Quantum Inf Process (2013) 12:1173–1183
DOI 10.1007/s11128-012-0461-0

Cryptanalysis of a new circular quantum secret sharing protocol for remote agents

Zhen-Chao Zhu · Ai-Qun Hu · An-Min Fu

Received: 9 June 2012 / Accepted: 23 July 2012 / Published online: 10 August 2012

Abstract In a recent paper (Lin and Hwang in Quantum Inf Process, 2012. doi:10.1007/s11128-012-0413-8), a new circular quantum secret sharing (QSS) protocol for remote agents was presented. The protocol is designed with entangling a Bell state and several single photons to form a multi-particle GHZ state. For each shared bit among n party, the qubit efficiency has reached $1/2n + 1$ which is the best among the current circular QSS protocol. They claim that the protocol is more suitable for a remote agents' environment as that the newly generated photons are powerful enough to reach to the next receiver. However, we show that the protocol is not secure as the first agent and the last agent in the protocol can illegally obtain all the secret messages without introducing any error.

Keywords Quantum secret sharing · Controlled-Not gate · GHZ state · Qubit efficiency

The concept of quantum cryptography was introduced by Wiesner [1] in the late sixties of the twentieth century, it exploits the principles of quantum mechanics to enable secure distribution of private information. Unfortunately, Wiesner's innovative pioneering work paper was not accepted at that time owing to the technical conditions limits. The most important event in the development of quantum cryptography is that Bennett and Brassard [2] used four quantum states to put forward the first quantum

Z.-C. Zhu (✉) · A.-Q. Hu
Information Security Research Center, Southeast University,
Nanjing 210096, China
e-mail: zhuzc@seu.edu.cn

A.-M. Fu
School of Computer Science and Technology, Nanjing University of Science and Technology,
Nanjing 210094, China

key distribution (QKD) protocol in 1984, in the protocol, two legitimate parties, Alice and Bob, can generate a secret key over a long distance and then use the secret key to encrypt and decrypt secret messages. QKD provides a means to deliver key material for one-time pad (OTP) which is the only method that has been proven to be information-theoretically secure over an optical network [3]. Like the development of classical cryptography, the research branches such as quantum signature (QS) [4], quantum identification (QI) [5], quantum secret sharing (QSS) [6] and so on, have been brought to researcher's attentions. Compared with QKD, QS and QI, QSS has a more complex security analysis, we know that the attack power of the dishonest agent is much stronger than the outside eavesdropper as that both the outside eavesdropper's and the inside dishonest agent's attacks must be considered. The first QSS protocol [6] was proposed by Hillery, Bužek and Berthiaume in 1999, which allows to distribute the shares securely in the presence of an eavesdropper even if he has unlimited resources. Since then, the design and security analysis of QSS protocols have attracted a great deal of attention [7–33].

Recently, a multiparty circular quantum secret sharing protocol based on the controlled-NOT (CNOT) gate for remote agents was proposed (we will call it LH protocol hereafter) [34]. The implementation of LH protocol only requires all agents to equip a CNOT gate and a single photon generator, when an agent receives the photons, he/she can perform CNOT between the received photons and the ones he/she produced, and then send the newly produced ones to the next agent. Due to the fact that new photons are generated by each agent and then sent to the next one, this new strategy allows agents located in long distance to cooperate to derive the secret dealer's key. The qubit efficiency of the scheme is 1/2n+1, which is the best among the circular-based QSS schemes. They claim that the proposed scheme is congenitally free from all the attacks. Nevertheless, we show that LH protocol does not satisfy the security requirement of QSS in the sense that only the unauthorized set can gain access to the dealer's secret in the protocol without introducing any errors.

Now let us provide a brief review of LH protocol [34]. Without loss of generality, we take the same notations as that in the LH protocol. Suppose that the dealer Alice wants to send a secret key K_A to her three agents: Bob, Charlie and David, she will first split K_A into three shadows K_B, K_C, and K_D, which will later be delivered to Bob, Charlie, and David, respectively, the three agents can deduce the key if and only if they cooperate. The transmission sequence is determined as: Alice $\rightarrow$ Bob $\rightarrow$ Charlie $\rightarrow$ David $\rightarrow$ Alice. This four-party LH protocol can be detailed as follows.

(1) Alice prepares N EPR pairs all in the state $\left|\phi^{+}\right\rangle$. She takes the first and the second particle of each EPR pairs to form the sequences S_h and S_t respectively, then Alice shuffles S_t to S_t'. Alice prepares N decoy photons randomly chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and then randomly inserts these photons into S_t' to form S_t^*. Alice sends S_t^* to Bob and keeps S_h in her quantum memory.

(2) After confirming that Bob has received S_t^*, Alice announces the positions and the measurement bases of the decoy photons. Bob picks up the decoy photons and performs the measurement on the corresponding single photons. Bob reports the measurement results to Alice. Alice can judge if there are eavesdroppers in the quantum channel. If the error rate exceeds the threshold, the process is

aborted. Otherwise, Bob can obtain S_t'. Bob prepares a single photons sequence S_B in which single photons are randomly chosen from $\{|0\rangle, |1\rangle\}$. Bob takes each photon in S_B as the target qubit and the corresponding photon in S_t' as the control qubit to perform CNOT operation. The sequence S_B will be shuffled to S_B'. Afterwards, Bob prepares N decoy photons and mixes them with S_B' to form S_B^*. Bob subsequently sends S_B^* to Charlie and keeps S_t' in his quantum memory.

