Dynamic quantum secret sharing

Heng-Yue Jia\textsuperscript{a,b}, Qiao-Yan Wen\textsuperscript{a}, Fei Gao\textsuperscript{a,*}, Su-Juan Qin\textsuperscript{a}, Fen-Zhuo Guo\textsuperscript{a}

\textsuperscript{a} State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
\textsuperscript{b} State Key Laboratory of Integrated Services Networks, Xidian University, Xi’an 710071, China

1. Introduction

Secret sharing is an important branch of cryptography, which has wide applications in information security theory and technology. Suppose a department supervisor Alice authorizes some agents, Bob\textsubscript{1}, Bob\textsubscript{2}, …, Bob\textsubscript{n}, to act in her name, but she wants them to take action when they reach unanimous agreement. In this case, Alice can use secret sharing scheme, and the whole procedure can be divided into three steps. Firstly, Alice chooses n strings randomly and sends each agent a string. Then Alice encodes secret message by her key, which is generated by the bitwise exclusive-OR of all strings, and publishes the ciphertext. At last, all agents work together to recover Alice’s message.

In 1979, Shamir [1] and Blakley [2] proposed the first secret sharing schemes, respectively. In realistic situations, the composition of agent group may change before the final reconstruction because of individuals’ leaving or joining or groups’ splitting or combing. In the case of adding a new agent or removing an old agent, the security of the secret key may become fragile. Hence, the issue of the member change is very interesting and significant in theory and practice. So far, some dynamic secret sharing schemes, such as schemes with disenrollment capability and protocols for member expansion [3–7], have been discussed.

Quantum secret sharing (QSS) is the generalization of classical secret sharing to quantum scenario, and it has been attracting much attention since 1999. The classical information as well as quantum information can be shared by using quantum resource [8–22]. In addition, some experimental schemes for quantum secret sharing have been demonstrated [23–27]. However, all of the these quantum schemes have limited flexibility in dealing with the dynamic joining and leaving of agents. In this Letter, we take into account this realistic problem and try to solve it.

In classical secret sharing, the agent change can be achieved in a simple manner. If the ciphertext has not been published, Alice can add a new agent Bob\textsubscript{n+1} by sending a random string to him as he is an original one, and she also can delete any agent by discarding his string public. In 1985, Gavrila and Blakley [28] proposed the quantum secret sharing (QSS) scheme, in which a sender shares a secret with a classical or quantum agent. In this case, the eavesdropper accesses to all of Alice’s transmissions, then he can learn the contents of her message.

In this Letter we consider quantum secret sharing (QSS) between a sender and a dynamic agent group, called dynamic quantum secret sharing (DQSS). In the DQSS, the change of the agent group is allowable during the procedure of sharing classical and quantum information. Two DQSS schemes are proposed based on a special kind of entangled state, starlike cluster states. Without redistributing all the shares, the changed agent group can reconstruct the sender’s secret by their cooperation. Compared with the previous quantum secret sharing scheme, our schemes are more flexible and suitable for practical applications.

© 2012 Elsevier B.V. All rights reserved.
et al. [29], which consists of one qubit located at the center and \( n \) surrounding two-qubit arms (shown in Fig. 1). This genuine entangled state has been used in the constructions of two-dimensional and three-dimensional cluster states [29,30]. Recently, the starlike cluster state is also exploited in Refs. [30,31] for topological one-way computation. This motivates us to investigate the usefulness of the state for DQSS. An interesting fact is, as we will see, the corresponding graph state will be suitable for DQSS.

This Letter is organized as follows. First, in Section 2, we introduce the starlike cluster state. In Section 3.1, we describe the basic multi-party quantum scheme for sharing a classical bit. Then we discuss the situation of member changes in Section 3.2. Secondly, we devise schemes for sharing a qubit in Section 4.1 and give the solutions to the member changes in Section 4.2. Finally, some discussions and conclusions are given in the last section.

2. Starlike cluster state

Since the starlike cluster state is relevant to the graph theory, let us begin with the concept of a graph. A graph \( G = (V, E) \) is given by a vertex set \( V = \{1, 2, \ldots, m\} \) and an edge set \( E = \{(i, j) \mid i, j \in V\} \). The neighborhood of a given vertex \( i \in V \), written \( N_i \), is defined as the set of vertices \( j \) for which \( (i, j) \in E \). And \( G[N_i] \) denotes the subgraph of \( G \) which consists of vertices \( N_i \) and all edges of \( G \) linking two vertices in \( N_i \). When a vertex is deleted, together with the edges incident with \( i \), the new graph is denoted with \( G - \{i\} \). Moreover, \( E(A, B) = \{(i, j) \in E \mid i \in A, j \in B, i \neq j\} \) denotes the set of edges between sets \( A, B \subset V \).

