Genuine Quantum Secure Communication

You-Bang Zhan

School of Physics and Electronic Electrical Engineering,
Huaiyin Normal University, Huaian 223300, P. R. China

E-mail address: ybzhan@hytc.edu.cn

Abstract

A novel protocol of quantum cryptography, called genuine quantum secure communication (GQSC), is proposed by using a new method for local quantum measurement discrimination (LQMD). After secure quantum channel being established, the transmission of secret messages in the GQSC protocol does not require classical channel. Compared with the previous protocols of quantum secure direct communication, the advantage of the present protocol is not only more security, but also higher covert.

Keywords Quantum secure direct communication, Local quantum measurement discrimination, Superluminal Communication

PACS numbers 03.67.Dd, 03.67.Hk, 03.65.Ud

1. Inteoduction

Quantum cryptography [1] is commonly considered as one the most striking progress of quantum information theory, which enables two legitimate partners communicate in privacy, and use quantum mechanics to guarantee the security of communication. An important application of quantum cryptography is quantum key distribution (QKD) [2]. In a QKD scheme, two communicators firstly establish a shared secret key through the transmission of quantum signals and use this key to encrypt (decrypt) the secret messages. The non-cloning theorem [3] ensures the unconditional security of QKD as an eavesdropper Eve cannot eavesdrop the communication without leaving a trace in the results. Since Bennett and Brassard presented the standard BB84 QKD protocol [2] in 1984, a variety of QKD protocols have been proposed, such as Einstein-Podolsky-Rosen (EPR) protocol [4], two-state protocol [5], and six-state protocol [6], etc.

In recent years, a new concept in quantum cryptography, quantum secure direct communication (QSDC) has been proposed [7-9]. Different from QKD [2] whose object is to generate a private key between two remote partied, QSDC can transmit the secret messages directly without creating a key to encrypt them beforehand, so it is more demanding on security. Since then, the QSDC has attracted a great deal of attention (*e.g*. Refs. [10-19]). However, in the existing QSDC protocols the classical channel is indispensable, because to complete the transmission of secret massages the sender must transmit her measurement results to the receiver over a classical communication channel.

In the past few decades, one of the central problems of quantum information theory is quantum state discrimination [20]. It is well-known that two pure states cannot be perfectly discriminated unless

they are orthogonal. An object closely related to quantum state discrimination is the discrimination of quantum operation, including unitary operations, quantum channels, and quantum measurements, etc. Several researchers [21-24] have reported that the local quantum operation can be distinguished with certainty despite their uncertain nature. For two separated parties, however, in the existing researches, it has been pointed [22-25] that, since the operations employed by the other distant party, the no-signaling constraint holds that entanglement cannot be used for nonlocal discrimination of quantum operations without help of classical information. In recent work [29], we have shown that local quantum measurement discrimination (LQMD) can be completed via selective projective measurements and numerous seven-qubit GHZ states without help of classical communication. In the present paper, we proposed a novel protocol of quantum cryptography, called genuine quantum secure communication (GQSC), which enables the sender to transmit secret massages without classical channel. In this GQSC protocol, the receiver can extract the secret messages of the sender by using the LQMD without help of classical communication.

2. Local Quantum Measurement Discrimination with Eight-Qubit GHZ States

To ensure the result of measurements in the LQMD more reliable, here an eight-qubit GHZ state is employed. Now let us consider two observers, Alice and Bob, who share an eight-qubit GHZ state

$$\left|G\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00000000\right\rangle + \left|11111111\right\rangle\right)_{A_1A_2A_3A_4A_5A_6A_7B} \quad , \tag{1}$$

where qubits A_1, A_2, …, A_7 belong to Alice and B to Bob, respectively. Assume that Alice and Bob agreed in advance that Alice should measure her qubits before an appointed time. Now, let Alice employ two different kinds of measurement on the state $\left|G\right\rangle$. In the first kind of measurement, Alice performs in turn common projective measurements (CPMs) on the qubits A_1, A_2, …,and A_7 under the basis $\left\{\left|+\right\rangle,\left|-\right\rangle\right\}$, where $\left|+\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right)$, $\left|-\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle - \left|1\right\rangle\right)$. It is easy found that, after Alice's measurements, 64 possible final collapsed states of the qubit B will always be $\frac{1}{8\sqrt{2}}\left|+\right\rangle_B$ or $\frac{1}{8\sqrt{2}}\left|-\right\rangle_B$. Now let us turn to the second kind of measurement. To complete the LQMD, Alice will employ a novel kind of projective measurements, which we refer to as selective projective measurements (SPMs), with a series of single-qubit correlative measuring basis, on her qubits. Firstly, Alice measures the qubit A_1 in the state $\left|G\right\rangle$ under the basis $\left\{\left|\nu\right\rangle,\left|\nu^{\perp}\right\rangle\right\}$, where $\left|\nu\right\rangle = x\left|0\right\rangle + y\left|1\right\rangle$, $\left|\nu^{\perp}\right\rangle = y\left|0\right\rangle - x\left|1\right\rangle$, x and y are real, $x^2 + y^2 = 1$, and let $x = \sqrt{6}/3$, $y = \sqrt{3}/3$. Assume that Bob knows the coefficients x and y . If the result of Alice's measurement is $\left|\nu\right\rangle_{A_1}$, the qubits A_2, A_3, …, A_7 and B will be collapsed into the state

