Quantum Information Processing (2021) 20:7
https://doi.org/10.1007/s11128-020-02916-x

COMMENT

Analysis of efficient and secure dynamic quantum secret sharing protocol based on Bell states

Tian-Yin Wang[1,2] · Xiao-Xuan Wang[1] · Xiao-Qiu Cai[1] · Chun-Yan Wei[1] · Rui-Ling Zhang[3]

Received: 8 June 2020 / Accepted: 27 October 2020 / Published online: 6 January 2021

Abstract
Dynamic secret sharing can deal with the problems of both adding agents and revoking ones, which makes it more practical and flexible compared with general secret sharing. In this work, we analyze an efficient and secure dynamic quantum secret sharing protocol based on Bell states, and find that there is an unnoticed problem that it does not satisfy the requirement for dynamic secret sharing in the sense that if the access structure has been completed, then both adding an agent and revoking one become impossible by the way in this protocol; or else if adding an agent or revoking one can be realized, then the previous access structure has not been implemented in fact. Furthermore, we discuss how to solve this problem and give a possible way to improve this protocol.

Keywords Quantum secret sharing · Dynamic secret sharing · Bell states

1 Introduction

Quantum secret sharing is a basic primitive in quantum cryptography, which was firstly introduced by Hillery, Buzěk and Berthiaume [1]. In contrast to classical secret sharing [2], the security of quantum secret sharing is based on the fundamental principles of

✉ Tian-Yin Wang
wangtianyin79@163.com

Xiao-Qiu Cai
xiaoqiucai@aliyun.com

Rui-Ling Zhang
ruilingzhang@163.com

1 School of Mathematical Science, Luoyang Normal University, Luoyang 471934, China

2 Smart Travel Collaborative Innovation Center of Zhongyuan Economic Area, Luoyang Normal University, Luoyang 471934, China

3 School of Information Technology, Luoyang Normal University, Luoyang 471934, China

quantum physics such as no-cloning of unknown quantum states, and hence quantum secret sharing allows a dealer to securely distribute a secret among agents in the presence of opponents even if they have infinite computing resources. Contributing to the superiority of information-theoretic security, quantum secret sharing has attracted much attention, and numerous proposals for quantum secret sharing have been reported including both theoretical and experimental aspects [3–14].

Secret sharing has many practical applications in the field of information security and distributed computing, and it is inevitable to add a new agent or delete one due to various reasons in some special cases. For example, in a large company, there are a lot of persons who may join in it, while some employees quit from it every week. A simple way is to restart the secret distribution algorithm and then renew the shared secret while distributing a new share for each agent. However, this way is generally costly and will limit the practical application of secret sharing. Accordingly, the concept of dynamic secret sharing protocols was introduced, in which the number of the agents can be increased or decreased without re-executing the secret distribution algorithm, and thus, it gives an economical and convenient way to solve this problem. So far, a lot of dynamic secret sharing schemes have been presented [15], especially in the field of quantum secret sharing; Yang et al. firstly gave a dynamic quantum secret sharing scheme in 2011, which was the beginning of the research of dynamic quantum secret sharing [16]. After that, both the design and cryptanalysis of dynamic quantum secret sharing schemes attracted much attention [17–29].

Recently, an efficient and secure dynamic quantum secret sharing protocol based on Bell states was reported (for the sake of simplicity, we will call it YT-protocol hereafter) [30]. Furthermore, as mentioned in [30], the YT-protocol has the following merits over the existing protocols. Firstly, it is immune to eavesdropping attack, collusion attack, and the dishonest revoked agent attack. Secondly, it is secure against Trojan horse attack because one-step photon transmission is adopted. Thirdly, it is simple and efficient because the agents only perform a single-particle measurement. Finally, when adding or revoking an agent in the YT-protocol, the remaining agents need not perform any local unitary operation, transmit classical messages, or be online.

In this paper, we give an analysis of the YT-protocol, and find that there is a neglected problem that it does not satisfy the requirement for dynamic secret sharing in the sense that if the access structure has been completed, then both adding an agent and revoking one become impossible by the way in this protocol; otherwise, if adding a new agent or revoking one is realized, then the previous access structure has not been really implemented, i.e., the agents cannot recover the shared secret even if they cooperate with each other before the phase of adding a new agent or revoking one. Finally, we discuss how to solve this problem and give a way to improve this protocol.

The rest of this paper is organized as follows. In Sect. 2, a brief description of the YT-protocol is reviewed. In Sect. 3, we analyze the YT-protocol and then show the existing problem in this protocol. In Sect. 4, we study how to deal with this problem and improve this problem. Finally, conclusions are given in Sect. 5.