As introduced in Ref. [32], each (undirected, finite) graph \( G \) can be associated with a graph state, and the corresponding graph state \( |G\rangle \) is obtained by applying a sequence of controlled-\( Z \) gates \( CZ = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11| \) to empty graph state \( |+\rangle^\otimes |V\rangle \), i.e.,

\[
|G\rangle = \prod_{(i,j) \in E} CZ_{ij}|+\rangle^\otimes |V\rangle,
\]

where \(|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\) and \(|V\rangle\) is the order of the set \( V \).

As important tools, some interesting results of the local Pauli measurements on graph state need to be introduced. Suppose \( X, Y \) and \( Z \) are the Pauli operations. If a measurement of \( X \) (or \( Y \) or \( Z \)) is performed on a qubit with vertex \( i \in V \), written \( X_i \) (or \( Y_i \) or \( Z_i \)), then the system of the other qubits is local unitary equivalent to new graph state \( |G'\rangle \), which is associated with simple graph \( G' \). Specifically,

\[
G' = \begin{cases} 
G \Delta E(N_i, N_j) & \text{for } X_i, \\
G \Delta E(N_i, N_j) - [i] & \text{for } Y_i, \\
G - [i] & \text{for } Z_i.
\end{cases}
\]

Starlike cluster state with \( n \) two-qubit arms, denoted by \( |SC_n\rangle \), hereinafter, is the \((2n + 1)\)-particle entangled state corresponding to the starlike graph (see Fig. 1). Here, we denote the center qubit with \( A \) and the two-qubit arms with \( B_i A_i \) (\( i \in \{1, 2, \ldots, n\} \)) respectively. The expression of \( |SC_n\rangle_{AB_1A_1 - B_n A_n} \) is given by

\[
|SC_n\rangle_{AB_1A_1 - B_n A_n} = |0\rangle_A |\alpha_0^{AB_1A_1 - B_n A_n}| + |1\rangle_A |\alpha_1^{AB_1A_1 - B_n A_n}|,
\]

where

\[
|\alpha_0^{AB_1A_1 - B_n A_n}| = \prod_{1 \leq i \leq n} \left( (|0\rangle + |1\rangle)_{B_iA_i} \right),
\]

\[
|\alpha_1^{AB_1A_1 - B_n A_n}| = \prod_{1 \leq i \leq n} \left( (|0\rangle - |1\rangle)_{B_iA_i} \right).
\]

According to the rules of Pauli measurements on graph state, a fantastic feature of \( |SC_n\rangle \), named scalability, can be explored. The scalabilty means that the \( |SC_n\rangle \) state can be tailored to \( |SC_{n+1}\rangle \) or \( |SC_{n-1}\rangle \) state agilely. For example, \( CZ \) operations can be used to add a two-qubit arm, and \( Z \) measurement performed on qubit \( B_i \) (\( i \in \{1, 2, \ldots, n\} \)) can be used to delete the arm \( B_i A_i \). Different from the carriers often used in quantum cryptographic protocols, \( |SC_n\rangle \) state is very suitable for quantum secret sharing with dynamic agent group.

3. Dynamic sharing of classical information

In this section, let us first describe a quantum secret sharing scheme based on \( |SC_n\rangle \) state which allows Alice to establish a classical key with \( n \) agents, \( B_1, B_2, \ldots, B_n \). It is a basic scheme such that all agents together can recover Alice’s secret. Afterwards we show how to add or delete a member in this scheme.

3.1. Basic quantum secret sharing process

We divide the whole basic sharing process into three phases, initialization phase, distribution phase and reconstruction phase.

**Initialization phase.** Alice prepares a large enough number of \((2n + 1)\)-qubit cluster states in Eq. (1). Then Alice sends particle \( B_i \) (\( 1 \leq i \leq n \)) of each entangled state to Bob. That is, each \( |SC_n\rangle_{AB_1A_1 - B_n A_n} \) state is shared in a way that Bob possesses particle \( B_i \) and Alice possesses the other particles.

