Vol 16 No 9, September 2007
1009-1963/2007/16(09)/2549-08

Chinese Physics

© 2007 Chin. Phys. Soc.
and IOP Publishing Ltd

Secure deterministic communication scheme based on quantum remote state preparation*

Guo Ying(郭 迎)[a)b)†], Chen Zhi-Gang(陈志刚)[a)], and Zeng Gui-Hua(曾贵华)[b)]

[a)] *School of Information Science and Engineering, Central South University, Changsha* 410083, *China*
[b)] *Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai* 200030, *China*

(Received 20 December 2006; revised manuscript received 1 March 2007)

Based on the techniques of the quantum remote state preparation via a deterministic way, this paper proposes a quantum communication scheme to distribute the secret messages in two phases, i.e., the carrier state checking phase and the message state transmitting phase. In the first phase, the secret messages are encoded by the sender using a stabilizer quantum code and then transmitted to the receiver by implementing three CNOT gates. In the second phase, the communicators check the perfectness of the entanglement of the transmitted states. The messages can be distributed to the receiver even if some of the transmitted qubits are destroyed.

Keywords: Quantum deterministic communication, quantum error-correction code, quantum cryptography, quantum computing

PACC: 0365, 0367

1. Introduction

Quantum key distribution (QKD), the approach using quantum mechanics principles for the distribution of the secret keys between the communicators with negligibly small leakage of information to an eavesdropper, has been developed rapidly since Bennett and Brassard designed the original QKD protocol in 1984 (BB84 protocol).[1] Currently, there are many QKD schemes,[2−6] which may be divided into two categories, i.e., nondeterministic QKD schemes,[5] and deterministic QKD schemes.[6] In the nondeterministic QKD, the sender, Alice, chooses randomly two sets of the measuring basis to produce two kinds of the orthogonal states, and transmits them to the receiver, Bob. After receiving the states, Bob also chooses randomly one of two sets of basis to measure them. There is only a certain probability that Alice and Bob choose the same measurement basis. So Alice cannot determine which qubits have been received by Bob before exchanging the classical information. The nondeterministic property leads to loss of lots of qubits; hence, the transmitting efficiency is very low. However, in the deterministic QKD, Alice and Bob can choose the same orthogonal basis for the measurements. Thus, Bob can deterministically obtain Alice's information if quantum channel is not disturbed seriously.

Different from QKD, whose object is to establish the random keys between the communicators, quantum secure deterministic communication (QSDC) is to transmit the exact messages.[7−11] Thus, it must satisfy two conditions. Firstly, the transmitted messages should be read out directly by the legitimate receivers, and no additional classical information should be required. Secondly, the messages, which may be encoded in some distributed qubits, should not be leaked to an eavesdropper (Eve), even if she catches hold of quantum channel.

After the initial QSDC was proposed by making use of the single-qubit states,[7] Boström and Felbinger presented the 'ping–pong' protocol to distribute the classical messages with the two-qubit-entangled states.[8] However, Eve can eavesdrop on the distributed messages if channel is noisy, and the protocol can be attacked without eavesdropping.[10,11] Afterward, Cai and Li presented an improved 'ping–pong' protocol,[12] which allows one entanglement state to carry two classical bit messages. The security is ensured via the conjugate measurement basis. However, it is still insecure while being implemented in noisy channel, and it is vulnerable to the opaque attack. Then, Deng and Long proposed a QSDC scheme by making use of the single photons in batches.[9] The

*Project supported by the National Natural Science Foundation of China (Grant Nos 60472018, 60573127 and 10547125), the Doctoral Programs Foundation of the Ministry of Education of China (Grant No 20020247063).
†E-mail: yingguo1001@sjtu.edu.cn

states of the single photons themselves serve as an one-time pad, and the secret classical messages are encoded by two different unitary operations, which may be viewed as a modification of BB84 protocol. However, there may be some loss during the process of the transmissions of the qubits in their scheme.

Recently, many quantum error correction codes (QECC)[13−15] have been constructed in theoretics or experiment. Since the presented codes can offer some elegant ways to defend the secret messages from quantum noises or quantum loss, they can be used for the designation of a QSDC scheme implemented in the imperfect quantum channel. In this paper, we propose a new QSDC to distribute the secret quantum messages (or the classical messages) with high fidelity by making use of the entanglement state of QECC. The messages are distributed to the legal receivers via implementing three CNOT gates onto the non-orthogonal quantum states. The security of this scheme is also guaranteed by the transmissions of the non-orthogonal three-qubit-entangled states, which have been proved to be secure to be distributed in the imperfect channel.[16−18] The present scheme is simple to be implemented in practice with the current techniques.[19−21]

The paper is arranged as following. In Section 2, some notations and definitions of the stabilizer quantum code (SQC), which is a kind of QECC, are given before designing the QSDC scheme. In Section 3, the proposed scheme is described in detail to distribute the k-qubit messages with security. To show the unconditional security of this scheme, proofs are presented in Section 4. Finally, conclusions are drawn in Section 5.

2. Notations and definitions of SQC

In the single-qubit depolarizing channel, there are four basic operators: I, $X=\sigma_x$, $Z=\sigma_z$ and $Y=ZX$, where σ_x and σ_z are Pauli operators.[22] So, an arbitrary n-qubit operator in the n-qubit depolarizing channel belongs to the Pauli group $G_n=\{\mu_{\rm i}^{\otimes n}\}$, where $\mu_{\rm i}\in\{\pm I,\pm X,\pm Z,\pm Y,\ \pm{\rm i}I,\pm{\rm i}X,\pm{\rm i}Z,\pm{\rm i}Y\}$ and $\otimes n$ denotes the n-fold tensor product. All operators in G_n either commute or anti-commute with each other.