(3) After receiving S_B^*, Charlie performs the same security check as in Step 2 to publicly discuss the decoy photons in S_B^* with Bob. Charlie generates a sequence S_C in which single photons are randomly chosen from $\{|0\rangle, |1\rangle\}$ and then performs the CNOT operation, the single photons in S_B' is the control qubit and the single photons in S_C is the target qubits. Charlie shuffles S_C to S_C', and randomly inserts N decoy photons into S_C' to form S_C^*. He then sends S_C^* to David and keeps S_B' in his quantum memory.

(4) After receiving S_C^*, David will perform the similar procedure to ensure the security of transmission between Charlie and David. David creates S_D as the target qubits sequence and then performs the CNOT operation with S_C' as the control qubits. The shuffled sequence S_D' will be mixed with N decoy photons to form S_D^*, which will be sent to the dealer Alice.

(5) As soon as Alice receives S_D^*, she will perform the public discussion on the decoy photons of S_D^* with David. After that, she publishes her shuffled information and requests the other agents to do so. Each party can recover his/her stored S_i' ($i = \{h, t, B, C, D\}$) into the correct order of S_i accordingly. Alice performs Bell measurement on the corresponding photon pairs of S_h and S_D to obtain N sets of two-bit master key (K_A), where the K_A is "00" if the Bell measurement is $\left|\phi^+\right\rangle$, "01" if $\left|\phi^-\right\rangle$, "10" if $\left|\psi^+\right\rangle$, and "11" if $\left|\psi^-\right\rangle$.

(6) Bob (Charlie, David) will convert the Z-basis initial states of his prepared sequences $S_B(S_C, S_D)$ and the X-basis measurement results of his owned $S_t(S_B, S_C)$ into N sets of two-bit shadow keys $K_B(K_C, K_D)$ respectively. The two-bit code of the initial state and the measurement result is defined as "00" if $|0\rangle|+\rangle$, "01" if $|0\rangle|-\rangle$, "10" if $|1\rangle|+\rangle$, and "11" if $|1\rangle|-\rangle$.

(7) The four keys should have the relationship that $K_A = K_B \oplus K_C \oplus K_D$. Alice selects half of the key bits in K_A for the final public discussion. Bob and David first publish their shadow's corresponding to the check bits. Then Charlie publishes his shadow corresponding to the check bits. If the error rate (i.e., $K_A^i \neq K_B^i \oplus K_C^i \oplus K_D^i$) exceeds a rational predetermined threshold, then Alice announces to restart the protocol. Otherwise, the other N bits of key can be shared among these four parties, in which all agents have to exclusive-OR their N corresponding bits of shadows to recover the shared key.

Lin and Hwang [34] claim that the LH protocol is congenitally free from the Trojan horse attacks as that the same photons are transmitted only one time to the next receiver and the protocol can nullify the intercept-resend attack as that the decoy photons are randomly inserted into the transmitted sequences. They also give the conclusion that the protocol is secure against entangle -measure attack and collusion attack. However, we know that the security of QSS requires that only the authorized set of agents can recover the secret. In LH protocol, the authorized set is composed of three agents. In the

next, we will show how the first agent Bob and the last agent David, the unauthorized set of agents, can infer Alice's key without introducing any error.

Now, let us give an outline of our attack strategy. In step 2, after obtaining the sequence S_t' from the received sequence S_t^*, Bob not only prepares a single photons sequence S_B but also prepares N EPR pairs all in state $\left|\phi^+\right\rangle$. Bob takes the first and the second particle of each EPR pairs to form the sequence S_{hf} and the sequence S_{tf} respectively, Bob shuffles S_{tf} to obtain S_{tf}' and inserts N decoy photons into S_{tf}' to form S_{tf}^*, then Bob sends S_{tf}^* to Charlie while keeps S_{hf} in his quantum memory. After receiving S_{tf}^*, Charlie performs the same security check as in Step 2 with Bob to obtain S_{tf}'. Then Charlie generates S_C in which N single photons are randomly chosen from $\{|0\rangle, |1\rangle\}$, Charlie performs the CNOT operation with the single photons in S_{tf}' as the control qubit and the single photons in S_C as the target qubits. Charlie shuffles S_C to get S_C', and further inserts N decoy photons to form S_C^*. Charlie sends S_C^* to David while keeps S_{tf}' in his quantum memory. David performs the same security check to get S_C' and then generates a sequence S_{Df}, David performs the CNOT operation with the single photons in S_C' as the control qubits and the single photons in S_{Df} as the target qubits, David shuffles the sequence S_{Df} to get S_{Df}' and further inserts N decoy photons to form S_{Df}^*. David sends S_{Df}^* to Bob while keeps S_C' in his quantum memory. When David announces the positions and the measurement bases of the decoy photons, Bob performs measurement on the decoy photons of S_{Df}^* and then keeps S_{Df}' in his quantum memory.

