*Science in China Series G: Physics, Mechanics & Astronomy*

www.scichina.com
phys.scichina.com
www.springerlink.com



# Deterministic secure quantum communication over a collective-noise channel

GU Bin†, PEI ShiXin, SONG Biao & ZHONG Kun

College of Math and Physics, Nanjing University of Information Science and Technology, Nanjing 210044, China

**We present two deterministic secure quantum communication schemes over a collective-noise. One is used to complete the secure quantum communication against a collective-rotation noise and the other is used against a collective-dephasing noise. The two parties of quantum communication can exploit the correlation of their subsystems to check eavesdropping efficiently. Although the sender should prepare a sequence of three-photon entangled states for accomplishing secure communication against a collective noise, the two parties need only single-photon measurements, rather than Bell-state measurements, which will make our schemes convenient in practical application.**

deterministic secure quantum communication, quantum secure direct communication, collective-noise channel, single-photon measurements

The principles in quantum mechanics provide some novel ways for secure quantum communication. For example, quantum cryptography supplies a secure way for two legitimate users to generate a private key. Since Bennett and Brassard published the first protocol[1] in 1984, quantum cryptography has attracted a lot of attention and has become one of the most mature applications of quantum information techniques[2−7]. With a private key, the two parties can communicate their classical secret message securely. Another important branch of quantum communication is quantum secret sharing (QSS). It is a quantum version of classical secret sharing in which the sender Alice splits her private key $K_A$ into two pieces $K_B$ and $K_C$ and sends them to her two agents Bob and Charlie, respectively. When and only when Bob and Charlie cooperate, they can obtain the private key $K_A = K_B \oplus K_C$. QSS provides a novel way for sharing a private key among three parties[8−14]. Now, QSS is generalized to sharing an unknown quantum state[15−21].

Recent years have seen the concept of quantum secure direct communication (QSDC) proposed and widely followed[22−47]. Different from quantum cryptography whose task is to generate a private key, QSDC is to transmit a secret message directly, without private keys. From the point of security, QSDC has more demands than quantum cryptography as the secret message cannot be discarded. As pointed out by Deng and Long[23−25,47], for QSDC, the quantum states should be transmitted block by block, similar to quantum cryptography protocol proposed by Long and Liu[48]. In 2006, Li et al. divided secure quantum commu-

Received July 7, 2009; accepted July 31, 2009
doi: 10.1007/s11433-009-0303-y

†Corresponding author (email: gubin@nuist.edu.cn)

Supported by the National Natural Science Foundation of China (Grant No. 10847147) and the Science Foundation of Nanjing University of Information Science & Technology (Grant No. 20080279)

**Citation:** Gu B, Pei S X, Song B, et al. Deterministic secure quantum communication over a collective-noise channel. Sci China Ser G, 2009, 52(12): 1913-1918, doi: 10.1007/s11433-009-0303-y

nication into two classes[42]. One is QSDC and the other is deterministic secure quantum communication (DSQC)[47]. They both can be used to transmit secret message securely although there are some differences between these two classes of secure quantum communication. In a practical channel, DSQC has some advantages[42] over QSDC. The major advantage is that the qubits carrying the secret message are not transmitted again after the eavesdropping check[42] in DSQC, which will make DSQC more secure than QSDC over a noisy channel and make DSQC more convenient for quantum error correction.

In spite of the many schemes for DSQC[33−42,47], none of them discuss the efficient application over a noisy channel. In fact, the inevitable interaction between qubits transmitted and the environment decreases the fidelity of the qubits transmitted and even makes a quantum communication infeasible. For overcoming the decoherence of quantum states by the channel noise, some good methods have been proposed for quantum communication, such as entanglement purification[49], single-photon error rejection[50], decoherence-free subspace (DFS)[51], and so on. Entanglement purification can in principle distill some maximally entangled states from a mixed ensemble by consuming infinite quantum resource. Single-photon error rejection requires less quantum resource, but it can succeed probabilistically. DFS, composed of several qubits, suffering from the same noise in quantum channel will compensate the effect of noise and keeps the invariability against the noise. This good feature can be used to encode messages in quantum communication over a collective-noise channel[52,53]. Recently, Li et al. proposed an interesting quantum dense coding protocol for quantum cryptography over a collective-noise channel with DFS[54].

