



Splitting of quantum information using N -qubit linear cluster states

Sreraman Muralidharan^a, Sakshi Jain^b, Prasanta K. Panigrahi^{c,*}

^a School of EPS, Heriot-Watt University, Edinburgh, EH144AS, United Kingdom

^b Indian Institute of Technology, Mumbai – 400076, India

^c Indian Institute of Science Education and Research (IISER)–Kolkata, Mohanpur, BCKV main campus, Nadia-741252, West Bengal, India

ARTICLE INFO

Article history:

Received 21 December 2009

Received in revised form 18 August 2010

Accepted 7 October 2010

Keywords:

Entanglement

Teleportation

Secret sharing

Information splitting

ABSTRACT

We provide a number of schemes for the splitting up of quantum information among k parties using a N -qubit linear cluster state as a quantum channel, such that the original information can be reconstructed only if all the parties cooperate. Explicit circuits are provided for these schemes, which are based on the concept of measurement based locking and unlocking of quantum information. These are experimentally feasible as they require measurements to be performed only on product basis.

© 2010 Elsevier B.V. All rights reserved.

1. Introduction

Secret sharing between multiple parties, where one or more members can receive a desired message, with the concurrence of the sender and other members, is a subject of significant current interest. As is evident, this problem is of considerable importance in the area of intelligence sharing, banking and many other sectors of public interest. The classical methods of secret sharing are prone to eavesdropping and other forms of tampering, where the involved parties, may not be aware of the presence of eavesdroppers. The advent of quantum information [1] and communication has brought in a completely new perspective to this classical problem, wherein not only the channels of communication can be made secure, but also the presence of eavesdroppers can be detected [2]. The fundamental aspects of quantum mechanics, which makes this possible are, 1) the process of measurement necessarily affects the state being measured and, 2) the quantum correlations in the communication channels, arising from entanglement, an intrinsic quantum property, offers unique advantage of detecting tampering and other forms of external influence. The technique of splitting and sharing of quantum information among two or more parties, such that none of them can retrieve the information fully by operating on their own qubits, is usually referred to as Quantum information splitting (QIS). QIS of $|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$ and $(\alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1)$ has been proposed using GHZ [3,4] and asymmetric W states [5]. Later, QIS of $|\psi_1\rangle$ was experimentally demonstrated using single photon sources [6].

In the recent literature, a number of quantum networks, with only a few constituents have been analysed, which has demonstrated, the in-principle feasibility of quantum secret sharing and its advantage over, the classical protocols. In this context, a special class of entangled channels, the Cluster states [7–11], owing their origin to relatively better understood, Ising spin systems, have attracted considerable attention recently, because of their ability to carry out several quantum tasks, in a physically transparent manner [14].

Recently, the search for genuinely entangled channels, which can be used for the deterministic QIS of an arbitrary two qubit state $|\psi_2\rangle_{12} = \alpha|00\rangle + \mu|10\rangle + \gamma|01\rangle + \beta|11\rangle$, where $|\alpha|^2 + |\mu|^2 + |\gamma|^2 + |\beta|^2 = 1$ and $\alpha, \mu, \gamma, \beta \in \mathbb{C}$ has attracted much attention. It is worth mentioning that the GHZ and the asymmetric W states cannot be used for the QIS of arbitrary two qubit state $|\psi_2\rangle_{12}$, because they do not possess the required entangled structure to carry out the task [12]. However, a few specifically entangled multiqubit states [13–17] have been found useful for splitting $|\psi_2\rangle_{12}$ only among three parties. Further, these protocols required the parties to perform entangled measurements which are extremely difficult to realize in laboratory conditions. It is worth mentioning that one would require at least five qubits for splitting of an arbitrary two qubit state [14].

This motivates us to devise protocols for the splitting up of $|\psi_2\rangle_{12}$ among k parties, using a N -qubit linear cluster state by utilizing only product basis measurements. In general, an N -qubit linear cluster state can be represented as [8]

$$|C_N\rangle = \frac{1}{2^{N/2}} \bigotimes_{a=1}^N \left(|0\rangle_{\alpha} \sigma_z^{a+1} + |1\rangle_{\alpha} \right). \quad (1)$$

* Corresponding author. Tel.: +91 9748918201; fax: +91 3323348092.
E-mail address: prasanta@prl.res.in (P.K. Panigrahi).