To the sequence S_t^* received from Alice and the sequence S_B prepared by himself, Bob takes each photon in S_B as the target qubit and the corresponding photon in S_t' as the control qubit to perform CNOT operation. S_B will be shuffled to S_B'. Then Bob prepares N decoy photons and mixes them with S_B' to form S_B^*. Bob directly sends S_B^* to David while keeps S_t' in his quantum memory. After receiving S_B^*, David will perform the similar procedure to ensure the security of transmission and then gets S_B', David creates S_D as the target qubits sequence and then performs the CNOT operation with S_B' as the control qubits. The shuffled sequence S_D' will be mixed with N decoy photons to form S_D^*, which will be sent to the dealer Alice. Alice performs the public discussion on the decoy photons of S_D^* with David to ensure the quantum transmission is secure.

As soon as Bob and David get all the shuffled information published by Alice and Charlie, Bob will make joint measurement on the corresponding photons in S_{hf} and S_{Df} while David perform the measurement on the corresponding photons in S_C to deduce Charlie's secret information. In the next, we will show how David and Bob can achieve these ends. Bob keeps S_{hf} and S_{Df} while David keeps S_C. Besides these information, David knows the photons' initial states in S_{Df} as the sequence is produced by him. In the condition that Bob's measurement result is $\left|\phi^+\right\rangle$, there are following four situations.

(a) If David remembers that the initial state of the corresponding photons in S_{Df} is $|0\rangle$ while his measurement result of the corresponding photons in S_C is $|+\rangle$, through analyzing Eqs. (1)–(4) which give the relationships of the states in S_{hf}, S_{tf}, S_C and S_{Df} after Charlie and David having performed CNOT operations on the corresponding sequences, Bob and David can deduce the joint bits of Charlie's initial prepared bit adding measurement result is $|0\rangle\,|+\rangle$.

(b) If David remembers that the initial state of the corresponding photons in S_{Df} is $|0\rangle$ while his measurement result of the corresponding photons in the S_C is $|-\rangle$, Bob and David can deduce that joint bits of Charlie's initial prepared bit adding measurement result is $|0\rangle\,|-\rangle$.
(c) If David remembers that the initial state of the corresponding photons in S_{Df} is $|1\rangle$ while his measurement result of the corresponding photons in S_C is $|+\rangle$, Bob and David can deduce that joint bits of Charlie's initial prepared bit adding measurement result is $|1\rangle\,|+\rangle$.
(d) If David remembers that the initial state of the corresponding photons in S_{Df} is $|1\rangle$ while his measurement result of the corresponding photons in S_C is $|-\rangle$, Bob and David can deduce that joint bits of Charlie's initial prepared bit adding measurement result is $|1\rangle\,|-\rangle$.

For simplicity, the discussion of the situations that Bob's measurement results are $\left|\phi^-\right\rangle$, $\left|\psi^+\right\rangle$ and $\left|\psi^-\right\rangle$ are omitted here, Table 1 gives the details of these relations among Bob's measurement results, joint bits of David's initial prepared bit adding measurement result and joint bits of Charlie's initial prepared bit adding measurement result.

$$
\begin{aligned}
|V\rangle_0 &= CNOT_{C,Df}\cdot CNOT_{tf,C}\left|\phi^+\right\rangle_{hf,tf}|0\rangle_C\,|1\rangle_{Df}\\
&= \frac{1}{\sqrt{2}}\left(|0000\rangle+|1111\rangle\right)_{hf,tf,C,Df}\\
&= \frac{1}{2}\left[\left|\phi^+\right\rangle(|++\rangle+|--\rangle)+\left|\phi^-\right\rangle(|+-\rangle+|-+\rangle)\right]_{hf,Df,tf,C}, \qquad (1)\\
|V\rangle_1 &= CNOT_{C,Df}\cdot CNOT_{tf,C}\left|\phi^+\right\rangle_{hf,tf}|0\rangle_C\,|1\rangle_{Df}\\
&= \frac{1}{\sqrt{2}}\left(|0001\rangle+|1110\rangle\right)_{hf,tf,C,Df}\\
&= \frac{1}{2}\left[\left|\psi^+\right\rangle(|++\rangle+|--\rangle)+\left|\psi^-\right\rangle(|+-\rangle+|-+\rangle)\right]_{hf,Df,tf,C}, \qquad (2)\\
|V\rangle_2 &= CNOT_{C,Df}\cdot CNOT_{tf,C}\left|\phi^+\right\rangle_{hf,tf}|1\rangle_C\,|0\rangle_{Df}\\
&= \frac{1}{\sqrt{2}}\left(|0011\rangle+|1100\rangle\right)_{hf,tf,C,Df}
\end{aligned}
$$

Table 1 Relations among Bob's measurement results, joint bits of David's initial prepared bit adding measurement result and joint bits of Charlie's initial prepared bit adding measurement result. Bob's measurement results are listed in the first column, joint bits of David's initial bit adding measurement result are listed in the first row

