Vol 18 No 2, February 2009
1674-1056/2009/18(02)/0435-05

Chinese Physics B

© 2009 Chin. Phys. Soc.
and IOP Publishing Ltd

Quantum secure direct communication with Greenberger–Horne–Zeilinger-type state (GHZ state) over noisy channels*

Zhang Xiao-Long(张小龙)[a)†], Zhang Yue-Xia(张月霞)[a)], and Wei Hua(魏 华)[b)c)]

[a)] *Center for Modern Physics and Department of Physics, Chongqing University, Chongqing* 400044, *China*
[b)] *State Key Laboratory of Magnetic Resonance and Atomic and Molecular Physics, Wuhan Institute of Physics and Mathematics, Chinese Academy of Sciences, Wuhan* 430071, *China*
[c)] *Graduate School of Chinese Academy of Sciences, Beijing* 100190, *China*

(Received 22 June 2008; revised manuscript received 31 July 2008)

We propose a quantum error-rejection scheme for direct communication with three-qubit quantum codes based on the direct communication of secret messages without any secret key shared in advance. Given the symmetric and independent errors of the transmitted qubits, our scheme can tolerate a bit of error rate up to 33.1%, thus the protocol is deterministically secure against any eavesdropping attack even in a noisy channel.

Keywords: quantum communication, GHZ state, quantum entanglement
PACC: 0367

The main difference in character between quantum physics and classical physics lies in the nonclassical and counterintuitive phenomena, such as nonlocality and entanglement. The first protocol of quantum secret communication with quantum entanglement was first proposed by Ekert in 1991,[1] which was later shown to be equivalent to the pioneering work by Bennett and Brassard of 1984.[2] For a history of the subject, see Ref.[3]. Since then unconditional security of quantum secret communication has been strictly proved.[4] In a usual protocol two distant parties, traditionally called Alice and Bob, communicate over an open channel that is unintelligible to a third party, usually called eavesdropper 'Eve'. This process is protected by the premise that nonorthogonal states cannot be cloned ('no-cloning' theoretics[5]) or discriminated exactly. With the help of a public channel, each bit string can be used to establish a shared secret key or a verification string between the sender, Alice, and the receiver, Bob. Then they use this secret key to encrypt a message sent through a classical public channel.[6] In Ref.[7] a scheme for secure direct communication was proposed in which the message could be read after transmitting an additional classical information for each qubit. In Ref.[8], a 'ping-pong' protocol was presented which allowed the generation of a deterministic key or even direct secret communication.

In the presence of a considerable quantum channel loss, however, Eve may obtain some information that is hidden in the channel loss without being detected if she replaces the original lossy channel with a less lossy one.[9,10] Furthermore, the original 'ping-pong' protocol might also be attacked without being detected,[11] which means that a smart Eve can just capture the travel qubit and simply perform a σ_z operation if need be, then forward this qubit. Alice and Bob will have zero probability of detecting Eve's attack. This can be found from Eq.(4) in Ref.[8], for any σ_z operation always leads to $\beta \equiv 0$, i.e. the detection probability is always zero. Although Alice might receive one bit of information for each message run, the information that Alice has gained may be a pile of useless random bits.

The aim of this paper is to modify the 'ping-pong' protocol into an unconditional secret protocol even in a noisy quantum channel. The basic idea of our scheme is to encode information by local operations

*Project supported partly by the National Natural Science Foundation of China (Grant Nos 10774163, 10804132 and 10747167), the Natural Science Foundation Project of Chongqing, Chongqing Science and Technology Committee (CQ CSTC) (Grant No 2008BB0152) and partly by the National Major Fundamental Research Program of China (Grant No 2006CB921203).
†E-mail: xlzhang168@gmail.com

into a three-qubit Greenberger–Horne–Zeilinger-type state (GHZ state)[12] and by performing quantum error rejection measurement. As a practical condition, we take into account the channel noise, imperfect GHZ source, storage error and computation error. Fortunately, the last three types of errors can be fixed by quantum error correction[13] and fault-tolerant quantum computation techniques.[14] In our scheme, we suppose that Alice prepares three photons in the maximally entangled three-qubit state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right). \tag{1}$$

During the communication process she keeps one photon, the 'home qubit' and sends the other two photons, the 'travel qubits', to Bob ('ping!'). Bob first checks the parity of the two qubits by using a polarizing beam splitter (PBS). If the two outcoming qubits have the same value, he performs an operation $\sigma_x \otimes \sigma_x$ or $I \otimes I$ (i.e. he does nothing actually.) on the travel two qubits, or else discards both of the travel qubits. Then he sends the travel qubits back to Alice ('pong!'). After receiving the travel qubits, Alice works on a joint GHZ measurement and will obtain corresponding states according to what Bob has done. Thus she can receive information from Bob. To ensure the security of the information, we design the two communication modes, i.e. 'message mode' and 'control mode', which are a little different from those in Ref.[8] and are explicitly described below as an algorithm.