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}\left(x|0000000\rangle + y|1111111\rangle\right)_{A_2A_3A_4A_5A_6A_7B}, \quad (2)$$

she can measure the qubits A_2, A_3, …, A_7 under the basis $\{|+\rangle, |-\rangle\}$, successively. After that, the qubit B will be in the state $\frac{1}{8}|\mu^+\rangle_B$ or $\frac{1}{8}|\mu^-\rangle_B$, here $|\mu^+\rangle = \frac{1}{\sqrt{2}}\left(x|0\rangle + y|1\rangle\right)$ and $|\mu^-\rangle = \frac{1}{\sqrt{2}}\left(x|0\rangle - y|1\rangle\right)$. If Alice's measurement outcome is $|\nu^\perp\rangle_{A_1}$, the state of the qubits A_2, A_3, …, A_6 and B will be

$$|\phi_1'\rangle = \frac{1}{\sqrt{2}}\left(y|0000000\rangle - x|1111111\rangle\right)_{A_2A_3A_4A_5A_6A_7B}. \quad (3)$$

Then Alice measures the qubit A_2 under the basis $\{|\lambda_1\rangle, |\lambda_1^\perp\rangle\}$, which is given by

$$|\lambda_1\rangle = \frac{1}{F_2}\left(\frac{x}{y}|0\rangle + \frac{y}{x}|1\rangle\right),$$

$$|\lambda_1^\perp\rangle = \frac{1}{F_2}\left(\frac{y}{x}|0\rangle - \frac{x}{y}|1\rangle\right), \quad (4)$$

where $F_2 = \left[\left(x/y\right)^2 + \left(y/x\right)^2\right]^{1/2}$. Corresponding to Alice's measurement outcome $|\lambda_1\rangle_{A_2}$ or $|\lambda_1^\perp\rangle_{A_2}$, the qubits A_3, … , A_7 and B will be collapsed into the state $|\phi_2\rangle$ or $|\phi_2'\rangle$ with probability 1/2 each, which are given by

$$|\phi_2\rangle = \frac{1}{\sqrt{2}F_2}\left(x|000000\rangle - y|111111\rangle\right)_{A_3A_4A_5A_6A_7B},$$

$$|\phi_2'\rangle = \frac{1}{\sqrt{2}F_2}\left(\frac{y^2}{x}|000000\rangle + \frac{x^2}{y}|111111\rangle\right)_{A_3A_4A_5A_6A_7B}. \quad (5)$$

As mentioned above, one can easily see that the goal of our SPMs is as much as possible to make the qubit B collapsed into the state $\frac{1}{R}|\mu^+\rangle$ or $\frac{1}{R}|\mu^-\rangle$ after all, where R is a constant or a coefficient related to x and y. To present the SPMs more clearly, by described above, we can generalize the general approach of the SPMs as follows:

If the qubits A_{n+1}, A_{n+2}, …, A_m and B are collapsed into the state

$$\left|\phi_n'\right\rangle=\frac{1}{\sqrt{2}T_n}\left(\frac{y^{p_n}}{x^{p_n-1}}\left|00\cdots00\right\rangle+\frac{x^{p_n}}{y^{p_n-1}}\left|11\cdots11\right\rangle\right)_{A_{n+1}A_{n+2}\cdots A_mB}, \quad (6)$$

where $n=1,2,\cdots,m$, $T_n=F_1F_2\cdots F_n$, $p_n=2^{n-1}$, $F_n=\left[\left(x/y\right)^{p_n}+\left(y/x\right)^{p_n}\right]^{\frac{1}{2}}$, and let $F_1=1$, Alice should employ a new single-qubit projective measurement on the qubit A_{n+1} under the basis $\left\{\left|\lambda_n\right\rangle,\left|\lambda_n^{\perp}\right\rangle\right\}$, which is given by

$$\left|\lambda_n\right\rangle=\frac{1}{F_{n+1}}\left[\left(\frac{x}{y}\right)^{p_n}\left|0\right\rangle+\left(\frac{y}{x}\right)^{p_n}\left|1\right\rangle\right],$$

$$\left|\lambda_n^{\perp}\right\rangle=\frac{1}{F_{n+1}}\left[\left(\frac{y}{x}\right)^{p_n}\left|0\right\rangle-\left(\frac{x}{y}\right)^{p_n}\left|1\right\rangle\right]. \quad (7)$$

