Multiparty Quantum Remote Secret Conference*

Xi-Han Li[1,2], Chun-Yan Li[1,2], Fu-Guo Deng[1,2,3†], Ping Zhou[1,2], Yu-Jie Liang[1,2] and Hong-Yu Zhou[1,2,3]
[1] *The Key Laboratory of Beam Technology and Material Modification of Ministry of Education, Beijing Normal University, Beijing 100875, People's Republic of China*
[2] *Institute of Low Energy Nuclear Physics, and Department of Material Science and Engineering, Beijing Normal University, Beijing 100875, People's Republic of China*
[3] *Beijing Radiation Center, Beijing 100875, People's Republic of China*
(Dated: February 1, 2008)

We present two schemes for multiparty quantum remote secret conference in which each legitimate conferee can read out securely the secret message announced by another one, but a vicious eavesdropper can get nothing about it. The first one is based on the same key shared efficiently and securely by all the parties with Greenberger-Horne-Zeilinger (GHZ) states, and each conferee sends his secret message to the others with one-time pad crypto-system. The other one is based on quantum encryption with a quantum key, a sequence of GHZ states shared among all the conferees and used repeatedly after confirming their security. Both these schemes are optimal as their intrinsic efficiency for qubits approaches the maximal value.

PACS numbers: 03.67.Hk, 03.65.Ud

Quantum communication supplies some novel ways for transmitting message securely. For example, quantum key distribution (QKD) [1, 2, 3, 4, 5, 6], the original application of quantum mechanics, can be used to create a private key between two authorized users, Alice and Bob. The noncloning theorem forbids a vicious eavesdropper, say Eve to copy an unknown quantum state without disturbing it. By analysing the error rate of samples chosen randomly, Alice and Bob can determine whether there is an eavesdropper in the quantum line [1]. With quantum secret sharing (QSS) [7, 8, 9, 10, 11, 12, 13], a boss can generate a private key with his agents, i.e., $K_A = K_B \oplus K_C \oplus K_D \oplus \cdots$. Here K_A is the key of the boss Alice, K_i $(i = B, C, D, \cdots)$ are the keys of Alice's agents. In this way, Alice can send her secret message to her agents who can read out it if and only if they cooperate, otherwise none can obtain a useful information about the message. Also, QSS provides a secure way for sharing an unknown state [14, 15, 16, 17].

Recently, a new branch of quantum communication, quantum secure direct communication (QSDC) was proposed and has been actively pursued [18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29]. QSDC makes a party communicate another one directly and securely, different from QKD. In detail, the sender sends his secret message directly to the receiver without creating a private key and then encrypting the message with it. As pointed out in Ref. [30], a secure quantum direct communication protocol requires the users to transmit the quantum states in a date block. Moreover, the two legitimate users can detect the eavesdropper before they encode the secret message on the quantum states, and can read out the message directly without exchanging an additional classical bit for each qubit except for those used for checking eavesdropping. In this way, the two-step QSDC protocol [18] and the quantum one-time pad QSDC protocol [19] proposed by Deng *et al.* satisfy all the requirements. So do the protocol with quantum superdense coding [20] and that with multi-particle Green-Horne-Zeilinger (GHZ) state [21].

Another class of quantum communication protocols used to transmit secret message is called deterministic secure quantum communication (DSQC) [31], such as the schemes [22, 23] with quantum teleportation and entanglement swapping, and those [25, 26] based on secret transmitting order of particles. Although the secret message can be read out only after the two authorized users exchange an additional classical bit for each qubit, none of the users needs to transmit the qubits that carry the secret message, which maybe make those protocols more secure than others in a noise channel and more convenient for quantum error correction [31]. In particular, we introduced a DSQC protocol with only single-photon measurements and a feasible quantum signal, nonmaximally entangled states [31].

More recently, two novel concepts for direct communication are proposed. One is quantum secret report in which many agents report directly their secret messages to a boss in one-way direction [32]. The other is quantum broadcast communication [33] with which one can broadcast his secret message to many legitimate receivers. In this Letter, we will present two schemes for multiparty quantum remote secret conference (MQRSC) in which any legitimate conferee can send securely his secret message to the other legitimate parties who participate in a remote secret conference, but a vicious eavesdropper can get nothing about the messages. The first one is based on the same classical key shared efficiently and privately by all the parties with Greenberger-Horne-Zeilinger (GHZ) states. The other one is based on quantum encryption

*Supported by the National Natural Science Foundation of China under Grant Nos. 10604008 and 10435020, and Beijing Education Committee under Grant No. XK100270454.
†To whom correspondence should be addressed. Email address: fgdeng@bnu.edu.cn

with a quantum key, a sequence of GHZ states shared among all the parties and used repeatedly after confirming their security.

