eve can't eavesdrop any useful information, that is, when the legitimate users realize secure communication, as shown in Fig. 3.

**Theorem:** Supposed that $X$ is a random variable Alice send to Bob, $Y$ is the outcome of Bob's measurements through legal channel and $Z$ is the outcome of Eve's measurements through wiretap channel. $C_s$ is defined as [36]

$$C_s = \max(I(X;Y) - I(X;Z)). \tag{6}$$

In order to achieve this goal, it is necessary to maximize the reliable communication rate from the source to the legitimate receiver $I(X;Y)$, but the premise is that the eavesdropper reduces the output of the source $I(X;Z)$ as much as possible.

**Definition:** The quantum wiretap channel has been described by a single quantum operation $T$ from Alice to Bob and Eve together. The legal channel and the wiretapper channel are defined $\varepsilon = \mathrm{Tr}_E \circ T$ and $\varepsilon' = \mathrm{Tr}_B \circ T$ [37], respectively.

In other words, the main difference between classical wiretap channel and quantum wiretap channel [38, 39] comes from the no-cloning theorem, that is, Alice's input state can not be duplicated and then sent through both channels $\varepsilon$ and $\varepsilon'$. According to Wyner's wiretap channel theory, there exised an encoding method that allows the secure transmission of information at a rate lower than the secrecy capacity, provided that the secrecy capacity is positive. Notablly, the legal channel and wiretap channel are all quantum channel, thus, $I(X;Y)$ and $I(X;Z)$ are all replaced by the Holevo quantity [37].

**Theorem:** Supposed $\chi(\cdot)$ is Holevo quantity, $\chi_1$ and $\chi_2$ are quantum version of $I(X;Y)$ and $I(X;Z)$, respectively. $S(\cdot)$ is the von Neumann entropy, $P$ is a probability distribution over a finite set $\Omega$, $\rho(\cdot)$ is density operator, and $\Upsilon := \{\rho(x) : x \in \Omega\}$ is a set of states labeled by elements of $\Omega$,

$$\begin{aligned}
\chi_1(P,\Upsilon) &= S\left(\sum_{x\subseteq\Omega} P_X(x)\varepsilon(\rho(x))\right) \\
&\quad - \sum_{x\subseteq\Omega} P_X(x) S(\varepsilon(\rho(x))), \\
\chi_2(P,\Upsilon) &= S\left(\sum_{x\subseteq\Omega} P_X(x)\varepsilon'(\rho(x))\right) \\
&\quad - \sum_{x\subseteq\Omega} P_X(x) S(\varepsilon'(\rho(x))), \\
C_s &\geq \max_P(\chi_1(P,\Upsilon) - \chi_2(P,\Upsilon)).
\end{aligned} \tag{7}$$

Some relevent proofs are in Ref. [40].

Similar to the original two-step QSDC protocol, the security of the first step guarantees the security of the proposed scheme. Assuming Eve performs a coherent attack [41] where she attaches an auxiliary system $|E\rangle$ to quantum channel and performs $U_i$, then she sends system B to Bob. Then the original EPR relationship between Alice and Bob becomes

$$\begin{aligned}
\rho_{AB} &= \mathrm{Tr}_E(U_{BE}|E\rangle |\psi^-\rangle \langle\psi^-| \langle E| U_{BE}^\dagger), \\
\rho_{AB_{\theta_i}} &= \mathrm{Tr}_E(U_{BE}|E\rangle |\psi_{\theta_i}^-\rangle \langle\psi_{\theta_i}^-| \langle E| U_{BE}^\dagger).
\end{aligned} \tag{8}$$

To simplify the effect of the attack on the system, an additional operation that randomly chosen from $U$ is applied, the $\rho_{AB}$ and $\rho_{AB_{\theta_i}}$ are simplified to

$$\rho_{AB} = \begin{pmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 \\ 0 & 0 & \lambda_3 & 0 \\ 0 & 0 & 0 & \lambda_4 \end{pmatrix}, \tag{9}$$

and

$$\rho_{AB_{\theta_i}} = \begin{pmatrix} \lambda_{\theta_i,1} & 0 & 0 & 0 \\ 0 & \lambda_{\theta_i,2} & 0 & 0 \\ 0 & 0 & \lambda_{\theta_i,3} & 0 \\ 0 & 0 & 0 & \lambda_{\theta_i,4} \end{pmatrix}. \tag{10}$$