If the result of Alice's measurement is $\left|\lambda_n\right\rangle$, the qubits A_{n+2}, A_{n+3},…, A_m and B will be collapsed into the state $\left|\phi_{n+1}\right\rangle$, which is given by

$$\left|\phi_{n+1}\right\rangle=\frac{1}{\sqrt{2}T_{n+1}}\left(x\left|00\cdots00\right\rangle+y\left|11\cdots11\right\rangle\right)_{A_{n+2}A_{n+3}\cdots A_mB}, \quad (8)$$

she can measure the qubits A_{n+2}, A_{n+3}, …, A_m under the basis $\left\{\left|+\right\rangle,\left|-\right\rangle\right\}$ successively, the qubit B will be collapsed into the state $\frac{1}{2^dT_{n+1}}\left|\mu^+\right\rangle$ or $\frac{1}{2^dT_{n+1}}\left|\mu^-\right\rangle$, here $d=\left(m-n-1\right)/2$.

If the outcome of Alice's measurement is $\left|\lambda_n^{\perp}\right\rangle$, the qubits A_{n+2}, A_{n+3}, …, A_m and B will be collapsed into the state $\left|\phi_{n+1}'\right\rangle$, which is given by

$$\left|\phi_{n+1}'\right\rangle=\frac{1}{\sqrt{2}T_{n+1}}\left(\frac{y^{p_{n+1}}}{x^{p_{n+1}-1}}\left|00\cdots00\right\rangle-\frac{x^{p_{n+1}}}{y^{p_{n+1}-1}}\left|11\cdots11\right\rangle\right)_{A_{n+2}A_{n+3}\cdots A_mB}, \quad (9)$$

she should repeat above similar approach, until the result of measurement $\left|\lambda_{m-1}\right\rangle_{A_m}$ or $\left|\lambda_{m-1}^{\perp}\right\rangle_{A_m}$ in the basis $\left\{\left|\lambda_{m-1}\right\rangle,\left|\lambda_{m-1}^{\perp}\right\rangle\right\}$ has been obtained, and the qubit B has been collapsed into the state $\frac{1}{T_m}\left|\mu^+\right\rangle_B$ or $\frac{1}{\sqrt{2}T_m}\left(\frac{y^{p_m}}{x^{p_m-1}}\left|0\right\rangle-\frac{x^{p_m}}{y^{p_m-1}}\left|1\right\rangle\right)_B$ after all.

By above general approach, after Alice's measurements, 128 possible final collapsed states of the qubit B can be obtained. The relation of the results of Alice's measurement and the possible final

collapsed states of the qubit B can be expressed as follows:

$$
\begin{aligned}
|\nu\rangle_{A_1} &\rightarrow |\psi_1^{\pm}\rangle = \frac{1}{8}|\mu^{\pm}\rangle_B && (64\ terms)\\
|\lambda_1\rangle_{A_2} &\rightarrow |\psi_2^{\pm}\rangle = \frac{1}{4\sqrt{2}T_2}|\mu^{\pm}\rangle_B && (32\ terms)\\
|\lambda_2\rangle_{A_3} &\rightarrow |\psi_3^{\pm}\rangle = \frac{1}{4T_3}|\mu^{\pm}\rangle_B && (16\ terms)\\
|\lambda_3\rangle_{A_4} &\rightarrow |\psi_4^{\pm}\rangle = \frac{1}{2\sqrt{2}T_4}|\mu^{\pm}\rangle_B && (8\ terms)\\
|\lambda_4\rangle_{A_5} &\rightarrow |\psi_5^{\pm}\rangle = \frac{1}{2T_5}|\mu^{\pm}\rangle_B && (4\ terms)\\
|\lambda_5\rangle_{A_6} &\rightarrow |\psi_6^{\pm}\rangle = \frac{1}{\sqrt{2}T_6}|\mu^{\pm}\rangle_B && (2\ terms)\\
|\lambda_6\rangle_{A_7} &\rightarrow \begin{cases} |\psi_7^{+}\rangle = \frac{1}{T_7}|\mu^{-}\rangle_B & (1\ term)\\ |\psi_7^{-}\rangle = \frac{1}{\sqrt{2}T_7}\left(\frac{y^{64}}{x^{63}}|0\rangle - \frac{x^{64}}{y^{63}}|1\rangle\right)_B & (1\ term)\end{cases}
\end{aligned}
\tag{10}
$$

Thus much Alice's selective measurements have been completed. From Eq. (10), it is easy noted that, after Alice performing the SPMs on her all qubits, the states $\frac{1}{g_n T_n}|\mu^{\pm}\rangle$ ($g_n = 2^{(7-n)/2}, n = 1,2,\cdots,7$) in all 128 collapsed states of the qubit B accounted for 127, and the state $|\psi_7^{-}\rangle_B$ for 1. On the other hand, by simple claculation, one can find that, after Alice's measurememts the probability of the qubit B being in the state $\frac{1}{g_n T_n}|\mu^{\pm}\rangle$ ($g_n = 2^{(7-n)/2}, n = 1,2,\cdots,7$) is 0.75, and in the state $|\psi_7^{-}\rangle_B$ is 0.25. It must be pointed out that it is just these measured results of the SPM that led to the realization of the LQMD.