(A) Alice prepares three qubits in the GHZ state $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)$. She stores one qubit as the home qubit and sends the other two qubits, for example, the latter two qubits, as the travel qubits to Bob through the quantum channel.

(B) Bob first checks the parities of the two travel qubits in the z basis just as the linear optical element.[15,16] He discards those pairs whenever the codes have different values and announces which pair has been discarded through the public channel. If the codes have the same value, then Bob takes the following action. After the parity check operation, there are only two codes left, i.e.

$$\left|\psi^0\right\rangle \Rightarrow \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)$$

and

$$\left|\psi^1\right\rangle \Rightarrow \frac{1}{\sqrt{2}}\left(|110\rangle + |001\rangle\right). \tag{2}$$

(C) With probability c, Bob switches to the control mode and proceeds with (D), or else he proceeds with (E).

(D): (D-1) With probability p, Bob performs a CNOT operation between the travel qubits, with one of them used as a target and the other as a controller. Then he rotates the control qubit into the dressed states $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ and measures it in the basis $\{|\pm\rangle\}$. After measuring the control qubit, Bob sends other two qubits that he has randomly prepared in the basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ to Alice. When Alice announces the arrival of the qubits, Bob informs her that it is a control run this time, and tells her the measurement result of the control qubit and also the information about the backed two qubits that he has just prepared randomly and can be used to check the errors in the process of 'pong'. Then Alice switches to the control mode, and measures her home qubit in the basis $\{|\pm\rangle\}$. She should also measure the travel back qubits according to the information that Bob has prepared them. If Alice and Bob have different measurement outcomes, Eve is detected. (D-2) With probability $1-p$, Bob sends the travel qubits back to Alice directly without any operation. If Alice's measurement does not result in $\frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)$, there is an Eve on line. In this case Alice has probability P=0.5 of finding out Eve's attack.. Otherwise, this communication continues.

(E) Define $U_0 = I \otimes I$ and $U_1 = \sigma_x \otimes \sigma_x$ for Bob's operation, where I is the unit matrix and σ_x is the Pauli x matrix. Bob applies one of the two possible unitary operations to the travel qubits and then sends them back to Alice. When Alice receives the travel qubits, she first checks their parities just as Bob has done, then works with a joint GHZ measurement to distinguish the following GHZ states such as

$$\left|\psi^0\right\rangle \Rightarrow U_0\left|\psi\right\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) \rightarrow 0$$

and

$$\left|\psi^1\right\rangle \Rightarrow U_1\left|\psi\right\rangle = \frac{1}{\sqrt{2}}\left(|110\rangle + |001\rangle\right) \rightarrow 1.$$

Then Bob and Alice restart a new turn of communication until all the communication information is successfully transmitted.

Now we analyse the error rates due to channel noise and eavesdropping. Without loss of generality, we suppose that the channel is binary-symmetric, which means that it acts on each bit independently

and has equal distribution to the errors of σ_x, σ_y, σ_z. In a practical channel there are five kinds of operations for one qubit, i.e. I, σ_x, σ_y, σ_z, and σ_0, where I is the unit matrix; σ_x, σ_z and σ_y denote a bit-flip error only, a phase-flip only, and a combination of both errors, respectively; σ_0 represents the channel loss error.