To guarantee the security of the transmission from Alice to the agents, Alice chooses randomly some sample entangled units to check whether the particles are eavesdropped. The checking procedure is as follows. For every chosen sample state, Alice first tells agents its position and measures the particle \( A \) in \(|0\rangle \) or \(|1\rangle \) basis (the basis of \( Z \) measurement). Next, each agent measures his corresponding particle of the sample state in \(|0\rangle \) or \(|1\rangle \) basis (the basis of \( X \) measurement) and publishes the outcome. After that, according to Bob’s public information, Alice measures the particle \( A \) using the basis different from Bob’s. Finally, Alice analyzes the error rate based on the correlation shown in Eq. (1). If the error rate exceeds a specified threshold, Alice and her agents discard all the entangled particles and abort the protocol. Otherwise, Alice will securely use the remaining entangled states to split her secret information. In regard to the “specified threshold”, the value is 0 if the quantum resource is transmitted in a noise-free channel. While in a noisy channel, the error rate is closely related to the amount of information that an eavesdropper would have. And a reasonable threshold can be calculated with the methods of information theory by considering all possible attacks, just as some
discussions made for the famous BB84 protocol [33]. Here, similar to the threshold of BB84 protocol, the threshold value would guarantee that the amount of information obtained by the eavesdropper is less than that Alice’s agents have. That is to say, the legitimate parties can distill secret information.

**Distribution phase.** To distribute the secret key among the parties, Alice measures particle \( A \) of each \( |SC_n\rangle_{AB_A1} \) state in \( \{+\}, \{-\} \) basis and takes the measurement result as a key bit, recorded by \( a \in \{0, 1\} \). After producing enough bits, Alice encodes the secret information using the key and publishes the ciphertext.

**Reconstruction phase.** For each entanglement unit, Bob, \( 1 \leq i \leq n \), measures his particle \( B_i \) in \( \{|0\}, \{|1\}\) basis and records by \( b_i \in \{0, 1\} \). All agents combine the results of their measurements and compute \( b = \bigoplus_{i=1}^{n} b_i \), where \( \bigoplus \) denotes modulo 2 addition. If \( b = 0 \), they can conclude that Alice’s corresponding key bit \( a = 0 \), otherwise \( a = 1 \). In this way, they can recover the whole secret key bit by bit and decrypt Alice’s message.

Let us see how it works in detail. Without loss of generality, let us take sharing one bit as an example. After Alice's measurement in distribution phase. The whole state can be written as

\[
|SC_n\rangle_{AB_A1} \rightarrow |B_{A1}..Ba\rangle \rightarrow \frac{1}{\sqrt{2}}(\{|0\rangle + |1\rangle\})_{B_1..B_{A1}} \\
= +\langle -A(\langle 0^0_1 - \langle 0^1_1\rangle)_{B_1A_1..Ba}\rangle.
\]  

(2)

The effect can be seen in the system of the other particles. That is, the state \((\langle 0^0_1 + \langle 0^1_1\rangle)_{B_1A_1..Ba}\) is the superposition of all terms with even number of \(|1\)’s in agents’ subsystem, and state \((\langle 0^0_1 - \langle 0^1_1\rangle)_{B_1A_1..Ba}\) includes all terms with odd number of \(|1\)’s. If Alice’s measurement result is \( a = 0 \), there must be an even number of \(|1\)’s in all agents’ results. Otherwise, there is an odd number of \(|1\)’s.

There are two additional points to notice here. First, the measurement outcome of particle \( A_i \) in \( \{|0\}, \{|1\}\) basis is correlated with the measurement outcome of particle \( A_i \) in \( \{|+, |-\}\) basis. This means that Alice can verify the agents’ shares. Second, before and after Alice’s measurement on particle \( A \), the reduced density matrix of single-particle \( B_i \) (i.e. \( \{|0\}, \{|1\}\) basis) is not changed, i.e.

\[
\rho_{B_i} = \frac{1}{2}(\{|0\rangle \langle 0| + |1\rangle \langle 1|\})
\]

This means that Bob cannot get any information about Alice’s bit from his own share. Moreover, no information about the Alice’s bit can be revealed for any \( n - 1 \) agents. Hence, this basic scheme is a perfect \( n, n \) threshold scheme.

**3.2. Protocol for member changes**

In practice, along with department development and market requirement, member changes of the agent group are inevitable. Now we look at the procedure for adding or deleting one agent in above scheme. And the problems are considered and discussed in different cases.

**Case C1. Between initialization and distribution.**

At this point, the state \( |SC_n\rangle_{AB_A1} \) as the initial quantum channel, has been shared by Alice and her agents. If Alice receives a member’s application for joining (or leaving) the agent group, she can add (or delete) an arm for the initiate (or removed) member as follows.

**Add a member.** If Alice approves of a new agent Bob_{n+1}’s joining, she should distribute a share to him. That is, Alice adds a new two-particle arm \( B_{n+1}A_{n+1} \) to each \( |SC_n\rangle_{AB_A1} \) state and sends particle \( B_{n+1} \) to Bob_{n+1}.