The paper has been organized as follows. We first describe explicit circuits for the generation of N -qubit linear cluster states. In the next section, we study the splitting of arbitrary two qubit quantum information $|\psi_2\rangle_{12}$ among k different parties. Explicit circuits for the same have been constructed, wherein the measurements have been performed on the product basis. In the last section, we explain the protocol further by giving illustrations of QIS using five and six qubit cluster states.

In general, any N -qubit linear cluster state can be generated from $|000\dots 0\rangle_{123\dots N}$ by implementing the circuit diagram shown in Fig. 1.

2. QIS of $|\psi_2\rangle_{12}$ among k parties

The protocol for the splitting of an arbitrary two qubit secret $|\psi_2\rangle_{12}$ among k different parties using $|C_N\rangle$ can be divided into two major steps: “Locking” and “unlocking” of quantum secret. We label the participants Alice, $Bob_1, Bob_2, \dots, Bob_{k-1}$ and Charlie, where Charlie is designated to get the final state. Before distributing the qubits among the parties, the qubits of $|C_N\rangle$ are swapped in the following manner,

$$|C_N\rangle \xrightarrow{\text{Swap}(N-2,N), \dots, \text{Swap}(3,5), \text{Swap}(1,3)} (|C'_N\rangle), \text{ if } N \text{ is odd} \quad (2)$$

$$|C_N\rangle \xrightarrow{\text{Swap}(N/2,N), \text{Swap}(1, N/2+1), \dots, \text{Swap}(2,4)} (|C'_N\rangle), \text{ if } N \text{ is even} \quad (3)$$

where $\text{Swap}(i,j)$ represents the swapping of “ i ”th and “ j ”th qubits respectively. We now distribute the qubits such that $|c_1\rangle$ and $|c_2\rangle$ belong to Alice, $|c_3\rangle$ and $|c_4\rangle$ belong to Bob_1 , qubit $|c_5\rangle$ to Bob_2, \dots and the qubits $|c_{N-1}\rangle$ and $|c_N\rangle$ to Charlie, where the “ i ”th qubit ($i \geq N$) of $|C_N\rangle$ is denoted by $|c_i\rangle$. The QIS scheme for $N=5$ and 6 will be explicated below. For $N \geq 6$, we let Alice, Bob_1 , and Charlie possess two qubits each and each of the remaining $(N-5)$ participants possess one qubit.

2.1. Locking the quantum secret

In order to lock $|\psi_2\rangle_{12}$ among the other participants, she initially swapped the qubits of $|C_N\rangle$ as per the rule discussed above and swaps the qubit $|\psi_2\rangle_2$ and $|C_N\rangle_2$, as is explicitly shown in Fig. 2. This is followed by a $CNOT$ gate between $|\psi_1\rangle$ and $|\psi_2\rangle$, a Hadamard on $|\psi_2\rangle$ in order to “break” the entangled measurements into product measurements. She measures each of her four qubits individually in the basis $(|0\rangle, |1\rangle)$ and conveys the outcome of the measurement to Charlie via four classical bits. The information is thus locked amongst the parties $Bob_1, Bob_2, \dots, Bob_{(N-5)}, (N>5)$ and Charlie such that none of them can obtain the quantum secret by operating on their own qubits. The circuits explicitly constructed for this protocol are shown in Fig. 2 or Fig. 3 for a even or odd N respectively.

2.2. Unlocking the quantum secret

For unlocking $|\psi_2\rangle_{12}$, the parties should act as follows. Initially, Bob_1 performs a $CNOT_{3,4}$ operation on the two qubits $|c_3\rangle$ and $|c_4\rangle$,

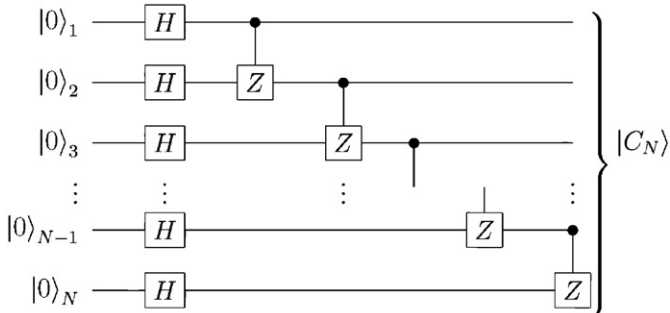


Fig. 1. Circuit diagram for the generation of $|C_N\rangle$.