	$\|0\rangle\,\|+\rangle$	$\|0\rangle\,\|-\rangle$	$\|1\rangle\,\|+\rangle$	$\|1\rangle\,\|-\rangle$
$\left\|\phi^+\right\rangle$	$\|0\rangle\,\|+\rangle$	$\|0\rangle\,\|-\rangle$	$\|1\rangle\,\|+\rangle$	$\|1\rangle\,\|-\rangle$
$\left\|\phi^-\right\rangle$	$\|0\rangle\,\|-\rangle$	$\|0\rangle\,\|+\rangle$	$\|1\rangle\,\|-\rangle$	$\|1\rangle\,\|+\rangle$
$\left\|\psi^+\right\rangle$	$\|1\rangle\,\|+\rangle$	$\|1\rangle\,\|-\rangle$	$\|0\rangle\,\|+\rangle$	$\|0\rangle\,\|-\rangle$
$\left\|\psi^-\right\rangle$	$\|1\rangle\,\|-\rangle$	$\|1\rangle\,\|+\rangle$	$\|0\rangle\,\|-\rangle$	$\|0\rangle\,\|+\rangle$

$$= \frac{1}{2}\left[\left|\psi^{+}\right\rangle(|{+}{+}\rangle - |{-}{-}\rangle) + \left|\psi^{-}\right\rangle(|{-}{+}\rangle - |{+}{-}\rangle)\right]_{hf,Df,tf,C}, \quad (3)$$

$$|V\rangle_3 = CNOT_{C,Df} \cdot CNOT_{tf,C}\left|\phi^{+}\right\rangle_{hf,tf}|1\rangle_C|1\rangle_{Df}$$
$$= \frac{1}{\sqrt{2}}(|0010\rangle + |1101\rangle)_{hf,tf,C,Df}$$
$$= \frac{1}{2}\left[\left|\phi^{+}\right\rangle(|{+}{+}\rangle - |{-}{-}\rangle) + \left|\phi^{-}\right\rangle(|{-}{+}\rangle - |{+}{-}\rangle)\right]_{hf,Df,tf,C}. \quad (4)$$

In the same time, Bob and David will deduce Alice's information through cooperation. After getting all the shuffled information published by Alice and Charlie, Bob and David will keep the sequence S_t and the sequence S_B respectively, then they perform measurement on the photons in S_t and the corresponding photons in S_B. In the same time, they also know the photons' initial states in S_B and S_D as they were produced by them. In the condition that Bob's measurement result on the photons in S_t is $|+\rangle$ and the initial state of the corresponding photons in S_B is $|0\rangle$. There are following four situations.

(a) If David remembers that the initial state of the corresponding photons in S_D is $|0\rangle$ while his measurement result of the corresponding photons in S_B is $|+\rangle$, through the analysis the Eq. (5), Bob and David can deduce that Alice's measurement result must be is $\left|\phi^{+}\right\rangle$.

$$|U\rangle_0 = CNOT_{BD} \cdot CNOT_{tB}\left|\phi^{+}\right\rangle_{ht}|0\rangle_B|0\rangle_D$$
$$= \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)_{htBD}$$
$$= \frac{1}{2}\left[\left|\phi^{+}\right\rangle(|{+}{+}\rangle + |{-}{-}\rangle) + \left|\phi^{-}\right\rangle(|{+}{-}\rangle + |{-}{+}\rangle)\right]_{hDtB}, \quad (5)$$

$$|U\rangle_1 = CNOT_{BD} \cdot CNOT_{tB}\left|\phi^{+}\right\rangle_{ht}|0\rangle_B|1\rangle_D$$
$$= \frac{1}{\sqrt{2}}(|0001\rangle + |1110\rangle)_{htBD}$$
$$= \frac{1}{2}\left[\left|\psi^{+}\right\rangle(|{+}{+}\rangle + |{-}{-}\rangle) + \left|\psi^{-}\right\rangle(|{+}{-}\rangle + |{-}{+}\rangle)\right]_{hDtB}, \quad (6)$$

$$|U\rangle_2 = CNOT_{BD} \cdot CNOT_{tB}\left|\phi^{+}\right\rangle_{ht}|1\rangle_B|0\rangle_D$$
$$= \frac{1}{\sqrt{2}}(|0011\rangle + |1100\rangle)_{htBD}$$
$$= \frac{1}{2}\left[\left|\psi^{+}\right\rangle(|{+}{+}\rangle - |{-}{-}\rangle) + \left|\psi^{-}\right\rangle(|{-}{+}\rangle - |{+}{-}\rangle)\right]_{hDtB}, \quad (7)$$

$$|U\rangle_3 = CNOT_{BD} \cdot CNOT_{tB}\left|\phi^{+}\right\rangle_{ht}|1\rangle_B|1\rangle_D$$
$$= \frac{1}{\sqrt{2}}(|0010\rangle + |1101\rangle)_{htfBD}$$
$$= \frac{1}{2}\left[\left|\phi^{+}\right\rangle(|{+}{+}\rangle - |{-}{-}\rangle) + \left|\phi^{-}\right\rangle(|{-}{+}\rangle - |{+}{-}\rangle)\right]_{hDtB}. \quad (8)$$

Table 2 Relations among joint bits of Bob's initial prepared bit adding measurement result, joint bits of David's initial prepared bit adding measurement result and Alice's measurement result. Joint bits of Bob's initial bit adding measurement result are listed in the first column, joint bits of David's initial bit adding measurement result are listed in the first row

	$\|0\rangle\|+\rangle$	$\|0\rangle\|-\rangle$	$\|1\rangle\|+\rangle$	$\|1\rangle\|-\rangle$
$\|0\rangle\|+\rangle$	$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$
$\|0\rangle\|-\rangle$	$\|\phi^-\rangle$	$\|\phi^+\rangle$	$\|\psi^-\rangle$	$\|\psi^+\rangle$
$\|1\rangle\|+\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|\phi^+\rangle$	$\|\phi^-\rangle$
$\|1\rangle\|-\rangle$	$\|\psi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|\phi^+\rangle$

(b) If David remembers that the initial state of the corresponding photons in S_D is $|0\rangle$ while his measurement result of the corresponding photons in S_B is $|-\rangle$, through the analysis the Eq. (5), Bob and David can deduce that Alice's measurement result must be $|\phi^-\rangle$.

