IJCAT International Journal of Computing and Technology, Volume 1, Issue 5, June 2014
ISSN : 2348 - 6090
www.IJCAT.org

Two-Way Quantum Communication: Secure Exchange of Quantum Information Encoded in Arbitrary Number of Qubits

[1] Ajay K Maurya, [2] Manoj K Mishra, [3] Hari Prakash

[1, 2] Physics Department, University of Allahabad, Allahabad-211002, India

[3] Indian Institute of Information Technology, Allahabad-211002, India

Abstract - In this work, we generalize the secure quantum information exchange (SQIE) protocol [J. Phys. B: At. Mol. Opt. Phys. 44 (2011) 115504], originally proposed for secure exchange of single qubit information with each of Alice and Bob, to the case of secure exchange of multi-qubit information. We investigate the security of the original and generalized SQIE protocols against the number of qubits with the controller Charlie.

Keywords **- Quantum entanglement, Quantum communication, Quantum teleportation, Qubit, Generalized Bell states**

1. Introduction

Communication (exchange of information) involves at least a sender to transmit the information and a receiver. Faithful communication occurs only when the receiver is able to reconstruct the exact information that the sender intended to transmit. All the existing practical communication systems, either secure (private) or insecure (public), are capable of transmitting the classical messages (encoded in a string of bits '0' and '1') over a classical channel and are governed by the laws of classical physics.

Over the past decade, researchers have made appreciable progress in the field of quantum information theory and realized that the performance of communication can be enhanced by using transmission channels, which are governed by the laws of quantum mechanics. For example, quantum cryptography [1] allows to distribute a secret-key between two legitimate users say, Alice (sender) and Bob (receiver) with no assumptions of computational powers of eavesdropper, Eve. Another example is quantum superdense coding [2] that allows to send two-bit classical message by sending a single two-level particle and sharing an EPR pair, while classically it is required to send a four-level particle. Thus, transmission capacity of classical information transfer is doubled by using EPR-correlation as quantum channel. The two examples given above are the steps towards the transmission of classical information over a quantum channel.

Now let us consider transmission of qubits. Since no-cloning theorem does not allow us to have many copies of an unknown qubit, which avoids us to extract complete information about the state of an unknown qubit and therefore it is not possible to transmit an unknown qubit in the form of classical information to the receiver through a classical channel. Also anyhow if state of qubit is known (*i.e.*, θ & ϕ of qubit $\cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$ are known), then since θ & ϕ can have infinite possible values that will require infinite number of bits sending to the receiver to construct the qubit. For these reasons, it is not possible to transfer quantum information encoded in a qubit through classical channel.

To overcome such problem, Bennett et al [3] introduced the idea of quantum teleportation (QT) that involves complete transfer of quantum states of a qubit from sender (Alice) to receiver (Bob) using quantum entanglement and restricted amount of classical communication. The idea of QT has been extended from single qubit to multi qubits [4-6] and several schemes have been proposed for experimental realization of QT for photonic states [7], photonic-polarized states [8], optical coherent states [9-10] and atomic states [11-12]. Also several experiments have demonstrated QT with photonic-polarized state [13], quantum state of nucleus [14] and atomic qubits [15-16].

M. Hillery [17] using GHZ state proposed quantum secret sharing in which quantum information splits into two receivers, while Karlsson and Bourennane [18] used GHZ state to teleport single qubit to one of the two receivers, such that only one of them (anyone) can completely

reconstruct the qubit depending upon the local measurement result of the other receiver. The use of more than two entangled qubits leads us to the concept of controlled QT in which quantum state can be reconstructed only by one receiver and the local measurement and classical communication by other receiver. Controlled QT is found to be useful in one-way secure quantum networking and in cryptographic conferencing [19-20]. Many authors presented the controlled QT scheme to teleport single qubit information state using GHZ like states [21] and W-state [22]. Further the idea of controlled QT was extended by many authors [23] for teleporting multi-qubit information states.

