Deterministic secure direct communication using GHZ states and swapping quantum entanglement

2005 J. Phys. A: Math. Gen. 38 5761

(http://iopscience.iop.org/0305-4470/38/25/011)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **38** (2005) 5761–5770 doi:10.1088/0305-4470/38/25/011

Deterministic secure direct communication using GHZ states and swapping quantum entanglement

T Gao[1,2,3], **F L Yan**[1,4] **and Z X Wang**[3]

[1] CCAST (World Laboratory), PO Box 8730, Beijing 100080, People's Republic of China
[2] College of Mathematics and Information Science, Hebei Normal University, Shijiazhuang 050016, People's Republic of China
[3] Department of Mathematics, Capital Normal University, Beijing 100037, People's Republic of China
[4] College of Physics, Hebei Normal University, Shijiazhuang 050016, People's Republic of China

E-mail: gaoting@heinfo.net

Received 7 February 2005, in final form 6 May 2005
Published 8 June 2005
Online at stacks.iop.org/JPhysA/38/5761

Abstract

We present a deterministic secure direct communication scheme via entanglement swapping, where a set of ordered maximally entangled three-particle states (GHZ states), initially shared by three spatially separated parties, Alice, Bob and Charlie, functions as a quantum information channel. After ensuring the safety of the quantum channel, Alice and Bob apply a series of local operations on their respective particles according to the tripartite stipulation and the secret message they both want to send to Charlie. By three of Alice, Bob and Charlie's Bell measurement results, Charlie is able to infer the secret messages directly. The secret messages are faithfully transmitted from Alice and Bob to Charlie via initially shared pairs of GHZ states without revealing any information to a potential eavesdropper. Since there is no transmission of the qubits carrying the secret message between any two of them in the public channel, it is completely secure for direct secret communication if a perfect quantum channel is used.

PACS numbers: 03.67.Dd, 03.67.Hk

1. Introduction

Cryptography is the art of enabling two parties to communicate in private. Effective cryptosystems make it easy for parties who wish to communicate to achieve privacy, but make it very difficult for third parties to 'eavesdrop' on the content of the conversation. A simple, yet highly effective private key cryptosystem is the *Vernam cipher*, sometimes called a one time pad. The great feature of this system is that as long as the key strings are truly secret, it is provably secure. The major difficulty of private key cryptosystems is secure distribution

of key bits, since a malevolent third party may be eavesdropping on the key distribution, and then use the intercepted key to decrypt some of the messages in transmission.

One of the earliest discoveries in quantum computation and quantum information was that quantum mechanics can be used to do key distribution in such a way that Alice and Bob's security cannot be compromised. This procedure is known as *quantum cryptography or quantum key distribution* (QKD). The basic idea is to exploit the quantum mechanical principle that observation in general disturbs the system being observed. In 1984, Bennett and Brassard proposed the first quantum cryptography protocol [1] using quantum mechanics to distribute keys between Alice and Bob, without any possibility of compromise. Since then numerous QKD protocols have been proposed, such as Ekert's 1991 protocol (Ekert91) [2], the Bennett–Brassard–Mermin 1992 protocol (BBM92) [3], the B92 protocol [4] and other protocols [5–22].

Recently, Shimizu and Imoto [23, 24] and Beige *et al* [25] presented novel quantum secure direct communication (QSDC) schemes, in which the two parties communicate important messages directly without first establishing a shared secret key to encrypt them and the message is deterministically sent through the quantum channel, but can be read only after the transmission of an additional piece of classical information for each qubit. Boström and Felbinger [26] put forward a communication scheme, the 'ping-pong protocol', which also allows for deterministic communication. This protocol can be used for the transmission of either a secret key or a plain text message. Wójcik discussed the security of the 'ping-pong protocol' in a noisy quantum channel [27]. Deng *et al* [28] suggested a two-step quantum direct communication protocol using an Einstein–Podolsky–Rosen pair block. However, in all these QSDC schemes it is necessary to send the qubits with secret messages (message-coding sequence) in the public channel. Therefore, Eve can attack the qubits in transmission and make the communication interrupt.

More recently, Yan and Zhang [29] presented a QSDC scheme using Einstein-Podolsky-Rosen pairs and teleportation [30]. By means of controlled quantum teleportation [31], we proposed two controlled QSDC protocols [32, 33]. Since in these protocols there are no particles carrying secret messages to be transmitted in the public channel, so the communication cannot be interrupted by any eavesdropper. Therefore, they are completely secure for direct secret communication as long as a perfect quantum channel is used.