SQC $[[n,k,d]]$ has the stabilizer denoted by

$$\mathcal{S}=\left\{\prod_{j=1}^{n-k}M_j^{b_j}:b_j\in\{0,1\},j=1,2,\cdots,n-k\right\},\tag{1}$$

where $M_1,\cdots,M_{n-k}\in G_n$ are (mutually commuting) generators of $\mathcal{S}$. Code words of SQC are states generated by the eigenvectors associated with eigenvalue '1' of $\mathcal{S}$, i.e.,

$$C(\mathcal{S})=\{|\upsilon\rangle:M|\upsilon\rangle=|\upsilon\rangle,M\in\mathcal{S}\}.\tag{2}$$

It can correct, at most, $t=(d-1)/2$ quantum errors. The normalizer can be denoted by

$$\mathcal{N}(\mathcal{S})=\{\bar{Z}:\bar{Z}M=M\bar{Z},\bar{Z}\in G_n,M\in\mathcal{S}\}.\tag{3}$$

There are $n+k$ (mutually commuting) independent generators of $\mathcal{N}(\mathcal{S})$ denoted by $\{\bar{Z}_m:1\le m\le n+k\}$. For two arbitrary operators $\bar{Z}_i,\bar{Z}_j\in\mathcal{N}(\mathcal{S})$, it is easy to see that $\bar{Z}_i+\bar{Z}_j$ and $\bar{Z}_i\bar{Z}_j$ belong to $\mathcal{N}(\mathcal{S})$. It implies that $\mathcal{N}(\mathcal{S})$ can generate a linear subspace of G_n. Thus, k operators $\mathcal{Z}_1,\cdots,\mathcal{Z}_k$ can be selected from $\mathcal{N}(\mathcal{S})$ such that the set

$$\Omega=\{M_1,\cdots,M_{n-k},\mathcal{Z}_1,\cdots,\mathcal{Z}_k\}\tag{4}$$

is an independently commuting set. For $\mathcal{Z}_i\in\Omega$ $(1\le i\le k)$, there is an operator $\mathcal{X}_i\in G_n$ satisfying $\mathcal{X}_i\mathcal{Z}_i=-\mathcal{Z}_i\mathcal{X}_i$, $\mathcal{X}_iM_l=M_l\mathcal{X}_i$ and $\mathcal{X}_i\mathcal{Z}_j=\mathcal{Z}_j\mathcal{X}_i$ for $j\ne i$, where $1\le j\le k$ and $1\le l\le n-k$. Since the encoding on n qubits can be written as the tensor product of the (single) qubit states,[13] the encoder of SQC generates a logical state

$$\begin{aligned}|q_k\rangle_L&=\frac{1}{\sqrt{2^{n-k}}}\left(\prod_{i=1}^{n-k}(I^{\otimes n}+M_i)\right)\mathcal{X}_1^{c_1}\cdots\mathcal{X}_k^{c_k}|\mathbf{0}_n\rangle)\\&=\frac{1}{\sqrt{2^{n-k}}}\left(\mathcal{X}_1^{c_1}\cdots\mathcal{X}_k^{c_k}\sum_{M\in\mathcal{S}}M|\mathbf{0}_n\rangle\right),\end{aligned}\tag{5}$$

where $\{|q_k\rangle=|c_1\cdots c_k\rangle:c_i\in\{0,1\},1\le i\le k\}$ are the basis of the k-qubit messages and $|\mathbf{0}_n\rangle=|0\cdots0\rangle$ is the initially prepared n-qubit state. Thus, the k-qubit messages, denoted by $|c\rangle=\sum_k m_k|q_k\rangle$, can be encoded into the n-qubit state $|c\rangle_L=\sum_k m_k|q_k\rangle_L$ via Eq.(5).

To encode $|c\rangle$ into $|c\rangle_L$, one should perform the corresponding operators $\mathcal{X}_1^{c_1}\cdots\mathcal{X}_k^{c_k},M_1,\cdots,M_{n-k}$ onto the initial state $|\mathbf{0}_n\rangle$ according to Eq.(5). On the other hand, to recover $|c\rangle$ from the received state, denoted by $|c'\rangle_L$, we must perform the recovery operators R_i to detect and correct quantum errors, along with the inverse transforms in Eq.(5).[23]

To get R_i, we need to calculate the syndromes s of the error operators of $|c'\rangle_L$ by making use of the generators of $\mathcal{S}$. Note that the syndromes s may be defined as $s = (s_1 \cdots s_{n-k})$, where $\{s_l : s_l \in \{0,1\}, M_l|c'\rangle_L = (-1)^{s_l}|c'\rangle_L, 1 \le l \le n-k\}$. If the number of the destroyed qubits of $|c'\rangle_L$ is, at most, t, we can obtain R_i to recover $|c\rangle$ from $|c'\rangle_L$ by making use of the generators of SQC.[22]

3. Descriptions of the present scheme

When two photons are maximally entangled, each photon is not polarized at all. Denote the horizontal state and the vertical polarization state by $|0\rangle$ and $|1\rangle$, respectively. Thus, the two-qubit state

$$|\Phi_1(h,t)\rangle = \frac{1}{\sqrt{2}}(|0_h\rangle|0_t\rangle + |1_h\rangle|1_t\rangle) \tag{6}$$

is a maximally entangled state in two-photon Hilbert space $\mathcal{H} = \mathcal{H}_h \otimes \mathcal{H}_t$, where two subscripts h and t express two photons p_h and p_t in the entangled state, respectively.