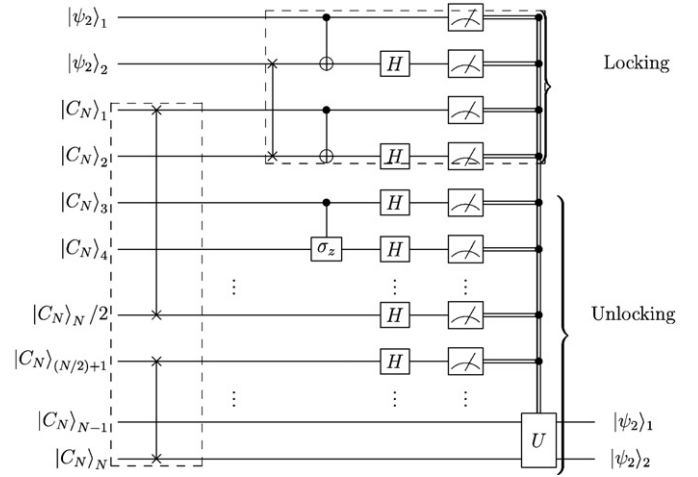


Fig. 2. Circuit diagram for the locking and unlocking in QIS using $|C_N\rangle$ (N is even).

projects the two qubits on the computational basis given by, $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$ and conveys the outcome of the measurement to Charlie via two cbits. The other participants, $Bob_i, i \in 2, \dots, (N-5)$ perform a Hadamard measurement $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ and conveys the outcome to Charlie via cbits. Once Charlie obtains all the $(N-4)$ measurement results (including Alice's measurement outcome), he can perform a suitable set of operations on his two qubits and deterministically obtain $|\psi_2\rangle_{12}$. Thus, Alice's quantum secret $|\psi_2\rangle_{12}$ which was initially split among $(N-5)$ intermediate parties was sent to Charlie by performing only product basis measurements. This completes the proposed QIS scheme. The quantum circuits in Figs. 2 and 3, depending on whether N is even or odd, show these steps clearly.

3. Illustrations

We shall now illustrate the above proposed protocol explicitly for $N=5$ and $N=6$ respectively. We shall also provide relations between the classical bits received by Charlie by the different parties and the local operations to be performed by him in order to deterministically obtain $|\psi_2\rangle_{12}$.

3.1. QIS of $|\psi_2\rangle_{12}$ using five qubit cluster state $|C_5\rangle$

The five qubit cluster state

$$|C_5\rangle = \frac{1}{2}(|00101\rangle - |00010\rangle - |11001\rangle + |11110\rangle), \quad (4)$$

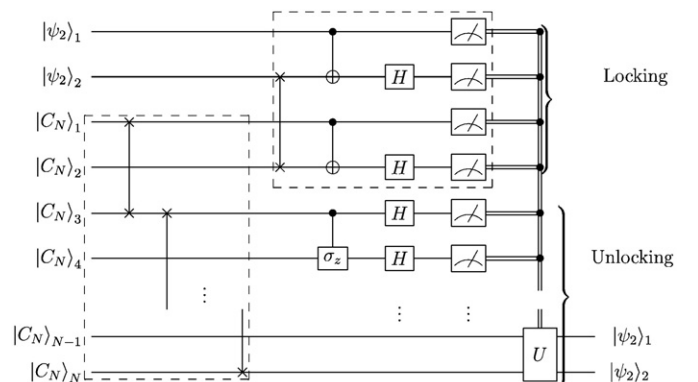


Fig. 3. Circuit diagram for the locking and unlocking in QIS using $|C_N\rangle$ (N is odd).

can be generated using the circuit shown in Fig. 1. After performing the required SWAP operations between qubits 1 and 3 and the qubits 3 and 5, the resultant state is given by,

$$|C'_5\rangle = \frac{1}{2}(|00010\rangle + |01101\rangle - |10100\rangle - |11011\rangle). \quad (5)$$