2 The YT-protocol

In this section, let us give a brief description of YT-protocol [30]. Without loss of generality, we take the four-party dynamic quantum secret sharing as an example. Suppose that the dealer (Alice) wants her master key to be shared among three agents (Bob, Charlie and David) in such a way that her master key can be recovered if and only if all agents cooperate together. The four-party YT-protocol can be described as follows.

2.1 The four-party protocol

The four-party YT-protocol includes the following several steps.

Step 1 Alice prepares $3n$ Bell states $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and then equally divides the $3n$ states $|\Phi^+\rangle$ into three segments $\mathtt{BS}_B = \{q_1^{\mathtt{BS}_B^i}, q_2^{\mathtt{BS}_B^i}\}$, $\mathtt{BS}_C = \{q_1^{\mathtt{BS}_C^i}, q_2^{\mathtt{BS}_C^i}\}$, and $\mathtt{BS}_D = \{q_1^{\mathtt{BS}_D^i}, q_2^{\mathtt{BS}_D^i}\}$ for $i = 1, 2, \ldots, n$. Then, she takes all the first and second particles from each Bell state in each segment to form the ordered sequences $S_1^{\mathtt{BS}_B} = \{q_1^{\mathtt{BS}_B^i}\}$, $S_2^{\mathtt{BS}_B} = \{q_2^{\mathtt{BS}_B^i}\}$, $S_1^{\mathtt{BS}_C} = \{q_1^{\mathtt{BS}_C^i}\}$, $S_2^{\mathtt{BS}_C} = \{q_2^{\mathtt{BS}_C^i}\}$, $S_1^{\mathtt{BS}_D} = \{q_1^{\mathtt{BS}_D^i}\}$, $S_2^{\mathtt{BS}_D} = \{q_2^{\mathtt{BS}_D^i}\}$. Alice prepares n decoy photons randomly chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and then inserts them into the sequences $S_2^{\mathtt{BS}_B}$, $S_2^{\mathtt{BS}_C}$, $S_2^{\mathtt{BS}_D}$ to form $S_2^{'\mathtt{BS}_B}$, $S_2^{'\mathtt{BS}_C}$, $S_2^{'\mathtt{BS}_D}$, respectively. Finally, she sends $S_2^{'\mathtt{BS}_B}$, $S_2^{'\mathtt{BS}_C}$, $S_2^{'\mathtt{BS}_D}$ to Bob, Charlie, David, respectively, and keeps $S_1^{\mathtt{BS}_B}$, $S_1^{\mathtt{BS}_C}$, $S_1^{\mathtt{BS}_D}$ for herself.

Step 2 After receiving the sequences $S_2^{'\mathtt{BS}_B}$, $S_2^{'\mathtt{BS}_C}$, $S_2^{'\mathtt{BS}_D}$ from Alice, Bob, Charlie, and David individually send an acknowledgment to her. Then, Alice announces both the bases and the positions of the decoy photons in $S_2^{'\mathtt{BS}_B}$, $S_2^{'\mathtt{BS}_C}$, $S_2^{'\mathtt{BS}_D}$. According to the measurement results of Bob, Charlie and David, Alice checks eavesdropping. If no eavesdropping is detected, she sends an acknowledgment to Bob (Charlie and David) through an authenticated classical channel. Otherwise, Alice asks Bob (Charlie and David) to abort the process and starts a new one.

Step 3 After the eavesdropping check, Alice has three sequences $S_1^{\mathtt{BS}_B}$, $S_1^{\mathtt{BS}_C}$, $S_1^{\mathtt{BS}_D}$, Bob, Charlie and David have $S_2^{\mathtt{BS}_B}$, $S_2^{\mathtt{BS}_C}$ and $S_2^{\mathtt{BS}_D}$, respectively. Then, she gets the measurement results $\mathtt{MR}_A = \{\mathtt{MR}_{A_1}, \mathtt{MR}_{A_2}, \ldots, \mathtt{MR}_{A_n}\}$ by performing the GHZ measurement on the ith particles (i.e., $q_1^{\mathtt{BS}_B^i}, q_1^{\mathtt{BS}_C^i}, q_1^{\mathtt{BS}_D^i}$) from $S_1^{\mathtt{BS}_B}$, $S_1^{\mathtt{BS}_C}$, $S_1^{\mathtt{BS}_D}$ for $i = 1, 2, \ldots, n$. Bob, Charlie, and David get the measurement results $\mathtt{MR}_B = \{\mathtt{MR}_{B_1}, \mathtt{MR}_{B_2}, \ldots, \mathtt{MR}_{B_n}\}$, $\mathtt{MR}_C = \{\mathtt{MR}_{C_1}, \mathtt{MR}_{C_2}, \ldots, \mathtt{MR}_{C_n}\}$, $\mathtt{MR}_D = \{\mathtt{MR}_{D_1}, \mathtt{MR}_{D_2}, \ldots, \mathtt{MR}_{D_n}\}$, respectively, by performing the X-basis measurements on each particle in their sequences.

