Improving the Security of N-user Quantum Key distribution with N Quantum Channels

Liu Xiaofen , Chen Licong ,Pan Rijing
School of Mathematics and Computer Science ,Key Lab of Network Security and Cryptography
Fujian Normal University,
Fuzhou 350007, China

***Abstract*-In a recent paper [C.H. Hong et al., Opt. Commun. 283 (2010) 2644], a n-user quantum key distribution protocol with n quantum channels was presented. By analyzing its security, it is shown that this protocol is insecure for Trent, a dishonest third party, who can steal the key without being detected by a special attack strategy. We give a description of this strategy and then put forward an improved protocol, which can stand against this attack. Furthermore, the improved protocol is feasible in the current technology conditions, because it is just required an incomplete Bell-state measurement in implementation of it.**

Keyword-Quantum key distribution, Entanglement swapping, Einstein-Podolsky-Rosen pairs

I. INTRODUCTION

Quantum key distribution (QKD) is one of the most important applications in the field of quantum information. In contrast to classical cryptography, the security of QKD is guaranteed by elementary principles of quantum mechanics, and therefore QKD has the unconditional security in theory. As a result, QKD has attracted a lot of attention, and has processed quickly[1-8], since the first QKD protocol was proposed by Bennett and Brassard in 1984 [9].

Recently, a *n*-user quantum key distribution (MQKD) protocol was presented [8], which is called the Hong protocol hereinafter. In this protocol, there are *n* users and a third party (Trent). With the help of Trent, any two parties (Alice and Bob) among these legal users can establish a secure quantum channel, via which they are able to perform key distribution between them. Utilizing the principle of entanglement swapping, only *n* quantum channels are required to achieve this aim in the Hong protocol, while the number of channels generally required is $n(n-1)/2$ in this case. Moreover, the authors of Ref. [8] analyzed the security of the Hong protocol and thought that it is secure. However, we will show that by a special strategy Trent can attain the key alone without introducing any errors in the Hong protocol.

II. THE ORIGINAL HONG PROTOCOL

Now, let us review briefly the Hong protocol. Before this, for the sake of convenience, we define an Einstein-Podolsky-Rosen (EPR) pair which is in one of the four Bell states as follows:

$$\begin{aligned}&\left|\varphi(u,v)\right\rangle_{i,j}\\&=2^{-1/2}(\left|0\right\rangle\left|0\oplus v\right\rangle+(-1)^{u}\left|1\right\rangle\left|1\oplus v\right\rangle)\ ,\ u,v\in\{0,1\}\end{aligned}\tag{1}$$

Here, the subscripts *i* and *j* indicate two qubits in an entangled pair, and $\oplus$ represents addition modulo 2.

In the Hong protocol, according to her secret $a\in\{0,1\}$, Alice prepares an EPR pair in the state $\left|\varphi(0,s_a)\right\rangle_{T_A A}$. Then, Alice sends the qubit T_A to Trent and holds the qubit *A* in her site. Meanwhile, Bob prepares two particles T_B and *B* in the state $\left|\varphi(0,0)\right\rangle_{T_B B}$, and transmits the qubit T_B to Trent. Here, the particular process to ensure the security of the channel between Trent and Alice (Bob) is not important to us, so we do not describe it in detail. After that, Trent performs a Bell state measurement on the qubits T_A and T_B, which discriminate these two particles is in the state $\left|\phi^{\pm}\right\rangle=2^{-1/2}(\left|0\right\rangle\left|0\right\rangle\pm\left|1\right\rangle\left|1\right\rangle)=\left|\varphi(*,0)\right\rangle$ or $\left|\psi^{\pm}\right\rangle=2^{-1/2}(\left|0\right\rangle\left|1\right\rangle\pm\left|1\right\rangle\left|0\right\rangle)=\left|\varphi(*,1)\right\rangle$, and sends the measurement result to Alice. In terms of the rule of entanglement swapping [10,11], we know that the qubits *A* and *B* are also collapsed onto a corresponding Bell state. These possible results can be found through the following process:

$$\begin{aligned}&\left|\varphi(0,a)\right\rangle_{T_A A}\left|\varphi(0,0)\right\rangle_{T_B B}\\&=2^{-1}(\left|\varphi(0,0)\right\rangle\left|\varphi(0,a)\right\rangle+\left|\varphi(1,0)\right\rangle\left|\varphi(1,a)\right\rangle\\&\quad+\left|\varphi(0,1)\right\rangle\left|\varphi(0,a\oplus1)\right\rangle+\left|\varphi(1,1)\right\rangle\left|\varphi(1,a\oplus1)\right\rangle)_{T_A T_B BA}\end{aligned}\tag{2}$$