Entanglement swapping [34] is a method that enables one to entangle two quantum systems that do not have direct interaction with one another. Based on entanglement swapping, we presented a QSDC scheme [35]. In this paper, we introduce another QSDC scheme achieved by swapping quantum entanglement, in which a set of ordered three-particle Greenberger–Horne–Zeilinger (GHZ) states initially shared by three spatially separated parties, Alice, Bob and Charlie, functions as a quantum information channel. The proposed QSDC scheme is simultaneous mutual communications among different pairs of parties, one for Alice and Charlie and another for Bob and Charlie. After ensuring the safety of the quantum channel, Alice and Bob encode secret classical bits by applying predetermined unitary operations on GHZ triplets. The secret messages encoded by local operations are faithfully transmitted from two distant senders (Alice and Bob) to a remote receiver (Charlie) without revealing any information to a potential eavesdropper.

2. A simultaneous mutual quantum secure direct communication protocol between the central party and other two parties

In this section we propose a simultaneous mutual quantum secure direct communication scheme which utilizes shared GHZ states and entanglement swapping between communicating parties, in the form of three people (Alice, Bob and Charlie).

2.1. Notation

Let us start by illustrating entanglement swapping. We first define four Bell states (EPR pairs) as

$$\Phi^{\pm} \equiv \tfrac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \qquad \Psi^{\pm} \equiv \tfrac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \tag{1}$$

and eight GHZ states as

$$\begin{aligned} |P^{\pm}\rangle &\equiv \tfrac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle), & |Q^{\pm}\rangle &\equiv \tfrac{1}{\sqrt{2}}(|001\rangle \pm |110\rangle), \\ |R^{\pm}\rangle &\equiv \tfrac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle), & |S^{\pm}\rangle &\equiv \tfrac{1}{\sqrt{2}}(|011\rangle \pm |100\rangle). \end{aligned} \tag{2}$$

Suppose three parties, Alice, Bob and Charlie, share two GHZ triplets $|P^{+}\rangle_{123}$ and $|P^{+}\rangle_{456}$ where Alice has qubits 1 and 4, Bob possesses 2 and 5 and particles 3 and 6 are in Charlie's side. Two operations are performed on qubits 1 and 4, and 2 and 5 with the Bell basis, $\Phi^{\pm}$ and $\Psi^{\pm}$, by Alice and Bob, respectively; then the total state $|P^{+}\rangle_{123} \otimes |P^{+}\rangle_{456}$ is projected onto $\Phi^{+}_{14} \otimes \Phi^{+}_{25} \otimes \Phi^{+}_{36}$, $\Phi^{+}_{14} \otimes \Phi^{-}_{25} \otimes \Phi^{-}_{36}$, $\Phi^{-}_{14} \otimes \Phi^{+}_{25} \otimes \Phi^{-}_{36}$, $\Phi^{-}_{14} \otimes \Phi^{-}_{25} \otimes \Phi^{+}_{36}$, $\Psi^{+}_{14} \otimes \Psi^{+}_{25} \otimes \Psi^{+}_{36}$, $\Psi^{+}_{14} \otimes \Psi^{-}_{25} \otimes \Psi^{-}_{36}$, $\Psi^{-}_{14} \otimes \Psi^{+}_{25} \otimes \Psi^{-}_{36}$ and $\Psi^{-}_{14} \otimes \Psi^{-}_{25} \otimes \Psi^{+}_{36}$ with equal probability of $1/8$ for each. Previous entanglement of qubits 1, 2 and 3, and 4, 5 and 6 is now swapped into entanglement between 1 and 4, 2 and 5 and 3 and 6. Although we considered entanglement swapping with the initial state $|P^{+}\rangle_{123} \otimes |P^{+}\rangle_{456}$, similar results can be achieved with other GHZ states. For example, when Alice, Bob and Charlie originally share $|S^{+}\rangle_{123}$ and $|P^{+}\rangle_{456}$, there are eight possible measurement outcomes, $\Psi^{+}_{14} \otimes \Phi^{+}_{25} \otimes \Phi^{+}_{36}$, $\Psi^{+}_{14} \otimes \Phi^{-}_{25} \otimes \Phi^{-}_{36}$, $\Psi^{-}_{14} \otimes \Phi^{+}_{25} \otimes \Phi^{-}_{36}$, $\Psi^{-}_{14} \otimes \Phi^{-}_{25} \otimes \Phi^{+}_{36}$, $\Phi^{+}_{14} \otimes \Psi^{+}_{25} \otimes \Psi^{+}_{36}$, $\Phi^{+}_{14} \otimes \Psi^{-}_{25} \otimes \Psi^{-}_{36}$, $\Phi^{-}_{14} \otimes \Psi^{+}_{25} \otimes \Psi^{-}_{36}$ and $\Phi^{-}_{14} \otimes \Psi^{-}_{25} \otimes \Psi^{+}_{36}$ with equal probability $1/8$.