$|C'_5\rangle$ forms an important resource for QIS among three parties. The qubits are distributed such that Alice possesses the qubits 1 and 2 of $|C'_5\rangle$ along with $|\psi_2\rangle_{12}$, which is to be split among the two parties, Bob_1 and Charlie. We let Bob_1 possess qubit 3 and Charlie possess qubits 4 and 5. In the next step, Alice performs a measurement on each of her four qubits individually in the basis $(|0\rangle, |1\rangle)$, thereby locking the quantum secret in the Bob–Charlie system. She then conveys the outcome of her measurement to Charlie via four classical bits. It is worth mentioning that, at this stage Charlie cannot decipher $|\psi_2\rangle_{12}$, with Alice's measurement outcome alone. In order to unlock $|\psi_2\rangle_{12}$, Bob_1 performs a Hadamard measurement on his qubit (since no entangling operation is performed for $N \leq 5$) and sends the result to Charlie via one classical bit. Having obtained the outcomes of both Alice and Bob_1 , Charlie can now deterministically reconstruct $|\psi_2\rangle_{12}$ by applying suitable unitary operations on his qubits.

We denote the 4 classical bits sent by Alice to Charlie as, “ $a_1a_2a_3a_4$ ” and the single classical bit sent by Bob_1 as “ b_1 ”. The unitary local operation U to be performed by Charlie in order to obtain $|\psi_2\rangle_{12}$ is then given by,

$$U = (\bar{a}_4 \cdot \bar{a}_2 (\sigma_x \otimes I) + \bar{a}_4 \cdot a_2 (I \otimes \sigma_x) + a_4 \cdot \bar{a}_2 (I \otimes I) + a_4 \cdot a_2 (\sigma_x \otimes \sigma_x)) \cdot CNOT_{2,1} \cdot Swap_{1,2} \cdot ((\bar{a}_1 \oplus a_3) \cdot (\bar{a}_3 \oplus b_1) (I \otimes \sigma_z) + (\bar{a}_1 \oplus a_3) \cdot (a_3 \oplus b_1) (\sigma_z \otimes I) + (a_1 \oplus a_3) \cdot (\bar{a}_3 \oplus b_1) (\sigma_z \otimes \sigma_z) + (a_1 \oplus a_3) \cdot (a_3 \oplus b_1) (I \otimes I)). \quad (6)$$

Here, \oplus and \bar{a}_i denote the classical XOR and NOT respectively.

For instance, let us suppose that the cbits sent by Alice, $a_1a_2a_3a_4$ be 1110, and that by Bob be “1”. The unitary operation U that Charlie should apply on his two qubits is then given by, $U = (\sigma_x \otimes I) \cdot CNOT_{2,1} \cdot Swap_{1,2} \cdot (I \otimes \sigma_z)$. The local operations U for other classical messages can be obtained in a similar manner.

An explicit circuit showing the two stages, locking and unlocking of the $|\psi_2\rangle_{12}$ is given in Fig. 4. This protocol assumes significance, since five is the threshold number of qubits that is required for the QIS of an arbitrary two qubit state $|\psi_2\rangle_{12}$ in the case where both the parties involved need not meet. Further, this protocol is easier for experimental implementation than the previous protocol as it involves only product measurements [14].

3.2. QIS of $|\psi_2\rangle_{12}$ using six qubit cluster state

The six qubit linear cluster state $|C_6\rangle$ can be generated using the circuit shown in Fig. 1. We then perform swap operations ($Swap(1,4)$, $Swap(3,6)$) on $|C_6\rangle$ and the resultant cluster state is given by,

$$|C'_6\rangle = \frac{1}{2\sqrt{2}}(|010101\rangle - |010010\rangle - |001001\rangle + |001110\rangle + |100101\rangle - |100010\rangle - |111001\rangle - |111110\rangle). \quad (7)$$

This state can be used to establish the QIS protocol among $(N-3)=3$ parties namely, Alice, Bob_1 , and Charlie. To initialize the protocol, we let Alice possess the qubits 1 and 2 (along with $|\psi_2\rangle$), Bob_1 possess qubits 3 and 4 and Charlie possess qubits 5 and 6, as stated in the generalized scheme discussed in Section 3.1. Next, Alice performs a four particle computational basis measurement, and conveys the outcome to Charlie using four classical bits, thereby locking the quantum secret between Bob_1 and Charlie. In the next step, in order to unlock $|\psi_2\rangle_{12}$, Bob_1 performs a $CNOT_{3,4}$ operation on his two qubits. He measures the outcome in the computational basis as in the previous case after applying Hadamard states and sends the results to Charlie via two classical bits. Having known the outcomes of the measurement of Alice and Bob , Charlie can apply suitable unitary operation U and deterministically retrieve $|\psi_2\rangle_{12}$.