After applying the operation H on p_t of the state $|\Phi_1(h,t)\rangle$, one obtains

$$\begin{aligned} |\Phi_2(h,t)\rangle &= (I \otimes H)|\Phi_1(h,t)\rangle \\ &= \frac{1}{\sqrt{2}}(|0_h\rangle|+_t\rangle + |1_h\rangle|-_t\rangle), \end{aligned} \tag{7}$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ and $H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$. Assume the transmitted n-qubit message state $|c\rangle_L$ can be denoted by $|w_{1m}\rangle \cdots |w_{nm}\rangle$, where $|w_{im}\rangle$ $(1 \le i \le n)$ is an arbitrary single-qubit state of $|c\rangle_L$ corresponding to the message photon p_m. Obviously, we can calculate the following two relationships:

$$\begin{aligned} & C_{hm}(C_{mh}(C_{tm}(|\Phi_1(h,t)\rangle \otimes |w_{im}\rangle))) \\ &= |w_{ih}\rangle \otimes \frac{1}{\sqrt{2}}(|0_t\rangle|0_m\rangle + |1_t\rangle|1_m\rangle) \\ &= |w_{ih}\rangle \otimes |\Phi_1(t,m)\rangle, \end{aligned} \tag{8}$$

and

$$\begin{aligned} & C_{tm}(C_{mt}(C_{tm}(|\Phi_2(h,t)\rangle \otimes |w_{im}\rangle))) \\ &= |w_{it}\rangle \otimes \frac{1}{\sqrt{2}}(|0_h\rangle|+_m\rangle + |1_h\rangle|-_m\rangle) \\ &= |w_{it}\rangle \otimes |\Phi_2(h,m)\rangle, \end{aligned} \tag{9}$$

where C is a CNOT gate defined by $|00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$, $|\Phi_1(t,m)\rangle$ is an entanglement state of two photons p_t and p_m, and $|\Phi_2(h,m)\rangle$ is an entanglement state of two photons p_h and p_m.

We note that $\langle\Phi_2(h,t)|\Phi_1(h,t)\rangle \neq 0$ and $\langle w_{im}|\langle\Phi_2(h,t)|U^\dagger U|\Phi_1(h,t)\rangle|w_{im}\rangle \neq 0$, where U is an arbitrary unitary operation performed on three possible photons p_h, p_t and p_m. Thus, the properties in Eqs.(8) and (9) are perfectly suited for a cryptographic scenario of QSDC. To distribute the secret k-qubit messages $|c\rangle$ with security, the communicators should share n operators $\mathcal{X}_1, \cdots, \mathcal{X}_k, M_1, \cdots, M_{n-k}$ beforehand. Then, they implement the following four-step scheme, which is shown in Fig.1.

Step 1 Bob prepares the state $|\Phi_1(h,t)\rangle$ and performs an arbitrary operator $\mu \in \{I, H\}$ on p_h. Keeping p_h in his own hand and transmitting p_t to Alice, Alice and Bob share two possible entanglement states described in Eqs.(6) and (7).

Step 2 Alice prepares the message photon p_m corresponding to the transmitted qubit $|w_{im}\rangle$. She chooses one carrier state $|\Phi_1(h,t)\rangle$ or $|\Phi_2(h,t)\rangle$ as a carrier. After applying C_{tm} on p_t and p_m of $|\Phi_1(h,t)\rangle \otimes |w_{im}\rangle$ or $|\Phi_2(h,t)\rangle \otimes |w_{im}\rangle$, she returns p_t and p_m to Bob.

Step 3 When Bob receives p_t and p_m, he checks the perfectness of the entanglement of the initial carrier state $|\Phi_1(h,t)\rangle$ (or the state $|\Phi_2(h,t)\rangle$) and obtains $|w_{im}\rangle$ according to his operation μ. Namely, for $\mu = I$, Bob obtains $|\Phi_1(t,m)\rangle$ after performing C_{mh} and C_{hm}. If $|\Phi_1(t,m)\rangle = |\Phi_1(h,t)\rangle$, the transmitted carrier state is perfect without being destroyed. Then, he gains one-qubit state, denoted by $|w'_{im}\rangle$, by measuring the state of p_h. For $\mu = H$, he obtains $|\Phi_2(h,m)\rangle$ after performing C_{mt} and C_{tm}. If $|\Phi_2(h,m)\rangle = |\Phi_2(h,t)\rangle$, the transmitted carrier state is kept well. Then, he also obtains one-qubit state $|w'_{im}\rangle$ after measuring the state of p_t.

Step 4 After the communicators implement above steps for n scheme runs, Bob receives the distributed state $|c'\rangle_L = |w'_{1m}\rangle|w'_{2m}\rangle \cdots |w'_{nm}\rangle$, which may be different from $|c\rangle_L$ because of the effect of the noises of quantum channel and the possible attackers. However, if the number of the destroyed qubits of $|c'\rangle_L$ is no more than t, Bob can always recover the secret messages $|c\rangle$ from $|c'\rangle_L$ by making use of the decoder of SQC.