Step 4 According to the correlation of particles held by Alice, Bob, Charlie and David, their measurement results satisfy $\mathtt{MR}_A = \mathtt{MR}_B \oplus \mathtt{MR}_C \oplus \mathtt{MR}_D$; hereafter, the notation $\oplus$ denotes the addition of modulo 2. Therefore, if Bob, Charlie and David collaborate with each other, they can recover Alice's master key as $K_A = \mathtt{MR}_A = \mathtt{MR}_B \oplus \mathtt{MR}_C \oplus \mathtt{MR}_D = K_B \oplus K_C \oplus K_D$.

2.2 Adding a new agent

Assume that a new agent (Frank) wants to join the four-party protocol. Then, he can perform the following steps with Alice to complete this task.

Step A1 Alice prepares n Bell states $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and divides them into two sequences $S_1^{\mathrm{BS}_F} = \{q_1^{\mathrm{BS}_F^i}\}$, $S_2^{\mathrm{BS}_F} = \{q_2^{\mathrm{BS}_F^i}\}$. Then, she randomly inserts n decoy photons (i.e., $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$) into the sequence $S_2^{\mathrm{BS}_F}$ to form $S_2^{'\mathrm{BS}_F}$, and sends $S_2^{'\mathrm{BS}_F}$ to Frank.

Step A2 After confirming Frank has received $S_2^{'\mathrm{BS}_F}$, Alice performs a similar eavesdropping check with Frank to confirm the security of $S_2^{\mathrm{BS}_F}$.

Step A3 Alice performs the GHZ measurement on the ith particles (i.e., $q_1^{\mathrm{BS}_B^i}, q_1^{\mathrm{BS}_C^i}, q_1^{\mathrm{BS}_D^i}, q_1^{\mathrm{BS}_F^i}$) from $S_1^{\mathrm{BS}_B}$, $S_1^{\mathrm{BS}_C}$, $S_1^{\mathrm{BS}_D}$, $S_1^{\mathrm{BS}_F}$ for $i = 1, 2, \ldots, n$, to obtain the measurement results $\mathtt{MR}_{A'} = \{\mathtt{MR}_{A'_1}, \mathtt{MR}_{A'_2}, \ldots, \mathtt{MR}_{A'_n}\}$. Bob, Charlie, David and Frank get the measurement results $\mathtt{MR}_{B'} = \{\mathtt{MR}_{B'_1}, \mathtt{MR}_{B'_2}, \ldots, \mathtt{MR}_{B'_n}\}$, $\mathtt{MR}_{C'} = \{\mathtt{MR}_{C'_1}, \mathtt{MR}_{C'_2}, \ldots, \mathtt{MR}_{C'_n}\}$, $\mathtt{MR}_{D'} = \{\mathtt{MR}_{D'_1}, \mathtt{MR}_{D'_2}, \ldots, \mathtt{MR}_{D'_n}\}$, and $\mathtt{MR}_{F'} = \{\mathtt{MR}_{F'_1}, \mathtt{MR}_{F'_2}, \ldots, \mathtt{MR}_{F'_n}\}$, respectively, by performing the X-basis measurement on each particle in their sequences.

Step A4 Let Alice's master key be $K_{A'} = \mathtt{MR}_{A'}$. Bob, Charlie, David and Frank can recover Alice's master key as $\mathtt{MR}_{A'} = \mathtt{MR}_{B'} \oplus \mathtt{MR}_{C'} \oplus \mathtt{MR}_{D'} \oplus \mathtt{MR}_{F'}$ by cooperation.