(c) If David remembers that the initial state of the corresponding photons in S_D is $|1\rangle$ while his measurement result of the corresponding photons in S_B is $|+\rangle$, through the analysis the Eq. (6), Bob and Charlie can deduce that Alice's measurement result must be $|\psi^+\rangle$.

(d) If David remembers that the initial state of the corresponding photons in S_D is $|1\rangle$ while his measurement result of the corresponding photons in S_B is $|-\rangle$, through the analysis the Eq. (6), Bob and Charlie can deduce that Alice's measurement result must be $|\psi^-\rangle$.

For simplicity, the discussion of the situations that David's initial prepared bit adding measurement results are $|0\rangle|-\rangle$, $|1\rangle|+\rangle$ and $|1\rangle|-\rangle$ are omitted here, Table 2 gives the details of these relations among joint bits of Bob's initial prepared bit adding measurement result, joint bits of David's initial prepared bit adding measurement result and Alice's measurement result.

In the next, we will show how Bob and David can escape from being detected in the final public discussion. Through the analysis above, we know that Bob and David get all the information of Alice's secret and Charlie's secret. After having known the positions of the selected half of the key bits in K_A, Bob and David first find this half key bits and the corresponding joint bits of Charlie's initial prepared bits adding measurement results, they can get the information which they should publish in the discussion through the analyzing of the following equations.

$$
\begin{aligned}
|W\rangle_0 &= CNOT_{CD}\cdot CNOT_{BC}\cdot CNOT_{tB}\,|\phi^+\rangle_{ht}\,|0\rangle_B\,|0\rangle_C\,|0\rangle_D \\
&= \frac{1}{\sqrt{2}}\left(|00000\rangle + |11111\rangle\right)_{htBCD} \\
&= \frac{1}{2\sqrt{2}}\Big[|\phi^+\rangle\left(|+++\rangle + |--+\rangle + |+--\rangle + |-+-\rangle\right) \\
&\quad + |\phi^-\rangle\left(|+-+\rangle + |-++\rangle + |++-\rangle + |---\rangle\right)\Big]_{hDtBC}, \qquad (9) \\
|W\rangle_1 &= CNOT_{CD}\cdot CNOT_{BC}\cdot CNOT_{tB}\,|\phi^+\rangle_{ht}\,|0\rangle_B\,|0\rangle_C\,|1\rangle_D
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{1}{\sqrt{2}}\left(|00001\rangle + |11110\rangle\right)_{htBCD} \\
&= \frac{1}{2\sqrt{2}}\Big[\left|\psi^{+}\right\rangle\left(|+++\rangle + |--+\rangle + |+--\rangle + |-+-\rangle\right) \\
&\quad + \left|\psi^{-}\right\rangle\left(|+-+\rangle + |-++\rangle + |++-\rangle + |---\rangle\right)\Big]_{htBCD}, \qquad (10)\\
|W\rangle_2 &= CNOT_{CD}\cdot CNOT_{BC}\cdot CNOT_{tB}\left|\phi^{+}\right\rangle_{ht}|0\rangle_B|1\rangle_C|0\rangle_D \\
&= \frac{1}{\sqrt{2}}\left(|00011\rangle + |11100\rangle\right)_{htBCD} \\
&= \frac{1}{2\sqrt{2}}\Big[\left|\psi^{+}\right\rangle\left(|+++\rangle + |--+\rangle - |+--\rangle - |-+-\rangle\right) \\
&\quad + \left|\psi^{-}\right\rangle\left(|+-+\rangle + |-++\rangle - |++-\rangle - |---\rangle\right)\Big]_{htBCD}, \qquad (11)\\
|W\rangle_3 &= CNOT_{CD}\cdot CNOT_{BC}\cdot CNOT_{tB}\left|\phi^{+}\right\rangle_{ht}|0\rangle_B|1\rangle_C|1\rangle_D \\
&= \frac{1}{\sqrt{2}}\left(|00010\rangle + |11101\rangle\right)_{htBCD} \\
&= \frac{1}{2\sqrt{2}}\Big[\left|\phi^{+}\right\rangle\left(|+++\rangle + |--+\rangle - |+--\rangle - |-+-\rangle\right) \\
&\quad + \left|\phi^{-}\right\rangle\left(|+-+\rangle + |-++\rangle - |++-\rangle - |---\rangle\right)\Big]_{htBCD}, \qquad (12)\\
|W\rangle_4 &= CNOT_{CD}\cdot CNOT_{BC}\cdot CNOT_{tB}\left|\phi^{+}\right\rangle_{ht}|1\rangle_B|0\rangle_C|0\rangle_D \\
&= \frac{1}{\sqrt{2}}\left(|00111\rangle + |11000\rangle\right)_{htBCD} \\
&= \frac{1}{2\sqrt{2}}\Big[\left|\psi^{+}\right\rangle\left(|+++\rangle - |--+\rangle + |+--\rangle - |-+-\rangle\right) \\
&\quad + \left|\psi^{-}\right\rangle\left(|-++\rangle - |+-+\rangle - |++-\rangle + |---\rangle\right)\Big]_{htBCD}, \qquad (13)\\
|W\rangle_5 &= CNOT_{CD}\cdot CNOT_{BC}\cdot CNOT_{tB}\left|\phi^{+}\right\rangle_{ht}|1\rangle_B|0\rangle_C|1\rangle_D \\
&= \frac{1}{\sqrt{2}}\left(|00110\rangle + |11001\rangle\right)_{htBCD} \\
&= \frac{1}{2\sqrt{2}}\Big[\left|\phi^{+}\right\rangle\left(|+++\rangle - |--+\rangle + |+--\rangle - |-+-\rangle\right) \\
&\quad + \left|\phi^{-}\right\rangle\left(|---\rangle - |+-+\rangle + |-++\rangle - |+++\rangle\right)\Big]_{hDtBC}, \qquad (14)\\
|W\rangle_6 &= CNOT_{CD}\cdot CNOT_{BC}\cdot CNOT_{tB}\left|\phi^{+}\right\rangle_{ht}|1\rangle_B|1\rangle_C|0\rangle_D \\
&= \frac{1}{\sqrt{2}}\left(|00100\rangle + |11011\rangle\right)_{htBCD} \\
&= \frac{1}{2\sqrt{2}}\Big[\left|\phi^{+}\right\rangle\left(|+++\rangle - |--+\rangle - |+--\rangle + |-+-\rangle\right) \\
&\quad + \left|\phi^{-}\right\rangle\left(|++-\rangle - |+-+\rangle + |-++\rangle - |---\rangle\right)\Big]_{hDtBC}, \qquad (15)\\
|W\rangle_7 &= CNOT_{CD}\cdot CNOT_{BC}\cdot CNOT_{tB}\left|\phi^{+}\right\rangle_{ht}|1\rangle_B|1\rangle_C|1\rangle_D \\
&= \frac{1}{\sqrt{2}}\left(|00101\rangle + |11010\rangle\right)_{htBCD}
\end{aligned}
$$