2.2. Preparing a quantum channel

Suppose that three spatially separated parties wish to realize simultaneous mutual communications in secret among different pairs of parties, one for Alice and Charlie and another for Bob and Charlie. In order to achieve tripartite communications between one party and the other two parties in private at the same time, the first step is to establish a quantum channel (GHZ triplets). Obtaining these GHZ triplets could have come about in many different ways, such as Charlie prepares a sequence of GHZ triplets and then shares each triplet with Alice and Bob; or they could have met a long time ago and shared them, storing them until the present. Alice, Bob and Charlie then choose randomly a subset of GHZ triplets, and do some appropriate tests of fidelity. Passing the test certifies that they continue to hold sufficiently pure, entangled quantum states. However, if tampering has occurred, they throw out the GHZ triplets and reconstruct them. We will discuss the details in section 3.

2.3. The direct communication scheme by shared GHZ states and entanglement swapping

After ensuring the security of the quantum channel (GHZ states), Alice, Bob and Charlie begin secure direct communication. The QSDC scheme works as follows.

(1) Alice, Bob and Charlie randomly divide all pure GHZ triplets into N ordered groups $\{\xi(1)_{123}, \eta(1)_{456}\}, \{\xi(2)_{123}, \eta(2)_{456}\}, \ldots, \{\xi(N)_{123}, \eta(N)_{456}\}$, where $\xi(i)_{123}$ and $\eta(i)_{456}$ denote two GHZ states of Alice's particles 1 and 4, Bob's particles 2 and 5 and Charlie's 3 and 6 in the ith group. For simplicity, let us suppose that these GHZ triplets are in the state $|P^{+}\rangle$.

(2) Alice, Bob and Charlie agree that Alice encodes information by local operations

$$\begin{aligned} \sigma_{00} &= I = |0\rangle\langle 0| + |1\rangle\langle 1|, & \sigma_{01} &= \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|, \\ \sigma_{10} &= \mathrm{i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|, & \sigma_{11} &= \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| \end{aligned} \tag{3}$$

on GHZ triplets $\xi(i)_{123}$, and Bob by local operations

$$\sigma_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|, \qquad \sigma_1 = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|. \tag{4}$$

Alice and Charlie, and Bob and Charlie assign secretly two bits and one bit to Alice and Bob's respective operations as following encoding

$$\sigma_{00} \to 00, \quad \sigma_{01} \to 01, \quad \sigma_{10} \to 10, \quad \sigma_{11} \to 11, \tag{5}$$

and

$$\sigma_0 \to 0, \qquad \sigma_1 \to 1. \tag{6}$$

(3) Alice and Bob encode their respective messages (secret classical bits) on GHZ groups. Explicitly, both Alice and Bob apply a predetermined unitary operation on each of their particles 1 and 2 according to their respective secret message sequence.

Suppose Alice, Bob and Charlie initially share GHZ state $|P^+\rangle_{123}$, $|P^+\rangle_{456}$; then their original total state is

$$\begin{aligned} |P^+\rangle_{123} \otimes |P^+\rangle_{456} = \tfrac{1}{2\sqrt{2}}\big[&\Phi^+_{14} \otimes \Phi^+_{25} \otimes \Phi^+_{36} + \Phi^+_{14} \otimes \Phi^-_{25} \otimes \Phi^-_{36} + \Phi^-_{14} \otimes \Phi^+_{25} \otimes \Phi^-_{36} \\ &+ \Phi^-_{14} \otimes \Phi^-_{25} \otimes \Phi^+_{36} + \Psi^+_{14} \otimes \Psi^+_{25} \otimes \Psi^+_{36} + \Psi^+_{14} \otimes \Psi^-_{25} \otimes \Psi^-_{36} \\ &+ \Psi^-_{14} \otimes \Psi^+_{25} \otimes \Psi^-_{36} + \Psi^-_{14} \otimes \Psi^-_{25} \otimes \Psi^+_{36}\big]. \end{aligned} \tag{7}$$

If Alice wishes to transmit 11 to Charlie and Bob wants to send 1 to Charlie, then Alice performs a local operation σ_{11} on particle 1 and Bob applies σ_1 on his particle 2; thus the state $|P^+\rangle_{123}$ is turned into $|R^-\rangle_{123}$.

(4) Alice and Bob make a Bell measurement on particles 1 and 4, and 2 and 5, respectively. We can see the effects of measurements by Alice and Bob on Charlie's particles 3 and 6 if we express the product of GHZ states $|R^-\rangle_{123}$ and $|P^+\rangle_{456}$ in the following equation:

$$\begin{aligned} |R^-\rangle_{123} \otimes |P^+\rangle_{456} = \tfrac{1}{2\sqrt{2}}\big[&\Phi^-_{14} \otimes \Psi^+_{25} \otimes \Phi^+_{36} - \Phi^-_{14} \otimes \Psi^-_{25} \otimes \Phi^-_{36} + \Phi^+_{14} \otimes \Psi^+_{25} \otimes \Phi^-_{36} \\ &- \Phi^+_{14} \otimes \Psi^-_{25} \otimes \Phi^+_{36} + \Psi^-_{14} \otimes \Phi^+_{25} \otimes \Psi^+_{36} - \Psi^-_{14} \otimes \Phi^-_{25} \otimes \Psi^-_{36} \\ &+ \Psi^+_{14} \otimes \Phi^+_{25} \otimes \Psi^-_{36} - \Psi^+_{14} \otimes \Phi^-_{25} \otimes \Psi^+_{36}\big]. \end{aligned} \tag{8}$$

If Alice and Bob get measurement outcomes Φ^+_{14} and Ψ^-_{25}, respectively, then Charlie's two particles 3 and 6 will have the state Φ^+_{36}.