Clearly, after Alice performing the CPMs or SPMs on her qubits respectively, the final collapsed states of the qubit B are obvious different. If Alice employs the CPMs on her qubits, after Alice's measurement, 128 possible final collapsed states of the qubit B will always be $\frac{1}{8\sqrt{2}}|+\rangle_B$ or $\frac{1}{8\sqrt{2}}|-\rangle_B$. If Alice performs the SPMs on her qubits, after Alice's measurement, 128 possible final

collapsed states of the qubit B can be given by Eq. (10). It must be emphasized that, whether Alice's measurements are the CPMs or SPMs, since Alice and Bob agreed in advance that Alice should measure her qubits before an appointed time, one can know that the qubit B must be collapsed into the state corresponded to one of Alice's 128 results of measurement after Alice's measurements.

Now let us turn to depict the LQMD. Suppose that two spacelike separated observers, Alice and Bob, share 30 eight-qubit GHZ states, which are given by

$$\left|G^{(k)}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00000000\right\rangle + \left|11111111\right\rangle\right)_{A_1^{(k)}A_2^{(k)}A_3^{(k)}A_4^{(k)}A_5^{(k)}A_6^{(k)}A_7^{(k)}B^{(k)}}, \tag{11}$$

where $k = 1, 2, \cdots, 30$, and the qubits $A_1^{(k)}$, $A_2^{(k)}$, …, $A_7^{(k)}$ belong to Alice and $B^{(k)}$ to Bob, respectively. Different from previous quantum operation discrimination schemes, we assume that there is no classical channel between Alice and Bob. In this case, before the agreed time t, Alice randomly performs two different kinds of measurements, CPMs or SPMs, on her qubits in the state $\left|G^{(k)}\right\rangle$ ($k = 1, 2, \cdots, 30$) respectively. If Alice employs the CPMs on her qubits, after Alice's measurements, all qubits $B^{(k)}$ will be in the states $\frac{1}{8\sqrt{2}}\left|+\right\rangle_{B^{(k)}}$ or $\frac{1}{8\sqrt{2}}\left|-\right\rangle_{B^{(k)}}$. At the appointed time t, Bob measures his qubits $B^{(k)}$ all in the basis $\left\{\left|0\right\rangle, \left|1\right\rangle\right\}$. After Bob's measurements, by statistics theory, the probability of all qubits $B^{(k)}$ in the state $\left|0\right\rangle$ or $\left|1\right\rangle$ will be in the ratio of one to one. If Alice's measurements are the SPMs, by described above, after Alice's selective measurements, the probability of all qubits $B^{(k)}$ in the states $\frac{1}{g_n T_n}\left|\mu^+\right\rangle$ or $\frac{1}{g_n T_n}\left|\mu^-\right\rangle$ ($g_n = 2^{(7-n)/2}, n = 1, 2, \cdots, 7$) is $\left(0.75\right)^{30} \approx 0.00018$, *i.e.*, the probability of at least one qubit $B^{(k')}$ in the state $\left|\psi_7^-\right\rangle$ is $1-\left(0.75\right)^{30} \approx 0.99982$. This means that, after Alice's SPMs, at least one qubit $B^{(k')}$ will be collapsed into the state $\left|\psi_7^-\right\rangle$. Then, at the appointed time t, Bob measures the qubits $B^{(k)}$ all in the basis $\left\{\left|0\right\rangle, \left|1\right\rangle\right\}$. One can see that, after measurements of Bob, the probability of the qubits $B^{(k)}$ in the state $\left|0\right\rangle$ or $\left|1\right\rangle$ will be different from the case Alice employed the CPMs. To illustrate this clearly, without loss of generality, we first discuss the case in which only one qubit $B^{(k')}$ in the state $\left|\psi_7^-\right\rangle$ after Alice's measurements. From the state $\left|\psi_7^-\right\rangle$ in Eq. (10), it is easily found that, after Bob's measurements, the probability of the qubit $B^{(k')}$ in the state $\left|0\right\rangle$ or $\left|1\right\rangle$ will be in the ratio

