Faithful quantum secure direct communication protocol against collective noise*

Yang Jing(杨 静)[a], Wang Chuan(王 川)[a)b)†], and Zhang Ru(张 茹)[a]

[a] *School of Science, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*
[b] *Key Laboratory for Atomic and Molecular Nanosciences and Department of Physics, Tsinghua University, Beijing* 100084, *China*

(Received 13 April 2010; revised manuscript received 11 May 2010)

An improved quantum secure direct communication (QSDC) protocol is proposed in this paper. Blocks of entangled photon pairs are transmitted in two steps in which secret messages are transmitted directly. The single logical qubits and unitary operations under decoherence free subspaces are presented and the generalized Bell states are constructed which are immune to the collective noise. Two steps of qubit transmission are used in this protocol to guarantee the security of communication. The security of the protocol against various attacks are discussed.

Keywords: quantum secure direct communication, collective noise
PACC: 0367

Cryptography is the art of rendering secret messages unintelligible to any unauthorized parties. Conventional cryptosystems based on a mixture of mathematics, guesswork and wishful thinking which play an important role in the message protection. But such cryptosystems have several defects, such as the computational complexities. The idea of quantum cryptography was first proposed by Bennett and Brassard in 1984 and provided an entirely new way to solve the key distribution.[1] This quantum key distribution (QKD) protocol makes use of two non-orthogonal states of polarized photons to distribute cryptographic keys. Two remote users (traditionally called Alice and Bob) can exploit QKD to create a private key securely. In the beginning the sender Alice chooses one of the four polarizations (the horizontal and vertical polarized, or the $\pm 45^\circ$ polarized basis) randomly to prepare the initial states. Then the single photon states are transmitted to the receiver Bob. Bob measures the incoming states using one of the two bases (the horizontal and vertical measuring basis or the $\pm 45^\circ$ measuring basis) also choosing randomly. If they choose the same basis, then their results are perfectly correlated. The corresponding results are used as the raw keys. The security of QKD is guaranteed by the laws of quantum physics, the uncertainty principle and the non-cloning theorem. During the past decades, quantum key distribution has progressed quickly.[2−6]

Recently a novel quantum communication was proposed: the quantum secure direct communication (QSDC). Different from QKD, QSDC is to transmit important messages directly without first establishing random keys. So this communication system requires a higher security than QKD which could not implement a simple rejection.

In the year 2002, Boström and Felbinger put forward a ping–pong protocol[7] which is a quasi-secure direct communication scheme with an Einstein–Podolsky–Rosen (EPR) pair. The communication process has two modes (one is the controlled mode, the other is the message mode) to transmit the entanglement parties and the secret messages. However, the ping–pong scheme is not secure and it can be attacked under the denial of service attack.[8] In 2002, Long and Liu proposed a two-step highly efficient QKD protocol.[9] In this protocol, the sender Alice prepares an ordered EPR pair sequence, then divides them into two sequences which are sent in blocks by two steps. After the receiver Bob received the two sequences, he performs Bell state measurements on the EPR pairs and reads out state information. By analysing the error rate of communication and privacy amplification process, secure keys are generated between the two parties. Though the protocol was designed for QKD,

*Project supported by the National Fundamental Research Program (Grant No. 2010CB923202), the Fundamental Research Funds for the Central Universities (Grant No. BUPT2009RC0710), the National Natural Science Foundation of China (Grant Nos. 60937003 and 10947151).
†Corresponding author. E-mail: chuan-wang03@mails.tsinghua.edu.cn
© 2010 Chinese Physical Society and IOP Publishing Ltd

it is also fully a QSDC protocol. Later, Deng, Long and Liu proposed the two-step quantum direct communication protocol[10] to overcome the defects in the ping–pong scheme. In Deng–Long protocol, a set of ordered N EPR pairs are used as a data block for sending secret message directly. The ordered N EPR pairs are divided into two particle sequences, a checking sequence and a message-coding sequence which are sent in two steps. After transmitting the checking sequence in the first step, the two parties ensure the security of the quantum channel. Then the sender Alice encodes the secret message directly on the message-coding sequence and sends them to Bob. By combining the checking and message-coding sequences together, Bob reads out the encoded messages directly according to his Bell state measurements. Later, the idea of QSDC has been realized in many quantum systems and different protocols are presented in the following years.[11−24] Note that the qubits used in these protocol are not robust against decoherence which means that the qubits will be changed under the influence of the channel noise. Then the scheme is insecure in noisy channel.