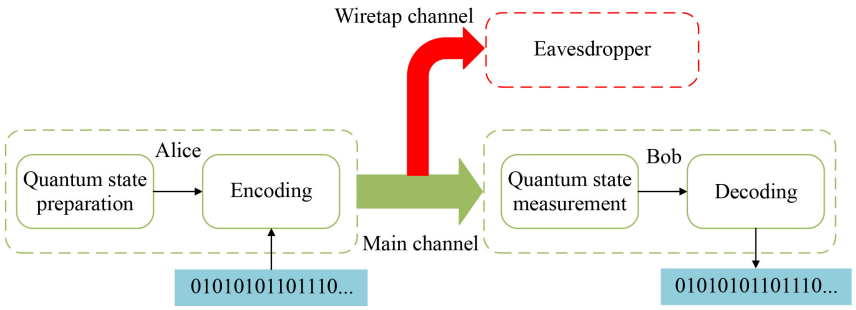



**Fig. 3** Wiretap channel model. The model comprises a transmitter, a legitimate receiver, and an eavesdropper. The channel between transmitter and legitimate receiver is the main channel, and the channel between transmitter and eavesdropper is the eavesdropper's channel.

The whole system $\psi_{ABE}$ can be expressed as

$$|\psi_{ABE}\rangle = \sum_{m=1}^{4} \sqrt{\lambda_m}\,|\Phi_m\rangle\,|E_m\rangle\,,$$
$$\left|\psi_{AB_{\theta_i}E}\right\rangle = \sum_{m=1}^{4} \sqrt{\lambda_{\theta_i,m}}\,|\Phi_{\theta_i,m}\rangle\,|E_m\rangle\,, \tag{11}$$

where $|\Phi_m\rangle$ and $|\Phi_{\theta_i,m}\rangle$ is the Bell state and the intermediate-basis Bell state of system $AB$, $|E_m\rangle$ is a set of orthogonal states of Eve's auxiliary system.

Finally, Eve intercepts all the qubits from Alice in the last step to obtain maximal information about the message and measure them. Tracing out system $B$ from $\psi_{ABE}$,

$$\rho_{AE} = Tr_B(|\psi_{ABE}\rangle\langle\psi_{ABE}|),$$
$$\rho_{AE_{\theta_i}} = Tr_B(\left|\psi_{AB_{\theta_i}E}\right\rangle\left\langle\psi_{AB_{\theta_i}E}\right|), \tag{12}$$

the encoded states are

$$\begin{aligned}
\rho_{AE,000} &= U_1\rho_{AE}U_1^\dagger,\\
\rho_{AE,001} &= U_2\rho_{AE}U_2^\dagger,\\
\rho_{AE,010} &= U_3\rho_{AE}U_3^\dagger,\\
\rho_{AE,011} &= U_4\rho_{AE}U_4^\dagger,\\
\rho_{AE_{\theta_i},100} &= U_1\rho_{AE_{\theta_i}}U_1^\dagger,\\
\rho_{AE_{\theta_i},101} &= U_2\rho_{AE_{\theta_i}}U_2^\dagger,\\
\rho_{AE_{\theta_i},110} &= U_3\rho_{AE_{\theta_i}}U_3^\dagger,\\
\rho_{AE_{\theta_i},111} &= U_4\rho_{AE_{\theta_i}}U_4^\dagger.
\end{aligned} \tag{13}$$

Even Eve measures all subsystems jointly, the information acquired from one subsystem on average in adjoint measurement cannot exceed that in single measurement of one subsystem, thus, the upper bound of $\chi_2(P,\Upsilon)$ is [14]

$$\begin{aligned}
\chi_2(P,\Upsilon) &\le S\left(\sum_a p_a\rho_{AE,a}\right) - \sum_a p_a S\left(\rho_{AE,a}\right)\\
&\le h(\epsilon_z) + h(\epsilon_x),
\end{aligned} \tag{14}$$