$$= \frac{1}{2\sqrt{2}}\left[\left|\psi^{+}\right\rangle(|++\rangle - |--+\rangle + |+--\rangle - |-+-\rangle) + \left|\psi^{-}\right\rangle(|-++\rangle - |+-+\rangle - |++-\rangle + |---\rangle)\right]_{htBCD}. \quad (16)$$

We assume that Alice's key bit is $\left|\phi^{+}\right\rangle$, there are following four situations.

(a) If Charlie's two-bit shadow key is $|0+\rangle$, through analyzing the Eqs. (9) and (14), Bob and David can publish their two-bit shadow key are $|0+\rangle$ and $|0+\rangle$, $|0-\rangle$ and $|0-\rangle$, $|1+\rangle$ and $|1+\rangle$ or $|1-\rangle$ and $|1-\rangle$ respectively.

(b) If Charlie's two-bit shadow key is $|0-\rangle$, through analyzing the Eqs. (9) and (14), Bob and David can publish their two-bit shadow key are $|0+\rangle$ and $|0-\rangle$, $|0-\rangle$ and $|0+\rangle$, $|1-\rangle$ and $|1+\rangle$ or $|1+\rangle$ and $|1-\rangle$ respectively.

(c) If Charlie's two-bit shadow key is $|1+\rangle$, through analyzing the Eqs. (11) and (15), Bob and David can publish their two-bit shadow key are $|0+\rangle$ and $|1+\rangle$, $|0-\rangle$ and $|1-\rangle$, $|1+\rangle$ and $|0+\rangle$ or $|1-\rangle$ and $|0-\rangle$ respectively.

(d) If Charlie's two-bit shadow key is $|1-\rangle$, through analyzing the Eqs. (11) and (15), Bob and David can publish their two-bit shadow key are $|0-\rangle$ and $|1+\rangle$, $|0+\rangle$ and $|1-\rangle$, $|1-\rangle$ and $|0+\rangle$ or $|1+\rangle$ and $|0-\rangle$ respectively. For simplicity, the discussion of the situations that Alice's key bit are $\left|\phi^{-}\right\rangle$, $\left|\psi^{+}\right\rangle$ and $\left|\psi^{-}\right\rangle$ are omitted here.

Table 3 gives the details of these relations among Alice's key bit, Charlie's two-bit shadow key and the set of two-bit shadow keys published by Bob and David

Table 3 Relations among Alice's key bit, Charlie's two-bit shadow key and two-bit shadow keys published by Bob and David. Alice's key bits are listed in the first column, Charlie's two-bit shadow key are listed in the first row