Decoherence, which is caused by the unwanted interaction of the system with its environment is a major obstacle in the realization of quantum information processors. Based on the type of interaction processes between the qubits and their environment, decoherence free subspaces (DFS) qubits which are immune to decoherence processes and to protect fragile quantum information against the detrimental effects of decoherence are founded.[25,26] There exist subspaces of the system's Hilbert space which are not affected by the various kinds of channel noise assumed to affect the states during information processing, and thus they are called decoherence free subspaces. In 2006, Zou *et al.* proposed a scheme for the generation of four-photon polarization-entangled decoherence-free states based on post-selection strategy and current experimental technology.[27] Later in 2009, Xia *et al.* proposed a scheme for generating the four photon polarization-entangled decoherence-free states.[28] The proposed setup involves only simple linear optical elements and conventional photon detectors which makes the protocol more realizable in experiments.

Here in this study, we develop a protocol for QSDC with DFS qubits based on the two-step QSDC protocol. The generalized Bell states and unitary operations on the basis of logical qubits are presented. Our QSDC scheme exhibits the same high coding capacity with Deng's protocol, moreover the protocol is immune to collective noise.

Under the influence of collective channel noise, the states of the transmitted qubits will be changed. The influence of the states are described by:

$$\begin{aligned} |0\rangle_r &= \cos\theta|0\rangle + \sin\theta|1\rangle, \\ |1\rangle_r &= -\sin\theta|0\rangle + \cos\theta|1\rangle, \end{aligned} \tag{1}$$

here the subscript r indicates the states which were affected by the collective rotation noise and θ is the parameter of the collective rotation noise. Also the collective dephasing noise can be described by: $|0\rangle_d = |0\rangle$, $|1\rangle_d = \mathrm{e}^{\mathrm{i}\phi}|1\rangle$. Here ϕ is the dephasing noise parameter and it fluctuates with time. Based on this alteration between the qubits and the environment, we introduce the DFS qubits which are used as the logical bits ($|0\rangle_{\mathrm{L}}$ and $|1\rangle_{\mathrm{L}}$). The logical bits can be described as:[26]

$$|0\rangle_{\mathrm{L}} = \frac{1}{2}(|01\rangle - |10\rangle) \otimes (|01\rangle - |10\rangle), \tag{2}$$

$$\begin{aligned} |1\rangle_{\mathrm{L}} = {} & \frac{1}{2\sqrt{3}}[2|1100\rangle + 2|0011\rangle - (|01\rangle + |10\rangle) \\ & \otimes (|01\rangle + |10\rangle)]. \end{aligned} \tag{3}$$

After using the $|0\rangle_{r(d)}$ and $|1\rangle_{r(d)}$ which were affected by noise into the logical quantum bits $|0\rangle_{\mathrm{L}}$ and $|1\rangle_{\mathrm{L}}$, it is obviously that the logical bits will not be altered.

Then we can achieve the four generalized Bell states:

$$|\psi^+\rangle_{\mathrm{L}} = \frac{1}{\sqrt{2}}(|0_{\mathrm{A}}\rangle_{\mathrm{L}}|1_{\mathrm{B}}\rangle_{\mathrm{L}} + |1_{\mathrm{A}}\rangle_{\mathrm{L}}|0_{\mathrm{B}}\rangle_{\mathrm{L}}), \tag{4}$$

$$|\psi^-\rangle_{\mathrm{L}} = \frac{1}{\sqrt{2}}(|0_{\mathrm{A}}\rangle_{\mathrm{L}}|1_{\mathrm{B}}\rangle_{\mathrm{L}} - |1_{\mathrm{A}}\rangle_{\mathrm{L}}|0_{\mathrm{B}}\rangle_{\mathrm{L}}), \tag{5}$$

$$|\phi^+\rangle_{\mathrm{L}} = \frac{1}{\sqrt{2}}(|0_{\mathrm{A}}\rangle_{\mathrm{L}}|0_{\mathrm{B}}\rangle_{\mathrm{L}} + |1_{\mathrm{A}}\rangle_{\mathrm{L}}|1_{\mathrm{B}}\rangle_{\mathrm{L}}), \tag{6}$$

$$|\phi^-\rangle_{\mathrm{L}} = \frac{1}{\sqrt{2}}(|0_{\mathrm{A}}\rangle_{\mathrm{L}}|0_{\mathrm{B}}\rangle_{\mathrm{L}} - |1_{\mathrm{A}}\rangle_{\mathrm{L}}|1_{\mathrm{B}}\rangle_{\mathrm{L}}). \tag{7}$$

