Indonesian Journal of Electrical Engineering and Computer Science
Vol. 4, No. 2, November 2016, pp. 406 ~ 411
DOI: 10.11591/ijeecs.v4.i2.pp406-411

A Quantum Entanglement Swapping Secret Sharing Agreement Model

Shuyue Wu
School of Electrical & Information Engineering, Hunan International Economics University
Changsha, China, Postcode: 410205
Corresponding author, email: matlab_bysj@126.com

Abstract

A verifiable quantum secret sharing protocol model is proposed based on entanglement swapping. The dealer communicates with the participants one by one. The detection pattern or information pattern are choosed by uniform distribution, until he can make sure the information safe to the participant, and then he communicates with the next participant. This agreement not only is to avoid eavesdropping outside, and it can prevent internal fraud, thus the accuracy and security are ensured for information sharing, the verifiable results are achieved.

Keywords*: quantum secret sharing (QSS); entanglements Wapping; communication; verifiable secret sharing*

1. Introduction

In recent years, the quantum communication has rapidly developed, its theory and application has become the focus of public attention, research focuses mainly quantum key distribution [1], quantum secret sharing (quantum secret sharing (QSS) [2], quantum secure communication [3], quantum authentication [4] and so on.

QSS basic idea is as follows: If Alice wants to send a secret message to Bob and Charlie, but Alice need to confirm the following points: (1) one representative is honest at least; (2) two agents cooperation can solve Alice's secret message, but each an agent can not obtain any information about this secret alone. It is noted that the quantum secret sharing is multi-communication (3-way and three more parties), and therefore it is in the communication process not only to exclude external eavesdropping, but also to prevent potential internal fraud.

Since 1999, Hillery et al proposed the first QSS protocol (it is called HBB99 Protocol) by GHZ entanglement [5], there are a variety of QSS scheme. In these programs, there are shared by the quantum mechanics characteristics are used to share classic information or directly any quantum news (quantum state) between sharers. According to quantum mechanics secret sharing feature relies, these programs can be divided into QSS based on entangled states and QSS based on product state. In 2005, Zhang presented a classic shared message ZM05 quantum secret sharing protocol based on entanglement swapping and local unitary operation [6]. In 2007, Wang proposed the entanglement swapping QSS protocol (ES-QSS) on the basis of the ZM05 protocol [7]. ZM05 protocol is based on two-particle entanglement and local unitary operation, it is compared to the HBB99 agreement, it is and simple; ES-QSS protocol is to improve ZM05 agreement, without the need for unitary operation, it is easier to implement.

A QSS improvement agreement was proposed based on entanglement Swapping [8]. The insecurity of the agreement is analyzed in this paper, and on this basis, a new protocol of improved QSS is proposed based on Entanglement Swapping. This agreement overcomes the agreement insecurity, it is not only to prevent external eavesdropping, spoofing of internal dishonest participants can be prevented, under the multi (more than 3 square) secret sharing situation, the typical two parties cooperate dishonest deception can be also prevented. The agreement ensures the accuracy and security of the shared information, and there is a verifiable feature.

Received September 9, 2016; Revised October 9, 2016; Accepted October 21, 2016

2. Materials and Methods

2.1. Entanglement Swapping QSS Protocol

QSS protocol principle is shown in Figure 1 [8], the protocol of the entanglement is four bell base-state:, it can be expressed as Formula (1):

$$\left|\varphi^{+}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle+\left|11\right\rangle\right)=\frac{1}{\sqrt{2}}\left(\left|++\right\rangle+\left|--\right\rangle\right)\left|\varphi^{-}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|00\right\rangle-\left|11\right\rangle\right)=\frac{1}{\sqrt{2}}\left(\left|+-\right\rangle+\left|-+\right\rangle\right)$$
$$\left|\psi^{+}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|01\right\rangle+\left|10\right\rangle\right)=\frac{1}{\sqrt{2}}\left(\left|++\right\rangle-\left|--\right\rangle\right)\left|\psi^{-}\right\rangle=\frac{1}{\sqrt{2}}\left(\left|01\right\rangle-\left|10\right\rangle\right)=\frac{1}{\sqrt{2}}\left(\left|+-\right\rangle-\left|-+\right\rangle\right) \quad (1)$$

Where, $\left|0\right\rangle$ and $\left|1\right\rangle$ are σ_z eigenstates, $\left|+\right\rangle=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle+\left|1\right\rangle\right)$ and $\left|-\right\rangle=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle-\left|1\right\rangle\right)$ are as σ_x eigenstates.