	$\|0+\rangle$	$\|0-\rangle$	$\|1+\rangle$	$\|1-\rangle$
$\left\|\varphi^{+}\right\rangle$	$(\|0+\rangle, \|0+\rangle)$	$(\|0+\rangle, \|0-\rangle)$	$(\|0+\rangle, \|1+\rangle)$	$(\|0-\rangle, \|1+\rangle)$
	$(\|0-\rangle, \|0-\rangle)$	$(\|0-\rangle, \|0+\rangle)$	$(\|0-\rangle, \|1-\rangle)$	$(\|0+\rangle, \|1-\rangle)$
	$(\|1+\rangle, \|1+\rangle)$	$(\|1-\rangle, \|1+\rangle)$	$(\|1+\rangle, \|0+\rangle)$	$(\|1-\rangle, \|0+\rangle)$
	$(\|1-\rangle, \|1-\rangle)$	$(\|1+\rangle, \|1-\rangle)$	$(\|1-\rangle, \|0-\rangle)$	$(\|1+\rangle, \|0-\rangle)$
$\left\|\varphi^{-}\right\rangle$	$(\|0-\rangle, \|0+\rangle)$	$(\|0+\rangle, \|0+\rangle)$	$(\|0-\rangle, \|1+\rangle)$	$(\|0+\rangle, \|1+\rangle)$
	$(\|0+\rangle, \|0-\rangle)$	$(\|0-\rangle, \|0-\rangle)$	$(\|0+\rangle, \|1-\rangle)$	$(\|0-\rangle, \|1-\rangle)$
	$(\|1-\rangle, \|1+\rangle)$	$(\|1+\rangle, \|1+\rangle)$	$(\|1+\rangle, \|0-\rangle)$	$(\|1+\rangle, \|0+\rangle)$
	$(\|1+\rangle, \|1-\rangle)$	$(\|1-\rangle, \|1-\rangle)$	$(\|1-\rangle, \|0+\rangle)$	$(\|1-\rangle, \|0-\rangle)$
$\left\|\psi^{+}\right\rangle$	$(\|0+\rangle, \|1+\rangle)$	$(\|0-\rangle, \|1+\rangle)$	$(\|0+\rangle, \|0+\rangle)$	$(\|0-\rangle, \|0+\rangle)$
	$(\|0-\rangle, \|1-\rangle)$	$(\|0+\rangle, \|1-\rangle)$	$(\|0-\rangle, \|0-\rangle)$	$(\|0+\rangle, \|0-\rangle)$
	$(\|1+\rangle, \|0+\rangle)$	$(\|1-\rangle, \|0+\rangle)$	$(\|1+\rangle, \|1+\rangle)$	$(\|1-\rangle, \|1+\rangle)$
	$(\|1-\rangle, \|0-\rangle)$	$(\|1+\rangle, \|0-\rangle)$	$(\|1-\rangle, \|1-\rangle)$	$(\|1+\rangle, \|1-\rangle)$
$\left\|\psi^{-}\right\rangle$	$(\|0-\rangle, \|0+\rangle)$	$(\|1+\rangle, \|0+\rangle)$	$(\|0-\rangle, \|0+\rangle)$	$(\|0+\rangle, \|0+\rangle)$
	$(\|0+\rangle, \|0-\rangle)$	$(\|1-\rangle, \|0-\rangle)$	$(\|0+\rangle, \|0-\rangle)$	$(\|0-\rangle, \|0-\rangle)$
	$(\|1-\rangle, \|0+\rangle)$	$(\|0+\rangle, \|1+\rangle)$	$(\|1-\rangle, \|1+\rangle)$	$(\|1+\rangle, \|1+\rangle)$
	$(\|1+\rangle, \|0-\rangle)$	$(\|0-\rangle, \|1-\rangle)$	$(\|1+\rangle, \|1-\rangle)$	$(\|1-\rangle, \|1-\rangle)$

respectively. For any pair of Alice's key bit and Charlie's shadow key, there are four possibilities Bob and David can choose to publish. It is obvious that the agent Charlie and the boss Alice cannot find this cheat. However, Bob and David can access Alice's secret message. Therefore, LH protocol [34] is not secure.

Actually, Bob does not need to shuffle S_{tf} and S_B to get S'_{tf} and S'_B, and then insert N decoy photons into S'_{tf} and S'_B to form S^*_{tf} and S^*_B respectively. David does not need to shuffle S_{Df} and S_D to get S'_{Df} and S'_D, and then further insert N decoy photons into S'_{Df} and S'_D to form S^*_{Df} and S^*_D respectively too. These actions are just to make sure that Bob and David's attacks can not be attacked by another attacker again.

We point out that if there are more than four parties are involved, LH protocol [34] still can not satisfy the security requirement of QSS as that the first agent and the last agent can control all the transmission channels between the agents and the Boss, it is difficult to prevent this attack if we do not change the protocol greatly.

It is important and interesting to consider following question. In the LH protocol [34], the authors claim that the scenario is as follows. The dealer Alice wants to send a secret key to three agents, she will first split the key into three shadows, which will later be delivered to Bob, Charlie, and David, respectively, the three agents can deduce the key if and only if they cooperate. However, the real scenario is precisely opposite to the description in the LH protocol [34], Alice's key is determined by the sequences which agents choose as for the target qubits and the corresponding measurement results. So the sharing secret information of LH protocol are determined by the agents but not the boss Alice, if the boss Alice wants the agents to share the secret pre-prepared by herself, LH protocol can not meet the her aspiration easily.

In summary, we propose a special attack strategy on LH protocol [34], in which the agent Bob and the agent David can fully extract the Boss Alice's secret key without introducing any error. We hope that the special attack is noticed in the following research.

Acknowledgments This work is supported by the National Natural Science Foundation of China, Grant No. 61101088, and the National Key Technology R&D Program, Grant No. 2012BAH38B05.