To guarantee the security of the transmission from Alice to Bob_{n+1}, Alice firstly prepares a large enough number of 3-qubit linear cluster states (shown in Fig. 2(a))

\[
|LC_3\rangle_{AB_{n+1}A_{n+1}} = \frac{1}{\sqrt{2}}(|00+\rangle + |11-\rangle)_{B_{n+1}A_{n+1}}
\]

(3)

and sends the particle \( B_{n+1} \) of each \( |LC_3\rangle_{AB_{n+1}A_{n+1}} \) state to the new agent Bob_{n+1}. After it is confirmed that Bob_{n+1} has received all the particles, Alice and Bob_{n+1} check the security of the channel. Alice chooses randomly some sample entangled units and tells Bob_{n+1} the positions. For each chosen 3-qubit linear cluster state, Bob_{n+1} measures his particle in \( \{|0\}, \{|1\}\) or \( \{|+, |-\} \) basis randomly and announces the measurement outcome. Then Alice measures the corresponding particles \( A \) and \( A' \) using the measurement basis different from Bob_{n+1}’s. According the correlation shown in Eq. (3), Alice can analyzes the error rate. If the error rate exceeds the threshold, Alice and Bob_{n+1} discard all the entangled \( |LC_3\rangle_{AB_{n+1}A_{n+1}} \) states and abort the procedure for adding a member.

Otherwise, Alice divides the shared \( |SC_n\rangle_{AB_A1} \) states and \( |LC_3\rangle_{AB_{n+1}A_{n+1}} \) states into pairs, one \( |SC_n\rangle_{AB_A1} \) state and one \( |LC_3\rangle_{AB_{n+1}A_{n+1}} \) state per pair. For each pair, Alice performs a CZ operation on the particle \( A \) and the particle \( A' \), followed by a Y measurement on particle \( A' \) (shown in Fig. 2(a)). By applying appropriate local operations [32], each pair can be transformed into a starlike cluster state with \( n + 1 \) two-qubit arms, i.e. \( |SC_{n+1}\rangle_{AB_A1..B_{n+1}A_{n+1}} \) state, which has been shared by Alice and \( n + 1 \) agents. After all pairs have been processed, the addition of a member is carried out.

**Delete a member.** For deleting an old agent Bob_{d} (\( d \in \{1, 2, \ldots , n\} \)), the arm \( B_{d}A_{d} \) of each shared \( |SC_n\rangle_{AB_A1} \) state needs to be removed. As shown in Fig. 2(b), a CZ operation is used for connecting \( A \) and \( A_{d} \), then a Y measurement is performed to disentangle the \( B_{d}A_{d} \) from the system. According the rules of Pauli measurements on graph state [32], the starlike cluster states with \( n - 1 \) arms can
be obtained, by appropriate local operations \[32\]. After all shared states \(|SCn⟩_{AB_{1}⋅⋅⋅B_{n}}⟩\) have been processed, \(B_{d}\) is deleted from the group by Alice.

Moreover, it should be pointed out that the method to add or delete arms is not unique. For example, there is another way to delete an agent. Alice can perform a two-qubit operation \(CZ^\dagger\) on particles \(A_{d}\) and \(A_{d}\) to disentangle both \(B_{d}\) and \(A_{d}\) from the quantum channel. The effect can be found by following expression

\[
CZ^\dagger_{A_{d}A_{d}}|SCn⟩_{AB_{1}⋯B_{n}}⟩ = \frac{1}{\sqrt{2}} \left[ (|0⟩ + |−1⟩)_{B_{d}A_{d}} \otimes \sum_{1 ≤ i ≤ n, i ≠ d} (|0⟩ + |−1⟩)_{B_{i}A_{i}} \right] + |1⟩_{A_{d}} \otimes \sum_{1 ≤ i ≤ n, i ≠ d} (|0⟩ + |−1⟩)_{B_{i}A_{i}}
\]

This fact shows that starlike cluster state is especially suitable to solve the dynamic problem in multi-party protocol.

Case C2. Between distribution and reconstruction.

At this point, the secret key has been distributed among the agent group, and the ciphertext has been published by Alice. If a member wants to join or leave the group, the whole quantum system of the agent group should be adjusted for the member changes.

Add a member. In order to join the agent group, the new agent \(B_{n+1}\) not only needs Alice's approval, but also should gain the admission and authorization from at least one original agent. Because the roles of all agents are same, without loss of generality, we assume \(B_{d}\) is the new agent's sponsor. For distributing a share to \(B_{n+1}\), Alice, \(B_{d}\), and \(B_{n+1}\) should share some new quantum channels \(|LC⟩_{B_{d}B_{n+1}A_{n}+1}⟩\) in a way that Alice holds particles \(A_{n+1}\), \(B_{d}\) holds particle \(B_{d}\), and \(B_{n+1}\) holds \(B_{n+1}\).