Hence, if Trent's measurement outcome is $\left|\varphi(p,q)\right\rangle_{T_A T_B}$, Alice can deduce that the particles *A* and *B* are projected into a Bell state $\left|\varphi(p,q\oplus a)\right\rangle_{AB}$, which constructs a quantum channel between Alice and Bob. After Trent declared the value of *q*, to ensure the security of this channel, Alice and Bob execute a eavesdropping-check process. In this check, they measure their own particles *A* and *B* in the basis $\sigma_z=\{\left|0\right\rangle,\left|1\right\rangle\}$ and obtain the measurement results *ma* and *mb*, respectively. It is obvious that these two results should satisfy the following condition,

$$mb=q\oplus a\oplus ma\tag{3}$$

So, utilizing the above equation, Alice and Bob can detect eavesdropping with the knowledge of Trent's announcement.

If the channel is secure, Alice and Bob are able to obtain their keys *ka* and *kb* by measuring their own qubits

in the basis σ_z, respectively. Here, $ka = q \oplus a \oplus ma$, and *kb*=*mb*. From Eq. (3), it is clear that *ka*=*kb*. In this way, Alice and Bob can share a common random key with the help of Trent.

III. THE ATTACK STRATEGY WITH ENTANGLEMENT SWAPPING

In Ref. [8], Hong *et al.* claimed that the Hong protocol is secure and not even Trent can access the key, since he does not know Alice's initial state, and there is no quantum channel between Trent and Alice (or Bob) after the entanglement swapping. However, it is not the case. If he is dishonest, Trent may eavesdrop the key without being detected, by using a special attack strategy. In the following, this attack strategy will be depicted in detail.

After receiving the qubits T_A and T_B, Trent measures the particle T_B in the basis σ_z and attains the outcome *mt*, instead of making a Bell measurement on these two particles according to the legal process. Because the initial state of the qubits T_B and B is $|\varphi(0,0)\rangle_{T_B B}$, the qubit B is collapsed onto the state $|mt\rangle_B$. In this way, it is apparent that Trent can attain the key at the end of protocol. After that, Trent makes a Bell measurement on the particles T_A and T_B, and tells Alice his measurement outcome, $|\varphi(p',q')\rangle_{T_A T_B}$.

In the Hong protocol, the eavesdropping check process is proposed to ensure its security. Hence, the success of this attack relies on Trent's announcement, which cannot introduce any errors in the eavesdropping attack. Next, it is shown that this attack cannot be detected in the check.

After the qubit T_B is measured by Trent, the qubits T_A, T_B and A is in the state

$$\begin{aligned} &|\varphi(0,a)\rangle_{T_A A}|mt\rangle_{T_B} \\ &= \frac{1}{2}[(|\varphi(0,mt)\rangle + |\varphi(1,mt)\rangle)|a\rangle \\ &+(|\varphi(0,mt\oplus 1)\rangle - |\varphi(1,mt\oplus 1)\rangle)|a\oplus 1\rangle]_{T_A T_B A} \end{aligned} \tag{4}$$

Then Trent makes a Bell state measurement on the qubits T_A and T_B, and sends this outcome $|\varphi(p',q')\rangle_{T_A T_B}$ to Alice. According to Eq.(4), we can derive that the qubit A is in the state $|a \oplus mt \oplus q'\rangle_A$. In the eavesdropping check, Alice and Bob measure the qubits A and B in the basis σ_z, and attain the results ma' and mb', respectively. Here, $ma' = a \oplus mt \oplus q'$ and $mb' = mt$. Hence, the following equation can be yielded

$$mb' = q' \oplus a \oplus ma' \tag{5}$$

Consequently, comparing Eq.(5) with Eq.(3), it can be deduced that Trent's announcement cannot introduce any errors in the eavesdropping check. That is to say, Trent is able to obtain the sharing key by the proposed attack strategy and the Hong protocol is insecure.