of one to u ($u=\left(\frac{x^{64}}{y^{63}}\right)^2/\left(\frac{y^{64}}{x^{63}}\right)^2\approx 6.15\times 10^{18}$), that is, the qubit $B^{(k')}$ will be always collapsed into the state $|1\rangle$. As a special case, we also assume that all the other 29 qubits $B^{(k)}$ are in the states $|\psi_1^{\pm}\rangle$ after Alice's measurements and then all the 29 qubits are in the state $|0\rangle$ after Bob's measurements. In this situation, one can easily find that the probability of the 30 qubits $B^{(k)}$ in the state $|0\rangle$ or $|1\rangle$ will be in the ratio of 1 to 1.655 after Bob's measurements. For general cases in which only one qubit $B^{(k')}$ in the state $|\psi_7^-\rangle$ and other 29 qubits $B^{(k)}$ collapsed randomly into the states $\frac{1}{g_n T_n}|\mu^{\pm}\rangle$ ($g_n=2^{(7-n)/2}$, $n=1,2,\ldots,7$) after Alice's measurements, it is easily found that the probability of the 30 qubits $B^{(k)}$ in the state $|0\rangle$ or $|1\rangle$ will be in the ratio of one to $w_{(1)}$ ($w_{(1)} > 1.655$) after Bob's measurements. Now we consider the case in which there are two qubits $B^{(k')}$ and $B^{(k'')}$ in the state $|\psi_7^-\rangle$ after Alice's measurements. Similar to the above described, one can find that the probability of the 30 qubits $B^{(k)}$ in the state $|0\rangle$ or $|1\rangle$ will be in the ratio of one to $w_{(2)}$ ($w_{(2)} \geq 3.43$) after Bob's measurements. For the cases in which more qubits $B^{(1)}$, $B^{(2)}$, …, $B^{(l)}$ ($l=3,4,\cdots,30$) collapsed into the state $|\psi_7^-\rangle$ after Alice's measurements, the probability of the 30 qubits $B^{(k)}$ in the state $|0\rangle$ or $|1\rangle$ will be in the ratio of one to $w_{(l)}$ ($w_{(l)} > w_{(2)}$, $l=3,4,\cdots,30$) after Bob's measurements. As mentioned above, after Alice's measurements, the probability of the 30 qubits $B^{(k)}$ in the state $|0\rangle$ or $|1\rangle$ will be in the ratio of one to W ($W \geq 1.655$) after Bob's measurements.

To ensure the result of Bob's measurements more reliable, it can be further supposed that Alice and Bob share 20 entangled states groups (ESGs), each consisting of 30 eight-qubit GHZ states $|G^{(k)}\rangle$ (see Eq. (11)). If Alice's measurements are the CPMs, it is easy found that, after Alice's and Bob's measurements, the probability of all qubits $B^{(k)}$ of each ESG in the state $|0\rangle$ or $|1\rangle$ will be still in the ratio of one to one. If Alice's measurements are the SPMs, by statistics theory, after Alice's and Bob's measurements, in all ESGs the probability of the qubits $B^{(k)}$ of each ESG in the state $|0\rangle$

or $|1\rangle$ will be in the ratio of one to W ($W \geq 1.655$). In accordance with these outcomes, Bob can discriminate that the measurements employed by Alice are CPMs or SPMs. Thus, the LQMD is completed successfully.

3. Genuine quantum secure communication protocol

Now we describe the details of our GQSC protocol by using the LQMD. Suppose there are two remote legitimate communicators, Alice and Bob. The sender Alice wants to transmit N_0 single-bit secret classical massages (say, 1001$\cdots$) to receiver Bob. In order to encode the secret messages, Alice and Bob should agree that two different kinds of measurements, CPMs and SPMs, represent the secret messages 0 and 1 respectively. Then the protocol proceeds as follows:

(S1) Alice prepares a large enough number (M) of EPR pairs in

$$|\Phi_n\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)_{A_{1(p)}B_{(p)}} , \tag{12}$$

where $p = 1, 2, \cdots, M$, and takes one qubit from each EPR pair to form a qubit sequence $\left\{A_{1(1)}, A_{1(2)}, \cdots, A_{1(M)}\right\}$, call the A sequence. The remaining qubits compose B sequence $\left\{B_{(1)}, B_{(2)}, \cdots, B_{(M)}\right\}$. Then, Alice stores the A sequence and sends B sequence to Bob.

(S2) To check if there eavesdropping in the line, Alice chooses a sufficiently large subset of qubits randomly in the A sequence as a checking set, call the C_A set. The remaining qubits in A sequence are reformed N_0 ordered qubit sequences as encoding-decoding sets (EDSs) $\left\{A_{1(i,j)}^{(k)}, A_{1(i,j)}^{(k)}, \cdots, A_{1(i,j)}^{(k)}\right\}$, call the $E_A^{(i)}$ sets, where $i = 1, 2, \cdots, N_0$, $k = 1, 2, \cdots, 30$, $j = 1, 2, \cdots, 20$.

(S3) After verifying that Bob has received all qubits of B sequence, Alice chooses randomly one of the two sets measuring bases (MBs), Z -MB $\left\{|0\rangle, |1\rangle\right\}$ and X -MB $\left\{|+\rangle, |-\rangle\right\}$, to measure the qubits in the C_A set. Then Alice publicly announces the C_A set and $E_A^{(i)}$ sets in A sequence, MB she has chosen for each qubit in C_A set and the results of her measurement.