To guarantee the security of quantum channels, Alice firstly prepares a large enough number of 3-qubit linear cluster states \(|LC⟩_{B_{d}B_{n+1}A_{n+1}}⟩\) and sends the particles \(B_{d}\) and \(B_{n+1}\) of each \(|LC⟩_{B_{d}B_{n+1}A_{n+1}}⟩\) state to \(B_{d}\) and \(B_{n+1}\) respectively. After \(B_{d}\) and \(B_{n+1}\) publically confirm that they have received all particles, Alice exploits the entanglement properties of \(|LC⟩\) state to check whether the particles are eavesdropped during the transmission. That is, Alice chooses randomly some sample entangled units and tells \(B_{d}\) and \(B_{n+1}\) the positions. For each chosen 3-qubit linear cluster state, \(B_{d}\) and \(B_{n+1}\) measure their particles \(B_{d}\) and \(B_{n+1}\) in \(|0⟩, |1⟩\) or \(|+⟩, |−⟩\) basis randomly and announce the measurement outcomes, respectively. According the correlation shown in Eqs. (3), Alice measures the corresponding particles \(A_{n+1}\) using an appropriate measurement basis. Then Alice analyzes the error rate. If the error rate exceeds the threshold, Alice, \(B_{d}\), and \(B_{n+1}\) discard all the \(|LC⟩_{B_{d}B_{n+1}A_{n+1}}⟩\ states and abort the procedure for adding a member.

Otherwise, Alice divides the shared \(|SCn⟩_{AB_{1}⋯B_{n}}⟩\ states and \(|LC⟩_{B_{d}B_{n+1}A_{n+1}}⟩\ states into pairs, one \(|SCn⟩_{AB_{1}⋯B_{n}}⟩\ state and one \(|LC⟩_{B_{d}B_{n+1}A_{n+1}}⟩\ state per pair. For each pair, \(B_{d}\) performs an operation CNOT\(^\dagger\) on particles \(B_{d}\) and \(B_{n+1}\), and Alice performs an operation CNOT\(^\dagger\) on the particles \(A_{n+1}\) and \(A_{n+1}\). Here

\[
CNOT^\dagger = |+⟩⟨+| + |−⟩⟨−|\]

and

\[
CNOT^\dagger = |+⟩⟨+| + |−⟩⟨−|.
\]

After that, \(B_{n+1}\) measures particle \(B_{n+1}\) in \(|0⟩, |1⟩\) basis and tells Alice the result by a classical bit \(b^\dagger\) \(∈\{0, 1\}\). Based on the measurement outcome, Alice performs an operation \((Z_{A_{n+1}})^{b^\dagger}\) on the particle \(A_{n+1}\), where \(Z^\dagger = |+⟩⟨+| − |−⟩⟨−|\). They repeat this process until all pairs have been processed.

By above method, a new agent \(B_{n+1}\) becomes a member of the agent group and plays a part in the reconstruction of the secret key. Taking sharing a bit 'U' as an example, we look at the procedure of adding an agent in detail. Combining with the new quantum channel, the whole system of Alice and Bob, \(1 ≤ i ≤ n + 1\) is

\[
(|a_{n}^0⟩ + |a_{n}^1⟩)_{B_{d}A_{1}⋯B_{i}A_{i}B_{i+1}⋯B_{n}A_{n+1}} = ((|a_{n}^0⟩ + |a_{n}^1⟩))_{B_{d}A_{1}⋯B_{i}A_{i}B_{d}A_{d}B_{n+1}} \otimes (|0⟩ + |+⟩ + |−⟩ + |−⟩)_{B_{d}A_{d}B_{n+1}} \otimes (|−⟩ + |−⟩ + |0⟩ + |+⟩)_{B_{d}A_{d}B_{n+1}}
\]

Performed \(B_{d}\)'s and Alice's two-particle operations, it turns into

\[
|0⟩_{B_{d}}(|a_{n}^0⟩ + |a_{n}^1⟩)_{B_{d}A_{1}⋯B_{i}A_{i}B_{d}A_{d}B_{n+1}} \otimes (|0⟩ + |+⟩ + |−⟩ + |−⟩)_{B_{d}A_{d}B_{n+1}} \otimes (|−⟩ + |−⟩ + |0⟩ + |+⟩)_{B_{d}A_{d}B_{n+1}}.
\]

After \(B_{d}\)'s and Alice's single-particle operations, a \((|a_{n+1}^0⟩ + |a_{n+1}^1⟩)_{B_{d}A_{1}⋯B_{i}A_{i}B_{d}A_{d}B_{n+1}}\) state is generated from a \((|a_{n+1}^0⟩ + |a_{n+1}^1⟩)_{B_{d}A_{1}⋯B_{i}A_{i}B_{d}A_{d}B_{n+1}}\) and a \(|LC⟩_{B_{d}B_{n+1}A_{n+1}}⟩\ state. From above equations, we can learn that \(B_{n+1}\) has obtained a usable share. Further, the role of \(B_{n+1}\) is as same as that of an original agent.