Very recently, in reference [24], idea of secure quantum information exchange (SQIE) is proposed, which enables faithful exchange of two unknown single qubit states between two legitimate users, Alice and Bob, using a special kind of six-qubit entangled (SSE) state and a third party Charlie. This protocol is secure in the sense that either both, Alice and Bob, obtain their required information states or if this end result is not obtained due to any reason, nobody gets the correct information state. Also Alice and Bob cannot reconstruct the required information states by mutual communication about their measurement results without involving Charlie.

Practically, not only exchange of single qubits but also the secure exchange of multi qubits will be required in the real world. For this reason, in the present paper, we extend the SQIE protocol from single qubit to multi qubits. Further, we also investigate the security of the original SQIE protocol and the generalized protocol when the number of qubits with the controller Charlie (the third party) is changed.

2. Generalization of SQIE Protocol to the Information States of Arbitrary Number of Qubits

In this section, we first present a brief review of the original SQIE protocol* [24] and then we will generalize this protocol to achieve secure exchange of information states involving an arbitrary number of qubits between Alice and Bob.

Let it be required that Alice has to send arbitrary information state $|\xi\rangle_A^I = [a_0|0\rangle + a_1|1\rangle]_A$ to Bob and at the same time, Bob has to send another information state $|\eta\rangle_B^I = [b_0|0\rangle + b_1|1\rangle]_B$ to Alice. This exchange process must be done in a way that both users get their required information states. However, if this is not obtained due to any reason, then nobody should get the correct information state.

For this purpose, we use the SSE states [24],

$$|\psi\rangle^E_{A_1,B_1,B_2,A_2,C_1,C_2} = \tfrac{1}{2}[\textstyle\sum_{i=0}^{3}|B\rangle^{(i)}_{A_1,B_1} \otimes |B\rangle^{(i)}_{B_2,A_2} \otimes |\phi\rangle^{(i)}_{C_1,C_2}], \quad (1)$$

where, $|B\rangle^{(0,1)} = \frac{1}{\sqrt{2}}[|00\rangle \pm |11\rangle]$, $|B\rangle^{(2,3)} = \frac{1}{\sqrt{2}}[|01\rangle \pm |10\rangle]$ are the standard bi-partite Bell states and $|\phi\rangle^{(0,1,2,3)}$ are different elements of the set $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$ taken in any arbitrary order. Entangled modes A_1 and A_2 are with Alice, B_1 and B_2 are with Bob, while C_1 and C_2 are with the controller Charlie. The superscripts E and I are used for entangled state and information states respectively.

We can write the initial state of composite system as,

$$\begin{aligned}|\psi\rangle_{A,A_1,B_1,B_2,A_2,C_1,C_2,B} &= |\xi\rangle_A^I \otimes |\psi\rangle^E_{A_1,B_1,B_2,A_2,C_1,C_2} \otimes |\eta\rangle_B^I \\ &= \tfrac{1}{2}[\textstyle\sum_{i=0}^{3}(|\xi\rangle_A^I \otimes |B\rangle^{(i)}_{A_1,B_1}) \otimes (|B\rangle^{(i)}_{B_2,A_2} \otimes |\eta\rangle_B^I) \\ &\qquad \otimes |\phi\rangle^{(i)}_{C_1,C_2}].\end{aligned} \quad (2)$$

From Appendix A, we see that,

$$\begin{aligned}|\xi\rangle_A^I \otimes |B\rangle^{(i)}_{A_1,B_1} &= \tfrac{1}{2}[\textstyle\sum_{r=0}^{3}|B\rangle^{(r)}_{A,A_1} \otimes (\sigma^{(i)}_{B_1}\sigma^{(r)}_{B_1})|\xi\rangle^I_{B_1}], \\ |\eta\rangle_B^I \otimes |B\rangle^{(i)}_{B_2,A_2} &= \tfrac{1}{2}[\textstyle\sum_{s=0}^{3}|B\rangle^{(s)}_{B,B_2} \otimes (\sigma^{(i)}_{A_2}\sigma^{(s)}_{A_2})|\eta\rangle^I_{A_2}],\end{aligned} \quad (3)$$

