Vol 16 No 5, May 2007
1009-1963/2007/16(05)/1229-04
Chinese Physics
© 2007 Chin. Phys. Soc.
and IOP Publishing Ltd

Secure deterministic communication in a quantum loss channel using quantum error correction code*

Wu Shuang(吴 双)†, Liang Lin-Mei(梁林梅), and Li Cheng-Zu(李承祖)

Department of Physics, School of Science, National University of Defense Technology, Changsha 410073, *China*

(Received 9 June 2006; revised manuscript received 1 December 2006)

The loss of a quantum channel leads to an irretrievable particle loss as well as information. In this paper, the loss of quantum channel is analysed and a method is put forward to recover the particle and information loss effectively using universal quantum error correction. Then a secure direct communication scheme is proposed, such that in a loss channel the information that an eavesdropper can obtain would be limited to arbitrarily small when the code is properly chosen and the correction operation is properly arranged.

Keywords: quantum error correction, quantum loss channel, deterministic communication
PACC: 0367, 0365

1. Introduction

Most quantum communication schemes are of a key distribution type.[1−5] That is, to acquire a key sequence of random bits after the transmission of a particle sequence and quantum private amplification, the communication is nondeterministic. Since 2002, some novel quantum communication protocols that allow secure direct communication[6−11] have been presented, in which the message is sent through the quantum channel deterministically. The receiver can decode the message using some public classical message or not. Compared with quantum key distribution (QKD) protocols, quantum deterministic communications are closer to the classical communication mode.

At present, most quantum secure direct communication (QSDC) protocols use single photons (particles) as information carriers. As is known, single photons would decay exponentially in a real quantum channel. In QSDC protocols, loss of photons would lead to an irretrievable information loss if every particle carries one bit. At the same time, some security problems would arise, for instance, the Ping–Pong protocol is insecure in a noisy quantum channel.[12] So we must consider the noise and loss of the channel when designing a QSDC scheme.

In this paper, we analyse the quantum loss channel first. By filling the vacancy with a particle in a standard state, the loss of particles is transformed into a general error type that can be corrected by general error correction codes. Then we propose a QSDC scheme based on quantum error correction (QEC). First, the messages to be transmitted are prepared in two orthogonal bases randomly, after they are encoded with QEC code, the particles are sent through the channel. During the transmitting process and at the receiving end, we apply QEC operations (including nondemolition measurements, vacancy replacements and error corrections) several times to improve the fidelity. Having checked and assured the security of the channel, the receiver can decode the message efficiently according to the sender's additional classical information.

2. Using QEC to defeat quantum loss

The discovery of QEC code[13] has greatly stimulated the research of quantum computation. Not surprisingly, it will reveal some novel properties when applying QEC to quantum communication.[14] During the quantum communication, the particles and the information would be lost due to absorption, decoherence or interception, etc., all of which would decrease the efficiency and security greatly.

Intuitively, if a noise process acts independently on different qubits in the code, then provided that

*Project supported by the National Natural Science Foundation of China (Grant No 10504042).
†E-mail: wuangwuang@yahoo.com.cn

the noise is sufficiently weak, error-correction should improve the storage fidelity of the encoded state over the unencoded state. It is not surprising that the error can be corrected after we replace the vacancy in the code word with a particle in a standard state, and the information is recovered. First we implement a particle number nondemolition measurement[15] to detect whether there has been any particle lost and which particle has been lost, then we replace the vacancy with a particle which is in state $|0\rangle$ according to the encoding base. The whole effect is that an arbitrary state is transformed to $|0\rangle$ state, which we call a quantum loss error. The process can be described with the following two operation elements:

$$E_1 : \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \qquad E_2 : \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}. \tag{1}$$

They are trace preserving in that $E_1^+E_1+E_2^+E_2 = I$, which satisfies the completeness relation in the operator-sum representation theory.

There is a theorem[16] that supposes C is a quantum code and R is the error-correction operation constructed to recover from a noise process ε with operation elements $\{E_i\}$. Suppose F is a quantum operation with operation elements $\{F_j\}$ which are linear combinations of the E_i, that is $F_j = \sum_i m_{ji}E_i$ for some matrix m_{ji} of complex numbers. Then the error-correction operation R also corrects the effects of the noise process F on the code C.