In this paper, we will propose two DSQC protocols over a collective-noise channel with DFS, following some ideas in ref. [54]. One is used against a collective-rotation noise with three-photon entangled states in which the state of the two photons transmitted is immune to this noise. The other is used against a collective-dephasing noise. The two legitimate users can analyze the error rate for eavesdropping check by using the correlation of their subsystems. Although the sender should prepare three-photon entangled states to complete the task of DSQC over a collective-noise channel, the two legitimate users need only single-photon measurements on their photons, not Bell-state measurements, which will make our schemes convenient in a practical application.

## 1 DSQC against a collective-rotation noise

A collective-rotation noise in a fiber can be written as[54]

$$\begin{aligned} U_r|H\rangle &= \cos\theta|H\rangle + \sin\theta|V\rangle, \\ U_r|V\rangle &= -\sin\theta|H\rangle + \cos\theta|V\rangle, \end{aligned} \tag{1}$$

where $\theta$ is the parameter of a collective-rotation noise which fluctuates with time $t$. $H$ and $V$ represent the horizontal and the vertical polarizations of photons, respectively. The two Bell states $|\phi^+\rangle_{B_1B_2} = \frac{1}{\sqrt{2}}(|H\rangle_{B_1}|H\rangle_{B_2} + |V\rangle_{B_1}|V\rangle_{B_2})$ and $|\psi^-\rangle_{B_1B_2} = \frac{1}{\sqrt{2}}(|H\rangle_{B_1}|V\rangle_{B_2} - |V\rangle_{B_1}|H\rangle_{B_2})$ both are immune to a collective-rotation noise. This good feature provides a novel way for secure quantum communication against a collective-rotation noise in a deterministic way, different from that with the single-photon error-rejection scheme[50].

The principle of our DSQC scheme against a collective-rotation noise can be described as follows.

(1) The sender Alice prepares a sequence of quantum systems which are in the three-photon entangled state $|\Phi^+\rangle_{AB_1B_2} = \frac{1}{\sqrt{2}}(|H\rangle_A|\phi^+\rangle_{B_1B_2} + |V\rangle_A|\psi^-\rangle_{B_1B_2})$. She divides the quantum systems into two sequences $S_A$ and $S_B$[83,84]. That is, the sequence $S_A$ is composed of the qubits $A$ in all quantum systems in turn and the sequence $S_B$ is composed of the qubits $B_1B_2$ in each quantum system.

(2) Alice sends the sequence $S_B$ to Bob and keeps the sequence $S_A$.

(3) After receiving the sequence $S_B$, Bob picks up some samples for eavesdropping check. That is, he measures the samples in Bell states $|\phi^+\rangle_{B_1B_2}$ and $|\psi^-\rangle_{B_1B_2}$ with one of the three measuring bases $Z_{B_1} \otimes Z_{B_2}$, $Z_{B_1} \otimes X_{B_2}$ and $X_{B_1} \otimes Z_{B_2}$ randomly.