where $\epsilon_x$ and $\epsilon_z$ are QBERs, $h(\cdot)$ is Shannon entropy, and $h(\epsilon_z) = h(\epsilon_{z_{\psi^-}}) + h(\epsilon_{z_{\psi^-_{\theta_i}}})$, $h(\epsilon_x) = h(\epsilon_{x_{\psi^-}}) + h(\epsilon_{x_{\psi^-_{\theta_i}}})$, $\epsilon_x = \lambda_2 + \lambda_4$, $\epsilon_z = \lambda_3 + \lambda_4$, $\epsilon_{x_{\psi^-_{\theta_i}}} = \lambda_{\theta_i,2} + \lambda_{\theta_i,4}$, and $\epsilon_{z_{\psi^-_{\theta_i}}} = \lambda_{\theta_i,3} + \lambda_{\theta_i,4}$.

In the absence of transmission disturbance, the information amount of $Y$ received by Bob is consistent with that of $X$ sent by Alice. In this scheme, each quantum bit encodes 3 bit information. Thus, $H(Y) = H(X) = 3$ bit/symbol. In practical transmission, due to transmission, interference and other factors, bite error rate will be introduced, leading to the existence of transfer entropy $H(Y|X)$. The randomness of $H(Y|X)$ is mainly related to bite error rate. Hence, the capacity of the main channel $\chi_1(P,\Upsilon)$ is determined by the bit error rate between classical information Alice and Bob [14],

$$\chi_1(P,\Upsilon) = H(Y) - H(Y|X) = 3 - h_8(\boldsymbol{e}), \tag{15}$$

where $\boldsymbol{e}$ is the bite error rate distribution of the main channel which can be obtained through the decoding process. The lower bound of the secrecy capacity of the two-step protocol is [14]

$$\begin{aligned}
C_s &= \chi_1(P,\Upsilon) - \chi_2(P,\Upsilon)\\
&\ge [3 - h_8(\boldsymbol{e})] - [h(\epsilon_x) + h(\epsilon_z)]\,.
\end{aligned} \tag{16}$$

Considering the block reception rate of Bob $Q_B$ and Eve

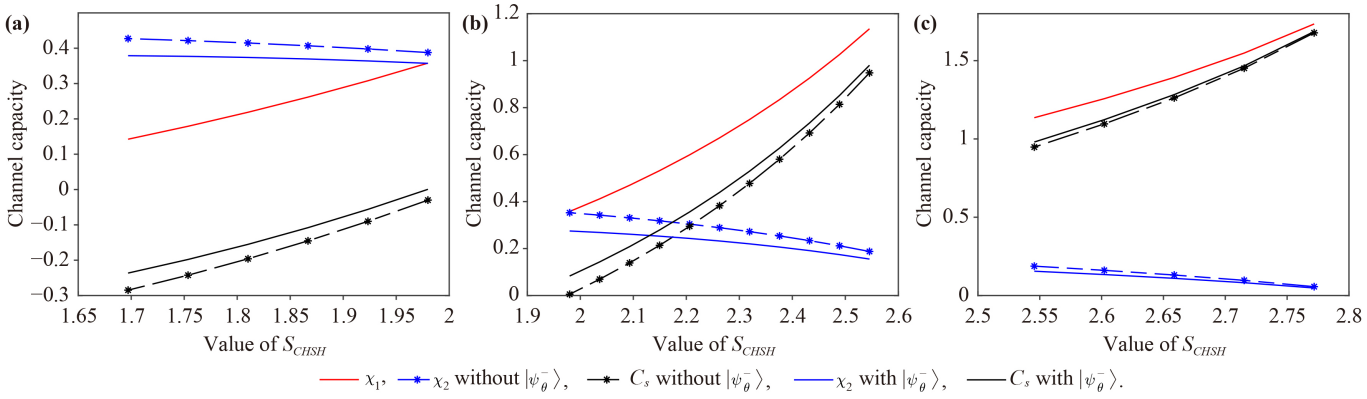



**Fig. 4** The relation of channel capacity and the value of $S_{CHSH}$. In **(a)**, based on the starting positions on the left, the lines from top to bottom are the capacity of the wiretap channel without intermediate-basis EPR pairs, the capacity of the wiretap channel with intermediate-basis EPR pairs, the capacity of the main channel, the capacity of the secrecy channel with intermediate-basis EPR pairs, and the capacity of the secrecy channel without intermediate-basis EPR pairs. In **(b)** and **(c)**, based on the starting positions on the left, the lines from top to bottom are the capacity of the main channel, the capacity of the wiretap channel without intermediate-basis EPR pairs, the capacity of the wiretap channel with intermediate-basis EPR pairs, the capacity of the secrecy channel with intermediate-basis EPR pairs, and the capacity of the secrecy channel without intermediate-basis EPR pairs. Simulation parameters: reception rates $Q_B$ and $Q_E$ are all set to 1.