Delete a member. If Alice wants to delete an old agent \(B_{d}\) \(d ∈ \{1, 2, ..., n\}\), she should disentangle Bob's particles from the entangled states. For each quantum system shared by Alice and her agents, Alice measures particle \(A_{d}\) in \(|+⟩, |−⟩\) basis and publishes the measurement outcome by a classical bit \(a_{d} ∈ \{0, 1\}\). Since particles \(A_{d}\) and \(B_{d}\) have the correlation as shown in Eqs. (1) and (2), Bob's bit \(b_{d}\) can be determined by \(a_{d}\), i.e. \(b_{d} = a_{d}\)

By above way, Bob's share is known by other agents. Hence Bob\(_{d}\) is disqualified from the reconstruction. That is, Alice deletes the agent Bob\(_{d}\) from the agent group.

In this section, we present a DQSS scheme for sharing a classical bit, which allows member changes in two cases. The procedures of adding an agent in both cases are secure and economic. On the one hand, they are against eavesdropping. The checking procedures guarantee the security of the transmission from Alice to her agent(s) and make them share the genuine \(|LC⟩\) states. In addition, the reduced matrix of each original agent remains unchanged in this procedure. This implies that any agent will gain no information about the new one's share. On the other hand, they are also save cost and better use of resources. As stated above, quantum channels for the new member are constructed and checked locally between Alice and her agent(s) first. The original shared states and \(|LC⟩\) states cannot be connected unless the transmission is secure.
Hence, the original shared quantum systems are not affected and consumed for adding a new member. In the process of deleting an agent, there are no particles transmitted, and the operations can be completed only by Alice. Hence it is secure and efficient.

Finally, let us conclude this section with a discussion of the resources necessary to implement our scheme. Suppose Alice wants to share a N-bit information. In our basic sharing process, it is necessary to use, on average, 2N \( |SC_n\rangle \) states to distribute the key. If we instead use the hybrid scheme consisting of classical secret sharing and BB84 protocol \cite{28}, 2nN particles are required. In both schemes, the number of particles sent from Alice to her agents is 2nN. But the number of classical bits needed in our scheme is much less than the hybrid scheme. Due to entanglement, Alice just needs N classical bits to transmit the ciphertext and no more need to send a random string to each agent. Besides, our scheme allows the agents to join or leave Alice’s group dynamically during the sharing process. For the member changes at different times, the resources needed in our scheme are different. In Case C1, 2N \( |LC_1\rangle \) states are needed to add a new agent, and Alice transmits 2N particles and N classical bits to the new agent. For deleting an agent, no extra resources and quantum transmissions are needed. In this case, the cost of our scheme for adding and deleting an agent is equal to that of the hybrid scheme. In Case C2, to add a new agent, 2N \( |LC_2\rangle \) states are needed, and Alice should send 4N particles: 2N particles to send to the new agent and another 2N particles to send to his sponsor. Then the sponsor needs N classical bits to tell Alice his measurement outcomes. In the hybrid scheme, 2nN particles and nN bits are needed to send because every original agent should send 2N particles and N bits to the new agent. For deleting an old agent, only N classical bits are needed in both scheme. Comparing with the hybrid scheme, just one original agent is needed when adding a new member in our scheme. It can be learnt that our scheme is more economical for n > 2.

4. Dynamic sharing of quantum information

In this section, we discuss the dynamic quantum scheme for sharing quantum information. Suppose Alice has a string of qubits, and she wants to split the quantum information to n agents such that all agents can recover the secret key only when they work together.

4.1. Basic quantum information splitting process

Similar to the sharing of classical information, there are three phases in the basic procedure. However, limited by no-cloning theorem, only one copy of Alice’s quantum information can be received. Hence, only one of the agents will possess the final information. Let us now describe the procedure for splitting a qubit (the qubit string can be shared one qubit at a time).

**Initialization phase.** As stated in classical information sharing, Alice and her agents, Bob_1, Bob_2, …, Bob_n, share the genuine \( |SC_n\rangle \) states, where Bob_i \( (i \in \{1, \ldots, n\}) \) possesses particle \( B_i \), and Alice possesses particles \( A, A_1, \ldots, A_n \). Besides, Alice has another particle \( S \), which is in the state \(|\xi\rangle_S = |0\rangle_S + |1\rangle_S = (|\alpha|^2 + |\beta|^2 = 1)\).