Now, let us describe the principle of our MQRSC protocol based on the same private key shared by all the parties of the secret conference. Suppose there are three remote conferees, say Alice, Bob and Charlie. They first share the same key, say $K_A = K_B = K_C$ securely and then use them to encrypt their secret messages with classical one time-pad crypto-system. Here K_A, K_B and K_C are the classical keys obtained by Alice, Bob and Charlie, respectively. In detail, they can use some three-particle GHZ states to create their keys efficiently. The GHZ-state is

$$\begin{aligned}|\psi\rangle_{ABC} &= \frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{ABC}, \\ &= \frac{1}{\sqrt{2}}[(|+x\rangle_A|+x\rangle_B+|-x\rangle_A|-x\rangle_B)|+x\rangle_C \\ &\quad +(|+x\rangle_A|-x\rangle_B+|-x\rangle_A|+x\rangle_B)|-x\rangle_C. \end{aligned} \tag{1}$$

Here $|0\rangle = |+z\rangle$ and $|1\rangle = |-z\rangle$ are the eigenvectors of the measuring basis (MB) σ_z, and $|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ and $|-x\rangle = \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ are those of the MB σ_x. That is, a remote conferee, say Alice prepares a three-particle quantum system in the GHZ state $|\psi\rangle_{ABC}$, and then sends the particle B to Bob and the particle C to Charlie. All the three conferees choose the MBs σ_z and σ_x with the probabilities $1-p$ and p to measure their particles. After comparing in public their MBs, the three conferees keep their outcomes obtained when they all choose the MB σ_z or the MB σ_x. The probabilities that they obtain a correlated result with the MBs σ_z and σ_x are $(1-p)^3$ and p^3, respectively.

Alice, Bob and Charlie choose all the outcomes obtained with the MB σ_x and a subset of those with the MB σ_z as the samples to analyse the security of the transmission, similar to Bennett-Brassard-Mermin 1992 (BBM92) QKD protocol [3] and the modified Bennett-Brassard 1984 (BB84) QKD protocol [5]. If the transmission is secure, the three conferees can get the same private key by distilling the remaining outcomes obtained with the MB σ_z. Assume that the ratio of the number of sample particles to that of particles transmitted is r. As the symmetry, $p^3 = r/2$ (half of the samples are the outcomes obtained by the conferees with the MB σ_x). Then the probability that the three remote conferees obtain their raw key, p_{rk} without eavesdropping is

$$p_{rk} = (1-\sqrt[3]{\frac{r}{2}})^3 p_t p_d, \tag{2}$$

where p_t and p_d are the probabilities of the transmission and the detectors, respectively.

In essence, this MQRSC protocol is just a special QKD protocol. That is, all the conferees generate first the same private key with GHZ states efficiently and then use it to encrypt and decrypt their messages. Different from QSS [7, 8, 9, 10, 11, 12, 13], all the authorized conferees are honest. They can take the measurement with the MB σ_z on the GHZ states to obtain the same outcomes, and use all the outcomes obtained with the MB σ_x as the samples for eavesdropping check.

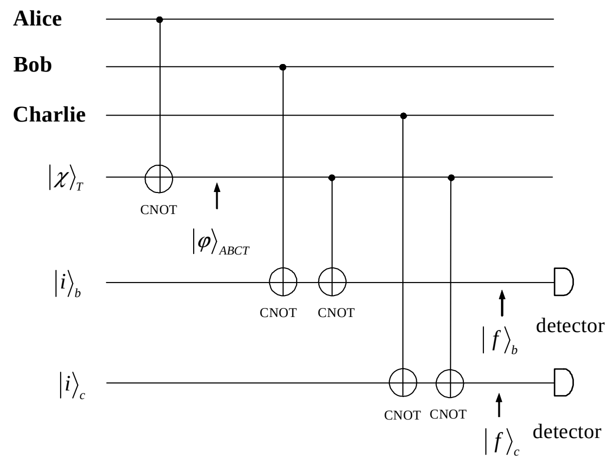

FIG. 1: The principle of the multiparty quantum remote secret conference scheme based on quantum encryption with GHZ states. CNOT: controlled not gate.