$Q_E$ that represent the receiving capability of Bob and Eve channels. The lower channel capacity bound of $C_s$ is given by [14]

$$C_s \geq Q_B\left[3 - h_8(\boldsymbol{e})\right] - Q_E\left[h(\epsilon_x) + h(\epsilon_z)\right]. \tag{17}$$

Figure 4 shows the channel capacity of the proposed QSDC protocol. Figure 4(a) depicts the extreme adverse condition where the two particles lose their entanglement completely. $\psi_{\theta_i}^-$ cannot improve the security of the protocol, and the $C_s$ of the two protocols are all negative. Therefore, the transfer process is unsafe. In Fig. 4(b), when entanglement between the two particles exists but is not strong, two $C_s$ are still positive, but compared with Fig. 4(c), they decrease. Figure 4(c) describes when a channel is almost perfect and entanglement of the two particles is intact, $C_s$ in the original two-step QSDC protocol and the new protocol are all positive, thus, the transfer process under coherent attack is secure. Besides, the blue solid line is always lower than the blue dotted line, which means the upper bound Eve can steal reduces, so that the amount of effective information between legitimate parties increases.

### 3.2 Security analysis under an optional eavesdropping strategy

Now consider a more powerful strategy that Eve can employ a higher dimension ancilla system since the Stinespring dilation theorem [42] allows Eve to resort to a four-dimensional system or two qubits to carry out an attack in order to obtain a higher probability of guessing right. The attack process can be reexpressed as

$$U_{BE}\left|a\right\rangle\left|E'\right\rangle = \left|a\right\rangle\left|F_a\right\rangle + \left|a^{\perp}\right\rangle\left|D_a\right\rangle, \tag{18}$$

where $\left|\alpha\right\rangle \in \{\left|0\right\rangle, \left|1\right\rangle, \left|+\right\rangle, \left|-\right\rangle\}$ and $\left\langle\alpha|\alpha^{\perp}\right\rangle = 0$. $\left|E'\right\rangle$ is a higher-dimensional ancilla system, $\left|F_\alpha\right\rangle$ and $\left|D_\alpha\right\rangle$ are Eve's state after the interaction under guessing right or wrong, respectively.

For the proposed protocol, the optional unitary interactions are [32]

$$\begin{aligned}
&U\left|0\right\rangle\left|E'\right\rangle = \left|0\right\rangle\left|F_0\right\rangle + \left|1\right\rangle\left|D_0\right\rangle,\\
&U\left|1\right\rangle\left|E'\right\rangle = \left|1\right\rangle\left|F_1\right\rangle + \left|0\right\rangle\left|D_1\right\rangle,\\
&U\left|+\right\rangle\left|E'\right\rangle = \left|+\right\rangle\left|F_+\right\rangle + \left|-\right\rangle\left|D_+\right\rangle,\\
&U\left|-\right\rangle\left|E'\right\rangle = \left|-\right\rangle\left|F_-\right\rangle + \left|+\right\rangle\left|D_-\right\rangle.\\
&U\left|\theta_i\right\rangle\left|E'\right\rangle = \left|\theta_i\right\rangle\left|F_{\theta_i}\right\rangle + \left|\theta_i^{\perp}\right\rangle\left|D_{\theta_i}\right\rangle,\\
&U\left|\theta_i^{\perp}\right\rangle\left|E'\right\rangle = \left|\theta_i^{\perp}\right\rangle\left|F_{\theta_i^{\perp}}\right\rangle + \left|\theta_i\right\rangle\left|D_{\theta_i^{\perp}}\right\rangle,
\end{aligned} \tag{19}$$

where $\left|F_{0,1,+,-,\theta_i,\theta_i^{\perp}}\right\rangle$ and $\left|D_{0,1,+,-,\theta_i,\theta_i^{\perp}}\right\rangle$ are Eve's ancillary states after the interaction. And the relations between Eve's states in the two bases are

$$\begin{aligned}
&2\left|F_{\pm}\right\rangle = \left|F_0\right\rangle + \left|F_1\right\rangle \pm \left|D_0\right\rangle \pm \left|D_1\right\rangle,\\
&2\left|D_{\pm}\right\rangle = \left|F_0\right\rangle - \left|F_1\right\rangle \mp \left|D_0\right\rangle \pm \left|D_1\right\rangle.
\end{aligned} \tag{20}$$