References

1. Wiesner, S.: Conjugate Coding. SIGACT News **15**, 78–88 (1983)
2. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: Proceedings IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, pp. 175–179. IEEE, New York (1984)
3. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**, 656–715 (1949)
4. Zeng, G.H., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A **65**(4), 042312 (2002)
5. Crépeau, C., Salvail, L.: Quantum oblivious mutual identification. In: Proceedings of Eurocrypt, pp. 133–147. Springer, Berlin (1995)
6. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**(3), 1829–1834 (1999)
7. Gottesman, D.: Theory of quantum secret sharing. Phys. Rev. A **61**(4), 042311 (2000)
8. Guo, G.P., Guo, G.C.: Quantum secret sharing without entanglement. Phys. Lett. A **310**(4), 247–251 (2003)
9. Hsu, L.Y.: Quantum secret-sharing protocol based on Grover's algorithm. Phys. Rev. A **68**(2), 022306 (2003)

10. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A **69**(5), 052307 (2004)
11. Li, Y., Zhang, K., Peng, K.: Multiparty secret sharing of quantum information based on entanglement swapping. Phys. Lett. A **324**(5-6), 420–424 (2004)
12. Hsu, L.Y., Li, C.M.: Quantum secret sharing using product states. Phys. Rev. A **71**(2), 022321 (2005)
13. Zhang, Z.J., Man, Z.X.: Multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys. Rev. A **72**(2), 022303 (2005)
14. Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A **72**(4), 044302 (2005)
15. Deng, F.G., Long, G.L., Zhou, H.Y.: An efficient quantum secret sharing scheme with Einstein-Podolsky-Rosen pairs. Phys. Lett. A **340**(1-4), 43–50 (2005)
16. Zhang, Z.J., Li, Y., Man, Z.X.: Multiparty quantum secret sharing. Phys. Rev. A **71**(4), 044301 (2005)
17. Zhang, Z.J.: Multiparty quantum secret sharing of secure direct communication. Phys. Lett. A **342** (1-2), 60–66 (2005)
18. Deng, F.G., Zhou, H.Y., Long, G.L.: Circular quantum secret sharing. J. Phys. A Math. Gen. **39**(45), 14089–14099 (2006)
19. Zhou, P., Li, X.H., Liang, Y.J., Deng, F.G., Zhou, H.Y.: Multiparty quantum secret sharing with pure entangled states and decoy photons. Phys. A **381**, 164–169 (2007)
20. Zhang, Z.J., Gao, G., Wang, X., Han, L.F., Shi, S.H.: Multiparty quantum secret sharing based on the improved Boström-Felbinger protocol. Opt. Commun. **269**(2), 418–422 (2007)
21. Han, L.F., Liu, Y.M., Liu, J., Zhang, Z.J.: Multiparty quantum secret sharing of secure direct communication using single photons. Opt. Commun. **281**(9), 2690–2694 (2008)
22. Wang, T.Y., Wen, Q.Y., Chen, X.B., Guo, F.Z., Zhu, F.C.: An efficient and secure multiparty quantum secret sharing scheme based on single photons. Opt. Commun. **281**(24), 6130–6134 (2008)
23. Deng, F.G., Li, X.H., Zhou, H.Y.: Efficient high-capacity quantum secret sharing with two-photon entanglement. Phys. Lett. A **372**(12), 1957–1962 (2008)
24. Gu, B., Li, C.Q., Xu, F., Chen, Y.L.: High-capacity three-party quantum secret sharing with superdense coding. Chin. Phys. B **18**(11), 4690–4694 (2009)
25. Sun, Y., Wen, Q.Y., Gao, F., Chen, X.B., Zhu, F.C.: Multiparty quantum secret sharing based on Bell measurement. Opt. Commun. **282**(17), 3647–3651 (2009)
26. Gu, B., Mu, L., Ding, L., Zhang, C., Li, C.: Fault tolerant three-party quantum secret sharing against collective noise. Opt. Commun. **283**(15), 3099–3103 (2010)
27. Zhu, Z.C., Zhang, Y.Q.: Cryptanalysis and improvement of a quantum secret sharing protocol between multiparty and multiparty with single photons and unitary transformations. Chin. Phys. Lett. **27**(6), 060303 (2010)
28. Shi, R.H., Huang, L.S., Yang, W., Zhong, H.: Multiparty quantum secret sharing with Bell states and Bell measurements. Opt. Commun. **283**(11), 2476–2480 (2010)
29. Zhu, Z.C., Zhang, Y.Q., Fu, A.M.: Efficient quantum secret sharing scheme with two-particle entangled states. Chin. Phys. B **20**(4), 040306 (2011)
30. Lin, J., Hwang, T.: An enhancement on Shi et al.'s multiparty quantum secret sharing protocol. Opt. Commun. **284**(5), 1468–1471 (2011)
31. Zhu, Z.C., Zhang, Y.Q., Fu, A.M.: Comment on "Reply to Comment on 'Efficient high-capacity quantum secret sharing with two-photon entanglement'". Int. J. Theor. Phys. **50**(1), 308–313 (2011)
32. Yang, C.W., Tsai, C.W., Hwang, T.: Thwarting intercept-and-resend attack on Zhang's quantum secret sharing using collective rotation noises. Quantum Inf. Process. **11**(1), 113–122 (2012)
33. Zhu, Z.C., Zhang, Y.Q., Fu, A.M.: Cryptanalysis and improvement of a quantum secret sharing scheme based on χ-type entangled states. Chin. Phys. B **21**(1), 010307 (2012)
34. Lin, J., Hwang, T.: New circular quantum secret sharing for remote agents. Quantum Inf. Process. (2012). doi:10.1007/s11128-012-0413-8