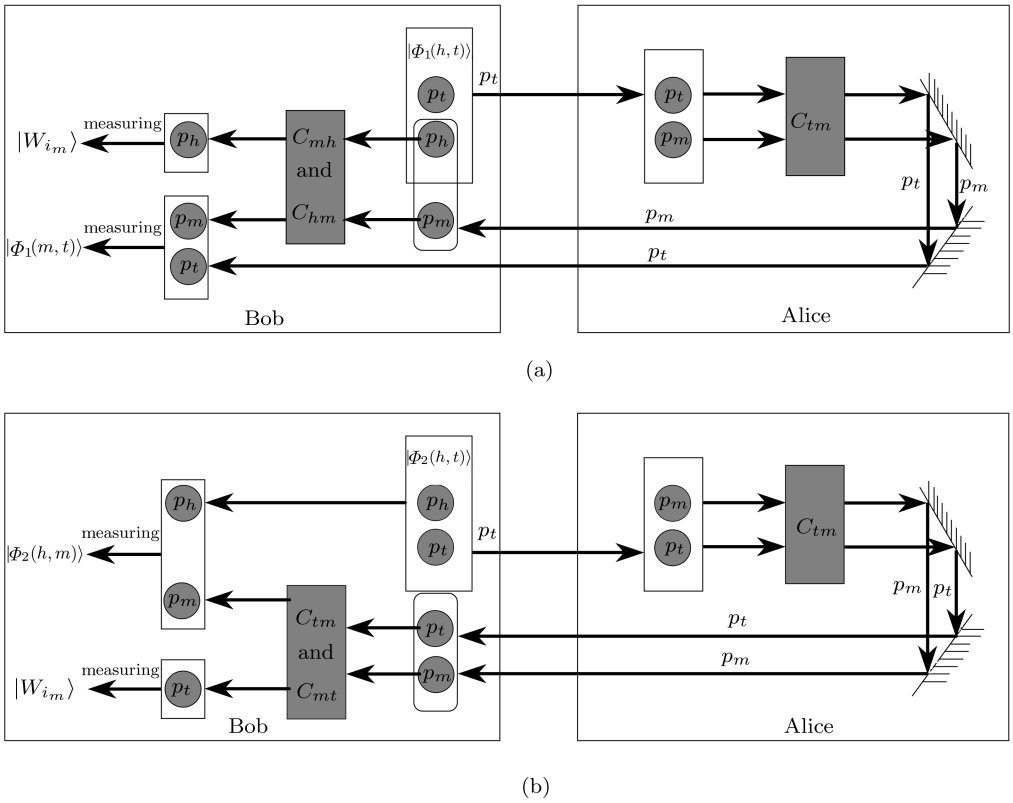


Fig.1. (a) The process of the message state transmitting phase and carrier state checking phase using the state $\Phi_1(h,t)$, and (b) the process of message state transmitting phase and carrier state checking phase using the state $\Phi_2(h,t)$.

The perfectness of the entanglement of the carrier states, $|\Phi_1(h,t)\rangle$ and $|\Phi_2(h,t)\rangle$, is important in the present scheme. Since there is only one carrier state distributed for one scheme run, the approach in EPR protocol[5] to check the perfectness of the entanglement of the distributed state is unavailable in this scheme. Thus, the relations in Eqs.(8) and (9) are utilized to check the perfectness of the distributed carrier state.

According to Eqs.(6) and (7), the random operation μ may yield two possible states $C_{tm}|\Phi_1(h,t)\rangle|w_{im}\rangle$ and $C_{tm}|\Phi_2(h,t)\rangle|w_{im}\rangle$. It is easy to prove $\langle w_{im}|\langle\Phi_2(h,t)|C_{tm}^{\dagger}C_{tm}|\Phi_1(h,t)\rangle|w_{im}\rangle \neq 0$, which guarantees that the optimal Bell analyser[24] will not be useful in the present scheme. Subsequently, many attack strategies, such as man-in-the-middle attack[25] and Trojan horse attack,[26] can also be prevented.

4. Security analysis

Analogous to classic cryptography, attack strategies in quantum cryptography include the passive attack strategy and the active attack strategy. The attackers, Eve, can eavesdrop ciphertext in the former strategy. However, Eve may change or alter ciphertext in the later strategy. Generally, the active attack strategy is beyond the framework of quantum cryptosystem since it belongs to the framework of quantum authentication, including quantum identity verification,[27,28] quantum signature,[29] and so on. So, only the passive attack strategy is focused in this paper.

Security analysis of the present scheme can be divided into two stages: the stage for the carrier state $|\Phi_1\rangle$ or $|\Phi_2\rangle$, and the stage for the transmitted state $|w_{im}\rangle$. In the first stage, the aim is to check the perfectness of the entanglement of the carrier state. However, in the second stage, the aim is to analyse the security of the transmitted state $|w_{im}\rangle$.

Theorem 1 Assume that Eve takes an attack strategy by applying an arbitrary operation $U(\varepsilon)$ on $|\Phi_1\rangle$ or $|\Phi_2\rangle$. Then, $U(\varepsilon)$ can be detected easily by Bob, which implies that Eve can not gain $|w_{im}\rangle$ without being detected.