IV. THE IMPROVED PROTOCOL

Before giving a possible improved protocol, it should be noted that generation and measurement of two Bell states is sufficient in the Hong protocol. Since the complete Bell-state measurement has to fail due to low efficiency in practice, this feature is worthwhile and valuable in implementation of the Hong protocol. Thus, in designing the improved protocol, How to retain this feature should be considered.

Now, for the sake of convenience, the whole procedure of the improved protocol is depicted as follows.

(1) In terms of her secret "$a_1, \cdots, a_n$, $a_i \in \{0,1\}$", Alice prepares a sequence of EPR pairs in the states $|\varphi(0,a_i)\rangle$. Then, she divides them into two sequences S_{TA} and S_A, where S_{TA} is the set of the first qubits of these two-qubit entangled pairs and S_A is that of the second qubits. Finally, Alice sends S_{TA} to Trent and restores S_A in a safe place.

(2) After Trent receives the sequence S_{TA}, Alice selects randomly a sufficiently large subset from the sequence S_A, and measures these particles in the basis σ_z or $\sigma_x = \{|\pm\rangle = 2^{-1/2}(|0\rangle \pm |1\rangle)\}$, which is chosen at random. Then, she tells Trent the positions of these particles and her measurement basis through a classical channel. Trent measures the corresponding particles in the sequence S_{TA} by using Alice's information of measurement basis. By comparing their outcomes, Alice and Trent can determine whether the quantum channel between them is secure or not.

(3) In the same way, Bob prepares a sequence of EPR pairs in the state $|\varphi(0,b_i)\rangle$ according to his secret "$b_1, \cdots, b_n$, $b_i \in \{0,1\}$". After that, he transmits the sequence S_{TB} to Trent and keeps S_B in his hand.

(4) Trent performs a series of Bell measurements on a sequence of two particles composed of one from S_{TA} and the other from S_{TB}. Meanwhile, in terms of the rule of entanglement swapping, the corresponding two qubits of S_A and S_B collapse into a Bell state, which constructs a quantum channel between Alice and Bob. These possible results can be found through the following equation,

$$\begin{aligned} &|\varphi(0,a_i)\rangle_{T_A A}|\varphi(0,b_i)\rangle_{T_B B} \\ &= 2^{-1}(|\varphi(0,0)\rangle|\varphi(0,a_i \oplus b_i)\rangle \\ &+|\varphi(1,0)\rangle|\varphi(1,a_i \oplus b_i)\rangle \\ &+|\varphi(0,1)\rangle|\varphi(0,a_i \oplus b_i \oplus 1)\rangle \\ &+|\varphi(1,1)\rangle|\varphi(1,a_i \oplus b_i \oplus 1)\rangle)_{T_A T_B BA} \end{aligned} \tag{6}$$

For example, if Trent's outcome is $|\varphi(p_i,q_i)\rangle$, the other two particles are projected into the Bell state

$\left|\varphi(p_i, q_i \oplus a_i \oplus b_i)\right\rangle$. Here, the measurement is only required to distinguish the state $\left|\varphi(*,0)\right\rangle$ from $\left|\varphi(*,1)\right\rangle$. Hence, Trent just declares the value of q_i finally.

(5) Alice randomly chooses some particles in the sequence S_A as a sample, which are measured in the basis σ_z, and tells Bob the positions of these particles and measurement results ma_i. Bob then performs measurements on the corresponding particles in the sequence S_B in the basis σ_z, and obtains measurement outcomes mb_i. According to Eq.(6), it is obvious that these two results should satisfy the following condition.

$$mb_i = q_i \oplus a_i \oplus b_i \oplus ma_i \tag{7}$$

So, Alice and Bob can use their measurement outcomes to check quantum channels with the knowledge of Trent's announcement q_i. If the error rate exceeds the threshold, Alice and Bob discard these entangled particles and abort the communication. Otherwise, they continue the protocol.