If $a_1a_2a_3a_4$ denotes the four cbits sent by Alice and b_1b_2 denote the ones sent by Bob , then the local unitary operation to be performed by Charlie, corresponding to the different messages, is given by,

$$U = \left[\bar{a}_4 \cdot ((\sigma_x \otimes I) \cdot ((\bar{a}_1 \oplus a_2 \oplus b_1) \oplus (a_3 \oplus b_2))) + (I \otimes I) \cdot ((a_1 \oplus a_2 \oplus b_1) \oplus (a_3 \oplus b_2)) \right] + a_4 \cdot ((I \otimes \sigma_x) \cdot ((\bar{a}_1 \oplus a_2 \oplus b_1) \oplus (a_3 \oplus b_2))) + (\sigma_x \otimes \sigma_x) \cdot ((a_1 \oplus a_2 \oplus b_1) \oplus (a_3 \oplus b_2)) \cdot CNOT_{2,1} \cdot ((\bar{a}_1 \oplus a_3) \cdot ((\sigma_z \otimes I) \cdot ((\bar{a}_3 \oplus b_2))) + (I \otimes \sigma_z) \cdot (a_3 \oplus b_2)) + (a_1 \oplus a_3) \cdot ((\sigma_z \otimes \sigma_z) \cdot ((\bar{a}_3 \oplus b_2))) + (I \otimes I) \cdot (a_3 \oplus b_2) \right]. \quad (8)$$

For instance, if the four cbits sent by Alice, $a_1a_2a_3a_4$ are 0100 and that by Bob b_1b_2 are 01, then the unitary operation U is given by, $U = (I \otimes \sigma_x) \cdot CNOT_{2,1} \cdot (I \otimes \sigma_z)$. Appropriate local operations corresponding to other messages can be obtained in a similar way.

An explicit circuit showing locking and unlocking of the $|\psi_2\rangle_{12}$ for the case of $|C_6\rangle$ is shown below in Fig. 5.

4. Conclusion

In this paper, we have explicated the creation and the use of N -qubit cluster states for the generalization of quantum information splitting

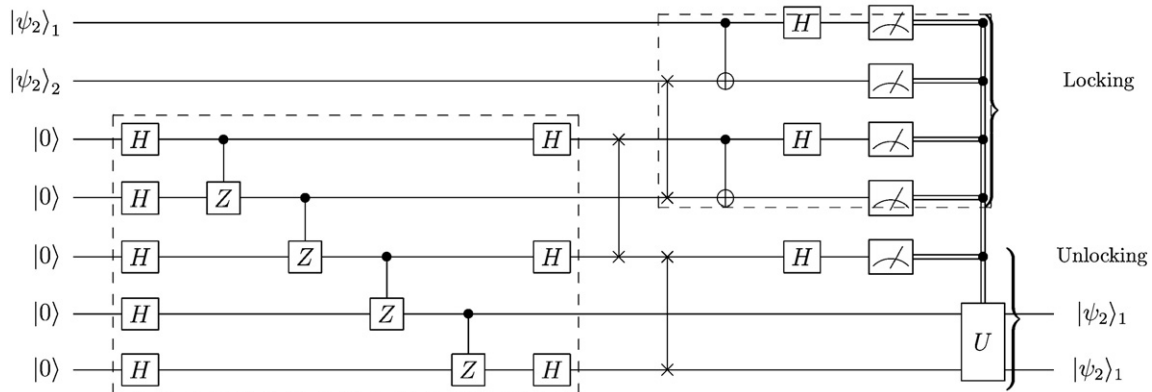


Fig. 4. Circuit diagram for the locking and unlocking in QIS using $|C_5\rangle$.