2.3 Revoking an agent

Here, we consider a five-party case, i.e., one dealer (Alice) and four agents (Bob, Charlie, David and Frank). Alice has four sequences $S_1^{\mathrm{BS}_B}, S_1^{\mathrm{BS}_C}, S_1^{\mathrm{BS}_D}, S_1^{\mathrm{BS}_F}$, and Bob, Charlie, David and Frank have the sequences $S_2^{\mathrm{BS}_B}, S_2^{\mathrm{BS}_C}, S_2^{\mathrm{BS}_D}, S_2^{\mathrm{BS}_F}$, respectively. If Alice wants to revoke Bob, then she performs the GHZ measurement only on the ith particles from $S_1^{\mathrm{BS}_C}, S_1^{\mathrm{BS}_D}, S_1^{\mathrm{BS}_F}$, for $i = 1, 2, ..., n$, to obtain the measurement results $\mathtt{MR}_{A''} = \{\mathtt{MR}_{A''_1}, \mathtt{MR}_{A''_2}, \ldots, \mathtt{MR}_{A''_n}\}$. Then $S_2^{\mathrm{BS}_C}$, $S_2^{\mathrm{BS}_D}$ and $S_2^{\mathrm{BS}_F}$ evolve into n GHZ states, similar to $\mathtt{MR}_{A''}$. Consequently, Alice's master key becomes $K_{A''} = \mathtt{MR}_{A''} = \mathtt{MR}_C \oplus \mathtt{MR}_D \oplus \mathtt{MR}_F$ by this way.

3 The analysis of YT-protocol

From Sect. 2, it can be seen that after the secure distributing of particles, the dealer Alice holds all the first particles $S_1^{\mathrm{BS}_B}, S_1^{\mathrm{BS}_C}, S_1^{\mathrm{BS}_D}$ of $3n$ Bell states $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and the three agents Bob, Charlie and David have the n second particles $S_2^{\mathrm{BS}_B}, S_2^{\mathrm{BS}_C}$ and $S_2^{\mathrm{BS}_D}$ of these $3n$ Bell states. Furthermore, if Alice performs the GHZ measurement on the ith particles (i.e., $q_1^{\mathrm{BS}_B^i}, q_1^{\mathrm{BS}_C^i}, q_1^{\mathrm{BS}_D^i}$) from $S_1^{\mathrm{BS}_B}, S_1^{\mathrm{BS}_C}, S_1^{\mathrm{BS}_D}$ for $i = 1, 2, \ldots, n$, then the ith particles (i.e., $q_2^{\mathrm{BS}_B^i}, q_2^{\mathrm{BS}_C^i}, q_2^{\mathrm{BS}_D^i}$) from $S_2^{\mathrm{BS}_B}, S_2^{\mathrm{BS}_C}, S_2^{\mathrm{BS}_D}$ collapse to one

of the eight three-particle GHZ states

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \tag{1}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle), \tag{2}$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle), \tag{3}$$

$$|\psi_4\rangle = \frac{1}{\sqrt{2}}(|100\rangle - |011\rangle), \tag{4}$$

$$|\psi_5\rangle = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle), \tag{5}$$

$$|\psi_6\rangle = \frac{1}{\sqrt{2}}(|010\rangle - |101\rangle), \tag{6}$$

$$|\psi_7\rangle = \frac{1}{\sqrt{2}}(|110\rangle + |011\rangle), \tag{7}$$

$$|\psi_8\rangle = \frac{1}{\sqrt{2}}(|110\rangle - |011\rangle). \tag{8}$$

More importantly, Alice's GHZ measurement result $\mathtt{MR}_A$, Bob's measurement result $\mathtt{MR}_B$, Charlie's measurement result $\mathtt{MR}_C$ and David's measurement result $\mathtt{MR}_D$ with X-basis satisfy

$$\mathtt{MR}_A = \mathtt{MR}_B \oplus \mathtt{MR}_C \oplus \mathtt{MR}_D. \tag{9}$$

Therefore, when Bob, Charlie and David collaborate with each other, they can recover Alice's master key K_A by computing

$$K_A = K_B \oplus K_C \oplus K_D \tag{10}$$

as $K_A = \mathtt{MR}_A$, $K_B = \mathtt{MR}_B$, $K_C = \mathtt{MR}_C$, $K_D = \mathtt{MR}_D$.

In a (k, n) threshold secret sharing protocol, a secret s is divided into n shares $s_1, s_2, \ldots, s_n$ such that any k of these shares can be used to reconstruct the secret s, but any set of $k-1$ or fewer shares contains absolutely no information about the secret s [2]. Furthermore, a secret sharing protocol consists of three phases: the phase of initialization, the phase of distributing shares, and the phase of recovering secret. To deal with the problems of adding and deleting agents, a dynamic secret sharing protocol is added the two phases: the phase of adding new agents, and the phase of revoking agents. Generally speaking, whether in a (k, n) threshold secret sharing protocol or in a (k, n) threshold dynamic secret sharing protocol, it is required that k or more than k agents can reconstruct the secret s after the phase of distributing shares, i.e., the access structure must be completed. In addition, when they reconstruct the shared secret s, they should have no further communication with the dealer. However, if the secret distribution has been completed among the agents in the YT-protocol,

then both adding an agent and revoking one become impossible by this way. Now we give a detailed analysis as follows.