The state $|\Phi^+\rangle_{AB_1B_2}$ can be written as follows:

$$\begin{aligned}
&|\Phi^+\rangle_{AB_1B_2}\\
&=\frac{1}{\sqrt{2}}(|H\rangle_A|\phi^+\rangle_{B_1B_2}+|V\rangle_A|\psi^-\rangle_{B_1B_2})\\
&=\frac{1}{2}[|+\rangle_A(|H\rangle_{B_1}|+\rangle_{B_2}-|V\rangle_{B_1}|-\rangle_{B_2})\\
&\quad+|-\rangle_A(|H\rangle_{B_1}|-\rangle_{B_2}+|V\rangle_{B_1}|+\rangle_{B_2})]\\
&=\frac{1}{2}[|+\rangle_A(|-\rangle_{B_1}|H\rangle_{B_2}+|+\rangle_{B_1}|V\rangle_{B_2})\\
&\quad+|-\rangle_A(|+\rangle_{B_1}|H\rangle_{B_2}-|-\rangle_{B_1}|V\rangle_{B_2})],
\end{aligned}\tag{2}$$

where $|+\rangle=\frac{1}{\sqrt{2}}(|H\rangle+|V\rangle)$ and $|-\rangle=\frac{1}{\sqrt{2}}(|H\rangle-|V\rangle)$ are the two eigenvectors of the measuring basis $X$.

(4) Bob tells Alice which qubits are chosen for eavesdropping check and the outcomes of the measurements on the samples.

(5) If Bob chooses the measuring basis $Z_{B_1}\otimes Z_{B_2}$, Alice chooses basis $Z_A$ to measure the photon $A$ corresponding to the sampling qubits $B_1B_2$; otherwise, Alice chooses basis $X_A$ to measure the photon $A$.

(6) Alice and Bob use the correlation between their samples to analyze the error rate for eavesdropping check. If the transmission of the sequence $S_B$ is secure, they measure the other quantum systems with the bases $Z_A$ and $Z_{B_1}\otimes Z_{B_2}$ for transmitting their secret message, respectively. They code the outcomes $|H\rangle_A$, $|H\rangle_{B_1}|H\rangle_{B_2}$, $|V\rangle_{B_1}|V\rangle_{B_2}$, $|+\rangle_A$, $|H\rangle_{B_1}|+\rangle_{B_2}$, $|V\rangle_{B_1}|-\rangle_{B_2}$, $|-\rangle_{B_1}|H\rangle_{B_2}$ and $|+\rangle_{B_1}|V\rangle_{B_2}$ as the classical bit 0. They code the outcomes $|V\rangle_A$, $|H\rangle_{B_1}|V\rangle_{B_2}$, $|V\rangle_{B_1}|H\rangle_{B_2}$, $|-\rangle_A$, $|H\rangle_{B_1}|-\rangle_{B_2}$, $|V\rangle_{B_1}|+\rangle_{B_2}$, $|+\rangle_{B_1}|H\rangle_{B_2}$ and $|-\rangle_{B_1}|V\rangle_{B_2}$ as the classical bit 1. If the error rate is higher than the threshold, Alice and Bob repeat the quantum communication from the beginning.

(7) Alice tells Bob the outcome $C_A=O_A\oplus M_A$. Here $O_A$ is the outcome of the measurement on photon $A$ in each quantum system for transmitting secret message and $M_A$ is just the secret message that Alice wants to tell Bob privately.

(8) Bob reads out the secret message directly with her outcome $O_B$, i.e. $M_A=C_A\oplus O_B$. Here $O_B$ is the outcome of the single-photon measurements on the photons $B_1$ and $B_2$.

From our scheme, one can see that a collective-rotation noise does not affect the fidelity of the quantum states transmitted. That is, this DSQC scheme is immune to a collective-rotation noise. On the other hand, although Alice should prepare a sequence of three-photon entangled states for DSQC over a collective-rotation noise channel, the two legitimate users need only single-photon measurements, not Bell-state measurements. This feature will make our scheme convenient in a practical application.

## 2 DSQC against a collective-dephasing noise

A collective-dephasing noise in a fiber can be written as[54]

$$U_p|H\rangle=|H\rangle,\quad U_p|V\rangle=\mathrm{e}^{i\phi}|V\rangle,\tag{3}$$

where $\phi$ is the parameter of a collective-dephasing noise which fluctuates with time $t$. A logical qubit composed of two physical qubits with an antiparallel parity is immune to a collective-dephasing noise, i.e.,

$$|0\rangle_B\equiv|H\rangle_{B_1}|V\rangle_{B_2},\quad |1\rangle_B\equiv|V\rangle_{B_1}|H\rangle_{B_2}.\tag{4}$$

The principle of our DSQC scheme against a collective-dephasing noise can be described as follows, similar to the case with a collective-rotation noise.