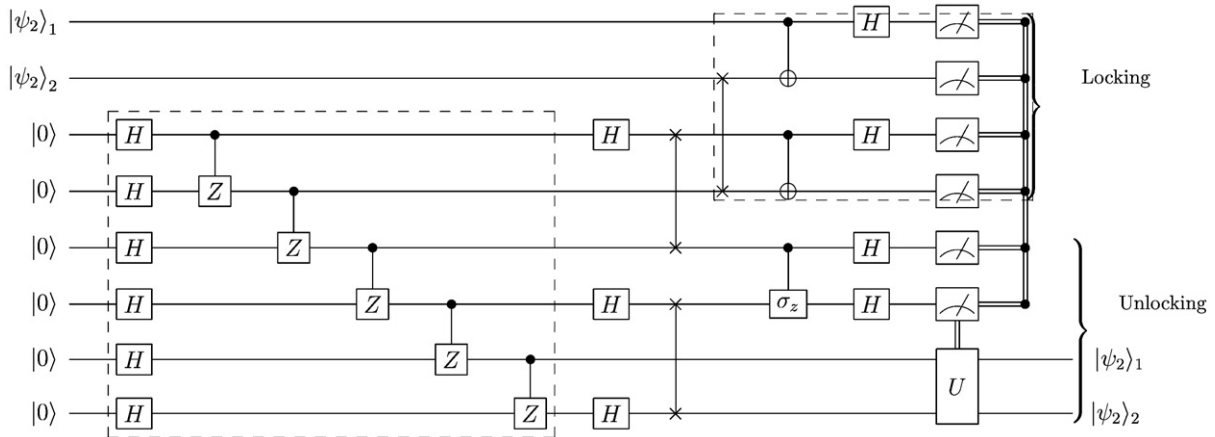


Fig. 5. Circuit diagram for the locking and unlocking of two qubit quantum secret using $|C_6\rangle$.

(QIS) protocol among k different parties. Explicit circuit diagrams involving only experimentally realizable quantum gates have been described. Unlike the presented scheme, most of the schemes that deal with the QIS of an arbitrary two qubit state in the literature involve splitting of quantum information only among limited number of parties. However, using the protocol proposed in this paper, one can have a QIS scheme that involves any number of parties. Secondly, the schemes developed so far in literature, either involve highly correlated multipartite measurements, which are extremely difficult to implement in experimental conditions or they use realizable Bell type measurements but with larger number of entangled photons. However, the illustrated protocol uses N -qubit linear cluster states $|C_N\rangle$ which employs only computational basis measurements thereby making it feasible for experimental realization. Further, the initial resource used, i.e., the cluster states are shown to be robust against decoherence [18]. We hope that this will lead to experimental realization of QIS of an arbitrary two qubit state among any number of involved parties, which has long been a challenge to the experimentalists.

References

- [1] M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge Univ. Press, 2002.
- [2] D. Gottesman, Phys. Rev. A 61 (2000) 042311.
- [3] M. Hillery, V. Bužek, A. Berthiaume, Phys. Rev. A 59 (1999) 1829.
- [4] S. Bandyopadhyay, Phys. Rev. A 62 (2000) 012308.
- [5] S.B. Zheng, Phys. Rev. A 74 (2006) 054303.
- [6] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, H. Weinfurter, Phys. Rev. Lett. 95 (2005) 230505.
- [7] R. Raussendorf, H.J. Briegel, Phys. Rev. Lett. 86 (2001) 5188.
- [8] H.J. Briegel, R. Raussendorf, Phys. Rev. Lett. 86 (2001) 910.
- [9] C.Y. Lu, X.Q. Zhou, O. Gühne, W.B. Gao, J. Zhang, Z.S. Yuan, A. Goebel, T. Yang, J.W. Pan, Nature 3 (2007) 91.
- [10] P.J. Blythe, B.T.H. Varcoe, New J. Phys. 8 (2006) 231.
- [11] Y. Soudagar, F. Bussières, G. Berln, S. Lacroix, J.M. Fernandez, N. Godbout, J. Opt. Soc. Am. B 24 (2007) 226.
- [12] S. Muralidharan, S. Karumanchi, R. Srikanth, P.K. Panigrahi, eprint, quant-ph/0907.3532.
- [13] S. Muralidharan, P.K. Panigrahi, Phys. Rev. A 77 (2008) 032321.
- [14] S. Muralidharan, P.K. Panigrahi, Phys. Rev. A 78 (2008) 062333.
- [15] S. Choudhury, S. Muralidharan, P.K. Panigrahi, J. Phys. A 42 (2009) 115303.
- [16] X.W. Wang, Z.H. Peng, C.X. Jia, Y.H. Wang, X.J. Liu, Opt. Commun. 282 (2009) 670.
- [17] S. Muralidharan, S. Karumanchi, P.K. Panigrahi, eprint, quant-ph/0804.4206v2.
- [18] W. Dur, H.J. Briegel, Phys. Rev. A 70 (2004) 180403.