(5) Alice and Bob inform Charlie that they have made a Bell measurement on particles 1 and 4, and 2 and 5 over a classical channel, respectively, but do not tell the results of their measurements.

(6) Charlie performs a Bell measurement on his particles 3 and 6 and deduces the outcomes of Alice and Bob's measurements.

From the calculation of entanglement swapping (equation (7)) and his measurement outcome Φ^+_{36}, Charlie could calculate that the initially whole state $|P^+\rangle_{123} \otimes |P^+\rangle_{456}$ should collapse to $\Phi^+_{14} \otimes \Phi^+_{25} \otimes \Phi^+_{36}$ or $\Phi^-_{14} \otimes \Phi^-_{25} \otimes \Phi^+_{36}$ without Alice and Bob's local operations.

(7) Charlie asks and gets Alice and Bob's measurement results publicly.

(8) Charlie can read out Alice and Bob's secret message by comparing his calculation result with Alice and Bob's practical measurement outcomes.

From the measurement results announced by Alice and Bob, and his calculation result, Charlie can infer that Alice and Bob have applied local operations σ_{11} and σ_1 on particles 1 and 2, respectively, such that $\Phi_{14}^- \otimes \Phi_{25}^- \otimes \Phi_{36}^+$ turns into $\Phi_{14}^+ \otimes \Psi_{25}^- \otimes \Phi_{36}^+$; since it is impossible for Alice and Bob to change $\Phi_{14}^+ \otimes \Phi_{25}^+ \otimes \Phi_{36}^+$ into $\Phi_{14}^+ \otimes \Psi_{25}^- \otimes \Phi_{36}^+$ by applying unitary operation $\sigma_{k_1 k_{1'}} \otimes \sigma_{k_2}$ ($k_1, k_{1'}, k_2 \in \{0, 1\}$) on particles 1 and 2, thus he obtains Alice's message 11 and Bob's 1. Finally, three spatially separated parties have realized deterministic secure direct communication between one party and the other two parties.

Remark 1. We should point out that the encoding schemes of equations (5) and (6) are secret, i.e. only Alice and Charlie know the encoding scheme (5), and only Bob and Charlie know equation (6). The reason is as follows. After Charlie performs a Bell measurement on his qubits 3 and 6, he asks Alice and Bob to declare their Bell measurement results on the qubits 1 and 4, and 2 and 5. This public declaration step is crucial. However, an eavesdropper who knows that the original initial state is $|P^+\rangle_{123} \otimes |P^+\rangle_{456}$ will do her calculation the same as Charlie. When she hears that Alice and Bob, respectively, obtained measurement results Φ_{14}^+ and Ψ_{25}^-, the eavesdropper looks at equation (7) and can easily deduce that such a measurement result can be obtained by applying one-qubit unitary operators on the following four cases: $\Phi_{14}^+ \otimes \Phi_{25}^- \otimes \Phi_{36}^-$, $\Phi_{14}^- \otimes \Phi_{25}^- \otimes \Phi_{36}^+$, $\Psi_{14}^+ \otimes \Psi_{25}^- \otimes \Psi_{36}^-$ and $\Psi_{14}^- \otimes \Psi_{25}^- \otimes \Psi_{36}^+$. Since Charlie's measurement result is secret (not publicly declared), the eavesdropper may pick the correct state only with a probability of $1/4$. If the information on the encoding scheme is not available to the eavesdropper, there is no way for the eavesdropper to find the correct classical bits. So it is necessary for the two pairs, Alice and Charlie, and Bob and Charlie, to keep their respective encoding schemes (5) and (6) private. In order to achieve privacy safely, Alice and Charlie, and Bob and Charlie may use secret keys generated by shared GHZ states to communicate the encoding method with each other. Since Alice, Bob and Charlie want to achieve simultaneous mutual communications in secret among different pairs of parties, one for Alice and Charlie and another for Bob and Charlie, they must be trustworthy and cooperative. Two communication parties Alice and Charlie (Bob and Charlie) can generate a secret key used to transmit their encoding scheme via initially shared pairs of GHZ states with the help of the third party Bob (Alice). The details of generating secret keys are as follows. Suppose Alice wants to send Charlie her encoding scheme. Each of Alice, Bob and Charlie performs a Bell measurement on their respective particles 1 and 4, 2 and 5, and 3 and 6, obtaining one of four possible results, Φ^+, Φ^-, Ψ^+ and Ψ^-. Bob tells Alice and Charlie of his measurement outcome. Depending on Bob's information, Alice and Charlie can infer the measurement result of each other. Alice and Charlie agree that each of the four Bell states carry two bits of classical message (there are $4! = 24$ kinds of encoding methods; they can choose one kind at random) and regard the information carrying by either Alice's measurement results or Bob's measurement results as secret key bits used to transmit their encoding scheme. For instance, if the original state is $|R^-\rangle_{123}|P^+\rangle_{456}$, and the outcome of Bob's measurement is Ψ_{25}^+, then according to her measurement result Φ_{14}^-, Alice can infer that the outcome of Charlie's measurement must be Φ_{36}^+. Similarly, Charlie can deduce Alice's measurement result Φ_{14}^- from his measurement outcome Φ_{36}^+. If Alice and Charlie encode Φ_{14}^+, Φ_{14}^-, Ψ_{14}^+ and Ψ_{14}^- as 00, 01, 10 and 11, then they share two classical bits 01. Alice and Charlie sacrifice some randomly selected bits to test the 'error rate'. If the error rate is too high, they abort this QKD protocol. Otherwise, they perform information reconciliation and privacy amplification [36–42] on the remaining bits to obtain secure final key bits for Alice informing Charlie of the encoding scheme (5). Using the same method, Bob and Charlie get a secret key for Bob sending the encoding scheme (6) to Charlie. Thus, in our QSDC scheme, the eavesdropper cannot get the encoding scheme of the classical bits on the unitary operators.