(1) The sender Alice prepares a sequence of quantum systems which are in the three-photon entangled state $|\Psi^+\rangle_{AB_1B_2}=\frac{1}{\sqrt{2}}(|H\rangle_A|HV\rangle_{B_1B_2}+|V\rangle_A|VH\rangle_{B_1B_2})$. Although the subsystem composed of the two photons $B_1$ and $B_2$ is entangled with the subsystem composed of the photon $A$, it is immune to a collective-dephasing noise. For DSQC, Alice divides the quantum systems into two sequences $S_A$ and $S_B$. That is, the sequence $S_A$ is composed of the qubits $A$ in all quantum systems in turn and the sequence $S_B$ is composed of the qubits $B_1B_2$ in each quantum system. Alice sends the sequence $S_B$ to Bob and keeps the sequence $S_A$.

(2) Bob picks up some samples for eavesdropping check after he receives the sequence $S_B$. That is, he measures the two photons $B_1$ and $B_2$ in each sample with one of the two measuring bases $Z_{B_1}\otimes Z_{B_2}$ and $X_{B_1}\otimes X_{B_2}$ randomly. The state $|\Phi^+\rangle_{AB_1B_2}$ can be written as follows

$$|\Psi^+\rangle_{AB_1B_2}$$

$$= \frac{1}{2}[|+\rangle_A(|+\rangle_{B_1}|+\rangle_{B_2} - |-\rangle_{B_1}|-\rangle_{B_2}) - |-\rangle_A(|+\rangle_{B_1}|-\rangle_{B_2} - |-\rangle_{B_1}|+\rangle_{B_2})]. \quad (5)$$

That is to say, the outcomes obtained by Alice and Bob are correlated if they choose two corresponding measuring bases.

(3) Bob tells Alice which qubits are chosen for eavesdropping check and the states obtained for the samples.

(4) If Bob chooses the measuring basis $Z_{B_1} \otimes Z_{B_2}$, Alice chooses basis $Z_A$ to measure the photon $A$ corresponding to the sampling qubits $B_1B_2$; otherwise, Alice chooses basis $X_A$ to measure the photon $A$.

(5) Alice and Bob use the correlation between their samples to analyze the error rate for eavesdropping check. If the transmission of the sequence $S_B$ is secure, they measure the other quantum systems with the bases $Z_A$ and $Z_{B_1} \otimes Z_{B_2}$, respectively. They code the outcomes $|H\rangle_A$, $|+\rangle_A$, $|H\rangle_{B_1}|V\rangle_{B_2}$, $|+\rangle_{B_1}|+\rangle_{B_2}$ and $|-\rangle_{B_1}|-\rangle_{B_2}$ as the classical bit 0. They code the outcomes $|V\rangle_A$, $|-\rangle_A$, $|V\rangle_{B_1}|H\rangle_{B_2}$, $|+\rangle_{B_1}|-\rangle_{B_2}$ and $|-\rangle_{B_1}|+\rangle_{B_2}$ as the classical bit 1. If the error rate is higher than the threshold, Alice and Bob repeat the quantum communication from the beginning.

(6) Alice tells Bob the outcome $C_A = O_A \oplus M_A$. Here $O_A$ is the outcome of the measurement on the photon $A$ in each quantum system for transmitting secret message and $M_A$ is just the secret message that Alice wants to tell Bob privately.

(7) Bob reads out the secret message directly with her outcome $O_B$, i.e. $M_A = C_A \oplus O_B$.