where $\sigma^{(i)}$'s are real matrices, I, σ_z, σ_x, $\sigma_x\sigma_z$ for i=0, 1, 2, 3 respectively. Using equations (3), we can write equation (2) as,

$$\begin{aligned}|\psi\rangle_{A,A_1,B_1,B_2,A_2,C_1,C_2,B} &= \tfrac{1}{8}[\sum_{i,r,s=0}^{3}(|B\rangle^{(r)}_{A,A_1} \otimes (\sigma^{(i)}_{B_1}\sigma^{(r)}_{B_1})|\xi\rangle^I_{B_1}) \\ &\qquad \otimes (|B\rangle^{(s)}_{B,B_2} \otimes (\sigma^{(i)}_{A_2}\sigma^{(s)}_{A_2})|\eta\rangle^I_{A_2}) \otimes |\phi\rangle^{(i)}_{C_1,C_2}]\end{aligned} \quad . \quad (4)$$

* The notations used here for original SQIE are not exactly the same as used earlier [24]. The change was required to make the generalization of these results, presented later in this section, more lucid and more presentable.

Alice and Bob perform Bell state measurement (BSM) on their qubits in modes A, A_1 and B, B_2 respectively and communicate their BSM results, say, r and s, in the forms of 2-cbits to Charlie through classical channels, while Charlie performs measurement in the computational basis $\{|0\rangle, |1\rangle\}$ on his qubits in modes C_1 and C_2. Based on the classical bits received and his own measurement results, Charlie decides the two 2-cbits information to be transmitted to each of Alice and Bob, which are necessary to make the correct unitary transformations on their particles A_2 and B_1 respectively for getting the replicas of required information states. From equation (4), it is clear that if result of Charlie's measurement is i, then Alice performs unitary transformation $(\sigma_{A_2}^{(i)}\sigma_{A_2}^{(s)})^{\dagger}$ and Bob performs unitary transformation $(\sigma_{B_1}^{(i)}\sigma_{B_1}^{(r)})^{\dagger}$.

We now generalize this SQIE protocol to secure exchange the information states of arbitrary number of qubits between Alice and Bob. For this, we consider that Alice wants to send to Bob arbitrary m-qubit information state, encoded in m-qubit modes $\{A\} \equiv (A_1, A_2, ..., A_m)$, expressed by

$$|\xi\rangle_{\{A\}}^{I} = [a_0|\tilde{0}\rangle + a_1|\tilde{1}\rangle + ... + a_M|\tilde{M}\rangle]_{\{A\}}, \qquad (5)$$

and Bob wants to send to Alice arbitrary n-qubit information state, encoded in n-qubit modes $\{B\} \equiv (B_1, B_2, ..., B_n)$, expressed by

$$|\eta\rangle_{\{B\}}^{I} = [b_0|\tilde{0}\rangle + b_1|\tilde{1}\rangle + ... + b_N|\tilde{N}\rangle]_{\{B\}}, \qquad (6)$$

with the same security that was there in the original SQIE protocol discussed above. Here, $M \equiv 2^m - 1$, $N \equiv 2^n - 1$ and for modes $\{A\}$, if $0 \le j \le M$ and $j = (j_1\, j_2 .... j_m)$ in the binary representation, state $|\tilde{j}\rangle_{\{A\}} = |j_1\, j_2 .... j_m\rangle_{\{A\}}$. 2^m-mutually orthogonal states $|\tilde{0}\rangle_{\{A\}}$, $|\tilde{1}\rangle_{\{A\}}$, ..., $|\tilde{M}\rangle_{\{A\}}$ form the computational basis for modes $\{A\}$. Similarly for modes $\{B\}$, if $0 \le j \le N$ and $j = (j_1\, j_2 .... j_n)$ in the binary representation, state $|\tilde{j}\rangle_{\{B\}} = |j_1\, j_2 .... j_n\rangle_{\{B\}}$. Superscripts I refer to information states.