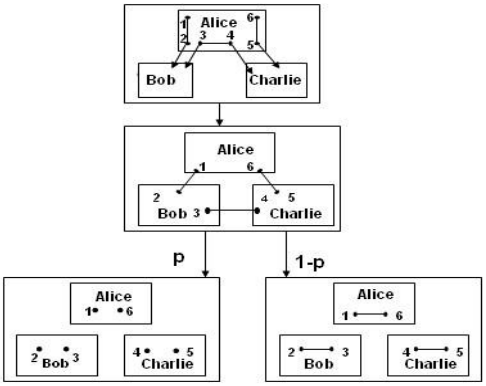

Figure 1. Entanglement Swapping QSS Protocol

Concrete steps (as Figure 1):

Step 1: Alice, Bob and Charlie mutually agreed, the four Bell states $\left|\varphi^{+}\right\rangle,\left|\varphi^{-}\right\rangle,\left|\psi^{+}\right\rangle$ and $\left|\psi^{-}\right\rangle$ are encoded as classical information bits 00, 01, 10 and 11. First, Alice generates three entangled states, they are in $\left|\varphi^{+}\right\rangle$, and the two particles of each entangled state are called particles 1 and 2, 3 and 4, 5 and 6. Then, Alice was saved in particles 1 and 6, the particles 2 and 3 was sent to Bob in random relative order, the particles 4 and 5 was also sent to Charlie in relative random order.

Step 2: until Alice has sent completely the particles, detection mode is selected followly by probability p, information mode is selected with probability 1-p. If Alice selects the detection mode, the communicating parties proceeds to step 3; otherwise, skip to step 4.

Step 3: Alice put the relative order of particles 2, 3 and particles 4, 5, respectively to advertisement Bob and Charlie, as they know that the relative order of the particles, Bob and Charlie can distinguish particles 2 and 5.

Next step implements security channel detection: To detect channel security between Alice and Bob, Bob randomly selected group of particles 2 or the corresponding measurement group, and measurement results and the final choice are put to tell Alice, Alice would use the measured group to measure the particle 1, the measurement results should be the same with Bob measured result, it is determined that the particles 2 is security in the transmission process to Bob, for external eavesdroppers, since the particles 2, 3 are send in random order, the external eavesdroppers can not tell the exact particle 2 and 3, so the security of particle 2 is fully able to represent quantum channel security from Alice to Bob.

Similarly, through the implementation of safety testing particle 5, security channel are known between Alice and Charlie. If these two quantum channels are both safe, to return to step 1, otherwise to terminate the communication.

Step 4: Alice, Bob and Charlie joint respectively Bell state measurement with particle 1, 6, particle 2, 3 and particle 4, 5, Table 1 can be obtained by the following equation expand relations. Therefore, Alice would share two bits of classic information with Bob and Charlie.in accordance with the respective Bell state measurement results.

$$\begin{aligned}
&\left|\varphi^{+}{}_{12}\right\rangle\otimes\left|\varphi^{+}{}_{34}\right\rangle\otimes\left|\varphi^{+}{}_{56}\right\rangle \\
=\ &\frac{1}{4}\cdot\left(\left|\varphi^{+}{}_{16}\right\rangle\left|\varphi^{+}{}_{23}\right\rangle\left|\varphi^{+}{}_{45}\right\rangle+\left|\varphi^{+}{}_{16}\right\rangle\left|\varphi^{-}{}_{23}\right\rangle\left|\varphi^{-}{}_{45}\right\rangle\right. \\
&+\left|\varphi^{+}{}_{16}\right\rangle\left|\psi^{+}{}_{23}\right\rangle\left|\psi^{+}{}_{45}\right\rangle+\left|\varphi^{+}{}_{16}\right\rangle\left|\psi^{-}{}_{23}\right\rangle\left|\psi^{-}{}_{45}\right\rangle \\
&+\left|\varphi^{-}{}_{16}\right\rangle\left|\varphi^{+}{}_{23}\right\rangle\left|\varphi^{-}{}_{45}\right\rangle+\left|\varphi^{-}{}_{16}\right\rangle\left|\varphi^{-}{}_{23}\right\rangle\left|\varphi^{+}{}_{45}\right\rangle \\
&+\left|\varphi^{-}{}_{16}\right\rangle\left|\psi^{-}{}_{23}\right\rangle\left|\psi^{+}{}_{45}\right\rangle+\left|\varphi^{-}{}_{16}\right\rangle\left|\psi^{-}{}_{23}\right\rangle\left|\psi^{-}{}_{45}\right\rangle \\
&+\left|\psi^{-}{}_{16}\right\rangle\left|\varphi^{+}{}_{23}\right\rangle\left|\psi^{-}{}_{45}\right\rangle-\left|\psi^{+}{}_{16}\right\rangle\left|\varphi^{+}{}_{23}\right\rangle\left|\psi^{-}{}_{45}\right\rangle \\
&+\left|\psi^{-}{}_{16}\right\rangle\left|\varphi^{-}{}_{23}\right\rangle\left|\psi^{-}{}_{45}\right\rangle-\left|\psi^{-}{}_{16}\right\rangle\left|\varphi^{+}{}_{23}\right\rangle\left|\psi^{-}{}_{45}\right\rangle \\
&\left.+\left|\psi^{-}{}_{16}\right\rangle\left|\psi^{-}{}_{23}\right\rangle\left|\varphi^{+}{}_{45}\right\rangle+\left|\psi^{-}{}_{16}\right\rangle\left|\psi^{-}{}_{23}\right\rangle\left|\varphi^{-}{}_{45}\right\rangle\right)
\end{aligned} \tag{2}$$