Same as the case with a collective-rotation noise, a collective-dephasing noise does not affect the fidelity of the quantum states transmitted in this DSQC scheme. Although Alice should prepare a sequence of three-photon entangled states for DSQC over a collective-rotation noise channel, the two legitimate users need only single-photon measurements, not Bell-state measurements.

## 3 Discussion and conclusion

In our two DSQC schemes, Bob first picks up the samples for eavesdropping check and then tells Alice their positions and their outcomes, by which all the samples can be used for checking eavesdropping, similar to ref. [23]. Of course, this process requires the two parties to be able to store quantum states. As the present techniques are not good enough to store an unknown quantum states, we can modify our DSQC schemes, following some ideas in ref. [42]. Now, Alice and Bob should first pick up the samples for checking eavesdropping independently and then measure the other quantum subsystems with $Z_A$ and $Z_{B_1} \otimes Z_{B_2}$, respectively. Suppose the probabilities that Alice and Bob sample the subsystems for eavesdropping check are $P_A$ and $P_B$, and the probabilities that Alice and Bob choose the measuring bases $Z_A$ and $Z_{B_1} \otimes Z_{B_2}$ are $P_A/2$ and $P_B/2$ respectively, the probability for them to obtain the correlated outcomes for eavesdropping check is $P_AP_B/2$. In addition, they have the probability $P_S = (1 - P_A)(1 - P_B)$ to obtain the outcomes for transmitting the secret message in a deterministic way. When the number of the bits of the secret message is large, the probability approaches 100%, without resorting to quantum storage technique.

Although the two parties of quantum communication exploit two photons transmitted to overcome the decoherence by a collective noise, the security of these two DSQC schemes is the same as that in two-step QSDC scheme for the first transmission of the checking sequence[23]. The two legitimate users exploit the correlation between two subsystems in a maximally entangled state to check eavesdropping. In our DSQC scheme against a collective-rotation noise, the two Bell states $|\phi^+\rangle_{B_1B_2} = \frac{1}{\sqrt{2}}(|H\rangle_{B_1}|H\rangle_{B_2} + |V\rangle_{B_1}|V\rangle_{B_2})$ and $|\psi^-\rangle_{B_1B_2} = \frac{1}{\sqrt{2}}(|H\rangle_{B_1}|V\rangle_{B_2} - |V\rangle_{B_1}|H\rangle_{B_2})$ act as the logical states $|0\rangle_B$ and $|1\rangle_B$, respectively, similar to two-step QSDC scheme[23]. In our DSQC scheme against a collective-dephasing noise, the two product states $|H\rangle_{B_1}|V\rangle_{B_2}$ and $|V\rangle_{B_1}|H\rangle_{B_2}$ act as the logical states $|0\rangle_B$ and $|1\rangle_B$, respectively. That is, in our two DSQC schemes against a collective noise, Alice and Bob exploit the correlation of the Bell state $\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$ to ensure the security of the sequence $S_B$, same as two-step QSDC scheme. In a word, our two DSQC schemes against a collective noise are secure in principle.

In conclusion, we have presented two DSQC schemes over a collective-noise. One is used to counteract a collective-rotation noise and the other is used to counteract a collective-dephasing noise. The two legitimate parties of quantum communication exploit the correlation of their subsystems in a maximally entangled state to check eavesdropping efficiently. Although the sender should prepare a sequence of three-photon quantum systems for accomplishing secure communication against a collective noise, the two parties need only single-photon measurements on their subsystems, instead of Bell-state measurements, which will make our schemes practically convenient.