From the YT-protocol, it can be seen that it also includes the five phases: the phase of initialization, the phase of distributing shares, the phase of recovering secret, the phase of adding new agents, and the phase of revoking agents in fact although the first three phases are not specified in this protocol. Here, we show that there is an unnoticed problem in the YT-protocol which results in the function of adding an agent or revoking one does not work. Specifically, in Step 3, Alice can obtain the measurement results $\mathtt{MR}_A = \{\mathtt{MR}_{A_1}, \mathtt{MR}_{A_2}, \ldots, \mathtt{MR}_{A_n}\}$ only after she performs the GHZ measurement on the ith particles (i.e., $q_1^{\mathtt{BS}_B^i}, q_1^{\mathtt{BS}_C^i}, q_1^{\mathtt{BS}_D^i}$) from $S_1^{\mathtt{BS}_B}$, $S_1^{\mathtt{BS}_C}$ and $S_1^{\mathtt{BS}_D}$ for $i = 1, 2, \ldots, n$. Moreover, as mentioned above, only after Alice completes her measurement, the ith particles (i.e., $q_2^{\mathtt{BS}_B^i}, q_2^{\mathtt{BS}_C^i}, q_2^{\mathtt{BS}_D^i}$) from $S_2^{\mathtt{BS}_B}$, $S_2^{\mathtt{BS}_C}$, $S_2^{\mathtt{BS}_D}$ collapse to one of the eight three-particle GHZ states, and then Bob, Charlie and David can get the measurement results $\mathtt{MR}_B = \{\mathtt{MR}_{B_1}, \mathtt{MR}_{B_2}, \ldots, \mathtt{MR}_{B_n}\}$, $\mathtt{MR}_C = \{\mathtt{MR}_{C_1}, \mathtt{MR}_{C_2}, \ldots, \mathtt{MR}_{C_n}\}$, $\mathtt{MR}_D = \{\mathtt{MR}_{D_1}, \mathtt{MR}_{D_2}, \ldots, \mathtt{MR}_{D_n}\}$, respectively, by performing the X-basis measurements on their sequences. Therefore, after the end of the phase of distributing shares, the three agents Bob, Charlie and David can reconstruct the shared secret K_A distributed by the dealer Alice by computing

$$\mathtt{MR}_B \oplus \mathtt{MR}_C \oplus \mathtt{MR}_D = \mathtt{MR}_A = K_A. \tag{11}$$

Nevertheless, in Sect. 2.2, adding a new agent is by the way of performing the GHZ measurement on the ith particles (i.e., $q_1^{\mathtt{BS}_B^i}, q_1^{\mathtt{BS}_C^i}, q_1^{\mathtt{BS}_D^i}, q_1^{\mathtt{BS}_F^i}$) from $S_1^{\mathtt{BS}_B}$, $S_1^{\mathtt{BS}_C}$, $S_1^{\mathtt{BS}_D}$, $S_1^{\mathtt{BS}_F}$ for $i = 1, 2, \ldots, n$, to obtain the measurement results $\mathtt{MR}_{A'} = \{\mathtt{MR}_{A'_1}, \mathtt{MR}_{A'_2}, \ldots, \mathtt{MR}_{A'_n}\}$. After that, Bob, Charlie, David and Frank can obtain the measurement results $\mathtt{MR}_{B'} = \{\mathtt{MR}_{B'_1}, \mathtt{MR}_{B'_2}, \ldots, \mathtt{MR}_{B'_n}\}$, $\mathtt{MR}_{C'} = \{\mathtt{MR}_{C'_1}, \mathtt{MR}_{C'_2}, \ldots, \mathtt{MR}_{C'_n}\}$, $\mathtt{MR}_{D'} = \{\mathtt{MR}_{D'_1}, \mathtt{MR}_{D'_2}, \ldots, \mathtt{MR}_{D'_n}\}$, and $\mathtt{MR}_{F'} = \{\mathtt{MR}_{F'_1}, \mathtt{MR}_{F'_2}, \ldots, \mathtt{MR}_{F'_n}\}$, respectively, by performing the X-basis measurement on their sequence. By this way, they can recover Alice's master key $K_{A'}$ by computing

$$\mathtt{MR}_{B'} \oplus \mathtt{MR}_{C'} \oplus \mathtt{MR}_{D'} \oplus \mathtt{MR}_{F'} = \mathtt{MR}_{A'} = K_{A'}. \tag{12}$$