Table 1. The Corresponding Relationship of Alice, Bob, Charlie Measurement Results

	Sharing secrets	Alice measurement results	Bob and Charlie measurement results
00	$\left\|\varphi^{+}{}_{16}\right\rangle$	$\left\{\left\|\varphi^{+}{}_{23}\right\rangle,\left\|\varphi^{-}{}_{45}\right\rangle\right\},\left\{\left\|\varphi^{-}{}_{23}\right\rangle,\left\|\varphi^{+}{}_{45}\right\rangle\right\},\left\{\left\|\psi^{-}{}_{23}\right\rangle,\left\|\psi^{+}{}_{45}\right\rangle\right\},\left\{\left\|\psi^{+}{}_{23}\right\rangle,\left\|\psi^{-}{}_{45}\right\rangle\right\}$	
01	$\left\|\varphi^{-}{}_{16}\right\rangle$	$\left\{\left\|\varphi^{+}{}_{23}\right\rangle,\left\|\varphi^{-}{}_{45}\right\rangle\right\},\left\{\left\|\varphi^{-}{}_{23}\right\rangle,\left\|\varphi^{+}{}_{45}\right\rangle\right\},\left\{\left\|\psi^{-}{}_{23}\right\rangle,\left\|\psi^{+}{}_{45}\right\rangle\right\},\left\{\left\|\psi^{+}{}_{23}\right\rangle,\left\|\psi^{-}{}_{45}\right\rangle\right\}$	
10	$\left\|\psi^{+}{}_{16}\right\rangle$	$\left\{\left\|\varphi^{+}{}_{23}\right\rangle,\left\|\varphi^{+}{}_{45}\right\rangle\right\},\left\{\left\|\varphi^{-}{}_{23}\right\rangle,\left\|\psi^{-}{}_{45}\right\rangle\right\},\left\{\left\|\psi^{+}{}_{23}\right\rangle,\left\|\varphi^{+}{}_{45}\right\rangle\right\},\left\{\left\|\psi^{-}{}_{23}\right\rangle,\left\|\varphi^{-}{}_{45}\right\rangle\right\}$	
11	$\left\|\psi^{-}{}_{16}\right\rangle$	$\left\{\left\|\varphi^{-}{}_{23}\right\rangle,\left\|\psi^{+}{}_{45}\right\rangle\right\},\left\{\left\|\varphi^{+}{}_{23}\right\rangle,\left\|\psi^{-}{}_{45}\right\rangle\right\},\left\{\left\|\psi^{-}{}_{23}\right\rangle,\left\|\varphi^{+}{}_{45}\right\rangle\right\},\left\{\left\|\psi^{+}{}_{23}\right\rangle,\left\|\varphi^{-}{}_{45}\right\rangle\right\}$	

2.2. Analysis of Insecurity

2.2.1. Insecure Analysis of ZM05 Protocol

ZM05 agreement emphasized that all entanglement are prepared first by Alice, after it is prepared, it is sent to Bob and Charlie. It is assumed that Bob is dishonest party, Bob intercept particles 4 and discard the particle 3 and particle 4, and then undesirable entangled states are prepared:

$$\left|\varphi^{-}{}_{3^{*}4^{*}}\right\rangle=\tfrac{1}{\sqrt{2}}\left(\left|00\right\rangle-\left|11\right\rangle\right)=\tfrac{1}{\sqrt{2}}\left(\left|+-\right\rangle+\left|-+\right\rangle\right) \tag{3}$$