1 Bennett C H, Brassadrd G. Quantum cryptography: Public-key distribution and coin tossing. In: Proceedings of IEEE Inter national Conference on Computers, Systems and Signal Processing. Bangalore: IEEE Press, 1984. 175–179

2 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. Rev Mod Phys, 2002, 74: 145–195

3 Wen H, Han Z F, Zhao Y B, et al. Multiple stochastic paths scheme on partially-trusted relay quantum key distribution network. Sci China Ser F-Inf Sci, 2009, 52(1): 18–22

4 Wang W Y, Wang C, Zhang G Y, et al. Arbitrarily long distance quantum communication using inspection and power insertion. Chin Sci Bull, 2009, 54(1): 158–162

5 Zhang L B, Zhong Y Y, Kang L, et al. Detection of infrared photons with a superconductor. Chin Sci Bull, 2009, 54(12): 2150–2153

6 Chen W, Han Z F, Mo X F, et al. Active phase compensation of quantum key distribution system. Chin Sci Bull, 2008, 53(9): 1310–1314

7 Li C Y, Li X H, Deng F G, et al. Complete multiple round quantum dense coding with quantum logical network. Chin Sci Bull, 2007, 52(9): 1162–1165

8 Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829–1834

9 Karlsson A, Koashi M, Imoto N. Quantum entanglement for secret sharing and secret splitting. Phys Rev A, 1999, 59: 162–168

10 Xiao L, Long G L, Deng F G, et al. Efficient multiparty quantum-secret-sharing schemes. Phys Rev A, 2004, 69: 052307

11 Zhang Z J, Li Y, Man Z X. Multiparty quantum secret sharing. Phys Rev A, 2005, 71: 044301

12 Zhang Z J, Man Z X. Multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys Rev A, 2005, 72: 022303

13 Deng F G, Li X H, Zhou H Y, et al. Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys Rev A, 2005, 72: 044302

14 Yan F L, Gao T. Quantum secret sharing between multiparty and multiparty without entanglement. Phys Rev A, 2005, 72: 012304

15 Deng F G, Li X H, Li C Y, et al. Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pairs. Phys Rev A, 2005, 72: 044301

16 Deng F G, Li C Y, Li Y S, et al. Symmetry multiparty-controlled teleportation of an arbitrary two-particle entanglement. Phys Rev A, 2005, 72: 022338

17 Deng F G, Li X H, Li C Y, et al. Quantum state sharing of an arbitrary two-qubit state with two-photon entanglements and Bell-state measurements. Eur Phys J D, 2006, 39: 459–464

18 Li X H, Zhou P, Li C Y, et al. Efficient symmetric multiparty quantum state sharing of an arbitrary m-qubit state. J Phys B, 2006, 39: 1975–1983

19 Wang Z Y, Yuan H, Shi S H, et al. Three-party qutrit-state sharing. Euro Phys J D, 2007, 41: 371–375

20 Man Z X, Xia Y J, An N B. Quantum state sharing of an arbitrary multiqubit state using nonmaximally entangled GHZ states. Euro Phys J D, 2007, 42: 333–340

21 Zhang Y Q, Jin X R, Zhang S. Secret sharing of quantum information via entanglement swapping. Chin Phys, 2006, 15: 2252–2255

22 Bostrom K, Felbinger T. Deterministic secure direct communication using entanglement. Phys Rev Lett, 2002, 89: 187902

23 Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A, 2003, 68: 042317

24 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319

25 Deng F G, Li X H, Li C Y, et al. Quantum secure direct communication network with Einstein-Podolsky-Rosen pairs. Phys Lett A, 2006, 359: 359–365

26 Cai Q Y, Li B W. Deterministic secure communication without using entanglement. Chin Phys Lett, 2004, 21(4): 601–603

27 Cai Q Y, Li B W. Improving the capacity of the Bostroem-Felbinger protocol. Phys Rev A, 2004, 69: 054301

28 Wang C, Deng F G, Li Y S, et al. Quantum secret direct communication with high-dimension quantum superdense coding. Phys Rev A, 2005, 71: 044305

29 Wang C, Deng F G, Long G L. Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state. Opt Commun, 2005, 253: 15–20

30 Li X H, Li C Y, Deng F G, et al. Quantum secure direct communication with quantum encryption based on pure entangled states. Chin Phys, 2007, 16: 2149–2153