As $\{I, X, Z, Y\}$ is a complete basis of the 2×2 Hilbert space, $\{E_1, E_2\}$ can be written as their linear combinations. According to the theorem above, the error-correction operations of the code that corrects the bit flip, phase flip, and the bit and phase flip errors would correct the quantum loss errors too.

Suppose in a channel a particle has a probability of p to lose, and $1-p$ not to alter. If the particles are not encoded, the information fidelity that the receiver has is $F_1 = \sqrt{1-p} \approx 1 - p/2 + o(p^2)$, where the fidelity is defined as $F(\rho,\sigma) \equiv \mathrm{tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}$ (ρ, σ are density matrices of the two states). Suppose we encode k qubits of information into an m qubit quantum code which corrects errors on any t qubits, and ρ is the density matrix of the initial code state. As the quantum loss channel acts independently on each of the qubits, it gives rise to a joint action on all m qubits of

$$\begin{aligned}\varepsilon^{\otimes m}(\rho) = {} & (1-p)^m\rho + \mathrm{C}_m^1(1-p)^{m-1}p\sum_{i=1}^{2}E_i\rho E_i^+ + \mathrm{C}_m^2(1-p)^{m-2}p^2\sum_{i_1=1}^{2}\sum_{i_2=1}^{2}E_{i_1}E_{i_2}\rho E_{i_2}^+E_{i_2}^+ + \cdots \\ & + \mathrm{C}_m^t(1-p)^{m-t}p^t\Big(\sum_{i_1=1}^{2}\cdots\sum_{i_t=1}^{2}\Big)(E_{i_1}\cdots E_{i_t})\rho(E_{i_t}^+\cdots E_{i_1}^+) + \cdots. \end{aligned} \tag{2}$$

As we can write $E_1 = (I+Z)/2$ and $E_2 = (X+\mathrm{i}Y)/2$, substituting these expressions in Eq.(2) gives

$$\begin{aligned}\varepsilon^{\otimes m}(\rho) = {} & (1-p)^m\rho + \mathrm{C}_m^1(1-p)^{m-1}p\Big[\frac{1}{4}(I+Z)\rho(I+Z) + \frac{1}{4}(I+\mathrm{i}Y)\rho(I-\mathrm{i}Y)\Big] \\ & + \mathrm{C}_m^2(1-p)^{m-2}p^2\frac{1}{16}[(I+Z)(I+Z)\rho(I+Z)(I+Z) + (I+Z)(I+\mathrm{i}Y)\rho(I-\mathrm{i}Y)(I+Z) \\ & + (I+\mathrm{i}Y)(I+Z)\rho(I+Z)(I-\mathrm{i}Y) + (I+\mathrm{i}Y)(I+\mathrm{i}Y)\rho(I-\mathrm{i}Y)(I-\mathrm{i}Y)] + \cdots . \end{aligned} \tag{3}$$

The fidelity before error-correction is

$$F_2 \geq \sqrt{(1-p)^m + \frac{1}{2}\mathrm{C}_m^1p(1-p)^{m-1}} = \sqrt{1 - \frac{1}{2}\mathrm{C}_m^1p + o(p^2)} = 1 - \frac{1}{4}\mathrm{C}_m^1p + o(p^2). \tag{4}$$

Once the error-correction operation is performed, all terms which have no more than t bit loss of errors in the sum would be recovered to the state ρ. Furthermore, when $k \leq t$, error-correction takes $(\sigma_1\cdots\sigma_k)\rho(\sigma_1\cdots\sigma_k)^+$ back to state ρ (where $k \leq t$; $\sigma_k \in \{X, Y, Z\}$), and the other terms will vanish after the error-correction. As they are taken to the orthogonal subspaces by the error processes, these terms disappear when the syndrome measurement is performed. Since the code can correct errors on t qubits, after error-correction the state of the system becomes

$$\begin{aligned}(R\circ\varepsilon^{\otimes m})(\rho) &= [(1-p)^m + \mathrm{C}_m^1(1-p)^{m-1}p + \mathrm{C}_m^2(1-p)^{m-2}p^2 + \cdots + \mathrm{C}_m^t(1-p)^{m-t}p^t]\rho + \cdots \\ &= (1 - \mathrm{C}_m^{t+1}p^{t+1} + \cdots)\rho + \cdots , \end{aligned} \tag{5}$$

where the high-order terms and the terms that have more than t bit errors are omitted. After error-correction, the information fidelity is

$$F_3 \geq \sqrt{1-\mathrm{C}_m^{t+1}p^{t+1}+\cdots} = 1-\frac{1}{2}\mathrm{C}_m^{t+1}p^{t+1}+o(p^{t+2}). \quad (6)$$