Assuming that the unitary $U_{BE}$ is such that Eve's unnormalized states are orthogonal of the following form (in Eve's two-qubit computational basis),

$$\begin{aligned}
\left|F_0\right\rangle &= \left(\sqrt{F}, 0, 0, 0\right)^{\mathrm{T}},\\
\left|F_1\right\rangle &= \left(\sqrt{F}\cos x, 0, 0, \sqrt{F}\sin x\right)^{\mathrm{T}},\\
\left|D_0\right\rangle &= \left(0, \sqrt{D}, 0, 0\right)^{\mathrm{T}},\\
\left|D_1\right\rangle &= \left(0, \sqrt{D}\cos y, \sqrt{D}\sin y, 0\right)^{\mathrm{T}},
\end{aligned} \tag{21}$$

where

$$F = 1 - D,\ D = \frac{1 - \cos x}{2 - \cos x + \cos y}, \tag{22}$$

and $x$, $y$ are two arbitrary angles. Then according to the conditional total output state,

$$\rho_{BE|_\alpha} = U\left|\alpha\right\rangle\left\langle\alpha\right| \otimes \left|E'\right\rangle\left\langle E'\right| U^{\dagger}, \tag{23}$$

Bob's conditional state is

$$\begin{aligned}
\rho_{B|_\alpha} &= Tr_E\left(\rho_{BE|_\alpha}\right)\\
&= F^{-1}\left\langle F_\alpha \mid \rho_{BE|_\alpha} \mid F_\alpha\right\rangle + D^{-1}\left\langle D_\alpha \mid \rho_{BE|_\alpha} \mid D_\alpha\right\rangle\\
&= F\left|\alpha\right\rangle\left\langle\alpha\right| + D\left|\alpha^{\perp}\right\rangle\left\langle\alpha^{\perp}\right|,
\end{aligned} \tag{24}$$

while Eve's conditional output state is

$$\rho_{E|_\alpha} = \left|F_\alpha\right\rangle\left\langle F_\alpha\right| + \left|D_\alpha\right\rangle\left\langle D_\alpha\right|. \tag{25}$$

In this way, Eve has a higher probability of correct guessing at the same QBER, as shown in Fig. 5.

Once again, according to the Wiretap channel model [36], the channel capacity of the QSDC protocol under a higher-dimensional attack is shown in Fig. 6. It can be seen that the preservation of entanglement is still the