With quantum memory [34], we can modify this MQRSC protocol to transmit the secret message directly and securely, without generating the same private classical key and then encrypt the message, similar to QSDC [18, 19, 20, 21]. To this end, the three conferees, Alice, Bob and Charlie, first share a sequence of three-particle GHZ states $|\psi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{ABC}$, and then use them as a quantum key for encrypting and decrypting the secret message transmitted. We give out all the steps for this multiparty quantum remote secret conference as follows.

(1) The three conferees, Alice, Bob and Charlie, share a sequence of three-particle GHZ-state quantum systems in the same state $|\psi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{ABC}$ securely, i.e., ordered N GHZ-state tripartite quantum systems. In detail, one of the three conferees, say Alice, prepares a sequence of three-particle GHZ states $|\psi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{ABC}$. For each GHZ state, Alice sends the particle B_j $(j=1,2,\ldots,N)$ to Bob and the particle C_j to Charlie, respectively. For checking eavesdropping, Alice chooses randomly some of the GHZ states as their samples, and requires Bob and Charlie to measure their correlated particles by choosing randomly the MB σ_x or the MB σ_y. Also Bob and Charlie announce in public their MBs and the outcomes of the measurements. Here $|+y\rangle = \frac{1}{\sqrt{2}}(|0\rangle+i|1\rangle)$ and $|-y\rangle = \frac{1}{\sqrt{2}}(|0\rangle-i|1\rangle)$, i.e.,

$$|\psi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{ABC},$$

$$= \frac{1}{\sqrt{2}}[(|+y\rangle_A|-y\rangle_B + |-y\rangle_A|+y\rangle_B)|+x\rangle_C$$
$$+(|+y\rangle_A|+y\rangle_B + |-y\rangle_A|-y\rangle_B)|-x\rangle_C. \quad (3)$$

When both Bob and Charlie choose the MB σ_x or the MB σ_y, Alice chooses the MB σ_x to measure her particle A as well, otherwise, Alice measures her particle with the MB σ_y. In this way, the three conferees always obtain the correlated outcomes of their measurements on the samples if there is no eavesdropper, similar to the two-step protocol [18] and BBM92 QKD protocol [3]. In a noise channel, they can obtain securely a short sequence of GHZ states with entanglement purification.

(2) The three conferees encrypt and decrypt their secret message directly with their quantum key. In detail, a conferee, say Alice wants to send her secret message to the other two conferees, Bob and Charlie. She first prepares ordered N traveling particles $S_T : [T_1, T_2, \ldots, T_N]$, and then encrypts the j-th ($j = 1, 2, \ldots, N$) traveling particle T_j by using a controlled-not (CNOT) gate with the particle A_j in her quantum key, shown in Fig.1. Suppose the state of a traveling particle T_j is $|\chi\rangle_T = \alpha|0\rangle + \beta|1\rangle$. Here $|\chi\rangle_T \in \{|0\rangle, |1\rangle\}$, i.e., $\alpha\beta = 0$. After the CNOT operation done by Alice with the particle A_j as the control qubit and the traveling particle T_j as the target qubit, the state of the quantum system composed of the particles A_j, B_j, C_j and T_j becomes

$$|\varphi\rangle_{ABCT} = \frac{1}{\sqrt{2}}(\alpha|0\rangle_A|0\rangle_B|0\rangle_C|0\rangle_T + \beta|0\rangle_A|0\rangle_B|0\rangle_C|1\rangle_T$$
$$+ \alpha|1\rangle_A|1\rangle_B|1\rangle_C|1\rangle_T + \beta|1\rangle_A|1\rangle_B|1\rangle_C|0\rangle_T). \quad (4)$$

Alice sends the traveling particles S_T to Bob. For reading out the information on the traveling particles S_T, Bob prepares a sequence of auxiliary particles $S_b : [b_1, b_2, \ldots, b_N]$ whose states are initially $|i\rangle_b = |0\rangle$, and takes a CNOT gate on an auxiliary particle b_j and a particle B_j in the quantum key by using the particle B_j as the control qubit. Moreover, Bob takes another CNOT gate on the traveling particle T_j and the auxiliary particle b_j by using the traveling particle as the control qubit. Thus the state of the auxiliary particle b_j is changed into the one $|f\rangle_b$ as the same as the original state of the traveling particle T_j. Whether the state $|\chi\rangle_T$ is $|0\rangle$ or $|1\rangle$ which represent the bit values 0 and 1 in the secret message respectively, Bob can read out this information with a measurement σ_z on the auxiliary particle b_j. Simultaneously, Bob sends the traveling particles S_T to a next conferee, say Charlie.