It shows that the information fidelity has been improved from $1-(1/4)\mathrm{C}_m^1 p$ to $1-(1/2)\mathrm{C}_m^{t+1}p^{t+1}$, and the average error probability for every bit decreases from p to about $(1/m)\mathrm{C}_m^{t+1}p^{t+1}$. As $\mathrm{C}_m^{t+1}p^{t+1}$ decreases to 0 exponentially when t increases, for a real channel, we can use a proper QEC code to recover the information effectively and restrict the ultimate error rate to an arbitrary small value. When a high loss rate appears in a long channel, we make loss-detection and error-correction several times in the middle of the channel, where the error-correction operation serves as a quantum repeater.[17] We can prove that after error correction the fidelity is much higher than before, although QEC operations may add some errors.

3. The QSDC scheme using QEC code

For convenience, we assume the sender Alice would like to send N bits of message to the receiver Bob. The N bits of message are divided into n blocks so that each has k bits. The QEC code they use is denoted as (m,k,t), i.e. k qubits of message are encoded into m physical qubits, and the code can correct t qubits of arbitrary errors. The process is as follows:

1) Alice creates $k\times n=N$ random check bits. Then she randomly inserts the n check blocks into the n message blocks to form a mixed sequence and remembers the positions of the check blocks.

2) She selects a random $2N$ bits string b, and performs a Hadamard transformation on each qubit in the mixed sequence for which b is 1.

3) She encodes the mixed sequence and sends them to Bob in turn.

4) Bob receives the qubits and performs a loss-detection and error-correction operation, then publicly announces this fact. Alice randomly announces a half of the check blocks' positions, bases and information encoded on them.

5) Bob decodes and measures them according to Alice's announcement, and publicly shares the result with her. If the error rate is high, they abort the result and restart the protocol from step 1).

6) Alice announces the bases of the remaining qubits and positions of the undeclared check bits, Bob would gain the information through direct measurements.

It should be pointed out that we use the QEC code to encode the qubits rather than the classical code because in a high-loss-rate channel we can set several QEC nodes at proper positions in the channel. The information fidelity can be improved and the quantum error-correction in the middle would not lead to any information leakage. A QEC node includes the procedures of first a nondemolition measurement, then a replacement of the vacancy, and finally the error-corrections. We use only half of the check bits' information to check the eavesdropper Eve's existence rather than the whole check bits for that once the whole information of the check bits is announced. Eve will gain half of the information if she intercepts all of the particles though she would be detected.

4. Simple security demonstration

4.1. Entanglement attack

Eve adds ancillary particles in the state $|E\rangle$ and performs a unitary operation $\hat{E}$ on both systems to entangle her ancillaries to the travelling particles. This action would disturb the code word and result in an error when Bob measures the check bits.

$$\begin{aligned}\hat{E}|0,E\rangle &= \hat{E}|0\rangle_A|E\rangle \\ &= \alpha|0\rangle_A|\varepsilon_{00}\rangle+\beta|1\rangle_A|\varepsilon_{01}\rangle \\ &= \alpha|0\varepsilon_{00}\rangle+\beta|1\varepsilon_{01}\rangle, \\ \hat{E}|1,E\rangle &= \hat{E}|1\rangle_A|E\rangle \\ &= \alpha'|0\rangle_A|\varepsilon_{10}\rangle+\beta'|1\rangle_A|\varepsilon_{11}\rangle \\ &= \alpha'|0\varepsilon_{10}\rangle+\beta'|1\varepsilon_{11}\rangle. \end{aligned} \quad (7)$$

As the operation Eve performs should be unitary, we have

$$\begin{aligned}&|\alpha|^2+|\beta'|^2=1, \\ &|\alpha'|^2+|\beta|^2=1, \\ &\alpha\beta^*+\alpha'^*\beta'=0. \end{aligned} \quad (8)$$

For every ancillary, Bob has a probability of $(1+2\eta)/4$ (where $\eta=|\beta|^2=|\beta'|^2=1-|\alpha|^2=1-|\alpha'|^2$) to obtain a wrong result. Suppose Eve adds totally s ancillaries. She would result in an error rate of $(s/N)(1+2\eta)/4$. When Bob measures the check

bits, if the error rate is greater than $(1/m)C_m^{t+1}p^{t+1}$, the eavesdropper would be detected. Even if s is too small to be detected, the information ratio she can obtain is no more than $4/(1+2\eta)(1/m)C_m^{t+1}p^{t+1}$.