If $p = \max\{m, n\}$, we give $2p$-qubits to Charlie. The problem at this moment is to write the entangled state corresponding to the SSE state of the original SQIE protocol. In the original protocol, Charlie had 2 qubits and SSE state had 2^2=4 terms. $2p$-qubits of Charlie thus requires 2^{2p} terms. If we consider generalized Bell states (GBS) [5] of modes $\{A'\} \equiv (A_1', A_2', ..., A_m')$ and $\{B'\} \equiv (B_1', B_2', ..., B_m')$ and of $\{B''\} \equiv (B_1'', B_2'', ..., B_n'')$ and $\{A''\} \equiv (A_1'', A_2'', ..., A_n'')$, there are only 2^{2m} and 2^{2n} GBS respectively and only one of these gives a family of 2^{2p} states if $m \ne n$. If $m > n$, 2^{2m}=2^{2p} but 2^{2n} falls shorter than 2^{2p} and if $n > m$, 2^{2n}=2^{2p} but 2^{2m} falls shorter than 2^{2p}. This problem is circumvented by repeating the members of smaller family of states $2^{2|m-n|}$ times.

Thus, if index i takes values 0, 1, ….., 2^{2p}-1, we can define indices $i' \equiv i \pmod{2^{2m}}$ and $i'' \equiv i \pmod{2^{2n}}$ and write GBS,

$$|E\rangle_{\{A'\},\{B'\}}^{(i)} = |E\rangle_{\{A'\},\{B'\}}^{(i')} \text{ and } |E\rangle_{\{B''\},\{A''\}}^{(i)} = |E\rangle_{\{B''\},\{A''\}}^{(i'')}.$$

The entangled state corresponding to SSE state of the original SQIE protocol can be written as,

$$|\psi\rangle_{\{A'\},\{B'\},\{B''\},\{A''\},\{C\}}^{E} = \frac{1}{2^p}\Big[\sum_{i=0}^{2^{2p}-1} |E\rangle_{\{A'\},\{B'\}}^{(i)} \otimes |E\rangle_{\{B''\},\{A''\}}^{(i)} \otimes |\phi\rangle_{\{C\}}^{(i)}\Big], \qquad (7)$$

Here, modes $\{C\} \equiv (C_1, C_2, ..., C_{2p})$ and states $\{|\phi\rangle_{\{C\}}^{(i)}\}$ are different orthogonal 2^{2p}-states belonging to the computational basis $(|\tilde{0}\rangle, |\tilde{1}\rangle, ..., |\tilde{P}\rangle)$, $(P \equiv 2^{2p} - 1)$ in 2^{2p}-dimensional Hilbert space, taken in any order. Superscript E refers to entangled state.

We may now specify the GBS. Since $0 \le i' \le 2^{2m} - 1$, if we express i' in quaternary basis as $i' = (i_1' i_2' .... i_m')$ and write

$$|E\rangle_{\{A'\},\{B'\}}^{(i')} = U_{\{B'\}}^{(i')}|E\rangle_{\{A'\},\{B'\}}^{(0)} = U_{\{B'\}}^{(i')}\frac{1}{2^{m/2}}\sum_{k=0}^{M}|\tilde{k}\rangle_{\{A'\}} \otimes |\tilde{k}\rangle_{\{B'\}}, \qquad (8)$$

where

$$U_{\{B'\}}^{(i')} = (\sigma_{B_1'}^{i_1'} \otimes \sigma_{B_2'}^{i_2'} \otimes ..... \otimes \sigma_{B_m'}^{i_m'}), \qquad (9)$$

and $\sigma^{(0,1,2,3)} = (I, \sigma_z, \sigma_x, \sigma_x\sigma_z)$. The other GBS can be expressed similarly in the form,

$$|E\rangle_{\{B''\},\{A''\}}^{(i'')} = (U_{\{A''\}}^{(i'')})|E\rangle_{\{B''\},\{A''\}}^{(i'')} = (U_{\{A''\}}^{(i'')})\frac{1}{2^{n/2}}\sum_{k=0}^{N}|\tilde{k}\rangle_{\{B''\}} \otimes |\tilde{k}\rangle_{\{A''\}}, \qquad (10)$$

where

$$U_{\{A''\}}^{(i'')} = (\sigma_{A_1''}^{i_1''} \otimes \sigma_{A_2''}^{i_2''} \otimes ..... \otimes \sigma_{A_n''}^{i_n''}), \quad (11)$$