This is obviously in conflict with the principles of quantum mechanics because when Alice performs GHZ measurement on the particles $S_1^{\mathtt{BS}_B}$, $S_1^{\mathtt{BS}_C}$, $S_1^{\mathtt{BS}_D}$, the particles in $S_2^{\mathtt{BS}_B}$, $S_2^{\mathtt{BS}_C}$, $S_2^{\mathtt{BS}_D}$ have been collapsed to one of the eight GHZ states $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_8\rangle\}$, and Bob, Charlie and David also have measured them with the X-basis. As a result, there is no particles to measure for Alice, Bob, Charlie and David any longer, which means that there is no way to establish the correlations among the particles distributed by Alice in Step 1 and add a new agent by this way. Of course, Alice can store the particles $S_1^{\mathtt{BS}_B}$, $S_1^{\mathtt{BS}_C}$, $S_1^{\mathtt{BS}_D}$ until the new agent Frank wants to join the four-party dynamic quantum secret sharing protocol as that does in the YT-protocol, which can realize the function of adding the new agent Frank. Nevertheless, this way will give rise to a more serious problem that Bob, Charlie and David cannot

recover the shared secret even if they cooperate with each other after the phase of distributing shares, i.e., the access structure is not completed, or they contact Alice to perform GHZ measurement on the particles $S_1^{\mathrm{BS}_B}$, $S_1^{\mathrm{BS}_C}$, $S_1^{\mathrm{BS}_D}$ to establish the access structure temporarily, which are also contrary to the requirement for dynamic secret sharing. In essence, this way is equivalent to a continuation of the phase of distributing shares, and all participants must store their particles, which makes it not practical because quantum store is expensive resource and cannot be easily realized with current technology; in other words, it is not efficient and practical compared with the way of restarting to perform Steps 1–4, which loses the meaning of dynamic secret sharing. Clearly, revoking an agent will face the similar problem.

As a result, The YT-protocol does not satisfy the requirement for dynamic secret sharing in the sense that if the secret distribution has been completed among the agents, then both adding an agent and revoking one become impossible by the way in this protocol.

4 The improvement

As we know, the main goal of dynamic secret sharing is to deal with the problem of adding an agent or revoking one in a secret sharing protocol. However, it has been shown that the YT-protocol does not implement this functionality. Now, we study how to improve the YT-protocol.

In classical secret sharing protocols, the agent change can be realized in the following ways [17]. If the ciphertext of the shared secret has not been published, the dealer Alice can add a new agent Frank by sending a random string to him as he is an original one, and she also can delete any agent by discarding the corresponding random string; otherwise, the agent change can be completed by the following manners. For adding a new agent Frank, every original agent updates his share by adding a random bit string of the same length and sending the random string to Frank. By exclusive-OR all the received strings, Frank can obtain his share. If Alice wants to withdraw Frank's authorization, Alice just needs to publish Frank's share.

In contrast to classical secret sharing, in which the ciphertext of the shared secret is public for the agents to verify the secret and prevent the possible deception from the dealer, quantum secret sharing is not based on public key cryptosystems, and therefore, the phase of publishing the ciphertext of the shared secret does not exist in dynamic quantum secret sharing in general. Furthermore, the dealer may also do not know the agents' shares. Therefore, it is more difficult to implement agent change.

A lot of novel proposals [17–29] for dynamic quantum secret sharing have been presented since this concept was firstly introduced by Yang et al in 2011 [16]. From the current works [16–29], we can find that adding new agents in dynamic quantum secret sharing can be completed by the similar manners as classical secret sharing; specifically, after the completion of access structure (before the completion of access structure, agent change is a continuation of the phase of distributing shares in essence, which can be easily solved, and thus we do not discuss this case any longer here), there are two ways to add an agent: One is that the dealer Alice adds a new agent Frank by securely sending a random string K_F to him as his share, while she renews

the shared secret K_A to $\widetilde{K}_A = K_A \oplus K_F$, and the other is that the original agents cooperate to generate a new share K_F for the new participant Frank. Clearly, the first way will change the original secret shared by agents, but each original share needs not be updated, and hence, all the original agents will not be involved in the phase of adding a new agent. On the contrary, the second way does not change the original secret shared by agents, and therefore, the dealer needs not be involved but the original agents must participant in the phase of adding a new agent.