(S4) In accordance with Alice's information, Bob takes the corresponding qubits in B sequence to form checking set C_B and the EDSs $E_B^{(i)}$. The EPR pairs composed of qubits $A_{1(i,j)}^{(k)}$ and $B_{(i,j)}^{(k)}$ can be expressed as

$$\left|\Phi_{(i,j)}^{(k)}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right)_{A_{1(i,j)}^{(k)}B_{(i,j)}^{(k)}}\quad,\tag{13}$$

where $i=1,2,\cdots,N_0$, $k=1,2,\cdots,30$, and $j=1,2,\cdots,20$. Then Bob uses the same MB as Alice to measure the corresponding qubits in the C_B set and compares his measurement results with Alice's to check the existence of eavesdropper Eve. If no eavesdropping exists, their measurement results should be completely correlated in an ideal condition. In this case, they continue to communication. Otherwise, they have to discard their communication.

Due to the method establishing quantum channel in our protocol is very similar to the previous protocols (*e.g.* , Ref. [9,10]), the discussions on the security analysis in Ref. [9,10] are suitable for the present protocol, so we do not repeat those discussions here further. It should be pointed out that Alice and Bob require the help of classical communication in above establishing secure quantum channel.

After insuring the security of the quantum channel, Alice should introduce six qubits $A_{r(i,j)}^{(k)}$ $\left(r=2,3,\cdots,7\right)$ with the initial state $\left|0\right\rangle$ in each EPR pair $\left|\Phi_{(i,j)}^{(k)}\right\rangle$ (see Eq. (13)), and perform in turn C-NOT gates on the qubits $A_{1(i,j)}^{(k)}$ and $A_{r(i,j)}^{(k)}$ $\left(r=2,3,\cdots,7\right)$ with qubit $A_{1(i,j)}^{(k)}$ as controlled qubit and $A_{r(i,j)}^{(k)}$ $\left(r=2,3,\cdots,7\right)$ as target qubits. After that, the EPR pairs $\left|\Phi_{(i,j)}^{(k)}\right\rangle$ will be transformed into the eight-qubit GHZ states, which are given by

$$\left|E_{(i,j)}^{(k)}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|00000000\right\rangle+\left|11111111\right\rangle\right)_{A_{1(i,j)}^{(k)}A_{2(i,j)}^{(k)}A_{3(i,j)}^{(k)}A_{4(i,j)}^{(k)}A_{5(i,j)}^{(k)}A_{6(i,j)}^{(k)}A_{7(i,j)}^{(k)}B_{(i,j)}^{(k)}}\quad,\tag{14}$$

where $i=1,2,\cdots,N_0$, $k=1,2,\cdots,30$, and $j=1,2,\cdots,20$.

Different from previous QSDC protocols [7-19], we suppose that, after established secure quantum channel, there is no classical channel in the following implementing quantum communication procedure. Hence, Alice and Bob need to pre-agree that Bob should check Alice's secret messages at a certain time T or at a certain time interval. Next, let us describe our GQSC protocol in the two cases in detail.

(Case 1) Assume Alice and Bob pre-agree at a certain time T, Bob should check Alice's secret messages. Before the time T, according to her secret bit string (1001⋯), Alice first performs the SPMs on the EDS $A_{n(1,j)}^{(k)}$ ($n=1,2,\cdots,7$, $k=1,2,\cdots,30$, $j=1,2,\cdots,20$), then performs CPMs on the $A_{n(2,j)}^{(k)}$, ⋯, successively. At the time T, Bob should check the states of qubits $B_{(i,j)}^{(k)}$, that is, he measures in turn his qubits $B_{(i,j)}^{(k)}$ $\left(i=1,2,\cdots,N_0\right)$ all in the basis $\left\{\left|0\right\rangle,\left|1\right\rangle\right\}$. After that, Bob can extract that Alice had employed the SPMs on the EDS $A_{n(1,j)}^{(k)}$ and there extract the bit 1, similarly, he can extract other bits, then he can obtain Alice's secret messages (1001⋯). Thus, the QSC has been

completed.