Certainly, on one hand, Charlie can also do the same operations as those done by Bob to read out the information about Alice's secret message, shown in Fig.1. On the other hand, Charlie can measure the traveling particles S_T after he takes a CNOT gate on each traveling particle T_j and the particle C_j in the quantum key by using the particle C_j as the control qubit. As all the quantum systems in the quantum key are in the GHZ state $|\psi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ABC}$, Charlie can recover the original state of each traveling particle T_j and then read out the information about Alice's message directly.

(3) The three conferees use their quantum key repeatedly to encrypt and decrypt their secret message in next round if they confirm that their quantum communication is secure. For checking the security of their quantum communication, the three conferees can choose a subset of quantum systems in their quantum key as samples to analyse their error rate, same as the process for sharing a sequence of GHZ states securely in the step 1. Certainly, the new quantum key is shorter a little than the original one.

This MQRSC protocol is secure if the quantum key is secure as it is just a quantum one-time pad cryto-system [1, 19] in this time. None can read out the secret message carried by the traveling particles S_T if he does not know the information about the quantum key as each traveling particle T_j is randomly in the states $|0\rangle$ and $|1\rangle$ after the conferee Alice encrypts it with her particle A_j and a CNOT gate, i.e, the density matrix for a traveling particle T is $\rho_T = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ whether its original state is $|0\rangle$ or $|1\rangle$. Thus this MQRSC protocol can be made to be secure.

It is straightforward to generalize these two MQSRC schemes to the case with M legitimate conferees, say Alice, Bob, Charlie, ..., and Mac. For the first MQSRC scheme, Alice, in this time, prepares an M-particle GHZ state

$$|\Psi\rangle_{AB\ldots M} = \frac{1}{\sqrt{2}}(|000\ldots 0\rangle + |111\ldots 1)_{AB\ldots M}, \quad (5)$$

and sends the particles B, C, ..., and M to Bob, Charlie, ..., and Mac, respectively. Each of the conferees takes the MBs σ_z and σ_x to measure his particle with the probabilities $1-p$ and p, respectively. Similar to the case with three conferees, the probability that all the conferees obtain the same outcomes with the MB σ_z in principle is $(1-p)^M$. Then the probability that the M remote conferees obtain their raw key, p'_{rk} without eavesdroppers is

$$p'_{rk} = (1 - \sqrt[M]{\frac{r}{2}})^M p'_t p'_d, \quad (6)$$

where p'_t and p'_d are the total probabilities of the transmission among the M conferees and their detectors, respectively. Here

$$p'_t = \prod_{l=2}^{M} p'_{tl}, \quad p'_d = \prod_{l=1}^{M} p'_{dl}, \quad (7)$$

where $p'_{dl} \leq 1$ is the probability of the detector of the l-th conferee, $p'_{tl} < 1$ is the probability of the transmission between the $(l-1)$-th conferee and the l-th conferee. Obviously, the probability p'_{rk} decreases largely with the increase of the number M.

For generalizing our second MQRSC scheme to the case with M conferees, all the conferees should first share securely a sequence of M-particle GHZ states $|\Psi\rangle_{AB\ldots M} = \frac{1}{\sqrt{2}}(|000\ldots0\rangle + |111\ldots1)_{AB\ldots M}$. This task can be accomplished with the same way as that in the case with three conferees. In the process of encrypting and decrypting their secret messages, Alice first encrypts her secret message on the traveling particles $S_T : [T_1, T_2, \ldots T_N]$ with the particles $S_A : [A_1, A_2, \ldots A_N]$ and CNOT gates, and then sends the particles S_T to Bob. Bob decrypts the secret message with his auxiliary particles S_b and the particles $S_B : [B_1, B_2, \ldots B_N]$ in the quantum key, and measures the auxiliary particles with the MB σ_z, not the traveling particles S_T. He sends the particles S_T to a next conferee, say Charlie, shown in Fig.1. All the other conferees just repeat the operations done by Bob except for the last one, Mac. After taking a CNOT gate on each traveling particle T_j and his particle M_j in the quantum key by using the particle M_j as the control qubit, Mac reads out Alice's message by measuring the traveling particles S_T with the MB σ_z. In order to use their quantum key repeatedly, all the conferees should check the security of their quantum communication by sampling some of the quantum systems in their quantum key for analysing their error rate, similar to that in the case with three conferees.