$\sigma^{(0,1,2,3)} = (I, \sigma_z, \sigma_x, \sigma_x\sigma_z)$ and $i'' \in (0,1,.....,2^{2n}-1)$ is decimal conversion of the quaternary number $(i_1''i_2''....i_n'')$.

Using equations (5), (6) and (7), the initial state of composite system can be written as,

$$\begin{aligned} &|\psi\rangle_{\{A\},\{A'\},\{B'\},\{B''\},\{A''\},\{C\},\{B\}} \\ &= |\xi\rangle_{\{A\}}^{I} \otimes |\psi\rangle_{\{A'\},\{B'\},\{B''\},\{A''\},\{C\}}^{E} \otimes |\eta\rangle_{\{B\}}^{I} \\ &= \frac{1}{2^p}\Big[\sum_{i=0}^{2^{2p}-1} \big(|\xi\rangle_{\{A\}}^{I} \otimes |E\rangle_{\{A'\},\{B'\}}^{(i)}\big) \\ &\qquad \otimes \big(|E\rangle_{\{B''\},\{A''\}}^{(i)} \otimes |\eta\rangle_{\{B\}}^{I}\big) \otimes |\phi\rangle_{\{C\}}^{(i)}\Big] \end{aligned} \quad . \quad (12)$$

Qubits in modes $\{A\},\{A'\},\{A''\}$ belong to Alice, qubits in modes $\{B\},\{B'\},\{B''\}$ belong to Bob and qubits in modes $\{C\}$ belong to Charlie.

From Appendix B, we see that the states, $|\xi\rangle_{\{A\}}^{I} \otimes |E\rangle_{\{A'\},\{B'\}}^{(i)}$ and $|E\rangle_{\{B''\},\{A''\}}^{(i)} \otimes |\eta\rangle_{\{B\}}^{I}$, in equation (12), can be rewritten as,

$$\begin{aligned} &|\xi\rangle_{\{A\}}^{I} \otimes |E\rangle_{\{A'\},\{B'\}}^{(i)} \\ &\quad = \frac{1}{2^m}\sum_{r=0}^{2^{2m}-1} |E\rangle_{\{A\},\{A'\}}^{(r)} \otimes U_{\{B'\}}^{(i)} U_{\{B'\}}^{(r)} |\xi\rangle_{\{B'\}}^{I} \end{aligned} \quad , \quad (13)$$

$$\begin{aligned} &|E\rangle_{\{B''\},\{A''\}}^{(i)} \otimes |\eta\rangle_{\{B\}}^{I} \\ &\quad = \frac{1}{2^n}\sum_{s=0}^{2^{2n}-1} |E\rangle_{\{B\},\{B''\}}^{(s)} \otimes U_{\{A''\}}^{(i)} U_{\{A''\}}^{(s)} |\xi\rangle_{\{A''\}}^{I} \end{aligned} \quad , \quad (14)$$

where the GBS $|E\rangle_{\{A\},\{A'\}}^{(r)}$ and $|E\rangle_{\{B\},\{B''\}}^{(s)}$ are given by equations (8) and (10) respectively, unitary matrices $U_{\{B'\}}^{(i)}$, $U_{\{A''\}}^{(i)}$, $U_{\{B'\}}^{(r)}$ and $U_{\{A''\}}^{(s)}$ are given by equations (9), (11), (B.3) and (B.6) respectively.