That is, if the eavesdropper understands that the operator Alice has applied is σ_z, she does not know that this corresponds to the classical bits 11. Therefore, our scheme is a deterministic QSDC scheme.

Remark 2. The crucial point in the proposed scheme is that the qubits carrying the encoded message are not transmitted in the public channel. Therefore, a potential eavesdropper cannot obtain any information.

Remark 3. In order to protect the transmitting information from the eavesdropper, Alice, Bob and Charlie can make use of classical error correction protocol [38]. That is, Alice and Bob encode their secret messages and Charlie decode these messages according to a pre-determined classical error correction protocol.

Note

(A) The above protocol is also a quantum key distribution (QKD) scheme based on GHZ states and entanglement swapping. If the communication parties want to distribute keys, Alice and Bob randomly generate their respective classical bit strings a and b, and then Alice divides her string a into lengths of two bits and encodes by applying the unitary operators on her qubits and in the same way Bob applies his operator for each classical bit of b. Alice, Bob and Charlie agree in advance that each of the four Bell states can carry two bits classical information and encode Φ^+, Φ^-, Ψ^+ and Ψ^- as 00, 01, 10 and 11, respectively. Protocol then follows as before. By Alice's measurement result Φ_{14}^+, only both Alice and Charlie derive $\Phi_{14}^- \xrightarrow{\sigma_{11}} \Phi_{14}^+$, i.e. Alice and Charlie obtain σ_{11} and Φ_{14}^- secretly. Since Alice's operator σ_{11} is certain and her measurement result Φ_{14}^+ is random, Alice and Charlie share two certain bits 11 and two random bits 01 in private. Similarly, from Bob's measurement outcome Ψ_{25}^-, Bob and Charlie obtain $\Phi_{25}^- \xrightarrow{\sigma_1} -\Psi_{25}^-$ and share one certain bit 1 and two random bits 01 privately. Therefore, in our proposed protocol, Alice and Bob perform one local operation on their respective particles 1 and 2, and Charlie shares 2 certain bits and 2 random bits with Alice, and 1 certain bit and 2 random bits with Bob secretly.

(B) Bob can also apply unitary operator $I = |0\rangle\langle 0| + |1\rangle\langle 1|$ and $\mathrm{i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$, and he and Charlie agree beforehand to the encoding: $I \to 0$, $\mathrm{i}\sigma_y \to 1$, instead of that in the above protocol.

(C) Particles 1 and 2 play symmetric and equal roles. That is, Alice (Bob) can use one local operation in equation (4) (equation (3)) and transmit one bit (two bits) of information to Charlie.

(D) There are $4! = 24$ ($2! = 2$) kinds of encoding method for one assigning two bits to local operations I, σ_x, $\mathrm{i}\sigma_y$ and σ_z (one bit to I and σ_z). Two communication parties can choose randomly one kind as their encoding scheme.