For the case of two travel qubits, there are 25 possibilities as shown in Table 1, in which only the operators $I \otimes I$ and $\sigma_z \otimes \sigma_z$ do not change the results of the travel qubits. After a parity check, there are eight evolutions $I \otimes I$, $\sigma_x \otimes \sigma_x$, $\sigma_y \otimes \sigma_y$, $\sigma_z \otimes \sigma_z$, $\{I \otimes \sigma_z\}$, $\{\sigma_y \otimes \sigma_x\}$ left, where $\{i \otimes j\}$ denotes both $i \otimes j$ and $j \otimes i$. During these evolutions, $\{I \otimes \sigma_z\}$ and $\{\sigma_y \otimes \sigma_x\}$ induce the results out of the encoding subspaces $\{|\psi^0\rangle, |\psi^1\rangle\}$ and these results will be discarded finally. In the case where the losing rate of one qubit, η, is small, the channel loss $\sigma_0 \otimes \sigma_0$ is negligible for both of the travel qubits lost (corresponding to a probability of η^2).[8] Although the evolutions $\sigma_x \otimes \sigma_x$ and $\sigma_y \otimes \sigma_y$ (with the probabilities of p_{x0}^2 and p_{y0}^2, respectively) will project $|\psi^0\rangle \Leftrightarrow |\psi^1\rangle$, which is indistinguishable to Bob, they will be found out due to their comparison with the measurement results on the home qubit in the control mode. Thus all kinds of errors can be completely detected. To check the channel error in the 'ping' process, we estimate the rate of taking an error as a message to be $\frac{p_{x0}^2 + p_{y0}^2}{p_{I0}^2 + p_{x0}^2 + p_{y0}^2 + p_{z0}^2}$, where the error rates of σ_x, σ_y and σ_z are denoted by p_{x0}, p_{y0} and p_{z0}, respectively and $p_{I0} = 1 - p_{x0} - p_{y0} - p_{z0}$. If Alice and Bob require the error rate of their communication to be less than 5% (assuming $p_{z0} = p_{x0} = p_{y0} = \frac{1 - p_{I0}}{3}$), we find that the condition $p_{I0} \geq 66.9\%$ must be fulfilled. In other words, our direct communication protocol can tolerate a quantum channel error rate with an upper limit of 33.1%. In contrast, the tolerable channel bit-flip and phase-flip rates (four-state protocol) in Refs.[15, 16] are 26% and 20% respectively in the symmetric channel with an independent noise.

Table 1. All probabilities of channel error for two qubits.

$I \otimes I$	$I \otimes \sigma_x$	$I \otimes \sigma_y$	$I \otimes \sigma_z$	$I \otimes \sigma_0$
$\sigma_x \otimes$	$\sigma_x \otimes \sigma_x$	$\sigma_x \otimes \sigma_y$	$\sigma_x \otimes \sigma_z$	$\sigma_x \otimes \sigma_0$
$\sigma_y \otimes I$	$\sigma_y \otimes \sigma_x$	$\sigma_y \otimes \sigma_y$	$\sigma_y \otimes \sigma_z$	$\sigma_y \otimes \sigma_0$
$\sigma_z \otimes I$	$\sigma_z \otimes \sigma_x$	$\sigma_z \otimes \sigma_y$	$\sigma_z \otimes \sigma_z$	$\sigma_z \otimes \sigma_0$
$\sigma_0 \otimes I$	$\sigma_0 \otimes \sigma_x$	$\sigma_0 \otimes \sigma_y$	$\sigma_0 \otimes \sigma_z$	$\sigma_0 \otimes \sigma_0$

Security proof — Most analyses of the security of quantum secret communication have dealt with single-particle eavesdropping strategies,[17] immediate or delayed measurements, and the so-called collective attacks,[18,19] in which Eve brings each signal particle into interaction with a separate probe system, and measures all probes together after hearing the public discussion between Alice and Bob. Security against the most general type of attack, the so-called joint attack, has been investigated in Ref.[20].

We now discuss the security of our protocol. First of all, we consider that Eve intercepts the particles (one or both of the travel qubits) that Alice has sent to Bob and then resends them after a measurement or sends other particles to Bob. Because the measurement of the polarization of the travel qubits leads to a completely random result, $\rho_{2,3}$=Tr$_1$ $\{|\psi\rangle\langle\psi|\} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)_{2,3}$ where the subscript 1 indicates the home qubit, and 2 and 3 refer to one of the two travel qubits separately. In this case Eve cannot elicit any useful information from the maximally mixed state without disturbing it. If Eve resends the travel qubits after a measurement or sends other particles to Bob, it will be detected in the control mode and even in the message mode for the change of error rate. For example, suppose that Eve performs a measurement in the z-basis on the captured travel qubits and then resends them to Bob. Eve's measurements of the travel qubits will result in $|00\rangle$ or $|11\rangle$ in an equal probability, thereby Alice's home qubit is collapsed into the state $|0\rangle$ or $|1\rangle$, correspondingly. So this eavesdropping by Eve will collapse the whole system into $|000\rangle$ or $|111\rangle$. In the message run, Alice's decoding measurements on the three-qubit will result in a completely random state between $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and $\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$. While the result $\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$ corresponds to an error of $\{I \otimes \sigma_z\}$ which makes Bob's encoding mapped out of the encode subspaces $\{|\psi^0\rangle, |\psi^1\rangle\}$. Thus this attack from the Eve might be detected even in the message run.