Using equations (13) and (14), equation (12) can be written as,

$$\begin{aligned} &|\psi\rangle_{\{A\},\{A'\},\{B'\},\{B''\},\{A''\},\{C\},\{B\}} \\ &= \frac{1}{2^p}\sum_{i=0}^{2^{2p}-1}\Big[\frac{1}{2^m}\Big\{\sum_{r=0}^{2^{2m}-1} |E\rangle_{\{A\},\{A'\}}^{(r)} \otimes U_{\{B'\}}^{(i)} U_{\{B'\}}^{(r)} |\xi\rangle_{\{B'\}}^{I}\Big\} \\ &\qquad \otimes \frac{1}{2^n}\Big\{\sum_{s=0}^{2^{2n}-1} |E\rangle_{\{B\},\{B''\}}^{(s)} \otimes U_{\{A''\}}^{(i)} U_{\{A''\}}^{(s)} |\eta\rangle_{\{A''\}}^{I}\Big\} \otimes |\phi\rangle_{\{C\}}^{(i)}\Big]. \end{aligned} \quad (15)$$

Alice may perform generalized $2m$-qubit Bell state measurement (BSM) on her qubits in modes $\{A\},\{A'\}$ and Bob may perform generalized $2n$-qubit BSM on his qubits in modes $\{B\},\{B''\}$, while Charlie measures his qubits in modes $\{C\}$, in the computational basis $\{|\tilde{0}\rangle, |\tilde{1}\rangle, ..., |\tilde{P}\rangle\}$. Alice and Bob may send their BSM results, say, r and s, to Charlie through $2m$-bit and $2n$-bit classical channels respectively. Depending on these classical information conveyed by Alice and Bob and his own result, Charlie can send classical information to Alice and Bob telling them to perform the required unitary transformations on their qubits $\{A''\}$ and $\{B'\}$ respectively, which generate the exact replicas of the corresponding information states. From equation (15), it can be seen that if result of Charlie's measurement is i, then Alice is required to perform unitary transformation $(U_{\{A'\}}^{(i)} U_{\{A'\}}^{(s)})^{\dagger}$ and Bob unitary transformation $(U_{\{B'\}}^{(i)} U_{\{B'\}}^{(r)})^{\dagger}$.

3. Security of SQIE Protocol with Respect to Change in the Number of Qubits Going to Charlie

In this section, we discuss security of SQIE protocol against the number of qubits with the controller Charlie. Let us first consider that there is no qubit with Charlie and the entangled state shared between Alice and Bob is just a product of the two standard bi-partite Bell states, $|\psi\rangle_{A_1,B_1,A_2,B_2}^{E} = |B\rangle_{A_1,B_1}^{(i)} \otimes |B\rangle_{A_2,B_2}^{(j)}$, with $i, j \in (0,1,2,3)$. Modes A_1, A_2 are with Alice and modes B_1, B_2 are with Bob. Such case is similar to two standard teleportation setups, one from Alice to Bob and other from Bob to Alice. There is no control of Charlie and this may lead to a situation when Alice sends her BSM result to Bob but Bob does not send his BSM result to Alice or vice versa, and thus makes the quantum information exchange insecure. In this case, there is unit probability for insecurity in the quantum information exchange, which is the upper bound of insecurity.

Let us next consider the second case when Charlie gets single qubit, *i.e.*, the entangled state shared between Alice, Bob and Charlie can be of the form,

$$|\psi\rangle^{E}_{A_1,B_1,A_2,B_2,C} = \frac{1}{\sqrt{2}}[|B\rangle^{(i)}_{A_1,B_1} \otimes |B\rangle^{(j)}_{A_2,B_2} \otimes |0\rangle_C + |B\rangle^{(i')}_{A_1,B_1} \otimes |B\rangle^{(j')}_{A_2,B_2} \otimes |1\rangle_C],$$