3. Security

The security of these schemes is limited by the quality of the quantum channel between the parties. We base our argument of security on a perfect quantum channel (that is, the shared GHZ states between the parties are maximally entangled and free of noise). Since the communication parties are spatially separated, and one cannot distinguish the noise introduced by the eavesdropper and the noise induced during the preparation and distribution phases, after generating and distributing such states, the parties may share an ensemble of noisy GHZ states. In order to share a perfect quantum information channel, they first purify noisy GHZ states and

then test the security of the quantum channel. Suppose that the three communication parties share an ensemble of N' identical mixed multipartite states, they can obtain perfect GHZ states by using an efficient multipartite entanglement distillation protocol—the multi-party hashing method [43] and its improvement [44]. After that, the parties verify if they share perfect maximally entangled GHZ states. They can utilize a similar method as in [32] to do the tests. In fact, as long as the states taken as the quantum information channel are the eigenvectors of $\sigma_x \otimes \sigma_x \otimes \sigma_x$, $\sigma_z \otimes \sigma_z \otimes I$ and $\sigma_z \otimes I \otimes \sigma_z$, then the quantum channel is perfect [44].

The procedure for obtaining perfect GHZ states by using an efficient multipartite entanglement distillation protocol—multi-party hashing method [43] and its improvement [44]—is as follows. Suppose three parties Alice, Bob and Charlie share an ensemble of N' identical mixed tripartite states ρ and they would like to distill out perfect GHZ states $|P^+\rangle$. The GHZ state $|P^+\rangle$ is the +1 eigenstate of the following set of commuting observables:

$$S_0 = \sigma_x \otimes \sigma_x \otimes \sigma_x, \qquad S_1 = \sigma_z \otimes \sigma_z \otimes I, \qquad S_2 = \sigma_z \otimes I \otimes \sigma_z. \tag{9}$$

Denote GHZ states in equation (2) by

$$\left|\mathrm{GHZ}_{p,i_1,i_2}\right\rangle_{\mathrm{ABC}} = \tfrac{1}{\sqrt{2}}(|0\rangle|i_1\rangle|i_2\rangle + (-1)^p|1\rangle|\overline{i_1}\rangle|\overline{i_2}\rangle), \tag{10}$$

where p and the i are zero or one and a bar over a bit value indicates its logical negation. Here, the three labels (p, i_1, i_2) correspond to the eigenvalues of the three stabilizer generators S_0, S_1, S_2 by correspondence relations:

$$\text{eigenvalue } 1 \longrightarrow \text{label } 0,$$
$$\text{eigenvalue } -1 \longrightarrow \text{label } 1.$$

According to [45, 46], Alice, Bob and Charlie can depolarize three-party density matrix ρ by the following steps. The three perform the operator $\sigma_x \otimes \sigma_x \otimes \sigma_x$ with a probability $1/2$, and then apply $\sigma_z \otimes \sigma_z \otimes I$ with a probability $1/2$. Finally, they also apply $\sigma_z \otimes I \otimes \sigma_z$ with a probability $1/2$. The overall operation corresponds to

$$\begin{aligned}\rho \longrightarrow \rho_{\mathrm{ABC}} = \tfrac{1}{8}(&\rho + (\sigma_x \otimes \sigma_x \otimes \sigma_x)\rho(\sigma_x \otimes \sigma_x \otimes \sigma_x) + (\sigma_z \otimes \sigma_z \otimes I)\rho(\sigma_z \otimes \sigma_z \otimes I)\\ &+ (\sigma_y \otimes \sigma_y \otimes \sigma_x)\rho(\sigma_y \otimes \sigma_y \otimes \sigma_x) + (\sigma_z \otimes I \otimes \sigma_z)\rho(\sigma_z \otimes I \otimes \sigma_z)\\ &+ (\sigma_y \otimes \sigma_x \otimes \sigma_y)\rho(\sigma_y \otimes \sigma_x \otimes \sigma_y) + (I \otimes \sigma_z \otimes \sigma_z)\rho(I \otimes \sigma_z \otimes \sigma_z)\\ &+ (\sigma_x \otimes \sigma_y \otimes \sigma_y)\rho(\sigma_x \otimes \sigma_y \otimes \sigma_y)).\end{aligned} \tag{11}$$

The overall operation makes ρ diagonal in the basis (10) by the following form:

$$\rho_{\mathrm{ABC}} = \begin{pmatrix} p_{000} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & p_{100} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & p_{011} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & p_{111} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & p_{010} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & p_{110} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & p_{001} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_{101} \end{pmatrix}, \tag{12}$$

without changing the diagonal coefficients. Thus, three parties Alice, Bob and Charlie share a large ensemble of a density matrix, ρ_{ABC}, that is GHZ diagonal. They can estimate its matrix elements reliably by using local operations and classical communications (LOCCs) only. Measuring along X, Y, Z basis and comparing the results of their local measurements, they can estimate the diagonal matrix elements in (12) by applying classical random sampling theory. (This is due to the commuting observable argument in [47].) By definition, any GHZ-basis