**Distribution phase.** Alice combines her qubit \(|\xi\rangle_S\) with the \( |SC_n\rangle \) and \( |A, A_1, \ldots, A_n\rangle \) respectively and performs a joint measurement on the particles \( S \) and \( A \) in Bell basis

\[
|\phi^+\rangle_{SA} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{SA},
\]

\[
|\psi^-\rangle_{SA} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{SA}.
\]

**Reconstruction phase.** In order to recover Alice’s qubit, Bob_i \( (i \in \{1, \ldots, n-1\}) \) measures his particle \( |\phi^\pm\rangle_{SA} \) in basis \(|0\rangle, |1\rangle\), and performs a joint measurement on the particles \( S \) and \( A \). Hence, the original shared quantum systems are not affected...

---

**Table 1**

<table>
<thead>
<tr>
<th>Outcomes of Alice</th>
<th>Bob_0’s state</th>
</tr>
</thead>
<tbody>
<tr>
<td>(</td>
<td>\phi^+\rangle_{SA} =</td>
</tr>
<tr>
<td>(</td>
<td>\phi^-\rangle_{SA} =</td>
</tr>
<tr>
<td>(</td>
<td>\psi^-\rangle_{SA} =</td>
</tr>
</tbody>
</table>
| Without loss of generality, suppose Bob_0 is chosen to be the holder of the qubit \(|\xi\rangle_S\), Alice measures particle \( A_0 \) with basis \(|0, 1\rangle\). It is agreed that measurement outcomes corresponds to a two-bit message: \(|\phi^+\rangle_{SA} = |00\rangle\rangle_{SA}, |\psi^+\rangle_{SA} = |11\rangle\rangle_{SA}| \rightarrow 00, \(|\phi^-\rangle_{SA} = |01\rangle\rangle_{SA}, |\psi^-\rangle_{SA} = |10\rangle\rangle_{SA}| \rightarrow 01, \(|\psi^-\rangle_{SA} = |10\rangle\rangle_{SA}, |\psi^-\rangle_{SA} = |10\rangle\rangle_{SA}| \rightarrow 10, \(|\phi^-\rangle_{SA} = |11\rangle\rangle_{SA}, |\psi^-\rangle_{SA} = |11\rangle\rangle_{SA}| \rightarrow 11. Then Alice tells Bob_0 the measurement outcome by classical bits.

---

**Reconstruction phase.** In order to recover Alice’s qubit, Bob_i \( (i \in \{1, \ldots, n-1\}) \) measures his particle in \(|0, 1\rangle\) basis and tells Bob_{n-1} his outcome with a classical bit \( b_i \). With the other agents’ information, Bob_n can reconstruct Alice’s qubit on particle \( B_n \) by performing an operation \( Z^H \) where \( b = \{0, 1\} \).

In above procedure, the effect of Alice’s joint measurement on the particles \( S \) and \( A \) can be found by expressing the entire system as

\[
|\xi\rangle_S \otimes |SC_n\rangle \otimes |A, A_1, B_1, \ldots, B_n\rangle = \left|\phi^+\right\rangle_{SA} |\alpha_0^0\rangle_B + |\beta_0^0\rangle_B \rangle_{B_1, B_1, \ldots, B_n} + |\phi^-\rangle_{SA} |\alpha_0^0\rangle_B - |\beta_0^0\rangle_B \rangle_{B_1, B_1, \ldots, B_n} + |\psi^+\rangle_{SA} |\alpha_0^0\rangle_B + |\beta_0^0\rangle_B \rangle_{B_1, B_1, \ldots, B_n} + |\psi^-\rangle_{SA} |\alpha_0^0\rangle_B - |\beta_0^0\rangle_B \rangle_{B_1, B_1, \ldots, B_n}.
\]

Based on the symmetry of \( |SC_n\rangle \) state and Eq. \(4\), it can be learnt that any one of the agents can recover the secret state. Let Bob_0 be the receiver, Alice measures the particle \( A_0 \). If Alice’s result is one of \(|\phi^+\rangle_{SA} = |00\rangle\rangle_{SA}, |\phi^-\rangle_{SA} = |00\rangle\rangle_{SA}, |\psi^+\rangle_{SA} = |11\rangle\rangle_{SA}, |\psi^-\rangle_{SA} = |11\rangle\rangle_{SA}| \), then Bob_0’s single-particle density matrix is

\[
\rho_{B_0} = |\alpha_0^0\rangle_B |\beta_0^0\rangle_B + |\beta_0^0\rangle_B \rangle_{B_1, B_1, \ldots, B_n} \rangle_{A_0} - |\beta_0^0\rangle_B \rangle_{B_1, B_1, \ldots, B_n} \rangle_{A_0}.
\]

Hence Bob_0 has amplitude information about Alice’s qubit. In the reconstruction phase, Bob_n can obtain the phase information based on the measurement outcomes of the other agents. And we show the relationship between the measurement outcomes and the state obtained by receiver Bob_n in Table 1.