(6) The remainder shared entangled pairs are used for generating key bits. Alice and Bob can obtain their keys ka_i and kb_i by measuring their own qubits in the basis σ_z, respectively. Here, $ka_i = q_i \oplus a_i \oplus ma_i$, and $kb_i = b_i \oplus mb_i$. From Eq.(7), it is clear that ka_i=kb_i. In this way, Alice and Bob can share a common random key with the help of Trent.

Next, we make a brief security analysis on the improved protocol. In the transmission of the sequences S_{TA} and S_{TB}, the improved protocol utilize the same method as the original Hong protocol to ensure the security of the transmission. Hence, the quantum channel is secure, in accordance with the security analysis in Ref. [8]. To stand against the present attack, we make a modification in Bob's side, which requires Bob execute the same action as Alice. In this way, the initial state of the EPR pair prepared by Bob in step (3) becomes unknown for Trent. Hence, it is evident that the dishonest Trent could not use the proposed attack strategy to eavesdrop the key.

V. SUMMARIES

In summary, we found that the *n*-user quantum key distribution protocol presented in Ref. [8] may have a security leak and proposed a special eavesdropping strategy for Trent, the dishonest third party, who helps any two users construct the quantum channel between them. With this attack, Trent can elicit the key freely and fully. Moreover, we put forward a possible way for improving the security of this protocol. In the improved protocol, an incomplete Bell-state measurement is adopted, which allows one to identify two Bell states. Consequently, as compared to the protocol with complete Bell-state measurement proposed in Ref. [12], the improved protocol is more feasible in the current technology conditions.

ACKNOWLEDGE

This work was supported by National Natural Science Foundation of China, Grant No. 60903152; a Key Project of Fujian Provincial Universities- Information Technology Research Based on Mathematics; and Fujian Province Natural Science Foundation, Grant Nos. 2010J01318, 2010J05128.

REFERENCES

[1] Nicolas Gisin; Jan Bouda; Vladimír Buzek et al. Quantum cryptography. Rev. Mod. Phys. [J], 2002, 74: 145

[2] Long Gui-Lu; Liu Xiao-Shu. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A [J], 2002, 65: 032302

[3] Wang Xiang-Bin. Beating the photon-number-splitting attack in practical quantum cryptography. Phys. Rev. Lett. [J], 2005, 94: 230503.

[4] Peng Cheng-Zhi; Zhang Jun; Yang Dong; et al. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. Phys. Rev. Lett. [J], 98: 010505

[5] Li Xi-Han; Deng Fu-Guo; Zhou Hong-Yu. Efficient quantum key distribution over a collective noise channel. Phys. Rev. A [J], 2008, 78: 022321

[6] Sun Ying; Wen Qiao-Yan; Gao Fei; Zhu Fu-Chen. Robust variations of the Bennett-Brassard 1984 protocol against collective noise. Phys. Rev. A [J], 2009, 80: 032321

[7] Wang Jin-Dong; Wei Zheng-Jun; Zhang Hui et al. Efficient quantum key distribution via single-photon two-qubit states. J. Phys. B: At. Mol. Opt. Phys. [J], 2010, 43: 095504

[8] Chang Ho Hong; Jin O Heo; Gyong Luck Khym et al. N quantum channels are sufficient for Multi-user quantum key distribution protocol between n users. Opt. Commun. [J], 2010, 283: 2644

[9] Charles H. Bennett; Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE, New York[M], 1984, PP175

[10] S. Bose; V. Vedral; P. Knight. Multiparticle generalization of entanglement swapping. Phys. Rev. A [J], 1998, 57: 822

[11] Jan Bouda; Vladimír Buzek. Entanglement swapping between multi-qudit systems. J. Phys. A [J], 2001, 34: 4301

[12] Wang Tian-Yin; Wen Qiao-Yan; Chen Xiu-Bo. Cryptanalysis and improvement of a multi-user quantum key distribution protocol. Opt. Commun. [J] 283: 5261