Here we propose the specific steps of the improved QSDC protocol as the following:

(i) The sender Alice prepares an ordered N EPR pairs in state $|\psi^+\rangle_{\mathrm{L}} = \frac{1}{\sqrt{2}}(|0_{\mathrm{A}}\rangle_{\mathrm{L}}|1_{\mathrm{B}}\rangle_{\mathrm{L}} + |1_{\mathrm{A}}\rangle_{\mathrm{L}}|0_{\mathrm{B}}\rangle_{\mathrm{L}})$. We denote the N ordered EPR pairs with $[(P_1(A)_{\mathrm{L}}, P_1(B)_{\mathrm{L}}), (P_2(A)_{\mathrm{L}}, P_2(B)_{\mathrm{L}}), (P_3(A)_{\mathrm{L}}, P_3(B)_{\mathrm{L}}) \ldots, (P_N(A)_{\mathrm{L}}, P_N(B)_{\mathrm{L}})]$. Here the subscript indicates the pair order in the sequence, and A and B represent the two particles, respectively.

(ii) The ordered N EPR pairs are divided into two sequences by Alice and transmitted to Bob in two steps. Here in this step, Alice takes one particle from each EPR pair to formulate an ordered EPR particle sequence S_{A}

$[P_1(A)_{\rm L}, P_2(A)_{\rm L}, P_3(A)_{\rm L}, \ldots P_N(A)_{\rm L}]$. The remaining EPR partner particles make up another particle sequence $S_{\rm B}$ $[P_1(B)_{\rm L}, P_2(B)_{\rm L}, P_3(B)_{\rm L}, \ldots P_N(B)_{\rm L}]$. The $S_{\rm A}$ sequence is called the message sequence and the $S_{\rm B}$ sequence is called the checking sequence.

(iii) Alice sends the checking sequence $S_{\rm B}$ $[P_1(B)_{\rm L}, P_2(B)_{\rm L}, P_3(B)_{\rm L}, \ldots P_N(B)_{\rm L}]$ to the receiver Bob, and she holds the message sequence $S_{\rm A}$. Then Alice and Bob use the checking sequence for the first step security checking. It is implemented by the following procedure:

(p.0) Bob chooses randomly a number of the photons from the $S_{\rm B}$ sequence and performs the $X = \frac{1}{\sqrt{2}}(|0\rangle_{\rm L} \pm |1\rangle_{\rm L})$ or $Z = |0(1)\rangle_{\rm L}$ basis measurement on the choose photons. Note that after this series of measurements, Bob will get $|0\rangle_{\rm L}$ or $|1\rangle_{\rm L}$ and $|0\rangle_{\rm L} + |1\rangle_{\rm L}$ or $|0\rangle_{\rm L} - |1\rangle_{\rm L}$.

(p.1) Through the classic channel, Bob announces the positions he has chosen for each photon to Alice.

(p.2) Alice measures the corresponding photons in the $S_{\rm A}$ sequence with the randomly chosen basis X or Z.

(p.3) Then Alice compares her basis and the measurement results with Bob's results publicly. If they chosen the same basis and their results are correlated, this means that there is no eavesdropping during transmission. Otherwise, if the error rate is larger than the threshold error rate, Alice and Bob conclude that the communication is insecure and abort the communication. In this step, the message has not been coded.