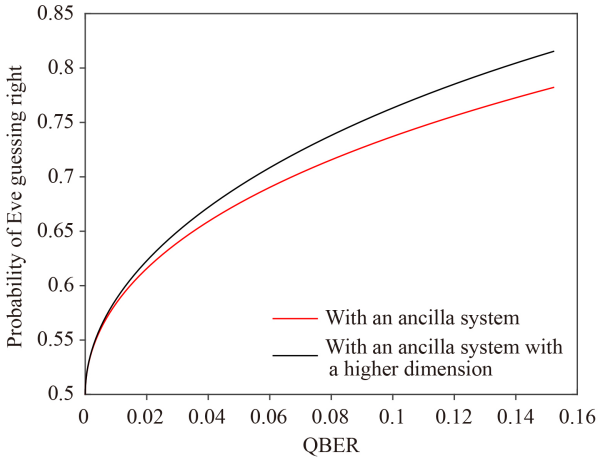



**Fig. 5** Eve's attack capability with different auxiliary systems.

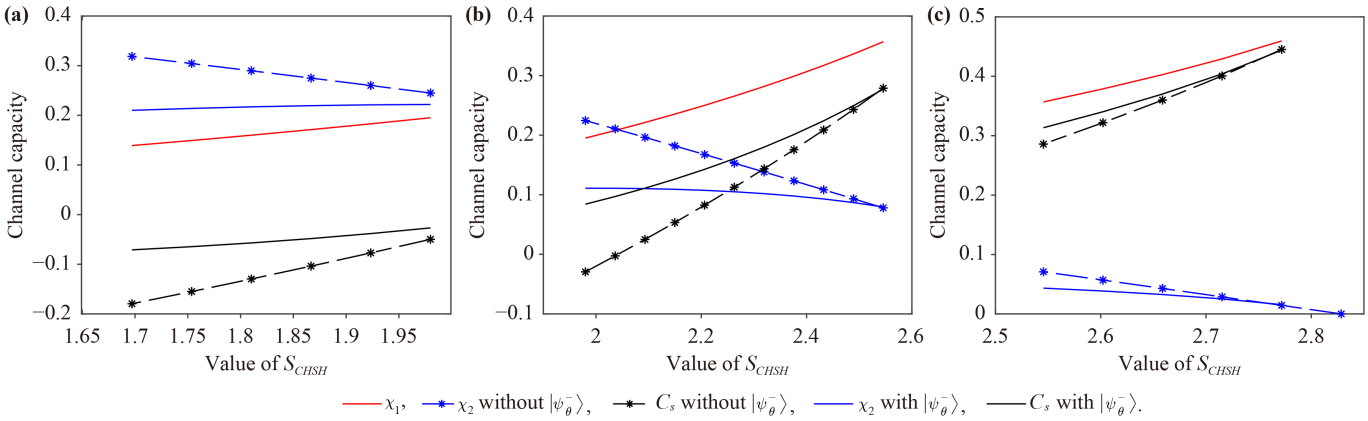



**Fig. 6** The relation of channel capacity and the value of $S_{CHSH}$. In **(a)**, the lines from top to bottom are the capacity of the wiretap channel without intermediate-basis EPR pairs, the capacity of the wiretap channel with intermediate-basis EPR pairs, the capacity of the main channel, the capacity of the secrecy channel with intermediate-basis EPR pairs, and the capacity of the secrecy channel without intermediate-basis EPR pairs. In **(b)**, the lines from top to bottom are the capacity of the wiretap channel without intermediate-basis EPR pairs, the capacity of the main channel, the capacity of the wiretap channel with intermediate-basis EPR pairs, the capacity of the secrecy channel with intermediate-basis EPR pairs, and the capacity of the secrecy channel without intermediate-basis EPR pairs. In **(c)**, based on the starting positions on the left, the lines from top to bottom are the capacity of the main channel, the capacity of the secrecy channel with intermediate-basis EPR pairs, the capacity of the secrecy channel without intermediate-basis EPR pairs, the capacity of the wiretap channel without intermediate-basis EPR pairs, and the capacity of the wiretap channel with intermediate-basis EPR pairs. Simulation parameters: reception rates $Q_B$ and $Q_E$ are all set to 1.

premise of protocol security. Although the $C_s$ in Figs. 6(b) and (c) are all positive, the channel capacity under higher-dimensional attack is much lower compared with that in Figs. 4(b) and (c). Fortunately, the intermediate-basis EPR pairs play a positive role in dealing with these two attacks, and both reduce the amount of information obtained by Eve.

## 4 Conclusion and discussion

We make a comparison of the original two-step protocol and the proposed protocol in Table 2 from aspects of efficiency and safety analysis.

Due to the intermediate-bisis EPR pairs, the probability of Eve choosing the correct measurement basis reduces from $\frac{1}{2}$ to $\frac{1}{3}$. Moreover, they not only enhance the security of particle transmission in the first step but also improve the transmission efficiency of information in the second step. In the security analysis of the new protocol, two attacks with different dimensions are considered. Under the premise of ensuring the security of the protocol, the amount of information obtained by Eve is lessened, hence, the amount of communication information between the legal parties is increased.

However, any quantum system inevitably interacts with the environment and thus results in decoherence. The effect of the noise should be carefully considered in order to estimate the success probability of the proposal. Therefore, the practical security of this protocol, including decoherence effect, active attack and passive attack of Eve will be studied by some exact and efficient quantum algorithms [43, 44]. The research on the practical security of the protocol will further optimize our protocol, which will be the focus of our future work. Therefore, the proposed protocol will further enrich the technology of QSDC and promote the implementation of a practical QSDC system.