In the control run of the first choice in (D), i.e. (D-1), after Bob's CNOT operation, the travel qubits as the control and the home qubits will be prepared into the EPR pair $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ if they are not disturbed. This means that Bob's measurements on the travel qubit in the dressed states $|\pm\rangle$ will make Alice's home qubit collapsed into$|+\rangle$ or $|-\rangle$, correspondingly. After receiving the classic message from Bob, Alice measures her home qubit also in

the dressed states $|\pm\rangle$. If both results are not coincident with each other, Bob knows that Eve is on line, and so Bob stops the communication. However, in the above intercept-resend strategy, Eve's attack will make the travel qubit the control and the home qubits that are collapsed into $|00\rangle$ or $|11\rangle$, which correspond to $|00\rangle \rightarrow \frac{1}{2}(|+\rangle+|-\rangle)\otimes(|+\rangle+|-\rangle)$ and $|11\rangle \rightarrow \frac{1}{2}(|+\rangle-|-\rangle)\otimes(|+\rangle-|-\rangle)$. Obviously, half of their results are not coincident with each other. In the second choice of (D), i.e. (D-2), if the measurements by Alice do not result in $\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)$, there should be an Eve on line. So in the ideal condition Alice has probability P=0.5 to detect Eve's attacks.

Here we consider a more generic attack and give a parallel proof as shown in Ref.[8] but in a noisy channel where Eve may hide herself by replacing the original lossy channel with a less lossy one.[9] Eve aims to find out what operation Bob has performed. But due to no access to Alice's home qubit, Eve's operations are only restricted to the travel qubits, whose states are completely indistinguishable from the complete mixture $\rho_{2,3}=\mathrm{Tr}_1\{|\psi\rangle\langle\psi|\}=\frac{1}{2}(|00\rangle\langle 00|+|11\rangle\langle 11|)_{2,3}$. We will show that any information Eve gains would make her face a nonzero detected probability. By replacing $|0\rangle$ and $|1\rangle$ with $|00\rangle$ and $|11\rangle$, respectively, we can rewrite Eq.(4) in Ref.[8] as

$$|\psi'\rangle=\hat{E}|00,\chi\rangle=\alpha|00,\chi_0\rangle+\beta|11,\chi_1\rangle. \quad (3)$$

When the noises of the channel are considered, the detection probability for Eve's attack cannot be simply expressed as $d=2|\beta|=1-2|\alpha|$. Instead, the effect of the error rate distribution of the channel noise should be involved. From the above discussion and a straightforward calculation the detection probability (d) for Eve's attack in the $A\rightarrow B$ process in the control run is obtained as shown below:

$$d=\beta^2-\frac{p_{x0}^2+p_{y0}^2}{p_{I0}^2+p_{x0}^2+p_{y0}^2+p_{z0}^2}.$$

Although the detection probability becomes smaller than that in the ideal condition,[8] it is an absolute probability, that is to say, Eve will be definitely present so long as $d>0$. Similarly, Eve can also be detected in the $B\rightarrow A$ process. The difference between the travel back qubits measured by Alice and those prepared by Bob indicates the error rate of the second run, 'pong'. If the estimated channel error rate is too high, the scheme is dead and should be restarted from the beginning.

Now we come to analyse how much information Eve can maximally gain in our scheme. Suppose that Bob encodes his bit by applying the operation $U_0=I\otimes I$ or $U_1=\sigma_x\otimes\sigma_x$ to the travel qubits with the probability p_0 and p_1, respectively, then the state of the travel qubit after Eve's attack will be expressed as

$$\rho=\begin{pmatrix}|\alpha|^2p_0+|\beta|^2p_1 & p_0\alpha\beta^*+p_1\alpha^*\beta\\ p_0\alpha^*\beta+p_1\alpha\beta^* & |\alpha|^2p_1+|\beta|^2p_0\end{pmatrix}.$$

Direct calculation of the roots of the characteristic polynomial $\det(\rho-\lambda)$ yields the values of eigenvalue λ of ρ, i.e.