(iv) After ensuring that the transmission of the checking sequence is secure, Alice encodes the remaining $S_{\rm A}$ sequence (the remaining photons in the $S_{\rm A}$ after the security checking, here it is called $S'_{\rm A}$). Alice chooses the four DFS unitary operations (I, H_x, H_y, H_z) on the logical particles ($|0\rangle_{\rm L}$ or $|1\rangle_{\rm L}$). Here the four DFS unitary operations are as follows:

$$I = |0\rangle_{\rm LL}\langle 0| + |1\rangle_{\rm LL}\langle 1|, \tag{8}$$

$$H_x = \frac{1}{\sqrt{3}}(V_{12} + 2V_{23}), \tag{9}$$

$$H_y = \frac{(V_{12} + 2V_{23})(-V_{12})}{\sqrt{3}}, \tag{10}$$

$$H_z = -V_{12}, \tag{11}$$

here the operation V_{ij} indicates the permutations of the physical qubits i and j of the logical state. The unitary operations do not need to change the state of the single photons but to exchange the positions of the photons. The unitary operations (I, H_x, H_y, H_z) make the following transformations:

$$I \otimes I|\psi^+\rangle_{\rm L} = |\psi^+\rangle_{\rm L}, \tag{12}$$

$$I \otimes H_x|\psi^+\rangle_{\rm L} = |\phi^+\rangle_{\rm L}, \tag{13}$$

$$I \otimes H_y|\psi^+\rangle_{\rm L} = |\phi^-\rangle_{\rm L}, \tag{14}$$

$$I \otimes H_z|\psi^+\rangle_{\rm L} = |\psi^-\rangle_{\rm L}. \tag{15}$$

Alice and Bob agree on that these logical unitary operations correspond to the classical information 00, 01, 10, and 11, respectively.

(v) In order to guarantee the security of this step transmission, Alice has to add "logical decoy photons" in the $S_{\rm A}$ sequence during the encoding process.

(vi) After the transition of the logical quantum bits, Alice tells Bob the positions of the sampling photons. By checking the sampling photons that Alice has chosen, Bob chooses the logical Z or X basis to measure them and gets an estimate of the error rate. If the error rate of the sampling pairs is reasonably low, Alice and Bob can then entrust the process. Otherwise, Alice and Bob abandon the transmission and repeat the procedures from the beginning. This is the second security analysis.

(vii) In the decoding process, Bob performs generalized Bell-state measurement on the $S'_{\rm A}$ and $S'_{\rm B}$ (the remaining photons in the $S_{\rm B}$ after the first security checking) sequences simultaneously. After the operation, Bob could read out the unitary operation for each logical qubits performed by Alice. Since that, Bob reads out the secret message transmitted by Alice. Similar to Deng's QSDC protocol,[10] two bits of information are transmitted during one round communication.

Note that in the current actual quantum channel, the QSDC process is more complicated. The main reason is that Alice and Bob need to determine which photons are lost during transmission. These operations need the developments of some quantum technologies, such as the quantum entanglement swapping,[29] entanglement purification,[30–32] entanglement concentration[33,34] and so on.

As discussed above, Alice and Bob ensure the security of the quantum channel before the secret message transmission in the first step security analysis. The eavesdropper Eve will be discovered if she attacks the channel. It is obvious that Eve cannot read out the information in the EPR pairs if she captures one of the two sequences, because the Bell states can not be readout by measuring one particle of an EPR pair alone. In this way, no secret message will be leaked to Eve. So the second security analysis procedure is

mainly to determine whether Eve destructs the quantum correlation between the $S'_{\rm A}$ sequence and $S'_{\rm B}$ sequence during the transmission of $S_{\rm A}$ sequence. Even if the channel is noisy, the communication is effective because the modified quantum bits (the logical bits) and the improved unitary operations are used. Moreover, the capacity is high in this protocol as the two-step QSDC scheme under noisy channel condition.[10]

Unlike the traditional security analysis in QKD, Eve is not allowed to get any information during communication as secure message is transmitted directly. The improved protocol is secure and immune to collective noise. It divides the entanglement particles into two sequences, the message sequence ($S_{\rm A}$) and the checking sequence($S_{\rm B}$). The first security analysis in the quantum channel is similar to BBM92[3] protocol. But the process is based on the measurement of the logical qubit. During the transmission of the first photon sequence, the sender of the quantum communication controls the other photon sequence all the time. The BBM92 QKD protocol has been proven to be unconditionally secure.[35,36] Under Eve's single qubit intercept-resend eavesdropping attack, she has to hide in the channel when Alice and Bob transmit the particles. For each logical qubit, she performs the logical qubit measurement and prepares the same qubit to sent to Bob. Both in the first step and second step transmission, since the transmitted particles are part of the entangled states, any measurement on part of the states will make them disentangled. Her intercept-resend attack on the transmitted qubits will introduce an error rate of 25%. Also Eve can not achieve the checking sequence and the message sequence simultaneously. So she can not read out the secret message. Another kind of eavesdropping attack is the Trojan horse attack. Since the secret information is encoded by Alice in the second step qubits transmission, then the qubits are sent to Bob and measured by Bob directly. In this process, Eve's Trojan horse signals are sent to Bob who does nothing but performs the measurement. So there is no send-return process during communication and Eve's Trojan horse attack can not acquire any useful information on the qubits in the communication.