Proof Without loss of the generality, we assume that Bob regards $|\Phi_1\rangle$ as the carrier state and Eve takes an attack strategy by introducing an ancil-

lary qubit in the state $|E_{\rm initi}\rangle$. Therefore, the complex state of $|\Phi_1\rangle$ and $|E_{\rm initi}\rangle$ can be denoted by $|\Phi_{\rm ABE}\rangle = |\Phi_1\rangle \otimes |E_{\rm initi}\rangle$. Operation $U(\varepsilon)$ applying on $|\Phi_{\rm ABE}\rangle$ yields

$$U(\varepsilon)|\Phi_{\rm ABE}\rangle = \frac{1}{2}(|0\rangle|0\rangle \otimes |E_1\rangle + |0\rangle|1\rangle \otimes |E_2\rangle + |1\rangle|0\rangle \otimes |E_3\rangle + |1\rangle|1\rangle \otimes |E_4\rangle), \quad (10)$$

where $\{E_i : i = 1, \cdots, 4\}$ is a set of Schmidt base.[22] After applying C_{tm}, C_{mh} and C_{hm} on $U(\varepsilon)|\Phi_{\rm ABE}\rangle \otimes |w_{im}\rangle$, one obtains

$$\begin{aligned} |\Gamma\rangle &= C_{hm}(C_{mh}(C_{tm}(U(\varepsilon)|\Phi_{\rm ABE}\rangle|w_{im}\rangle))) \\ &= \frac{1}{2}(|w_{im}\rangle|0\rangle|0\rangle \otimes |E_1\rangle + |w_{im} \oplus 1\rangle|1\rangle|0\rangle \otimes |E_2\rangle \\ &\quad + |w_{im} \oplus 1\rangle|1\rangle|0\rangle \otimes |E_3\rangle + |w_{im}\rangle|1\rangle|1\rangle \otimes |E_4\rangle). \end{aligned} \quad (11)$$

Thus, Eve cannot obtain state $|\Gamma\rangle = |w_{im}\rangle \otimes |\Phi_{\rm ABE}\rangle$. It implies that $U(\varepsilon)$ can be detected by Bob using the prepared carrier state. Moreover, the possibility, for which Eve gains the correct qubit, can be calculated as $P = 1/2$. Accordingly, the mutual information between Alice and Eve can be calculated as

$$I(A, E) = 1 - h(P) = 0, \quad (12)$$

where $h(x) = x\log_2(x) + (1-x)\log_2(1-x)$. Thus, it is impossible for Eve to gain the state $|w_{im}\rangle$, from which the secret messages $|c\rangle$ can be recovered.

Next, the secret messages $|c\rangle$ are proved to be distributed with unconditional security. We investigate the general individual attack strategy to prove the impossibility of Eve via the intercept-and-resend attack strategy to obtain any available information to decode the secret messages. Assume Eve intercepts the two-way channel by making use of two ancillary states, i.e., one-qubit state $|\varepsilon\rangle$ and two-qubit state $|\eta\rangle$. In the forward line L_{BA}, Eve applies the unitary operation O_1 on p_t and ε while Bob sends p_t to Alice. In the backward line L_{AB}, Eve applies the unitary operation O_2 on p_t, p_m and η when Alice sends p_t and p_m back to Bob.

Theorem 2 If Eve implements the general individual attack strategy by intercepting the two-way channel, she can not gain any available information to decode the messages $|c\rangle$.

Proof Assume Bob regards $|\Phi_1\rangle$ as the prepared carrier state one scheme run. Eve's operations O_1 and O_2 can be respectively denoted by

$$\begin{aligned} O_1|0_t\varepsilon\rangle &= A_\varepsilon|0_t\varepsilon_{00}\rangle + B_\varepsilon|1_t\varepsilon_{01}\rangle, \\ O_1|1_t\varepsilon\rangle &= B_\varepsilon|0_t\varepsilon_{10}\rangle + A_\varepsilon|1_t\varepsilon_{11}\rangle, \end{aligned} \quad (13)$$

and

$$\begin{aligned} O_2\,|0_t0_m\eta\rangle &= A_\eta\left|0_t0_m\eta_{00}^{(00)}\right\rangle + B_\eta\left|0_t1_m\eta_{01}^{(00)}\right\rangle + M_\eta\left|1_t0_m\eta_{10}^{(00)}\right\rangle + N_\eta\left|1_t1_m\eta_{11}^{(00)}\right\rangle, \\ O_2\,|1_t0_m\eta\rangle &= B_\eta\left|0_t0_m\eta_{00}^{(10)}\right\rangle + A_\eta\left|0_t1_m\eta_{01}^{(10)}\right\rangle + N_\eta\left|1_t0_m\eta_{10}^{(10)}\right\rangle + M_\eta\left|1_t1_m\eta_{11}^{(10)}\right\rangle, \\ O_2\,|0_t1_m\eta\rangle &= A_\eta\left|0_t0_m\eta_{00}^{(01)}\right\rangle + B_\eta\left|0_t1_m\eta_{01}^{(01)}\right\rangle + M_\eta\left|1_t0_m\eta_{10}^{(01)}\right\rangle + N_\eta\left|1_t1_m\eta_{11}^{(01)}\right\rangle, \\ O_2\,|1_t1_m\eta\rangle &= B_\eta\left|0_t0_m\eta_{00}^{(11)}\right\rangle + A_\eta\left|0_t1_m\eta_{01}^{(11)}\right\rangle + N_\eta\left|1_t0_m\eta_{10}^{(11)}\right\rangle + M_\eta\left|1_t1_m\eta_{11}^{(11)}\right\rangle. \end{aligned} \quad (14)$$