The entanglement two particles are called 3* and 4*, particle 3* is retained, the particles 4* is sent to Charlie, and then step is proceed by protocol. Since the particle 2 and particle 5 were not destroyed, and therefore Bob can not be found by eavesdropping detection process. If Alice increases safety, but also to detect particles 3 and 4. But Bob can deduce Charlie measurement results from his measurement results, the results of their measurements are announced, which should be obtained, so that Bob can escape the detection of eavesdropping. In information mode, Bob can be introduce particles 2,5 entangled state based on Charlie measurement results, and thus Alice's key is introduced, and Charlie can only get the wrong key based on information which was released by Bob. At this time, in the presence of dishonest Bob, the particles 1, 2, 3, 4, 5, 6 states can be expressed as $\left|\varphi^{+}{}_{12}\right\rangle\otimes\left|\varphi^{-}{}_{3^{*}4^{*}}\right\rangle\otimes\left|\varphi^{+}{}_{56}\right\rangle$, these are obtained in Table 2.

Table 2. When Dishonest Bob Exists, the Corresponding Relationship of Alice, Bob, Charlie Measurement Results

	Sharing secrets	Alice measurement results	Bob and Charlie measurement results
00	$\left\|\varphi^{+}{}_{16}\right\rangle$	$\left\{\left\|\varphi^{-}{}_{23}\right\rangle,\left\|\varphi^{+}{}_{45}\right\rangle\right\},\left\{\left\|\varphi^{+}{}_{23}\right\rangle,\left\|\varphi^{-}{}_{45}\right\rangle\right\},\left\{\left\|\psi^{+}{}_{23}\right\rangle,\left\|\psi^{-}{}_{45}\right\rangle\right\},\left\{\left\|\psi^{-}{}_{23}\right\rangle,\left\|\psi^{+}{}_{45}\right\rangle\right\}$	
01	$\left\|\varphi^{-}{}_{16}\right\rangle$	$\left\{\left\|\varphi^{-}{}_{23}\right\rangle,\left\|\varphi^{-}{}_{45}\right\rangle\right\},\left\{\left\|\varphi^{+}{}_{23}\right\rangle,\left\|\varphi^{+}{}_{45}\right\rangle\right\},\left\{\left\|\psi^{+}{}_{23}\right\rangle,\left\|\psi^{+}{}_{45}\right\rangle\right\},\left\{\left\|\psi^{-}{}_{23}\right\rangle,\left\|\psi^{-}{}_{45}\right\rangle\right\}$	
10	$\left\|\psi^{+}{}_{16}\right\rangle$	$\left\{\left\|\varphi^{-}{}_{23}\right\rangle,\left\|\psi^{+}{}_{45}\right\rangle\right\},\left\{\left\|\varphi^{+}{}_{23}\right\rangle,\left\|\psi^{-}{}_{45}\right\rangle\right\},\left\{\left\|\psi^{+}{}_{23}\right\rangle,\left\|\varphi^{-}{}_{45}\right\rangle\right\},\left\{\left\|\psi^{-}{}_{23}\right\rangle,\left\|\varphi^{+}{}_{45}\right\rangle\right\}$	
11	$\left\|\psi^{-}{}_{16}\right\rangle$	$\left\{\left\|\varphi^{-}{}_{23}\right\rangle,\left\|\psi^{-}{}_{45}\right\rangle\right\},\left\{\left\|\varphi^{+}{}_{23}\right\rangle,\left\|\psi^{+}{}_{45}\right\rangle\right\},\left\{\left\|\psi^{+}{}_{23}\right\rangle,\left\|\varphi^{+}{}_{45}\right\rangle\right\},\left\{\left\|\psi^{-}{}_{23}\right\rangle,\left\|\varphi^{-}{}_{45}\right\rangle\right\}$	

2.2.2. QSS Protocol Insecurity

For this agreement, Alice sent particles 2, 3 to Bob, Alice sent particles 4, 5 Charlie by random relative order. Although this can make external eavesdropper can not obtain the real transmission order, the key can not be obtained according to known transmitting particles, But for the internal fraudster, Bob tried to intercept particles 4, discarded particles 3, 4, and prepared a new entanglement 3*, 4*, 4* will be sent to Charlie. Now that Alice sends particles 4, 5 to Charlie in random order, it make Bob have a 50% probability to intercept particles 5, which will lead to trouble that Bob discard the original entanglement and replaced with a new deceptive entanglement. But there is still a 50% probability that Bob can successfully intercepted, it can still use their deceptive entanglement 3*, 4*, Charlie measurements are inferred, Bob can still have a chance to escape eavesdropping detection, so the agreement is still not completely safe.