(Case 2) Assume Alice and Bob pre-agree at a certain time interval to implement the QSC. In order to determine the time T for implementing quantum communication in the time interval (say, two weeks or one year), Alice and Bob should establish second secure quantum channel beforehand, called informing quantum channel (IQC), in which Alice can inform Bob if she had encoded her secret messages in the EDSs $E_A^{(i)}$. The IQC consists of a large enough number (m) of EDSs and each EDS is composed of 20 ED groups (EDGs), and each EDG consisting of 30 seven-qubit GHZ states, which are given by

$$\left|I_{(l,j)}^{(k)}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|00000000\right\rangle+\left|11111111\right\rangle\right)_{A_{1(l,j)}^{(k)}A_{2(l,j)}^{(k)}A_{3(l,j)}^{(k)}A_{4(l,j)}^{(k)}A_{5(l,j)}^{(k)}A_{6(l,j)}^{(k)}A_{7(l,j)}^{(k)}B_{(l,j)}^{(k)}}, \qquad (15)$$

where $l=1,2,\cdots,m$, $k=1,2,\cdots,30$, and $j=1,2,\cdots,20$. In the IQC, Alice possesses m ordered qubit sequences $\left\{A_{n(1,j)}^{(k)},A_{n(2,j)}^{(k)},\cdots,A_{n(l,j)}^{k},\cdots,A_{n(m,j)}^{(k)}\right\}$, where $n=1,2,\cdots,7$, $k=1,2,\cdots,30$, $j=1,2,\cdots,20$, as informing sets (call $I_A^{(l)}$ sets) and Bob possesses $I_B^{(l)}$ sets $\left\{B_{(1,j)}^{(k)},B_{(2,j)}^{(k)},\cdots,B_{(l,j)}^{(k)},\cdots,B_{(m,j)}^{(k)}\right\}$ respectively. In the certain time interval, if there is not need to transfer secret messages, Alice can, from time to time (*e.g.* ten minutes), perform CPMs on the qubits $A_{n(l,j)}^{(k)}$ in the $I_A^{(l)}$ set successively. When Alice wants to transmit her secret messages to Bob, she should first encode the secret messages by performed SPMs and CPMs on her qubits $A_{n(i,j)}^{(k)}$ in the $E_A^{(i)}$ sets, then she continues to perform SPMs on the qubits $A_{n(l,j)}^{(k)}$ in the $I_A^{(l)}$ set at twice (It is similar to the phone ringing in the classical communication). Meanwhile, Bob should check the partner qubits $B_{(l,j)}^{(k)}$ in the $I_B^{(l)}$ set via the LQMD every ten minutes. If the results of Bob's measurement show that Alice performs CPMs on her qubits $A_{n(l,j)}^{(k)}$ in the $I_A^{(l)}$ set, this indicates Alice did not transmit the secret messages. When Bob found that Alice performs twice SPMs on the qubits $A_{n(l,j)}^{(k)}$, he can check the qubits $B_{(i,j)}^{(k)}$ in the $E_B^{(i)}$ set by using the LQMD immediately. Similar to Case 1, Bob can extract Alice's secret messages. Thus our GQSC has been accomplished successfully.

Compared with previous QSDC protocols [7-19], there are several advantages in the present GQSC protocol. Firstly, as there is no classical communication in the present protocol, the speed of transmitting secret messages is no longer limited by the speed of light, but it depends on the speed of quantum state collapse (or speed of quantum information) [30]. In recent years, the results of some EPR experiments [30-33] set a lower bound on the speed of quantum information to 10^4 □ 10^7 times the speed of light. Obviously, if Alice and Bob are spaced far enough, the required time completed the

secret message transmission (including the time to complete measurement by the sender and the receiver) via the LQMD will be less than the required time by the classical communication. In other words, the present GQSC is a superluminal GQSC protocol. Secondly, transmission of secret messages in the present protocol is completed by the sender who measures her qubits of the EDSs in the quantum channel. As there is no transmission of qubits carrying the secret messages between the sender and the receiver, there is no chance for Eve to attack the secret messages in a perfect quantum channel is used. So our protocol is more secure. Finally, different from previous QSDC protocols, the transmission of secret messages in the present protocol does not require the help of classical channel. As there are no public information from classical communication as described in previous QSDC protocols [7-19], the outsider cannot know whether the quantum communication is in progress. Thus, the present protocol is more covert. As mentioned above, our GQSC is a genuine QSDC protocol.

4. Summary

In summary, a novel protocol of quantum cryptography, genuine quantum secure communication (GQSC), is presented. We have provided a detailed realization of the protocol by using a new method for local quantum measurement discrimination (LQMD). It is shown that, in this GQSC protocol, if both two observers (Alice and Bob) agreed in advance that one of them (*e.g*. Bob) should check Alice's secret messages at an appointed time (or at a certain time interval), the GQSC can been accomplished successfully without help of classical communication. This means that the present GQSC is a superluminal quantum secure communication protocol. Furthermore, our GQSC protocol has the advantage of not only more secure, but also higher covert. At present, there has been experiment implementing the eight-qubit GHZ state [34]. Thus, we believe that the present GQSC protocol is worth researching into both theoretically and experimentally.

References

[1] N. Gisis, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography. *Rev. Mod. Phys*. 2002, 74(1): 145

[2] C. H. Bebbett and G. Brassard, in: *Proccedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, IEEE Press, New York, 1984, PP. 175-179.