vector in equation (10) is a simultaneous eigenvector of the seven non-trivial stabilizer group elements $\sigma_x \otimes \sigma_x \otimes \sigma_x$, $\sigma_z \otimes \sigma_z \otimes I$, $\sigma_z \otimes I \otimes \sigma_z$, $-\sigma_y \otimes \sigma_y \otimes \sigma_x$, $I \otimes \sigma_z \otimes \sigma_z$, $-\sigma_y \otimes \sigma_x \otimes \sigma_y$ and $-\sigma_x \otimes \sigma_y \otimes \sigma_y$. If the error rates for all seven of the non-trivial group elements are denoted by $s_1, \ldots, s_7$, then

$$\begin{aligned}
p_{000} &= 1 - \tfrac{1}{4}(s_1 + s_2 + s_3 + s_4 + s_5 + s_6 + s_7),\\
p_{100} &= \tfrac{1}{4}(s_1 - s_2 - s_3 + s_4 - s_5 + s_6 + s_7),\\
p_{011} &= \tfrac{1}{4}(-s_1 + s_2 + s_3 + s_4 - s_5 + s_6 - s_7),\\
p_{111} &= \tfrac{1}{4}(s_1 + s_2 + s_3 - s_4 - s_5 - s_6 + s_7),\\
p_{010} &= \tfrac{1}{4}(-s_1 + s_2 - s_3 + s_4 + s_5 - s_6 + s_7),\\
p_{110} &= \tfrac{1}{4}(s_1 + s_2 - s_3 - s_4 + s_5 + s_6 - s_7),\\
p_{001} &= \tfrac{1}{4}(-s_1 - s_2 + s_3 - s_4 + s_5 + s_6 + s_7),\\
p_{101} &= \tfrac{1}{4}(s_1 - s_2 + s_3 + s_4 + s_5 - s_6 - s_7).
\end{aligned} \tag{13}$$

Since $s_1, \ldots, s_7$ can be determined by local operations and classical communications (LOCCs) by Alice, Bob and Charlie, the above equations relate the diagonal matrix element of the density matrix, ρ_{ABC}, to experimental observables.

Maneva and Smolin [43] constructed an efficient multipartite entanglement distillation protocol—multi-party hashing method—and showed that its yield (per input mixed state)

$$D_h = 1 - \max_{j>0}[\{H(b_j)\}] - H(b_0). \tag{14}$$

Here b_0 is formed by concatenating the unknown phase bits of all ρ_{ABC} while b_j are formed by concatenating the j th amplitude bits, and

$$\begin{aligned}
H(b_0) &= -\sum_{b_0=0,1}\left(\sum_{b_1,b_2=0,1} p_{b_0b_1b_2}\right)\log_2\left(\sum_{b_1,b_2=0,1} p_{b_0b_1b_2}\right),\\
H(b_1) &= -\sum_{b_1=0,1}\left(\sum_{b_0,b_2=0,1} p_{b_0b_1b_2}\right)\log_2\left(\sum_{b_0,b_2=0,1} p_{b_0b_1b_2}\right),\\
H(b_2) &= -\sum_{b_2=0,1}\left(\sum_{b_0,b_1=0,1} p_{b_0b_1b_2}\right)\log_2\left(\sum_{b_0,b_1=0,1} p_{b_0b_1b_2}\right).
\end{aligned} \tag{15}$$

Therefore, if $D_h > 0$, using Maneva and Smolin's multi-party hashing method, Alice, Bob and Charlie can distill out $N'D_h$ perfect (generalized) GHZ states $|P^+\rangle$. Chen and Lo [44] presented an improved hashing protocol and proved that its yield can be increased to

$$D'_h = 1 - \max\{H(b_1), H(b_2|b_1)\} - H(b_0) + I(b_0; b_1, b_2). \tag{16}$$

With the improved random hashing method of Chen and Lo, Alice, Bob and Charlie can distill out $N'D'_h$ perfect (generalized) GHZ states $|P^+\rangle$ if $D'_h > 0$.

The only place eavesdropping can affect the system is the distribution phase of the GHZ states between the communicating parties. If the eavesdropper couples her ancilla states during preparation or distribution of the GHZ state, the communicating parties can find her out by the method of [32], and remove the entanglement between the eavesdropper's particles and the GHZ tripartite by the multi-party hashing method [43]. That is, by testing the security of the quantum channel, the eavesdropper can be detected, and as long as $D_h > 0$ ($D'_h > 0$), the three communication parties can get perfect GHZ states. However, by testing the security of the quantum channel, if $D_h = 0$ ($D'_h = 0$), Alice, Bob and Charlie discard the quantum

channel and construct it again. In one word, in any case, as long as an eavesdropper exists, we can find her and ensure the safety of the quantum channel. Once the security of the quantum channel is assured, which means that Alice, Bob and Charlie share pure GHZ triplets (perfect quantum channel), no information is leaked to Eve. Hence our proposed protocol is secure, even if the shared quantum channels are public.