Alice and Bob perform the two-step transmission on the logical entangled qubits, the eavesdropper Eve might hide herself in the channel and make joint unitary operation on the logical b and a qubits with ancillary qubits. This kind of eavesdropping attack is called individual attack. And Eve's joint unitary operation on the b and a logical qubits are described by:

$$\begin{aligned}
\hat{J}_{\rm BE}|0\rangle_{{\rm L}_b}\otimes|e_{\rm E1}\rangle &= |0\rangle_{{\rm L}_b}\otimes|0_{\rm E1}\rangle,\\
\hat{J}_{\rm BE}|1\rangle_{{\rm L}_b}\otimes|e_{\rm E1}\rangle &= \cos\phi|1\rangle_{{\rm L}_b}\otimes|\xi_{\rm E1}\rangle+\sin\phi|0\rangle_{{\rm L}_b}\otimes|\xi'_{\rm E1}\rangle, \qquad (16)\\
\hat{K}_{\rm AE}|0\rangle_{{\rm L}_a}\otimes|e_{\rm E2}\rangle &= |0\rangle_{{\rm L}_a}\otimes|0_{\rm E2}\rangle,\\
\hat{K}_{\rm AE}|1\rangle_{{\rm L}_a}\otimes|e_{\rm E2}\rangle &= \cos\phi|1\rangle_{{\rm L}_a}\otimes|\xi_{\rm E2}\rangle+\sin\phi|0\rangle_{{\rm L}_a}\otimes|\xi'_{\rm E2}\rangle, \qquad (17)
\end{aligned}$$

where $\phi\in[0,\pi/4]$ characterize the strength of the attack, the subscript ${\rm L}_a$ and ${\rm L}_b$ denote the logical qubits belonging to a sequence and b sequence respectively.

Eve's behavior evolves the combined system of the entangled states and her ancillary qubits to

$$|\psi^+\rangle_{\rm L}|e_{\rm E1}e_{\rm E2}\rangle=\frac{1}{\sqrt{2}}(|0_{\rm A}\rangle_{\rm L}|1_{\rm B}\rangle_{\rm L}+|1_{\rm A}\rangle_{\rm L}|0_{\rm B}\rangle_{\rm L})|e_{\rm E1}e_{\rm E2}\rangle. \qquad (18)$$

In this protocol, the logical qubits are transmitted in two steps which means that at each time slot, there is only one logical qubit in the channel. So Eve performs her attack during the two-step transmission, for example, Alice's encoding operation is I, the evolution of the composite system is described by:

$$\begin{aligned}
|\psi^+\rangle_{\rm L}|e_{\rm E1}e_{\rm E2}\rangle &\rightarrow \hat{J}_{\rm BE}\frac{1}{\sqrt{2}}[|0\rangle_{{\rm L}_a}(\cos\phi|1\rangle_{{\rm L}_b}|\xi_{\rm E1}\rangle+\sin\phi|0\rangle_{{\rm L}_b}|\xi'_{\rm E1}\rangle)+|1\rangle_{{\rm L}_a}|0\rangle_{{\rm L}_b}|0_{\rm E1}\rangle]\\
&\rightarrow \hat{K}_{\rm AE}\frac{1}{\sqrt{2}}[|0\rangle_{{\rm L}_a}|0_{\rm E2}\rangle(\cos\phi|1\rangle_{{\rm L}_b}|\xi_{\rm E1}\rangle+\sin\phi|0\rangle_{{\rm L}_b}|\xi'_{\rm E1}\rangle)+(\cos\phi|1\rangle_{{\rm L}_a}|\xi_{\rm E2}\rangle\\
&\quad+\sin\phi|0\rangle_{{\rm L}_a}|\xi'_{\rm E2}\rangle)|0\rangle_{\rm Lb}|0_{\rm E1}\rangle]. \qquad (19)
\end{aligned}$$