for $i, j, i', j' \in (0,1,2,3)$ with $i \neq i'$ and $j \neq j'$. Modes A_1, A_2 are with Alice and modes B_1, B_2 are with Bob, while mode C is with Charlie. In this case, Alice and Bob cannot get the required information states without the assistance of Charlie by creating a direct classical channel between them. The reason is that they do not know which channel ($|B\rangle^{(i)}_{A_1,B_1} \otimes |B\rangle^{(j)}_{A_2,B_2}$ or $|B\rangle^{(i')}_{A_1,B_1} \otimes |B\rangle^{(j')}_{A_2,B_2}$) is setup between them, as it will be determined by Charlie's measurement result; result $|0\rangle_C$ sets the channel $|B\rangle^{(i)}_{A_1,B_1} \otimes |B\rangle^{(j)}_{A_2,B_2}$, while result $|1\rangle_C$ sets the channel $|B\rangle^{(i')}_{A_1,B_1} \otimes |B\rangle^{(j')}_{A_2,B_2}$ between Alice and Bob. However, if Alice and Bob want to ignore the role of Charlie by communicating classically directly to each other, the probability for getting the required information states successfully is half, *i.e.*, probability for insecurity in the quantum information exchange is half. Thus, the second case is more secure than the first one discussed earlier.

We can now consider the third case, when Charlie has two qubits, which is the original SQIE protocol, introduced by the authors [24]. In this case, if Alice and Bob want to ignore the role of Charlie by creating classical channel between them, there is only one-fourth probability that they are able to get the required information states successfully. The reason is that they do not know which channel ($|B\rangle^{(0)}_{A_1,B_1} \otimes |B\rangle^{(0)}_{A_2,B_2}$ or $|B\rangle^{(1)}_{A_1,B_1} \otimes |B\rangle^{(1)}_{A_2,B_2}$ or $|B\rangle^{(2)}_{A_1,B_1} \otimes |B\rangle^{(2)}_{A_2,B_2}$ or $|B\rangle^{(3)}_{A_1,B_1} \otimes |B\rangle^{(3)}_{A_2,B_2}$) is setup between them, as it will be determined by Charlie's measurement result ($|00\rangle$ or $|01\rangle$ or $|10\rangle$ or $|11\rangle$) respectively. Thus the third case is more secure than the two cases discussed earlier.

If we now increase the number of qubits going to Charlie to three, the entangled state shared between the parties may be of the form, *say*,

$$\begin{aligned}|\psi\rangle^{E}_{A_1,B_1,A_2,B_2,C_1,C_2,C_3} = \frac{1}{2\sqrt{2}}[&|B\rangle^{(0)} \otimes |B\rangle^{(0)} \otimes |000\rangle \\ &+ |B\rangle^{(1)} \otimes |B\rangle^{(1)} \otimes |001\rangle + |B\rangle^{(2)} \otimes |B\rangle^{(2)} \otimes |010\rangle \\ &+ |B\rangle^{(3)} \otimes |B\rangle^{(3)} \otimes |011\rangle + |B\rangle^{(0)} \otimes |B\rangle^{(1)} \otimes |100\rangle \\ &+ |B\rangle^{(1)} \otimes |B\rangle^{(0)} \otimes |101\rangle + |B\rangle^{(2)} \otimes |B\rangle^{(3)} \otimes |110\rangle \\ &+ |B\rangle^{(3)} \otimes |B\rangle^{(2)} \otimes |111\rangle]_{A_1,B_1,A_2,B_2,C_1,C_2,C_3}.\end{aligned}$$

We may involve any eight possible quantum channels between Alice and Bob out of the possible sixteen and Charlie's measurement on his qubits decides the effective channel. Hence, the probability that Alice and Bob are successful in the information exchange without the assistance of Charlie is only one-eighth.