However, it is more difficult to delete an agent in dynamic quantum secret sharing compared with adding a new agent. From the current works [16–29], we can find that if the dealer Alice knows the share held by the agent Frank, then it is not difficult to delete him because she can discarding Frank's share by the way of announcing it to agents or updating the original shared secret K_A to $\widehat{K}_A = K_A \oplus K_F$; otherwise, if the dealer Alice does not know the share held by Frank, then there is no way for her to delete Frank without his cooperation except that she restarts a new distribution phase with the other agents. Of course, if Frank sends his share K_F to Alice, then Alice can delete him by the same way as above. As noted in [18–29], the agent to be deleted must be honest; otherwise, this way is not valid any longer.

Based on the above analysis, we improve the YT-protocol just by modifying the phase of agent change as follows.

4.1 Adding an agent

When a new agent (Frank) needs to be added in the YT-protocol, Alice distributes a new share K_F to Frank by quantum key distribution or quantum secure communication. Then, she renews the master key K_A to $\widetilde{K}_A = K_A \oplus K_F = K_B \oplus K_C \oplus K_D \oplus K_F$. After that, the four agents Bob, Charlie, David and Frank can recover Alice's new master key $\widetilde{K}_A$ if they cooperate with each other. Of course, adding an agent Frank also can be done by the second way, i.e., every original agent (Bob, Charlie and David) updates his share by adding a random bit string of the same length and sending the random string to Frank. By exclusive-OR all the received strings R_B, R_C, R_D, Frank can obtain his share $K_F = R_B \oplus R_C \oplus R_D$.

4.2 Revoking an agent

Without loss of generality, we also consider the case of a five-party dynamic quantum secret sharing protocol, i.e., one dealer (Alice) and four agents (Bob, Charlie, David and Frank), and suppose that the agent Frank to be deleted is honest. Specifically, if the dealer Alice wants to take back Frank's authority, then she requires Frank to send back his share K_F for her. After that, she renews the secret K_A to $\widehat{K}_A = K_A \oplus K_F = K_B \oplus K_C \oplus K_D$. By this way, Frank's share is eliminated and only Bob, Charlie and David can recover Alice's new secret $\widetilde{K}_A$ if they cooperate with each other. If the agent (Frank) to be deleted is not honest, then it is rather difficult for Alice to delete him without the interaction with the other agents Bob, Charlie and David. It should be noted that if the dealer Alice is allowed to interact with them, then there is a way to deal with this problem, i.e., Alice distributes new shares $\widehat{K}_B$, $\widehat{K}_C$, $\widehat{K}_D$ for them by

quantum key distribution or quantum secure communication, respectively, and then, she renews the secret K_A to $\widehat{K}_A = \widehat{K}_B \oplus \widehat{K}_C \oplus \widehat{K}_D$.

5 Conclusion

In summary, we give an analysis of the YT-protocol and find a neglected problem that this scheme does not satisfy the requirement for dynamic secret sharing in the sense that if the secret distribution has been completed among the agents, then both adding an agent and revoking one become impossible by the way in this protocol. Furthermore, we also discuss how to deal with this problem and give a possible way to improve this protocol. It should be noted that as far as we are concerned, there is no way to delete a dishonest agent without the other agents' cooperation under this model at present. We hope this problem is noticed in the following work for dynamic quantum secret sharing.

Acknowledgements We are grateful to the anonymous reviewers and the editor for their very valuable comments. This work was supported by the National Natural Science Foundation of China (Grant Nos. 61602232, 61572246, 61902166), the Program for Science & Technology Innovation Research Team in Universities of Henan Province (Grant No. 18IRTSTHN014), the Postgraduate Education Reform Project of Henan Province (Grant No. 2019SJGLX094Y), the Key Scientific Research Project in Universities of Henan Province (Grant No. 21A110017), and the Youth Key Teacher Project of Luoyang Normal University.