[3] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned. *Nature* (*London*), 1982, 299(5886): 802

[4] A. K. Ekert, Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett*. 1991, 67(6): 661

[5] C. H. Bennett, Quantum cryptography without Bell's theorem. *Phys. Rev. Lett*. 1992, 68(21): 3121

[6] D. Bruss, Optical eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett*. 1998**,** 81(14): 3018

[7] A. Beige, B. G. Englert, C. Kurtsiefer, and H. Weinfurter, Secure communication with a pablicly known key. *Acta Phys. Pol. A*, 2002, 101(3): 357

[8] K. Bostrom and T. Felbinger, Deterministic secure direct communication using entanglement. *Phys. Rev. Lett*. 2002, 89(18): 187902

[9] G. L. Long and X. S. Liu, Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A*, 2002, 65(3): 032302

[10] F. G. Deng, G. L. Long, and X. S. Liu, Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys. Rev. A*, 2003, 68(4): 042317

[11] A. Wojcik, Eavesdropping on the "Ping-Pong" quantum communication protocol. *Phys. Rev. Lett*. 2003, 90(15): 157901

[12] Q. Y. Cai, The "Ping-Pong" protocol can be attacked without eavesdropping. *Phys. Rev. Lett*. 2003, 91(10): 109801

[13] F. G. Deng and G. L. Long, Secure direct communication with a quantum one-time pad. *Phys. Rev. A*, 2004, 69(5): 052319

[14] Q. Y. Cai and B. W. Li, Improving the capacity of the Bostrom-Felbinger protocol. *Phys. Rev. A*, 2004, 69(5): 054301

[15] C. Wang, F. G. Deng, Y. S. Li, X. S. Liu, and G. L. Long, Quantum secure direct communication with high-dimension quantum superdence coding. *Phys. Rev. A*, 2005, 71(4): 044305

[16] H. Lee, J. Lim, and H. Yang, Quantum direct communication with authentication. *Phys. Rev. A*, 2006, 73(4): 042305

[17] A. D. Zhu, Y. Xia, Q. B. Fan, and S. Zhang, Secure direct communication based on secret transmitting order of particles. *Phys. Rev. A*, 2006, 73(2): 022338

[18] S. Lin, Q. Y. Wen, F. Gao, and F. C. Zhu, Quantum secure direct communication with chi-type entangled states. *Phys. Rev. A*, 2008, 78(6): 064304

[19] Y. B. Zhan, L. L. Zhang, and Q. Y. Zhang, Quantum secure direct communication by entangled qutrits and entanglement swapping. *Opt. Commun*. 2009, 282(23): 4633

[20] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge Univ. Press, Cambridge, 2000).

[21] A. Acin, Statistical distinguishability between unitary operations. *Phys. Rev. Lett*. 2001, 87(17): 177901

[22] Z. Ji, Y. Feng, R. Duan, and M. Ying, Identification and distance measures of measurement apparatus. *Phys. Rev. Lett.* 2006, 96(20): 200401

[23] D. Mundarain and M. Orszag, Local quantum measurement discrimination. *Phys. Rev. A*, 2007, 75(1): 012107

[24] J. Fiurasek and M. Micuda, Optimal two-copy discrimination of quantum measurements. *Phys. Rev. A*, 2009, 80(4): 042312

[25] P. Eberhard, Bell's Theorem and the different concept of locality. *Nuovo Cim. B*, 1978, 46(2): 392

[26] G. C. Ghirardi, A. Rimini, and T. Weber, A general argument against superluminal transmission through the quantum mechanical measurement process. *Lett. Nuovo Cim*. 1980, 27(10): 293

[27] P. J. Bussey, "Super-luminal communication" in Einstein-Podolsky-Rosen experiments. *Phys. Lett. A*, 1982, 90(1-2): 9

[28] G. C. Ghirardi and T. Weber, Quantum mechanics and faster-than-light communication: methodological considerations. *Nuovo Cim. B*, 1983, 78(1): 9

[29] Y. B. Zhan, Local discrimination of quantum measurement without assistance of classical information. *J. Quantum Inform. Science*, 2015, 5(2): 71

[30] H. Zbinden, J. Brendel, N. Gisin, and W. Tittel, Experimental test of nonlocal quantum correlation in relativistic configurations. *Phys. Rev. A*, 2001, 63(2): 022111

[31] A. Stefanov, H. Zbinden, N. Gisin, and A. Suarez, Quantum correlations with spacelike

separated beam splitters in motion: experimental test of multisimultaneity. *Phys. Rev. Lett.* 2002, 88(12): 120404

[32] D. Salart, *et al*., Testing the speed of 'spooky action at a distance'. *Nature*, 2008, 454(7206): 861

[33] J. D. Bancal, *et al*., Quantum non-locality based on finite-speed causal influences leads to superluminal signaling. *Nature Phys*. 2012, 8(12): 867

[34] Y. F. Huang, *et al*., Experimental gereration of an eight-photon Greenberger-Horne-Zeilinger state. *Nature Commun*. 2011, 2, 546