After the two step transmission, Eve measures her ancillary qubits but reads out randomly results about

the secret message. The density matrix of the composite system is described by:

$$\boldsymbol{\rho} = \mathrm{Tr}_{ab}(\rho_{abE_1E_2}) = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos^2\phi & 0 \\ 0 & 0 & \sin^2\phi \end{pmatrix}. \tag{20}$$

Eve's attack on one logical qubit will also introduce a bit error rate of $\sin^2\phi/2$ on the security checking qubits. Then the eavesdropping behavior will be discovered by the security checking process between Alice and Bob.

Since the information encoded by Alice after the first step particle transmission, Eve's attack on the first sequence is useless but introduces bit errors. So we only consider the individual attack during the second step particle transmission. Generally speaking, we assume that Alice performs the encoding operation of I, H_x, H_y, H_z with probabilities p_0, p_1, p_2, p_3 respectively. Then we expand the composite system of the qubits with Eve's ancillary qubits under the basis $|0\rangle_{\mathrm{L}}|\xi\rangle|0\rangle_{\mathrm{L}}$, $|0\rangle_{\mathrm{L}}|\xi'\rangle|1\rangle_{\mathrm{L}}$, $|1\rangle_{\mathrm{L}}|\xi\rangle|1\rangle_{\mathrm{L}}$, $|0\rangle_{\mathrm{L}}|\xi|1\rangle_{\mathrm{L}}$, $|0\rangle_{\mathrm{L}}|\xi'\rangle|0\rangle_{\mathrm{L}}$ and $|1\rangle_{\mathrm{L}}|\xi\rangle|0\rangle_{\mathrm{L}}$.

$$\boldsymbol{\rho}' = \begin{pmatrix} \rho_1 & 0 \\ 0 & \rho_2 \end{pmatrix}. \tag{21}$$

where the two density matrix $\boldsymbol{\rho}_1$ and $\boldsymbol{\rho}_2$ are described by

$$\boldsymbol{\rho}_1 = \begin{pmatrix} p_1+p_2 & (p_1-p_2)\sin\phi & (p_1-p_2)\cos\phi \\ (p_1-p_2)\sin\phi & (p_1+p_2)\sin^2\phi & (p_1+p_2)\sin\phi\cos\phi \\ (p_1-p_2)\cos\phi & (p_1+p_2)\sin\phi\cos\phi & (p_1+p_2)\cos^2\phi \end{pmatrix}, \tag{22}$$

$$\boldsymbol{\rho}_2 = \begin{pmatrix} p_0+p_3 & (p_0-p_3)\sin\phi & (p_0-p_3)\cos\phi \\ (p_0-p_3)\sin\phi & (p_0+p_3)\sin^2\phi & (p_0+p_3)\sin\phi\cos\phi \\ (p_0-p_3)\cos\phi & (p_0+p_3)\sin\phi\cos\phi & (p_0+p_3)\cos^2\phi \end{pmatrix}. \tag{23}$$

Eve's ancillary qubit is described by the reduced density matrix $\boldsymbol{\rho}''$:

$$\boldsymbol{\rho}'' = \mathrm{Tr}_{ab}(\rho') = \frac{1}{2}\begin{pmatrix} 1+\cos^2\phi & 0 \\ 0 & \sin^2\phi \end{pmatrix}. \tag{24}$$

In fact, Eve's density matrix reveals her nothing but the randomly results $|0\rangle_{\mathrm{L}}$ and $|1\rangle_{\mathrm{L}}$ as the secret information is encoded by the two logical qubits Bell states. When the photon loss is small in low noise channel, Eve's attack will increase either the error rate or loss of signals. So Alice and Bob can analyze the error rate and the efficiency in the first security checking process to check the eavesdropping behaviour.

In this study, we proposed an improved QSDC protocol which is immune to both the collective rotation noise and collective dephasing noise. Also we analysed the security of communication under intercept-resend attack and individual attack on the logical qubits. The benefits of the improved QSDC protocol are mainly embodied in the following aspects:

(i) Confidential information can be transmitted directly without transmitting the keys first. Since the secure communication has been simplified.

(ii) The modified logical quantum bits are used to overcome the noise impaction. Even though the channel collective noise is in a very strong case, the security of the QSDC is also guaranteed.