3. Verifiable QOS Agreement based on Entanglement Swapping

Based on the above analysis, the main reason of the protocol insecure is that internal fraudster can always take the interception replacement method to manufacture fraudulent entangled particles. To solve this problem, a new quantum secret sharing protocol is proposed based on entanglement swapping, it is one verifiable QSS protocol based on Entanglement Swapping, and its principle is shown in Figure 2.

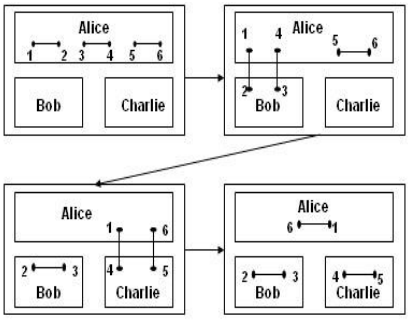

Figure 2. One Verifiable QSS Protocol based on Entanglement Swapping

3.1. Protocol steps

Step 1: Alice prepared three EPR pairs, they are respectively $\left|\varphi_{12}{}^{+}\right\rangle,\left|\varphi^{+}{}_{34}\right\rangle,\left|\varphi^{+}{}_{56}\right\rangle$.

Step 2: Alice will send particles 2 3 to Bob, Bob acknowledge receipt of two particles. Alice has an equal probability of performing the following two operations (ie, operation I and operation II are selected at equal probability order):

Operation I: Alice tests safety by QSS protocol methods, the quantum channel security is detected between Alice and Bob: If the channel is not secure, the next steps do not need, the transmission information is discarded; if the channel is safe, and the operation II is performed before the operation I is performed, or, if the operation II is first carried out, the delivered information is retained.

Operation II: Alice did Bell measurement to particle 1, 4, according to the principle of entanglement swapping, the measurement particles 1, 4 are in entanglement, then 1, 2, 3, 4 particle entanglement swapping occurs. At the same time, Bob did the corresponding Bell measurements to particle 2, 3, particle 2, 3 were also in the entangled state, the measurement result was part of the secret information which was shared by Bob. Corresponding measurement result is determined by the following equation:

$$\begin{aligned}&\left|\varphi^{+}_{12}\right\rangle\otimes\left|\varphi^{+}_{34}\right\rangle=\\&\frac{1}{2}(\left|\varphi^{+}_{23}\right\rangle\left|\varphi^{+}_{14}\right\rangle+\left|\varphi^{-}_{23}\right\rangle\left|\varphi^{-}_{14}\right\rangle\\&+\left|\psi^{+}_{23}\right\rangle\left|\psi^{+}_{14}\right\rangle+\left|\psi^{-}_{23}\right\rangle\left|\psi^{-}_{14}\right\rangle)\end{aligned} \quad (4)$$

Thus the transmission of part informationis completed separately between Alice and Bob, it does not involve the participation of a third party.

Step 3: Alice will send particles 4, 5 to Charlie, Charlie acknowledge receipt of two particles. Alice has to perform both of the following:

Operation III: Alice tests safety according to QQS Agreement methods, the quantum channel security is detected before Alice and Charlie. Because Alice knows Bell state of the particles 1, 4, after safety testing, if the channel unsafe is found, Alice can prepare a new EPR with Bell state, it is in the same state with original EPR pair, the protocol operation behind is continued; if the channel is safe, it does not need to be prepare EPR pair, the protocol operation behind is continued.

Operation IV: Alice does Bell measuring to particle 1, 6 accordingly, at this time 1, 6 particles are also the entanglement state. Corresponding measurement result is determined by the following equation:

$$\begin{aligned}&\left|\varphi^{+}_{14}\right\rangle\otimes\left|\varphi^{+}_{56}\right\rangle=\\&\frac{1}{2}(\left|\varphi^{+}_{45}\right\rangle\left|\varphi^{+}_{16}\right\rangle+\left|\varphi^{-}_{45}\right\rangle\left|\varphi^{-}_{16}\right\rangle\\&+\left|\psi^{+}_{45}\right\rangle\left|\psi^{+}_{16}\right\rangle+\left|\psi^{-}_{45}\right\rangle\left|\psi^{-}_{16}\right\rangle)\end{aligned} \quad (5)$$

Step 4: Alice announced the measurement results when Bell is performed to particle 1, 6. According to Table 1, Bob and Charlie used on measurements which Alice published; they can cooperate with each other to obtain the original secret information which Alice shared.