4.2. Intercept-resending attack

If Eve intercepts–resends s particles, as she did not know the positions and the basis of the check blocks, for every particle she intercepts, she has a probability of 1/4 to disturb the coding information and then Bob would gain a wrong result. Eve's action causes an error probability of $s/4N$. If it is higher than $(1/m)C_m^{t+1}p^{t+1}$, she would be detected. Even Eve is not detected, the information ratio she can obtain is no more than $(4/m)C_m^{t+1}p^{t+1}$.

Actually, the scheme is similar to the BB84 protocol except for the QEC encoding and decoding procedures. Following the above analysis, we can give an upper bound of error rate after we use the proper quantum encoding and correction procedures in the channel. Once the error rate is higher than the bound, we would conclude that there is an eavesdropper. As the basis of the message particles and the positions of the undeclared check bits have not been published yet, Eve would not gain any information. Theoretically, if the QEC code and the error-correction operations are properly arranged, the upper bound of error rate can be restricted to an arbitrarily small value, thus the information Eve can obtain would be restricted to arbitrarily small too.

5. Conclusion and discussion

In this paper, we have analysed the particle loss of quantum communication channel, when QEC code is used to encode the information. We can use a particle in a standard state to replace the vacancy resulting from quantum loss, then the error can be corrected and the information can be recovered once the error-correction operation is performed. We have proposed a QSDC scheme to work in the quantum loss channel. The eavesdropper can be detected effectively, after we carry out the eavesdropper check procedure, Bob would decode the message with the help of Alice's additional message of random bits. In a loss channel, we can limit the information that Eve can gain to arbitrarily small if we choose the QEC code and the error-correction operation properly.

The scheme we have presented can be easily extended to six-state protocol, all what we need to do is to encode and decode the information on three unorthogonal basis. The ideas of using QEC code to defeat quantum loss can be transplanted to other QSDC and QKD protocols. This would improve their efficiency and security. As the quantum nondemolition measurement,[18] quantum error correction and quantum memory[19] develop dramatically, the usage of QEC in quantum loss channel would be realistic.

Acknowledgments

We would like to thank Liu Wei-Tao, Wu Wei and Gao Ming for useful discussions.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing* (New York: IEEE) p175
[2] Ekert A 1991 *Phys. Rev. Lett.* **67** 661
[3] Bennett C H 1992 *Phys. Rev. Lett.* **68** 21
[4] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[5] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[6] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319
Deng F G and Long G L 2004 *Phys. Rev.* A **70** 012311
Deng F G and Long G L 2004 quant-ph/0408102
[7] Yan F L and Zhang X Q 2004 *Eur. Phys. J.* B **41** 75
[8] Lucamarini M and Mancini S 2005 *Phys. Rev. Lett.* **94** 140501
[9] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** (5) 893
[10] Kye W H, Kim C M, Kim M S and Park Y J 2005 *Phys. Rev. Lett.* **95** 040501
[11] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev.* A **73** 022338
[12] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901
[13] Calderbank A R and Shor P W 1996 *Phys. Rev.* A **54** 1098
[14] Dür W, Briegel H J, Cirac J I and Zoller P 1999 *Phys. Rev.* A **59** 169
[15] Walls D F and Milburn G J 1998 *Quantum Optics* (Beijing: Springer and World Publishing Corporation) p281
[16] Nielsen M A and Chuang I L 2003 *Quantum Computation and Quantum Information* (Beijing: Higher Education Press) p438
[17] Gingrich R M, Kok P, Lee H, Vatan F and Dowling J P 2003 *Phys. Rev. Lett.* **91** 217901
[18] Gerry Christopher C, Benmoussa A and Campos R A 2005 *Phys. Rev.* A **72** 053818
[19] Alexander A L, Longdell J J, Sellars M J and Manson N B 2006 *Phys. Rev. Lett.* **96** 043602