**Table 2** Comparison of the advantages and disadvantages of the new protocol and the original two-step protocol.

| | **The original two-step protocol** | **The proposed protocol** |
|---|---|---|
| Probability of Eve guessing right | $\frac{1}{2}$ | $\frac{1}{3}$ |
| Upper bound of the amount of secret information stole by Eve | Higher | Lower |
| Necessary quantum resource | $\|\psi^-\rangle$ | $\left\|\psi_{\theta_i}^-\right\rangle$, $\|\psi^-\rangle$ |
| Encoding methods | 4 kinds | 8 kinds |
| Encoding efficiency | 2 bit per operation | 3 bit per operation |

**Acknowledgements** This work was supported by the National Natural Science Foundation of China (Grant No. 62071381), Shaanxi Provincial Key R&D Program General Project (Grant No. 2022GY-023), ISN 23rd Open Project (Grant No. ISN23-06) of the State Key Laboratory of Integrated Services Networks (Xidian University), and Qinchuangyuan "Scientist + Engineer" Team Construction Project of Shaanxi Province of China (Grant No. 2022KXJ-009).

## References

1. P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, Proceedings of 35th Annual Symposium on Foundations of Computer Science, 1994, pp 124–134
2. R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM* 21(2), 120 (1978)
3. C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* 560, 7 (2014)
4. S. Srikara, K. Thapliyal, and A. Pathak, Continuous variable direct secure quantum communication using Gaussian states, *Quantum Inform. Process.* 19(4), 132 (2020)
5. D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Experimental quantum teleportation, *Nature* 390(6660), 575 (1997)
6. G. L. Long and X. S. Liu, Theoretically efficient high-capacity quantum-key distribution scheme, *Phys. Rev. A* 65(3), 032302 (2002)
7. Y. C. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, Long-distance continuous-variable quantum key distribution over 202.81 km fiber, *Phys. Rev. Lett.* 125(1), 010502 (2020)
8. M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, *Nature* 557(7705), 400 (2018)
9. A. Furusawa, J. L. Srensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, Unconditional quantum teleportation between distant solid-state quantum bits, *Science* 345(6196), 532 (1998)
10. S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, Advances in quantum teleportation, *Nat. Photonics* 9(10), 641 (2015)
11. P. Zawadzki, Advances in quantum secure direct communication, *IET Quantum Commun.* 2(2), 54 (2021)
12. 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(4), 042317 (2003)
13. F. G. Deng and G. L. Long, Secure direct communication with a quantum one-time pad, *Phys. Rev. A* 69(5), 052319 (2004)
14. J. Wu, Z. Lin, L. Yin, and G. L. Long, Security of quantum secure direct communication based on Wyners wiretap channel theory, *Quantum Eng.* 1(4), e26 (2019)
15. R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G. L. Long, Implementation and security analysis of practical quantum secure direct communication, *Light Sci. Appl.* 8(1), 22 (2019)
16. Z. Ye, D. Pan, Z. Sun, C. Du, and G. L. Long, Generic security analysis framework for quantum secure direct communication, *Front. Phys.* 16(2), 1 (2020)
17. J. Y. Hu, B. Yu, M. Y. Jing, L. T. Xiao, S. T. Jia, G. Q. Qin, and G. L. Long, Experimental quantum secure direct communication with single photons, *Light Sci. Appl.* 5(9), e16144 (2016)
18. W. Zhang, D. S. Ding, Y. B. Sheng, L. Zhou, B. S. Shi, and G. C. Guo, Quantum secure direct communication with quantum memory, *Phys. Rev. Lett.* 118(22), 220501 (2017)
19. F. Zhu, W. Zhang, Y. B. Sheng, and Y. D. Huang, Experimental long-distance quantum secure direct communication, *Sci. Bull. (Beijing)* 62(22), 1519 (2017)