The employed unitary operations ensure the following conditions,

$$\begin{aligned} &A_\varepsilon^2 + B_\varepsilon^2 = 1, \langle\varepsilon_{00}|\varepsilon_{10}\rangle + \langle\varepsilon_{01}|\varepsilon_{11}\rangle = 0, \\ &A_\eta^2 + B_\eta^2 + M_\eta^2 + N_\eta^2 = 1, \quad \sum_{ij}\langle\eta_{ij}^{(kl)}|\eta_{ij}^{(uv)}\rangle = 0, \end{aligned} \quad (15)$$

where $kl \neq uv$ for $i, j, k, l, u, v \in \{0, 1\}$. Without loss of the generality, we assume that

$$\begin{aligned} &\langle\varepsilon_{00}|\varepsilon_{01}\rangle = \langle\varepsilon_{00}|\varepsilon_{10}\rangle = \langle\varepsilon_{10}|\varepsilon_{11}\rangle = \langle\varepsilon_{01}|\varepsilon_{11}\rangle = 0, \\ &\langle\varepsilon_{00}|\varepsilon_{11}\rangle = \cos\theta_\varepsilon, \langle\varepsilon_{01}|\varepsilon_{10}\rangle = \cos\phi_\varepsilon, \\ &\left\langle\eta_{ij}^{(kl)}|\eta_{ij}^{(uv)}\right\rangle = \left\langle\eta_{ij}^{(kl)}|\eta_{i'j'}^{(kl)}\right\rangle = 0, \quad \left\langle\eta_{ij}^{(kl)}|\eta_{i'j'}^{(uv)}\right\rangle = \cos\theta_{\eta_{iji'j'}^{kluv}}, \end{aligned} \quad (16)$$

where $ij \neq i'j'$ and $0 \leq \theta_\varepsilon, \phi_\varepsilon, \theta_{\eta_{iji'j'}^{kluv}} \leq \pi/2$. After applying O_1 and O_2, we can calculate the resulting state as

$$\begin{aligned}
|\Phi_{1\mathrm{e}}^0\rangle &= C_{hm}(C_{mh}(O_2(C_{tm}(O_1(\Phi_1(h,t)|\varepsilon\rangle)|0_m\rangle)|\eta\rangle))) \\
&= \frac{1}{\sqrt{2}}\Big(A_\varepsilon A_\eta \left|000\varepsilon_{00}\eta_{00}^{(00)}\right\rangle + A_\varepsilon B_\eta \left|100\varepsilon_{00}\eta_{01}^{(00)}\right\rangle + A_\varepsilon M_\eta \left|010\varepsilon_{00}\eta_{10}^{(00)}\right\rangle + A_\varepsilon N_\eta \left|110\varepsilon_{00}\eta_{11}^{(00)}\right\rangle \\
&\quad + B_\varepsilon B_\eta \left|000\varepsilon_{01}\eta_{00}^{(10)}\right\rangle + B_\varepsilon A_\eta \left|100\varepsilon_{01}\eta_{01}^{(10)}\right\rangle + B_\varepsilon N_\eta \left|010\varepsilon_{01}\eta_{10}^{(10)}\right\rangle + B_\varepsilon M_\eta \left|110\varepsilon_{01}\eta_{11}^{(10)}\right\rangle \\
&\quad + B_\varepsilon A_\eta \left|101\varepsilon_{10}\eta_{00}^{(00)}\right\rangle + B_\varepsilon B_\eta \left|001\varepsilon_{10}\eta_{01}^{(00)}\right\rangle + B_\varepsilon M_\eta \left|111\varepsilon_{10}\eta_{10}^{(00)}\right\rangle + B_\varepsilon N_\eta \left|011\varepsilon_{10}\eta_{11}^{(00)}\right\rangle \\
&\quad + A_\varepsilon B_\eta \left|101\varepsilon_{11}\eta_{00}^{(10)}\right\rangle + A_\varepsilon A_\eta \left|001\varepsilon_{11}\eta_{01}^{(10)}\right\rangle + A_\varepsilon N_\eta \left|111\varepsilon_{11}\eta_{10}^{(10)}\right\rangle + A_\varepsilon M_\eta \left|011\varepsilon_{11}\eta_{11}^{(10)}\right\rangle\Big), \quad (17)
\end{aligned}$$

where the superscript '0' of the state $|\Phi_{1\mathrm{e}}^0\rangle$ means that Alice sends the state $|0\rangle$. The state of ε and η is given by the reduced matrix,

$$\rho_{10} = \frac{1}{2}\mathrm{Tr}_{htm}(|\Phi_{1\mathrm{e}}^0\rangle\langle\Phi_{1\mathrm{e}}^0|). \quad (18)$$

Similarly, when Alice sends $|1\rangle$ instead of $|0\rangle$, the resulting state can be calculated as

$$\begin{aligned}
|\Phi_{1\mathrm{e}}^1\rangle &= C_{hm}(C_{mh}(O_2(C_{tm}(O_1(\Phi_1(h,t)|\varepsilon\rangle)|1_m\rangle)|\eta\rangle))) \\
&= \frac{1}{\sqrt{2}}\Big(A_\varepsilon A_\eta \left|000\varepsilon_{00}\eta_{00}^{(01)}\right\rangle + A_\varepsilon B_\eta \left|100\varepsilon_{00}\eta_{01}^{(01)}\right\rangle + A_\varepsilon M_\eta \left|010\varepsilon_{00}\eta_{10}^{(01)}\right\rangle + A_\varepsilon N_\eta \left|110\varepsilon_{00}\eta_{11}^{(01)}\right\rangle \\
&\quad + B_\varepsilon B_\eta \left|000\varepsilon_{01}\eta_{00}^{(11)}\right\rangle + B_\varepsilon A_\eta \left|100\varepsilon_{01}\eta_{01}^{(11)}\right\rangle + B_\varepsilon N_\eta \left|010\varepsilon_{01}\eta_{10}^{(11)}\right\rangle + B_\varepsilon M_\eta \left|110\varepsilon_{01}\eta_{11}^{(11)}\right\rangle \\
&\quad + B_\varepsilon A_\eta \left|101\varepsilon_{10}\eta_{00}^{(01)}\right\rangle + B_\varepsilon B_\eta \left|001\varepsilon_{10}\eta_{01}^{(01)}\right\rangle + B_\varepsilon M_\eta \left|111\varepsilon_{10}\eta_{10}^{(01)}\right\rangle + B_\varepsilon N_\eta \left|011\varepsilon_{10}\eta_{11}^{(01)}\right\rangle \\
&\quad + A_\varepsilon B_\eta \left|101\varepsilon_{11}\eta_{00}^{(11)}\right\rangle + A_\varepsilon A_\eta \left|001\varepsilon_{11}\eta_{01}^{(11)}\right\rangle + A_\varepsilon N_\eta \left|111\varepsilon_{11}\eta_{10}^{(11)}\right\rangle + A_\varepsilon M_\eta \left|011\varepsilon_{11}\eta_{11}^{(11)}\right\rangle\Big). \quad (19)
\end{aligned}$$