4.2. Protocol for member changes

For member’s joining and leaving, we also consider the two cases as discussed in Section 3.2.

**Case Q1.** Between initialization and distribution.

At this point, Alice just needs to tailor the shared quantum channels as required. And the treatments are as same as those in the **Case C1**, so we will not repeat the description again.
Case Q2. Between distribution and reconstruction.

At this point, Alice's qubit has been split among the agents, and Bobb has the amplitude information about it. Now, we describe the procedure for adding or deleting an agent.

Add a member. If a new agent Bobb+1 eagers to join the agent group, he should gain the admissions of Alice and an original agent Bob (i ∈ [1, ..., n − 1]). Here we assume Bobb+1 = Bobb's sponsor. At first, similar to the Case C2, Alice, Bobb−1, and Bobb+1 share a genuine 3-qubit linear cluster state \([LC]_{+}B_{-,1}B_{-,1}A_{n+1},\) where Alice holds the particle \(A_{n+1},\) Bobb−1 holds the particle \(B_{-,1},\) and Bobb+1 holds particle \(B_{+,1}.\) Then Bobb−1 performs an operation \(\alpha^{*}_{B_{-,1}}B_{-,1}A_{n+1}\) on particles \(B_{-,1}A_{n+1}\) and Bobb+1 performs an operation \(\alpha^{*}_{B_{+,1}}A_{n+1}\) on the particles \(A_{n+1}A_{n+1}\). Here

\[Z^{*} = \mid i \rangle + \mid j \rangle + \mid k \rangle + \mid l \rangle + \mid m \rangle + \mid n \rangle + \mid o \rangle + \mid p \rangle + \mid q \rangle + \mid r \rangle \]

and

\[\alpha^{*} = \mid 0 \rangle + \mid 1 \rangle - \mid 2 \rangle - \mid 3 \rangle - \mid 4 \rangle - \mid 5 \rangle - \mid 6 \rangle - \mid 7 \rangle - \mid 8 \rangle - \mid 9 \rangle \]

Between distribution and reconstruction, members can leave the group by applying for Alice's permission, but to add a new member must get an original agent's recommendation and Alice's permission. All the joining or leaving of members can be handled by one.

It is known that QSS is a very important branch of quantum cryptography. So far, there are various theoretical protocols for the QSS, which can split sender's secret information among the agents group so that all agents must cooperate to read the information. In practice, Alice might adjust her agent group in accordance with work requirements, such as member expansion for new business or member reduction for the redundancies. Therefore, it is meaningful to investigate the secret sharing among the dynamic agent group. If Alice hasn't distributed the work, she usually makes personnel selection by herself. If the work has been distributed, Alice also can change her agent group, but the member addition is always proposed by original member according to the need. Our schemes are very suitable useful in these situation, and there may be other applications in quantum information processing.

However, we just consider the case of \((n, n)\) quantum secret sharing. It is worth pointing out that the member changes should be considered in a more general case, referred to as \((k, n)\) threshold scheme. Recently, following the ideas of the classical Shamir's scheme [1], a protocol for adding member in quantum \((k, n)\) threshold secret sharing has been proposed by Yang et al. [34], and no more than \(n - k\) members can be deleted without affecting the secret reconstruction in the threshold scheme. Although their scheme can generate a new share without a trusted party, it require all the parties to have capability of preparing general quantum states. Moreover, the cost of quantum resource and the number of the transmission for member expansion are considerable. Last but not least, in their scheme for member deletion, the discarding share is still effective, and the loss of a share would decrease the threshold \(k.\) Hence, how to design secure \((k, n)\) threshold QSS schemes with dynamic access structure is still a problem deserving of further study in future.

Acknowledgements

The authors are grateful to anonymous referees for their valuable and constructive comments. This work is supported by...
NSFC (Grant Nos. 61170270, 61100203, 60903152, 61003286, 61121061), NCET (Grant No. NCET-10-0260), SRFPD (Grant No. 20090005110010), Beijing Natural Science Foundation (Grant No. 4112040), the Fundamental Research Funds for the Central Universities (Grant Nos. BUPT2011YB01, BUPT2011RC0505, BUPT2010ZX02, 2011PTB-00-29, 2011RCJ15).

References