4. Summary

We present a new deterministic secure method for direct communication by GHZ states and swapping quantum entanglement, where the three spatially separated parties faithfully transmit secret messages and detect eavesdroppers by the correlations of entanglement swapping results. In our scheme the secret messages can be encoded directly and are faithfully transmitted from two senders Alice and Bob to a remote receiver Charlie at the same time via initially shared GHZ states without revealing any information to a potential eavesdropper. The distributed entangled particles shared by Alice, Bob and Charlie function as a quantum information channel for faithful transmission. Using $2N$ GHZ states, Alice can send $2N$ bit secret messages to Charlie; meanwhile, Bob can also transmit N bits of information to Charlie. Since there is no transmission of the qubit carrying the secret message between Alice and Bob, and Charlie in the public channel, it is completely secure for direct secret communication if a perfect quantum channel is used. That is, simultaneous many mutual QSDC schemes of the central party and the other two parties can be realized.

Acknowledgments

This work was supported by Hebei Natural Science Foundation under grant nos A2004000141 and A2005000140, and Natural Science Foundation of Hebei Normal University of China.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India)* (New York: IEEE) pp 175–9
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557
[4] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[5] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[6] Goldenberg L and Vaidman L 1995 *Phys. Rev. Lett.* **75** 1239
[7] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev.* A **51** 1863
[8] Koashi M and Imoto N 1997 *Phys. Rev. Lett.* **79** 2383
[9] Bennett C H, Brassard G, Briedbart S and Wiesner S 1984 *IBM Tech. Discl. Bull.* **26** 4363
[10] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018
[11] Hwang W Y, Koh I G and Han Y D 1998 *Phys. Lett.* A **244** 489
[12] Cabello A 2000 *Phys. Rev. Lett.* **85** 5635
[13] Cabello A 2000 *Phys. Rev.* A **61** 052312
[14] Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302
[15] Xue P, Li C F and Guo G C 2002 *Phys. Rev.* A **65** 022317
[16] Phoenix S J D, Barnett S M, Townsend P D and Blow K J 1995 *J. Mod. Opt.* **42** 1155
[17] Lo H-K, Chan H F and Ardehali M 2000 *Preprint* quant-ph/0011056
[18] Song D 2004 *Phys. Rev.* A **69** 034301
[19] Wang X B 2004 *Phys. Rev. Lett.* **92** 077902
[20] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829
[21] Buttler W T, Torgerson J R and Lamoreaux S K 2002 *Phys. Lett.* A **299** 38
[22] Inoue K, Waks E and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902

[23] Shimizu K and Imoto N 1999 *Phys. Rev.* A **60** 157
[24] Shimizu K and Imoto N 2000 *Phys. Rev.* A **62** 054303
[25] Beige A *et al* 2002 *Acta Phys. Pol.* A **101** 357
[26] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[27] Wójcik A 2003 *Phys. Rev. Lett.* **90** 157901
[28] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317
[29] Yan F L and Zhang X Q 2004 *Eur. Phys. J.* B **41** 75
[30] Bennett C H *et al* 1993 *Phys. Rev. Lett.* **70** 1895
[31] Karlsson A and Bourennane M 1998 *Phys. Rev.* A **58** 4394
[32] Gao T 2004 *Z. Naturforsch.* **59a** 597
[33] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 893
[34] Zukowski M, Zeilinger A, Horne M A and Ekert A K 1993 *Phys. Rev. Lett.* **71** 4287
[35] Gao T, Yan F L and Wang Z X 2004 *Nuovo Cimento* B **119** 313
[36] Maurer U M and Wolf S 1997 *Lecture Notes Comput. Sci.* **1294** 307
[37] Bennett C H, Brassard G, Crepeau C and Maurer U M 1995 *IEEE Trans. Inf. Theory* **41** 1915
[38] Hamming R W 1950 *Bell Syst. Tech. J.* **29** 147
[39] Brassard G and Salvail L 1994 *Lecture Notes in Comput. Sci.* **765** 410
[40] Buttler W T, Lamoreaux S K, Torgerson J R, Nickel G H, Donahue C H and Peterson C G 2003 *Phys. Rev.* A **67** 052303
[41] Pearson D 2004 *7th Int. Conf. on Quantum Communication, Measurement and Computing (Glasgow, UK) AIP Conf. Proc.* **734** pp 299–302
[42] Van Assche G, Cardinal J and Cerf N J 2004 *IEEE Trans. Inf. Theory* **50** 394
[43] Maneva E N and Smolin J A 2002 *AMS Contemporary Mathematics Series, Quantum Computation and Quantum Information Science* vol 305 ed S J Lomonaco and H E Brandt (Providence, RI: American Mathematical Society) p 203
[44] Chen K and Lo H-K 2004 *Preprint* quant-ph/0404133
[45] Dür W, Cirac J I and Tarrach R 1999 *Phys. Rev. Lett.* **83** 3562
[46] Dür W and Cirac J I 2000 *Phys. Rev.* A **61** 042314
[47] Lo H-K and Chau H F 1999 *Science* **283** 2050