The state of ε and η is given by the reduced matrix

$$\rho_{11} = \frac{1}{2}\mathrm{Tr}_{htm}(|\Phi_{1\mathrm{e}}^1\rangle\langle\Phi_{1\mathrm{e}}^1|). \quad (20)$$

Thus, the Holevo bound can be calculated as

$$\chi(\rho_1) = S(\rho_1) - \sum_{i=0,1} P_i S(\rho_{1i}) = 0, \quad (21)$$

where $S(\rho_1) = -\mathrm{Tr}(\rho_1 \log_2 \rho_1)$ is the von Neumann entropy, ρ_{1i} is a component in the mixed state ρ_1, and P_i is the probability of ρ_{1i} in ρ_1. Similarly, if Bob regards $|\Phi_2\rangle$ as the prepared carrier state, the Holevo bound can also be calculated as $\chi(\rho_2) = 0$. It shows that Eve can not obtain any available information from Alice by attacking the two-way channel.

Assume that Eve employs the positive operator values measure[26] to obtain as much information as possible. According to Eq.(19), the possibility, for which Eve gains the correct qubit, reads

$$\begin{aligned}
P_{\mathrm{c}} &= \frac{1}{2}\Big(1 + A_\varepsilon^2 A_\eta^2 \sin\theta_\varepsilon \sin\theta_{\eta_{0001}^{0010}} + A_\varepsilon^2 M_\eta^2 \sin\theta_\varepsilon \sin\theta_{\eta_{1011}^{0010}}\Big) \\
&\quad + B_\varepsilon^2 B_\eta^2 \sin\phi_\varepsilon \sin\theta_{\eta_{0001}^{1000}} + B_\varepsilon^2 N_\eta^2 \sin\phi_\varepsilon \sin\theta_{\eta_{1011}^{1000}}\Big). \quad (22)
\end{aligned}$$

Accordingly, the mutual information between Alice and Eve can be calculated as

$$I_{nd}(A,E) = 1 - h(P_{\mathrm{c}}). \quad (23)$$

Similarly, the probability of detecting Eve can be calculated as

$$\begin{aligned}
d &= \frac{1}{2}\Big(1 - A_\varepsilon^2 A_\eta^2 \cos\theta_\varepsilon \cos\theta_{\eta_{0001}^{0010}} - A_\varepsilon^2 M_\eta^2 \cos\theta_\varepsilon \cos\theta_{\eta_{1011}^{0010}}\Big) \\
&\quad - B_\varepsilon^2 B_\eta^2 \cos\phi_\varepsilon \cos\theta_{\eta_{0001}^{1000}} - B_\varepsilon^2 N_\eta^2 \cos\phi_\varepsilon \cos\theta_{\eta_{1011}^{1000}}\Big). \quad (24)
\end{aligned}$$

To obtain as much information as possible without being detected, Eve's strategy should make d as small as possible. For an optimal eavesdropping strategy, Eve may set $A_\varepsilon = A\eta = 1$ and $\theta_\varepsilon = \theta_{\eta_{0001}^{0010}} = \theta$. Combining Eqs.(22), (23) and (24), we can calculate the relationship of the mutual information and the detection probability as

$$I_{nd}(A,E) = 1 - h\left(\frac{1}{2} + d\right). \tag{25}$$

Once Eve is detected, Bob should give up the received messages. Since the messages $|c\rangle$ have been encoded into the n-qubit entanglement state $|c\rangle_L$, Eve's possibility to escape Bob's detection reads

$$P_{\rm e} = (1-d)^n. \tag{26}$$

Therefore, Eve's total information reads

$$\begin{aligned} I_t(A,E) &= P_{\rm e} \times nI_{nd}(A,E) \\ &= n(1-d)^n \left(1 - h\left(\frac{1}{2} + d\right)\right). \end{aligned} \tag{27}$$

Whatever the eavesdropping approach Eve adopts, i.e. choosing different d, Eve's information $I_t(A,E)$ about the secret messages $|c\rangle$ approaches to zero for sufficiently large n. This implies that the scheme is asymptotically secure in this way.

Next, we analyse the security of the scheme according to the utilized SQC with the parameters $[[n,k,d]]$. Let M be a random variable of the messages. Eve employs an arbitrary attack strategy $\mathcal{E}$ with the random variable denoted by E. Then, Alice and Eve's mutual information can be described by the following theorem.

Theorem 3 Let $I(M;E)$ be Shannon mutual information of M and E. If Eve attacks, at most, $\kappa \leq d-1$ qubits of $|c\rangle_L$, one obtains $I(M;E) = 0$. If Eve attacks, at least, d qubits of $|c\rangle_L$, the present scheme can be made asymptotically secure.