20. Z. Sun, R. Qi, Z. Lin, L. Yin, G. Long, and J. Lu, Design and implementation of a practical quantum secure direct communication system, 2018 IEEE Globecom Workshops (GC Wkshps), 18472318 (2018)
21. Z. R. Zhou, Y. B. Sheng, P. H. Niu, L. Yin, G. L. Long, and L. Hanzo, Measurement-device-independent quantum secure direct communication, *Sci. China Phys. Mech. Astron.* 63(3), 230362 (2020)
22. T. Li, Z. K. Gao, and Z. H. Li, Measurement-device–independent quantum secure direct communication: Direct quantum communication with imperfect measurement device and untrusted operator, *Europhys. Lett.* 131(6), 60001 (2020)
23. P. H. Niu, J. W. Wu, L. G. Yin, and G. L. Long, Security analysis of measurement-device-independent quantum secure direct communication, *Quantum Inform. Process.* 19(10), 356 (2020)
24. Z. Gao, M. Ma, T. Liu, J. Long, T. Li, and Z. Li, Free-space quantum secure direct communication based on decoherence-free space, *J. Opt. Soc. Am. B* 37(10), 3028 (2020)
25. D. Pan, Z. Lin, J. Wu, H. Zhang, Z. Sun, D. Ruan, L. Yin, and G. L. Long, Experimental free-space quantum secure direct communication and its security analysis, *Photon. Res.* 8(9), 1522 (2020)
26. X. F. Zou and D. W. Qiu, Three-step semiquantum secure direct communication protocol, *Sci. China Phys. Mech. Astron.* 57(9), 1696 (2014)
27. Z. Rong, D. Qiu, P. Mateus, and X. F. Zou, Mediated semi-quantum secure direct communication, *Quantum Inform. Process.* 20(2), 58 (2021)
28. Z. Rong, D. Qiu, and X. Zou, Two single-state semi-quantum secure direct communication protocols based on single photons, *Int. J. Mod. Phys. B* 34(11), 2050106 (2020)
29. Z. Rong, D. Qiu, and X. Zou, Semi-quantum secure direct communication using entanglement, *Int. J. Theor. Phys.* 59(6), 1807 (2020)
30. G. Chai, Z. W. Cao, W. Q. Liu, M. H. Zhang, K. X. Liang, and J. Y. Peng, Novel continuous-variable quantum secure direct communication and its security analysis, *Laser Phys. Lett.* 16(9), 095207 (2019)
31. 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(2), 024012 (2021)
32. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, *Adv. Opt. Photonics* 12(4), 1012 (2020)
33. A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* 67(6), 661 (1991)
34. D. Collins and N. Gisin, A relevant two qubit Bell inequality inequivalent to the CHSH inequality, *J. Phys. Math. Gen.* 37(5), 1775 (2004)
35. A. Khrennikov, CHSH inequality: Quantum probabilities as classical conditional probabilities, *Found. Phys.* 45(7), 711 (2015)
36. S. Leung-Yan-Cheong and M. Hellman, The Gaussian wire-tap channel, *IEEE Trans. Inf. Theory* 24(4), 451 (1978)
37. N. Cai, A. Winter, and R. W. Yeung, Quantum privacy and quantum wiretap channels, *Probl. Inf. Transm.* 40(4), 318 (2004)
38. I. Devetak, The private classical capacity and quantum capacity of a quantum channel, *IEEE Trans. Inf. Theory* 51(1), 44 (2005)
39. M. Hayashi, Quantum wiretap channel with non-uniform random number and its exponent and equivocation rate of leaked information, *IEEE Trans. Inf. Theory* 61(10), 5595 (2015)
40. A. Winter, Coding theorem and strong converse for quantum channels, *IEEE Trans. Inf. Theory* 45(7), 2481 (1999)
41. L. Zhou, Y. B. Sheng, and G. L. Long, Device-independent quantum secure direct communication against collective attacks, *Sci. Bull. (Beijing)* 65(1), 12 (2020)
42. D. Kretschmann, D. Schlingemann, and R. F. Werner, A continuity theorem for stinesprings dilation, *J. Funct. Anal.* 255(8), 1889 (2008)
43. 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 Inform.* 4(1), 52 (2018)
44. X. Y. Chen, N. N. Zhang, W. T. He, X. Y. Kong, M. J. Tao, F. G, Deng, Q. Ai, and G. L. Long, Global correlation and local information flows in controllable non-Markovian open quantum dynamics, *npj Quantum Inform.* 8(1), 22 (2022)