Quantum Route Selection based on Graph State

Lei Yan[1], Peng Luo[2,a], Hanyu Cui[3] Ronghua Shi[4], Ying Guo [5, b]

[1]School of Information Science & Engineering, Central South University, Changsha, 410083, China

[2]School of Information Science & Engineering, Central South University, Changsha, 410083, China

[3]School of Information Science & Engineering, Central South University, Changsha, 410083, China

[4]School of Information Science & Engineering, Central South University, Changsha, 410083, China

[5]School of Information Science & Engineering, Central South University, Changsha, 410083, China

[a]email: lp19902007@sina.com, [b]email: yingguo@csu.edu.cn

Keywords: Quantum Route; Graph State; Local complementation; Local Pauli Measurement

Abstract. Many quantum communication protocols involve multiple participants. With participants increasing, selecting designated legal participants in a nice way becomes more and more significant. In this paper, we develop a quantum route selection approach to the design of participant selection. Graph state is a special type of multi-particle entangled quantum state that can be represented by mathematical graph, where each vertex denotes a qubit and each edge denotes an Ising interaction. Motivated by the characteristics of graph state, we propose that each participant holds a vertex of graph state so that all legal participants are selected through a series of operations on specific vertices of graph state.

Introduction

Due to the growing concern over privacy and security of information, cryptography has received considerable attention. In recent years, quantum cryptography [1] that provides a new method for absolutely secure communication has got rapid development. More and more quantum communication protocols [2][3] are proposed.

Graph state [4] as a special kind of quantum state also has been deeply studied in applications. In [5] graph state is applied to Quantum Secret Sharing (QSS). Each participant holds a vertex that represents a qubit and sub-secrets are transferred from the dealer to participants through a serious of operations. Reference [6] demonstrates the entanglement of graph state. Graph state is not only very promising in term of physical implementation, but also great resource efficient for quantum information processing.

All proposed graph state-based quantum multi-party protocols do not consider the selection of participants and just use the ready-made graph state, which cannot choose legal participants from a set including n participants. In this paper we resort to graph state in the design of quantum routes election. What our approach differs from earlier work is the realization of free selection of legal participants. Through local Pauli measurement and local complementation operation on specific vertices of graph state, the designated vertices are deleted, that is to say the corresponding participants are ruled out. So the specific legal participants are selected.

Preliminaries

A graph $G=(V,E)$ consists of vertex set $V=\{v_i\}$ and edge set $E=\{e_{ij}=(v_i,v_j)\}$, where v_i and v_j are "neighbors" if and only if (iff) they are connected by an edge. The set of $v_i's$ neighbors is denoted N_i [4]. The graph state is generated from the initial state given by

$$\left|+\right\rangle^{\otimes n}=H^{\otimes n}\left|0\right\rangle^{\otimes n}, \quad (1)$$

where $\left|+\right\rangle=\left(\left|0\right\rangle+\left|1\right\rangle\right)/\sqrt{2}$ and H is the Hadamard transformation. By applying the two-qubit

controlled-phase (CZ) gate, the yielded graph state can be described as

$$|G\rangle = \prod_{(v_i,v_j)\in E} CZ_{(v_i,v_j)} |+\rangle^{\otimes n}. \tag{2}$$

The CZ operation only works for those adjoining vertices. In the graph state with n vertices, each vertex $v_i, \forall i = \{1,2,\cdots,n\}$, presents a qubit. The label of vertex can be defined as $(c_{i1}, c_{i2}, c_{i3},)$, with $c_{ij} \in N^*$, where c_{i1} and c_{i2} are used to describe the encoded classical information and c_{i3} is used to label the type of v_i and absorbed into graph itself. c_{i3} is described as the v_i being either v_i° for $c_{i3} = 0$; or $v_i^{\square}$ for $c_{i3} = 1$.

According to the afore-generated graph state $|G\rangle$, the labeled graph state is given by

$$\begin{aligned} |G_c\rangle &= \bigotimes_i \left(X_i^{c_{i1}} Z_i^{c_{i2}} \right) |\widehat{G}\rangle, \\ |\widehat{G}\rangle &= \bigotimes_{j\in v^{\square}} S_j |G\rangle, \end{aligned} \tag{3}$$

where $X = |0\rangle\langle 1| + |1\rangle\langle 0|, Z = |0\rangle\langle 0| - |1\rangle\langle 1|$ and $S = |0\rangle\langle 0| - i|1\rangle\langle 1|$. For the ease of encoding and manipulation of the encoded information, we consider the labeled graph state for $c_{i1} = 0$, i.e.,