Compared with quantum secret report [32] and quantum broadcast communication [33], each of the legitimate conferees can send his message to the other conferees, not the case in which only the agents can send their secret messages to a boss in a one-way direction [32] or a special one can send his message to his agents [33]. In our second MQRSC scheme, only the traveling particles S_T are transmitted among the M legitimate conferees after they share securely their quantum key, a short sequence of GHZ states which can be used repeatedly. As almost all the particles can be used to transmit the secret message, the intrinsic efficiency for qubits in these two MQRSC schemes approaches the maximal value. Thus they both are optimal.

In summary, we have presented two multiparty quantum remote secret conference schemes with GHZ states. One is based on the same classical key generated with M-particle GHZ states and the measurements with two biased measuring bases. The other is based on encrypting and decrypting with a quantum key, a sequence of GHZ states $|\Psi\rangle_{AB\ldots M} = \frac{1}{\sqrt{2}}(|000\ldots0\rangle + |111\ldots1)_{AB\ldots M}$. As their intrinsic efficiency for qubits approaches the maximal value, both are optimal.

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

[2] Bennett C H and Brassad G 1984 *Proc. IEEE Int.Conf. on Computers, Systems and Signal Processing (Bangalore, India* (New York: IEEE) p 175

[3] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[4] Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302
Deng F G and Long G L 2003 *Phys. Rev.* A **68** 042315
Deng F G and Long G L 2004 *Phys. Rev.* A **70** 012311

[5] Lo H K, Chau H F and Ardehali M 2005 *J. Cryptology* **18** 133

[6] Li C Y et al 2005 *Chin. Phys. Lett.* **22** 1049
Li C Y et al 2006 *Chin. Phys. Lett.* **23** 2896

[7] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[8] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162

[9] Guo G P and Guo G C 2003 *Phys. Lett.* A **310** 247

[10] Xiao L et al 2004 *Phys. Rev.* A **69** 052307

[11] Deng F G et al 2005 *Phys. Lett.* A **337** 329

[12] Zhang Z J et al 2005 *Phys. Rev.* A **71** 044301
Deng F G et al 2005 *Phys. Rev.* A **72** 044302

[13] Yan F L and Gao T 2005 *Phys. Rev.* A **72** 012304

[14] Li Y M, Zhang K S and Peng K C 2004 *Phys. Lett.* A **324** 420

[15] Deng F G et al 2005 *Phys. Rev.* A **72** 044301

[16] Deng F G et al 2005 *Phys. Rev.* A **72** 022338

[17] Li X H et al 2006 *J. Phys.* B **39** 1975
Deng F G et al 2006 *Euro. Phys. J.* D **39** 459

[18] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317

[19] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319

[20] Wang C et al 2005 *Phys. Rev.* A **71** 044305

[21] Wang C et al 2005 *Opt. Commun.* **253** 15

[22] Man Z X et al 2005 *Chin. Phys. Lett.* **22** 18

[23] Yan F L, Zhang X 2004 *Euro. Phys. J.* B **41** 75
Gao T, Yan F L and Wang Z X 2005 *J. Phys.* A **38** 5761
Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 893

[24] Li X H et al 2006 *Chin. Phys. Lett.* **23** 1080

[25] Zhu A D et al 2006 *Phys. Rev.* A **73** 022338

[26] Wang J et al 2006 *Phys. Lett. A* **358** 256

[27] Cai Q Y and Li B W 2004 *Chin. Phys. Lett.* **21** 601

[28] Cao H J and Song H S 2006 *Chin. Phys. Lett.* **23** 290

[29] Li X H et al 2005 *Preprint* arXiv: quant-ph/0512014

[30] Deng F G et al 2006 *Phys. Lett.* A **359** 359

[31] Li X H et al 2006 *J. Korean Phys. Soc.* **49** 1354

[32] Deng F G et al 2006 *Chin. Phys. Lett.* **23** 1676

[33] Wang J, Zhang Q and Tang C J 2006 quant-ph/0604179

[34] Sun C P et al 2003 *Phys. Rev. Lett.* **91** 147903