3.2. Protocol Analysis

This agreement was signed by Alice and other participants in a separate one-particle transfer, and the detection or measurement are completed in the first period after passing, so that the external eavesdropper can not obtain the real transmission order, the key can not be obtained according to known transmitting particles, for internal fraudster, because Alice and Bob or Charlie are both separate secret transfer, the two sides can prevent deception party during the channel security detection or information measurement, there are verifiable features. If Bob tries to intercept particles 4 and it can be successful, then it is deceptive to use their entanglement 3*, 4* trying to divine Charlie measurement results, at this time, particles 4 has no in the entanglement with particles 3, but it is in entanglement with particles 5, but Bob's own particle 2 is entanglement with particles 3, so Bob can not get any information about Charlie's secret, and it is good to avoid the risk which internal cheater intercepted displacement. It is compared with QSS protocol [8], the results is shown in Table 3.

Without loss of generality, it is extended to multi-party situation (our classical quartet as an example), assuming that two participants are dishonest, namely, Bob and David. In ZM05 agreement, Bob joint with David, they can smoothly theft [6], and the application of this agreement will avoid the theft occurred. Because Alice measured particles 1, 4, the particles 2, 3 can be forced to produce entanglement, so that, even if Bob will sent particle 2 to Davids, they

can not obtain any confidential information of Alice. So the improved agreement is both closed to prevent eavesdropping outside, but also in the presence of internal deception, on the one hand, internal displacement participants can be prevented to intercept particles, on the other hand, dishonest typical two-party cooperation deception can be prevented. In addition, the agreement is safe to present false particle spoofing attack [9].

Table 3. Compare Verifiable QSS Agreement with QSS Protocol [8]

content	verifiable QSS agreement	QSS protocol [8]
Particle pathway	Intermittent	One stop
safety	Safer	Insecurity
effectiveness	Higher	general
Verifiability	Verifiable	Conditions verification

4. Conclusion

The QSS protocol insecurity in the text [8] is analyzed in this study based on entanglement swapping, although all entangled state is produced by the Alice, and during transmission, the relative order of participants is randomly selected in the same two particles, however, in the presence of internal cheaters, there is still some probability of interception replaced attack. On this basis, we propose a one-verifiable QSS protocol based on entanglement swapping, one service thought is used in this protocols, it is one-stop messaging transfer, the security of information is ensureed before the next one transfer, it is not only to avoid eavesdropping external, and the exist threats of internal cheaters are prevented.

Acknowledgements

This study is sponsored by the Scientific Research Project (NO. 14A084) of Hunan Provincial Education Department, China.

References

[1] Bemett CH, Brassar DG. Quantum cryptography: public key distribution and coin tossing. New York: EEE. 1984: 175-179.
[2] Hillery M, Buzek V, Berthiaume A. Quantum secret sharing. *Phys. Rev. A.* 1999; 59: 1829-1834.
[3] Bostrom K, Felbinger T. Determin-istic secure direct communication using entanglement. *Phys. Rev. Lett.* 2002; 89: 187902-1-187902-4.
[4] Zeng Gui-Hua, Zhang Wei-ping. Identity verification in quantum key distribution. *Phys. Rev. A.* 2000; 61: 022301-022303.
[5] Hillery M, Buzek V. Quantum secret sharing. *Phys. Rev. A.* 1999; 59: 1830-1835.
[6] ZHANG Zhan-jun. Multiparty quantum secret sharing of classical messages based on entanglement swapping. *Phys. Rev. A.* 2005; 72: 022303-1-022303-4.
[7] WANG Jian, CHEN Huang-qing. Quantum secure communication protocols on the basis of entanglement swapping. *Journal of National University of Defense Technology.* 2007; 29(2): 56-60.
[8] WANG Jian, CHEN Huang-qing, etc. Quantum Secure Communication Protocols on the Basis of Entanglement Swapping. *Journal of National University of Defense Technology.* 2007; 29(2): 71-74.
[9] QIN SJ, WEN QY. Improving the security of multiparty quantum secret sharing against an attack with a fake signal. *Physical Letters A.* 2006; (357).