References

1. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**(3), 1829–1834 (1999)
2. Shamir, A.: How to shair a secret. Commun. ACM **22**(11), 612–613 (1979)
3. Xiao, L., Long, G.L., Deng, F.G., et al.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A **69**(5), 052307 (2004)
4. Schmid, C., Trojek, P., Bourennane, M., et al.: Experimental single qubit quantum secret sharing. Phys. Rev. Lett. **95**(23), 230505 (2005)
5. Qin, S.J., Gao, F., Wen, Q.Y., et al.: Cryptanalysis of the Hillery–Bužek–Berthiaume quantum secret sharing protocol. Phys. Rev. A **76**(6), 062324 (2007)
6. Wang, T.Y., Wen, Q.Y., Chen, X.B., et al.: An efficient and secure multiparty quantum secret sharing scheme based on single photons. Opt. Commun. **281**(24), 6130–6134 (2008)
7. Sun, Y., Wen, Q.Y., Gao, F., et al.: Multiparty quantum secret sharing based on Bell measurement. Opt. Commun. **282**(17), 3647–3651 (2009)
8. Shi, R.H., Huang, L.S., Yang, W., et al.: Multiparty quantum secret sharing with Bell states and Bell measurements. Opt. Commun. **283**(11), 2476–2480 (2010)
9. Shi, J.J., Shi, R.H., Tang, Y., et al.: A multiparty quantum proxy group signature scheme for the entangled-state message with quantum Fourier transform. Quantum Inf. Process. **10**(5), 653–670 (2011)
10. Li, Q., Long, D.Y., Chan, W.H., et al.: Sharing a quantum secret without a trusted party. Quantum Inf. Process. **10**(1), 97–106 (2011)
11. Song, T.T., Zhang, J., Gao, F.: Participant attack on quantum secret sharing based on entanglement swapping. Chin. Phys. B **18**(4), 1333–1337 (2009)
12. Wang, T.Y., Liu, Y.Z., Wei, C.Y., et al.: Security of a kind of quantum secret sharing with entangled states. Sci. Rep. **7**, 2485 (2017)
13. Zhou, Y., Yu, J., Yan, Z., et al.: Quantum secret sharing among four players using multipartite bound entanglement of an optical field. Phys. Rev. Lett. **121**(15), 150502 (2018)
14. Cai, X.Q., Wang, T.Y., Zhang, R.L., et al.: Security of verifiable threshold quantum secret sharing with sequential communication. IEEE Access **7**, 134854–134860 (2019)
15. Yuan, J.T., Li, L.X.: A fully dynamic secret sharing scheme. Inf. Sci. **496**, 42–52 (2019)

16. Yang, Y.G., Wang, Y., Chai, H.P., et al.: Member expansion in quantum (t, n) threshold secret sharing schemes. Opt. Commun. **284**(13), 3479–3482 (2011)
17. Jia, H.Y., Wen, Q.Y., Gao, F., et al.: Dynamic quantum secret sharing. Phys. Lett. A **376**(10–11), 1035–1041 (2012)
18. Hsu, J.L., Chong, S.K., Tsai, C.W.: Dynamic quantum secret sharing. Quantum Inf. Process. **12**(1), 331–344 (2013)
19. Wang, T.Y., Li, Y.P.: Cryptanalysis of dynamic quantum secret sharing. Quantum Inf. Process. **12**(5), 1991–1997 (2013)
20. Liao, C.H., Yang, C.W., Hwang, T.: Dynamic quantum secret sharing protocol based on GHZ state. Quantum Inf. Process. **13**(8), 1907–1916 (2014)
21. Mishra, S., Shukla, C., Pathak, A., et al.: An integrated hierarchical dynamic quantum secret sharing protocol. Int. J. Theor. Phys. **54**(9), 3143–3154 (2015)
22. Liu, H.W., Ma, H.Q., Wei, K.J.: Multi-group dynamic quantum secret sharing with single photons. Phys. Lett. A **380**, 2349–2353 (2016)
23. Qin, H., Dai, Y.: Dynamic quantum secret sharing by using d-dimensional GHZ state. Quantum Inf. Process. **16**(3), 64 (2017)
24. Du, Y.T., Bao, W.S.: Dynamic quantum secret sharing protocol based on two-particle transform of Bell states. Chin. Phys. B **27**(8), 080304 (2018)
25. Song, Y., Li, Z.H., Li, Y.M.: A dynamic multiparty quantum direct secret sharing based on generalized GHZ states. Quantum Inf. Process. **17**(9), 244 (2018)
26. Gao, G.: Cryptanalysis and improvement of dynamic quantum secret sharing protocol based on two-particle transform of Bell states. Quantum Inf. Process. **18**(6), 186 (2019)
27. Yang, C.W., Tsai, C.W.: Improved dynamic multiparty quantum direct secret sharing protocol based on generalized GHZ states to prevent collusion attack. Mod. Phys. Lett. A **35**(8), 2050040 (2020)
28. Yang, C.W., Tsai, C.W.: Participant attack and improving dynamic quantum secret sharing using d-dimensional GHZ state. Mod. Phys. Lett. A **35**(6), 2050024 (2020)
29. Wang, M.M., Kong, X.Y.: An asymmetric dynamic multiparty quantum secret sharing against active attacks. Int. J. Quantum Inf. **18**(3), 2050001 (2020)
30. Yang, C.W., Tsai, C.W.: Eficient and secure dynamic quantum secret sharing protocol based on Bell states. Quantumm Inf. Process. **19**, 162 (2020)