$$\lambda=\frac{1}{2}\left[1\pm\sqrt{1-4p_0p_1|\alpha^2-\beta^2|}\right].$$

In the case of $p_0=p_1=1/2$, and $\alpha=\beta=1/\sqrt{2}$, Eve can gain all the information with the von-Neumann entropy $I_0=1$ and the detection probability $d=\frac{1}{2}-\frac{p_{x0}^2+p_{y0}^2}{p_{I0}^2+p_{x0}^2+p_{y0}^2+p_{z0}^2}$. In our protocol $p_{I0}\geq 66.9\%$, the detection probability d=0.45. The process $B\rightarrow A$ is shown in Table 2, where listed in the first column are the types of joint channel errors (JCEs) before Bob's encoding. The correlated probability between Alice and Bob is

$$\begin{aligned}P(0|0)=&P(1|1)\\ =&|\alpha|^2\frac{p_{I0}^2+p_{z0}^2}{p_{I0}^2+p_{x0}^2+p_{y0}^2+p_{z0}^2}\\ &+|\beta|^2\frac{p_{x0}^2+p_{y0}^2}{p_{I0}^2+p_{x0}^2+p_{y0}^2+p_{z0}^2},\end{aligned}$$

and

$$\begin{aligned}P(0|1)=&P(1|0)\\ =&|\alpha|^2\frac{p_{x0}^2+p_{y0}^2}{p_{I0}^2+p_{x0}^2+p_{y0}^2+p_{z0}^2}\\ &+|\beta|^2\frac{p_{I0}^2+p_{z0}^2}{p_{I0}^2+p_{x0}^2+p_{y0}^2+p_{z0}^2}. \quad (4)\end{aligned}$$

As a further investigation of this protocol, one can check the result by comparing it with that obtained in the ideal channel condition.

Table 2. Probabilities of joint channel error in the "pong" process.

$I \otimes I$	P_{I0}^2	$(\|000\rangle + \|111\rangle)/\sqrt{2}$
$\sigma_z \otimes \sigma_z$	P_{z0}^2	$(\|000\rangle + \|111\rangle)/\sqrt{2}$
$\sigma_x \otimes \sigma_x$	P_{x0}^2	$(\|110\rangle + \|001\rangle)/\sqrt{2}$
$\sigma_y \otimes \sigma_y$	P_{y0}^2	$(\|110\rangle + \|001\rangle)/\sqrt{2}$
$\{I \otimes \sigma_z\}$	$2P_{I0}P_{z0}$	$(\|000\rangle - \|111\rangle)/\sqrt{2}$
$\{\sigma_y \otimes \sigma_x\}$	$2P_{x0}P_{y0}$	$(\|110\rangle - \|001\rangle)/\sqrt{2}$

In conclusion, we have presented a deterministically secure direct communication protocol, in which any kind of error can be detected in the transmission channel between Alice and Bob. Alice's measurements depend only on the distinguishability between the states $\left|\psi^0\right\rangle$ and $\left|\psi^1\right\rangle$. Experimentally, the preparation of the GHZ state has been tested in Ref.[21], and the parity check in our scheme is already available in experiment with linear optics. Therefore, we believe that the experimental realization of our protocol is feasible by using existing technology.

We are grateful to Mang Feng for his help.

References

[1] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[2] Bennett C H and Brassard G 1984 in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* Bangalore, India (New York: IEEE) p175–179

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

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

[5] Wootters W K and Zurek W H 1982 *Nature* (London) **299** 802

[6] Mi J L,Wang F Q, Lin Q Q and Liang R S 2008 *Chin. Phys.* B **17** 1178

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

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

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

[10] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2007 *Chin. Phys.* **16** 277

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

[12] Greenberger D M, Horne M A, Shimony A and Zeilinger A 1990 *Am. J. Phys.* **58** 1131

[13] Shor P W 1995 *Phys. Rev.* A **52** 2493
Steane A M 1996 *Phys. Rev. Lett.* **77** 793

[14] Knill E, Laflamme R and Zurek W H 1998 *Science* **279** 342

[15] Wang X B 2004 *Phys. Rev. Lett.* **92** 077902

[16] Chau H F 2002 *Phys. Rev.* A **66** 060302(R)

[17] Bennett C H and Brassard G 1992 *J. Cryptol.* **5** 3
Lütkenhaus N 1996 *Phys. Rev.* A **54** 97

[18] Biham E and Mor T 1997 *Phys. Rev. Lett.* **78** 2256

[19] Li C Y, Li X H, Deng F G and Zhou H Y 2008 *Chin. Phys.* B **17** 2352

[20] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818
Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1998 *Phys. Rev. Lett.* **80** 2022

[21] Pan J W, Bouwmeester D, Daniell M, Weinfurter H and Zeilinger A 2000 *Nature* (London) **403** 515