Physics Letters A 376 (2012) 1035–1041

Contents lists available at SciVerse ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Dynamic quantum secret sharing

Heng-Yue Jia [a,b], Qiao-Yan Wen [a], Fei Gao [a,*], Su-Juan Qin [a], Fen-Zhuo Guo [a]

[a] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
[b] State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China

ARTICLE INFO

Article history:
Received 24 June 2011
Received in revised form 3 February 2012
Accepted 3 February 2012
Available online 7 February 2012
Communicated by P.R. Holland

Keywords:
Quantum secret sharing
Dynamic
Starlike cluster state
Scalability

ABSTRACT

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.

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_1, Bob_2, ..., Bob_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 and 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_{n+1} 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. If the encoded message has been published, the agent change can be performed by following ways. For adding a new agent Bob_{n+1}, every original agent updates his string by adding a random bit string of the same length and sending the random string to Bob_{n+1}. By exclusive-OR all the received strings, Bob_{n+1} obtains his share. If Bob_i $(1 \leqslant i \leqslant n)$ wants to leave the group, Alice just needs to make Bob_i's string public. However, the secure transmission is of the utmost importance. If an eavesdropper accesses to all of Alice's transmissions, then he can learn the contents of her message.

On the basis of quantum mechanics, quantum cryptography can defeat the eavesdropper in the transmission. Following above basic idea, a plain dynamic quantum secret sharing (DQSS) scheme, which consists of the classical scheme and quantum key distribution (QKD) [28], can be obtained. But it should be pointed out that many transmissions are needed when a new agent joins the group, and it may bring the problems of feasibility and complexity.

In this Letter, we propose two efficient DQSS schemes. They are based on a special kind of multi-particle entangled state, called "starlike cluster". This quantum channel was constructed by Chen

* Corresponding author.
E-mail address: gaofei_bupt@hotmail.com (F. Gao).

0375-9601/$ – see front matter
doi:10.1016/j.physleta.2012.02.004

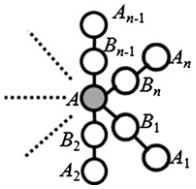

Fig. 1. Starlike cluster. The black node is the center qubit A and B_iA_i, $i \in \{1, 2, \ldots, n\}$ denotes a two-qubit arm.

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 starlike cluster state is very 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. Subsequently, we devise scheme 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, $E(A, B) = \{(i, j) \in E\colon\ i \in A,\ \ j \in B,\ \ i \neq j\}$ 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 $\mathrm{CZ} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11|$ to empty graph state $|+\rangle^{\otimes |V|}$, i.e.

$$|G\rangle = \prod_{\{i,j\}\in E} \mathrm{CZ}_{ij} |+\rangle^{\otimes |V|},$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ and $|V|$ 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 (Y or Z) is performed on a qubit associate with vertex $i \in V$, written X_i (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 a simple graph G'. Specifically,

$$G' = \begin{cases} G\Delta E(N_i, N_j)\Delta E(N_i \cap N_j, N_i \cap N_j)\Delta E(\{j\}, N_i - \{j\}), \\ \quad \text{for } \mathrm{X}_i, \\ G\Delta E(N_i, N_i) - \{i\}, \quad \text{for } \mathrm{Y}_i, \\ G - \{i\}, \quad \text{for } \mathrm{Z}_i. \end{cases}$$

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_iA_i ($i \in \{1, 2, \ldots, n\}$) respectively. The expression of $|SC_n\rangle_{AB_1A_1\cdots B_nA_n}$ is

$$\begin{aligned} &|SC_n\rangle_{AB_1A_1\cdots B_nA_n} \\ &\quad = \big[|0\rangle_A \big|\omega_n^0\big\rangle_{B_1A_1\cdots B_nA_n} + |1\rangle_A \big|\omega_n^1\big\rangle_{B_1A_1\cdots B_nA_n}\big], \end{aligned} \tag{1}$$

where

$$\begin{aligned} \big|\omega_n^0\big\rangle_{B_1A_1\cdots B_nA_n} &= \bigotimes_{1\leqslant i\leqslant n} \big(|0+\rangle + |1-\rangle\big)_{B_iA_i} \\ &= \bigotimes_{1\leqslant i\leqslant n} \big(|+0\rangle + |-1\rangle\big)_{B_iA_i}, \\ \big|\omega_n^1\big\rangle_{B_1A_1\cdots B_nA_n} &= \bigotimes_{1\leqslant i\leqslant n} \big(|0+\rangle - |1-\rangle\big)_{B_iA_i} \\ &= \bigotimes_{1\leqslant i\leqslant n} \big(|-0\rangle + |+1\rangle\big)_{B_iA_i}. \end{aligned}$$

According to the rules of Pauli measurements on graph state, a fantastic feature of $|SC_n\rangle$, named *scalability*, can be explored. The scalability 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_iA_i directly. 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, Bob_1, Bob_2, …, Bob_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 ($1 \leqslant i \leqslant n$) of each entangled state to Bob_i. That is, each $|SC_n\rangle_{AB_1A_1\cdots B_nA_n}$ state is shared in a way that Bob_i 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 $\{|0\rangle, |1\rangle\}$ basis (the basis of Z measurement). Next, each agent measures his corresponding particle of the sample state in the $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ basis (the basis of X measurement) and publishes the outcome. After that, according to Bob_i's public information, Alice measures the particle A_i using the basis different from Bob_i'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 remainder 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