$$|G_{c_2}\rangle = \bigotimes_i Z_i^{c_{i2}} |\widehat{G}\rangle. \tag{4}$$

As is mentioned above, each graph state $|G\rangle$ corresponds uniquely to the graph G. However, different graph states can be local unitary (LU) equivalent which is ensured by the LU-rule [7][8]. Before illustrating the LU-rule, the local complementation [4] as a closely conception with LU-rule is presented. Supposing $v \in V(G)$, the local complementation of G in v, i.e., $\sigma_v(G)$, is defined as: (a) $u, w \in N_v$: u and w are adjoined in another graph H, iff they are not adjoined in the initial graph G; (b) $u, w \notin N_v$: u and w are adjoined in another graph H, iff they are adjoined in the initial graph G. Consequently, the rule for graph state can be stated in what follows. Supposing $G = (V, E)$, performing local complementation on G in $a \in V(G)$ attains the LU-equivalent graph state

$$|\sigma_a(G)\rangle = U_a(G)|G\rangle, \tag{5}$$

where $U_a(G) = e^{-i\frac{\pi}{4}\sigma_x^a} e^{-i\frac{\pi}{4}\sigma_z^{N_a}}$. As usual, the matrices $\sigma_x^a, \sigma_y^a, \sigma_z^a$ are the Pauli matrices.

Graph state can also be expressed in the stabilizer [4] formalism through eigenequations as follows

$$K_i^{\circ,\square} |G_{c_2}\rangle = (-1)^{c_{i2}} |G_{c_2}\rangle, \forall i \in V, \tag{6}$$

where K_i° and $K_i^{\square}$ are stabilizers given by

$$K_i^{\circ} = X_i \underset{e_{i,j}\in E}{\otimes} Z_j, K_i^{\square} = Y_i \underset{e_{i,j}\in E}{\otimes} Z_j. \tag{7}$$

Stabilizers cannot be directly measured by the participants under local operations and classical communication (LOCC); rather participants locally measure in bases X_i, Y_i, Z_i to obtain a bit outcome s_i^X, s_i^Y and s_i^Z respectively [4][5]. Outcomes $S_i^{\alpha} = \{0,1\}$ correspond to measurement eigenvalues $\{+1,-1\}$. After applying these local Pauli measurements, participants can obtain the label bits. When the vertex v_i of the encoded graph state with circular vertices is measured by Pauli operator Z, the corresponding resultant graph state is similar to the original graph with the vertex v_i and its edges deleting and the labels of all vertices in N_i changing to $(0, c_{j2} \otimes s_i^z)$ [5].

Scheme Descriptions

Combining above-mentioned local Pauli measurement and local complementation operation can realize the quantum route selection with graph state. Without loss of generality, we consider the graph with four vertices shown in Fig.1. The following steps show the choice of the route of the specific participants.

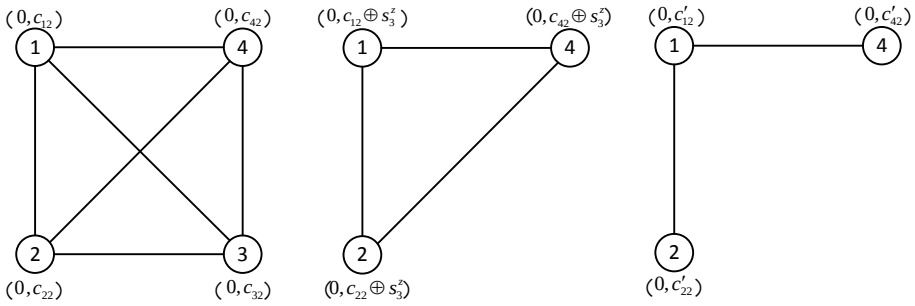
－S1：Generate a completely connected encoded graph state with four vertices.

－S2：Encode the label c_{32} into ‘0’ and perform the local Pauli Z on v_3.

－S3：Perform local complementation on v_1. The edge of $N_1(v_2, v_4)$ is deleted.

－S4：Perform modular operation on the second labels of v_2 and v_4 with ‘0’.

－S5：Select v_1,v_2 and v_4 to generate a new degraded encoded graph state.



(a)The initial four vertices completely connected encoded graph state

(b) Local Pauli Z is performed on v_3

(c) Local complementation is performed on v_1

Fig.1. Four vertices graph state quantum route selection

Through the above-mentioned steps, the completely connected graph state with four vertices can generate the degraded graph state with three designated vertices. This approach can be elegantly used for the route selection, meanwhile, we expect to transmit the message for some specially designated participants in the practical large-scale networks.