(iii) This scheme has a high coding capacity, an entangled state can carry two bit of classical information. Also the operations are easy to be realized.

In our improved protocol, the logical quantum bits are used to overcome the collective noise impaction. As discussed above, the $|0\rangle_{\mathrm{L}}$ is not altered by the noise and the same to the $|1\rangle_{\mathrm{L}}$. Each EPR pair can be used to carry two bits of information. However the presented scheme also has some disadvantages. That is, it uses more particles to construct the logical bits to overcome the noise. Because we use the improved logical quantum bits, more particles should be used to construct the logical bits compared with the QSDC

in Ref. [10], and the equipment becomes complicated. For example, the logical quantum bit $|0\rangle_{\rm L}$ is the superposition of four states in four particles. In practice, Alice and Bob should correct the environmental destruction on the entanglement system. These operations need the help of some quantum technologies.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* Bangalore, India (IEEE, New York), pp.175–179

[2] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[3] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[4] Deng F G and Long G L 2003 *Phys. Rev.* A **68** 042315

[5] Chen W, Han Z F, Mo X F, Xu F Z, Wei G and Guo G C 2008 *Chinese Sicence Bulletin* **53** 1310

[6] Li X H, Zhao B K, Sheng Y B, Deng F G and Zhou H Y 2009 *Int. J. Quant. Info.* **7** 1479

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

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

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

[10] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317

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

[12] Wang C, Deng F G, Li Y S, Liu X S and Long G L 2005 *Phys. Rev.* A **71** 044305

[13] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2007 *Chin. Phys.* **16** 3553

[14] Li X H, Li C Y, Deng F G, Zhou P, Liang Y J and Zhou H Y 2007 *Chin. Phys.* **16** 2149

[15] Gao F, Guo F Z, Wen Q Y and Zhu F C 2008 *Science in China* Series G-Physics Mechanics Astron, **51** 1853

[16] Yang Y G and Wen Q Y 2008 *Science in China Series* G-Physics Mechanics Astron **51** 176

[17] Gao T Z 2004 *Naturforsch* A **59** 597

[18] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev.* A **73** 022338

[19] Wang J, Zhang Q and Tang C J 2006 *Phys. Lett.* A **358** 256

[20] Song J, Zhu A D and Zhang S 2007 *Chin. Phys.* **16** 621

[21] Xia Y, Song J and Song H S 2007 *Opt. Comm.* **279** 395

[22] Xia Y and Song H S 2007 *Phys. Lett.* A **364** 117

[23] Song J, Xia Y and Song H S 2008 *Comm. Theor. Phys.* **49** 635

[24] Long G L, Deng F G, Wang C, Li X H, Wen K and Wang W Y 2007 *Frontiers of Physics in China* **2** 251

[25] Bacon D, Kempe J, Lidar D A and Whaley K B 2000 *Phys. Rev. Lett.* **85** 1758

[26] Kempe J, Bacon D, Lidar D A and Whaley K B 2001 *Phys. Rev.* A **63** 042307

[27] Zou X B, Shu J and Guo G C 2006 *Phys. Rev.* A **73** 054301

[28] Xia Y, Song J, Song H S and Zhang S 2009 *J. Opt. Soc. American* B **26** 129

[29] Zukowski M, Zeilinger A, Horne A and Ekert A K 1999 *Phys. Rev. Lett.* **71** 4287

[30] Bennett C H, Brassard G, Popescu S, Schumacher B, Smolin J A and Wcotters W 1996 *Phys. Rev. Lett.* **76** 722

[31] Deutsch D, Ekert A, Jozsa R, Macckiavello C, Popcscu S and Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818

[32] Sheng Y B, Deng F G and Zhou H Y 2008 *Phys. Rev.* A **77** 042308

[33] Zhao Z, Yang T, Chen Y A, Zhang A N and Pan J W 2003 *Phys. Rev. Lett.* **90** 207901

[34] Sheng Y B, Deng F G and Zhou H Y 2008 *Phys. Rev.* A **77** 062325

[35] Inamori H, Rallan L and Vedral V 2001 *J. Phys.* A: *Math. Gen.* **34** 6913

[36] Waks E, Zeevi A and Yamamoto Y 2001 *Phys. Rev.* A **65** 052310