Proof According to Shannon theory, the mutual information $I(M;E)$ can be described as

$$I(M;E) = H(M) - H(M|E), \tag{28}$$

where $H(M) = -\sum_{c\in M} p(c)\log p(c)$ and $H(M|E) = -\sum_{c\in M,\varepsilon\in E} p(c,\varepsilon)\log p(c|\varepsilon)$. If Eve attacks, at most, $\kappa \leq t$ qubits of $|c\rangle_L$, Bob can detect and correct the destroyed qubits easily by making use of the calculated error syndromes s. Thus, it is easy to obtain $p(E) = 1$ and $p(M|E) = p(M)$. Since $p(M,E) = p(E)p(M|E)$, one obtains $I(M;E) = 0$, which means that Eve can not obtain any information on the secret messages $|c\rangle$. If Eve attacks, κ ($t < \kappa \leq d-1$) qubits of $|c\rangle_L$, one also obtains $I(M;E) = 0$. In this case, Bob can detect this destroyed qubits brought, but he can not restore $|c\rangle$ from the received state $|c'\rangle_L$. If Eve attacks, at least, d qubits of $|c\rangle_L$, Bob can neither detect nor correct the destroyed qubits. However, in this case, Bob can take advantage of the checking phase in step 3 to catch hold of Eve. After n single-qubit states $|w_{1m}\rangle, \cdots, |w_{nm}\rangle$ are transmitted, the probability of Eve's eavesdropping without being detected is calculated as

$$s(c,\iota) = \frac{1-(1-\iota)^n}{\iota}, \tag{29}$$

where ι is detection probability for Eve's attack while Bob selects the phase for checking. For $\iota > 0$, with the increase of n, value $s(c,\iota)$ decreases exponentially, but is nonzero. In the limit $I(M;E) \to \infty$ (the messages of the infinite length), it can be obtained $s(c,\iota) \to 0$, which implies that the present scheme is asymptotically secure.

We note that Eve has no advantage over eavesdropping more than $d-1$ qubits of $|c\rangle_L$ since the secret messages $|c\rangle$ have been encoded into another entanglement state $|c\rangle_L$, which is the one-time pad itself. Thus, it is difficult for Eve to recover $|c\rangle$ with only some of the qubits eavesdropped from the travelling qubits. In addition, even if Eve obtains the error syndromes of the received state $|c'\rangle_L$, she gains no useful information about $|c\rangle$ since the error syndromes contain no information about the message state.[13,14] Anyway, as long as Eve is detected, the transmissions must be stopped immediately. Thus, Eve has nothing but a sequence of the random nonsense qubits.

5. Conclusion

A secure scheme of the quantum deterministic communication is proposed for the distribution of the messages. It can be implemented by a very simple way without influencing on the security of the transmitted messages. The advantage of the scheme is that the secret messages can be transmitted directly and exactly in the imperfect quantum channel and the damaged qubits of the received state can be recovered, which is different from the previous QSDC schemes.

References

[1] Bennett C H and Brassard G 1984 *Advances in Cryptology* Proceedings of Crypto'84, (Berlin: Springer) August 175

[2] He G and Zeng G 2006 *Chin. Phys.* **15** 1284

[3] Liang C, Fu D, Liang B, Liao J, Wu L, Yao D and Lu S 2001 *Acta Phys. Sin.* **50** 1429 (in Chinese)

[4] Yang Y, Wen Q and Zhu F 2005 *Acta Phys. Sin.* **54** 5544 (in Chinese)

[5] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
Bruβ D 1998 *Phys. Rev. Lett.* **81** 3018

[6] Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302

[7] Beige A, Englert B G, Kurtsiefer Ch and Weinfurter H 2002 *Acta Phys. Pol.* A **101** 357

[8] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

[9] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319

[10] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901

[11] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801

[12] Cai Q Y and Li B W 2004 *Phys. Rev.* A **69** 054301

[13] Calderbank A R, Rains E M, Shor P W and Sloane N J A 1998 *IEEE. Trans. Inform. Theory* **44** 1369

[14] Guo Y and Zeng G 2005 *J. Phys. Soc. Jap.* **74** 2949

[15] Tang Z, Li M, Wei Z, Lu F, Liao C and Liu S 2005 *Acta Phys. Sin.* **54** 2534 (in Chinese)

[16] Bagherinezhad S and Karimipour V 2003 *Phys. Rev.* A **67** 044302

[17] Hiller M, Buzek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[18] Lo H K and Chau H F 1999 *Science* **283** 2050

[19] Chen T Y, Zhang J, Boileau J C, Jin X M, Yang B, Zhang Q, Yang T, Laflamme R and Pan J W 2006 *Phys. Rev. Lett.* **96** 150504

[20] Ma H, Li Y, Zhao H and Wu L 2005 *Acta Phys. Sin.* **54** 5014 (in Chinese)

[21] Wu G, Zhou C, Chen X, Han X and Zeng H 2005 *Acta Phys. Sin.* **54** 3622 (in Chinese)

[22] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)

[23] Gottesman D 1997 Ph.D. thesis, California Institute of Technology, Pasadena

[24] Michler M, Mattle K, Weinfurter H and Zeilinger A 1996 *Phys. Rev.* A **53** R1209

[25] Schneier B 1994 *Applied Cryptography: Protocols, Algorithms, and Source Code in C* 2nd edition (New York: Wiley)

[26] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[27] Zeng G and Zhang W 2000 *Phys. Rev.* A **61** 032303

[28] Zeng G and Zhu H 2002 *Chin. Phys.* **51** 727

[29] Zeng G and Keitel C H 2002 *Phys. Rev.* A **65** 042312