Scheme extension

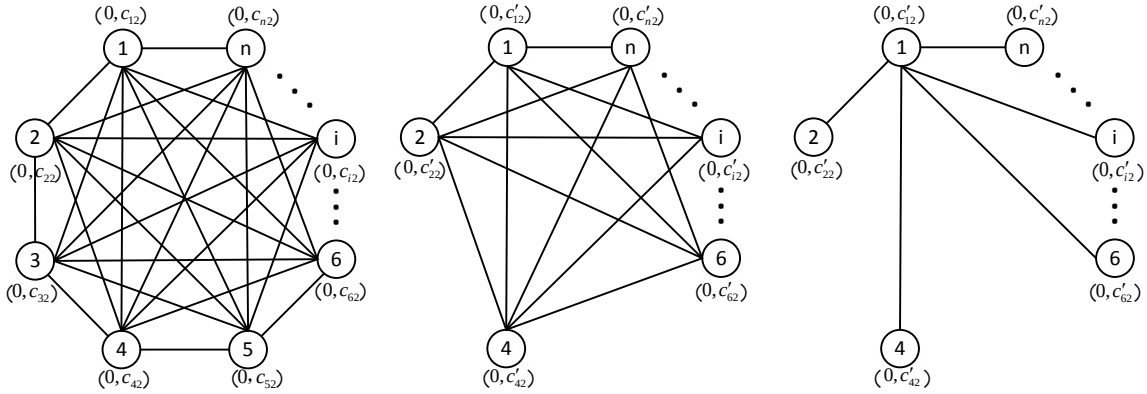
Majority of communication protocols in practice are far more than three participants, so the extension of above-mentioned scheme is necessary. Supposing that there is a set including n participants, k participants of the set are necessary for a communication protocol. That is to say all k authorized participants must be selected from the set. Referring to the above-mentioned four vertices scheme, n vertices quantum route selection can be realized with the following steps, as is shown in Fig.2.

Step S1: Generate a completely connected encoded graph states with n circular vertices, where each participant holds a vertex.

Step S2: Encode the n−k second labels c⋆2 into ‘0’ and perform the local Pauli Z on the n − k vertices.

Step S3: Select a participant from the remainder vertices as dealer. After performing local complementation on the dealer’s vertex, edges of N_D are deleted.

Step S4: Perform modular operation on the k second labels with ’0’, which results in the updated second labels c'_{i2}.



(a)The initial n vertices completely connected encoded graph state

(b) Local Pauli Z measurements are performed on the vertices that unauthorized participants hold

(c) Local complementation operations are performed on v_1

Fig.2. Quantum route selection of n participants

Quantum route selection involves n participants is realized with above-mentioned approach. The degraded graph state that includes designated k participants is generated. v_1 is selected as the dealer who can distribute information to other authorized participants through graph state. The degraded graph state can be used to any multi-party quantum communication scheme which involves selection of legal participant.

Conclusion

Quantum route selection based on graph state is investigated in this paper. The four vertices quantum route selection scheme is extended to n vertices, which realizes the route selection of large-scale quantum networks. The selected degraded graph state that consists of authorized legal participants can be used to any multi-party quantum communication protocol that involves selection of legal participant. The whole scheme has become the base of quantum multi-party communication protocol.

Acknowledgement

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61379153, 61401519, 61572529), the Research Fund for the Doctoral Program of Higher Education of China (Grant Nos. 20130162110012), the Program for New Century Excellent Talents in University of Ministry of Education of China (NCET-11-0510), MEST 2012-002521, NRF, Korea.

References

[1] Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography [J]. Reviews of Modern Physics, 2002, 74(1):145-195.

[2] Ursin R, Tiefenbacher F, Schmitt-Manderbach T, et al. Entanglement-based quantum communication over 144|[thinsp]|km [J]. Nature Physics, 2007, 3(7):481-486.

[3] Sougato B. Quantum communication through an unmodulated spin chain [J]. Physical Review Letters, 2002, 91(20).

[4] Hein M, Eisert J, Briegel H J. Multiparty entanglement in graph states (20 pages) [J]. Physical Review A Atomic Molecular & Optical Physics, 2004, 69(6):666-670.

[5] Markham D, Sanders B C. Graph States for Quantum Secret Sharing [J]. Physical Review A, 2008, 78(4):144-144.

[6] Sixia Y, Qing C, Lai C H, et al. Nonadditive Quantum Error-Correcting Code [J]. Physical Review Letters, 2008, 101(9):67-123.

[7] Glynn D G, On Self-Dual Quantum Codes and Graphs, Submitted to the Electronic [J]. Journal of Combinatorics (2002).

[8] Nest M V D, Dehaene J, Moor B D. Efficient algorithm to recognize the local Clifford equivalence of graph states [J]. Physical Review A, 2004, 70(3):423-433.