31 Li X H, Deng F G, Zhou H Y. Improving the security of secure direct communication based on the secret transmitting order of particles. Phys Rev A, 2006, 74: 054302

32 Qin S J, Wen Q Y, Meng L M, et al. Quantum secure direct communication over collective amplitude damping channel. Sci China Ser G-Phys Mech Astron, 2009, 52(8): 1208–1212

33 Beige A, Englert B G, Kurtsiefer C, et al. Secure communication with a publicly known key. Acta Phys Pol A, 2002, 101: 357–368
34 Yan F L, Zhang X Q. A scheme for secure direct communication using EPR pairs and teleportation. Eur Phys J B, 2004, 41: 75–78
35 Gao T, Yan F L, Wang Z X. Quantum secure direct communication by EPR pairs and entanglement swapping. Nuovo Cimento Della Societa Italiana Di Fisica B, 2004, 119: 313–318
36 Gao T, Yan F L, Wang Z X. Deterministic secure direct communication using GHZ states and swapping quantum entanglement. J Phys A, 2005, 38: 5761–5770
37 Gao T, Yan F L, Wang Z X. Quantum secure conditional direct communication via EPR pairs. Int J Mod Phys C, 2005, 16(8): 1293–1301
38 Gao T, Yan F L, Wang Z X. Controlled quantum teleportation and secure direct communication. Chin Phys, 2005, 14: 893–897
39 Man Z X, Zhang Z J, Li Y. Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations. Chin Phys Lett, 2005, 22: 18–21
40 Zhu A D, Xia Y, Fan Q B, et al. Secure direct communication based on secret transmitting order of particles. Phys Rev A, 2006, 73: 022338
41 Cao H J, Song H S. Quantum secure direct communication with W state. Chin Phys Lett, 2006, 23: 290–292
42 Li X H, Deng F G, Li C Y, et al. Deterministic secure quantum communication without maximally entangled states. J Korean Phys Soc, 2006, 49: 1354–1359
43 Qin S J, Wen Q Y, Meng L M, et al. Quantum secure direct communication over the collective amplitude damping channel. Sci China Ser G-Phys Mech Astron, 2009, 52(8): 1208–1212
44 Gao F, Guo F Z, Wen Q Y, et al. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication. Sci China Ser G-Phys Mech Astron, 2008, 51(5): 559–566
45 Yang Y G, Wen Q Y. Threshold quantum secure direct communication without entanglement Sci China Ser G-Phys Mech Astron, 2008, 51(2): 176–183
46 Yang Y G, Wen Q Y. Quasi-secure quantum dialogue using single photons. Sci China Ser G-Phys Mech Astron, 2007, 50(5): 558–562
47 Long G L, Deng F G, Wang C, et al. Quantum secure direct communication and deterministic secure quantum communication. Front Phys China, 2007, 2(3): 251–272
48 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002, 65: 032302
49 Bennett C H, Brassard G, Popescu S, et al. Purification of noisy entanglement and faithful teleportation via noisy channels. Phys Rev Lett, 1996, 76: 722–725
50 Li X H, Deng F G, Zhou H Y. Faithful qubit transmission against collective noise without ancillary qubits. Appl Phys Lett, 2007, 91: 144101
51 Walton Z D, Abouraddy A F, Sergienko A V, et al. Decoherence-free subspaces in quantum key distribution. Phys Rev Lett, 2003, 91: 087901
52 Boileau J C, Gottesman D, Laflamme R, et al. Robust polarization-based quantum key distribution over a collective-noise channel. Phys Rev Lett, 2004, 92: 017901
53 Li X H, Deng F G, Zhou H Y. Efficient quantum key distribution over a collective noise channel. Phys Rev A, 2008, 78: 022321
54 Li X H, Zhao B K, Sheng Y B, et al. Fault tolerant quantum dense coding with collective noise. arXiv:0904.0056