If we increase further the number of qubits going towards Charlie to four, the entangled state shared between them will be of the form, *say*,

$$|\psi\rangle^{E}_{A_1,B_1,A_2,B_2,C_1,C_2,C_3,C_4} = \frac{1}{4}[\sum_{i,j=0}^{3} |B\rangle^{(i)}_{A_1,B_1} \otimes |B\rangle^{(j)}_{A_2,B_2} \otimes |\phi\rangle^{(i)}_{C_1,C_2} \otimes |\phi\rangle^{(j)}_{C_3,C_4}],$$

where $|\phi\rangle^{(i)}$ and $|\phi\rangle^{(j)} \in (|00\rangle, |01\rangle, |10\rangle, |11\rangle)$. In this case, there are sixteen possible quantum channels between Alice and Bob and which one of these sixteen is effective, is decided by Charlie's measurement on his qubits. Hence the probability that Alice and Bob are successful in the information exchange without the assistance of Charlie is only one-sixteenth, *i.e.*, probability for insecurity in the quantum information exchange is only one-sixteenth.

It is clear that the security of the SQIE protocol cannot be increased any further by increasing the number of qubits going towards Charlie beyond four because there are only sixteen possible combinations of product of two standard bi-partite Bell states ($|B\rangle^{(i)}_{A_1,B_1} \otimes |B\rangle^{(j)}_{A_2,B_2}$). Thus if five qubits go to Charlie, the entangled state involves 16 quantum channels and 32 computational basis states of Charlie's qubits. Hence entangled state will have 32 terms and each quantum channel will appear twice. The probability for occurrence of right channel, if Charlie has been sidetracked, is one-sixteenth. Thus one-sixteenth is a lower bound for insecurity for quantum information exchange when Charlie gets four or more qubits.

This consideration can be generalized for exchange of multiple qubits. If Alice and Bob has to send *m* and *n* qubit states respectively, the number of possible quantum

channels between Alice and Bob is $2^{2(m+n)}$. Thus if Charlie gets l qubits, for $l < 2(m+n)$, the probability for insecurity is 2^{-l} and for $l \geq 2(m+n)$, it is $2^{-2(m+n)}$.

4. Conclusions

We generalized the original SQIE protocol to exchange the information states of arbitrary number of qubits between two users. We also discussed the security of SQIE protocol and its generalization against the number of qubits with the controller Charlie. We calculate the probability for success of Alice and Bob in getting correct exchange of quantum information without the assistance of Charlie, i.e., by establishing direct classical channel between them. We conclude that upper bound probability of insecurity in SQIE protocol is unity and it occurs when the role of Charlie is cut in the SQIE protocol by not sending any qubit to him. Also, the security of the SQIE protocol cannot be increased indefinitely by increasing the number of qubits going to Charlie. For intended exchange of m qubits of Alice with n qubits of Bob, if l qubits are being sent to Charlie, the probability of insecurity is 2^{-p}, where $p = \min(2(m+n), l)$.

Acknowledgements

We are thankful to *Prof. N. Chandra* and *Prof. R. Prakash* for their interest in this work. We would like to thank *Dr. D. K. Singh, Dr. D. K. Mishra, Dr. R. Kumar, Dr. P. Kumar*, *Mr. Vikram Verma*, and *Mr. Ajay K. Yadav* for helpful and stimulating discussions. Author MKM acknowledges financial support of UGC under UGC-SRF fellowship scheme and author AKM acknowledges financial support of UGC under UGC D. Phil scholarship scheme.

Appendix A

We can write the state $|\xi\rangle_A^I \otimes |B\rangle_{A_1,B_1}^{(i)}$ as,

$$|\xi\rangle_A^I \otimes |B\rangle_{A_1,B_1}^{(i)} = \sum_{r=0}^{3} |B\rangle_{A,A_1}^{(r)} {}^{(r)}\langle B| \left(|\xi\rangle_A^I \otimes |B\rangle_{A_1,B_1}^{(i)}\right). \quad \text{(A.1)}$$

Since we have

$$|B\rangle_{A_1,B_1}^{(i)} = \sigma_{B_1}^{(i)} |B\rangle_{A_1,B_1}^{(0)} = \frac{1}{\sqrt{2}} \sigma_{B_1}^{(i)} \sum_{k=0}^{1} |k\rangle_{A_1} \otimes |k\rangle_{B_1},$$

where $\sigma_{B_1}^{(i)}$ is real matrix I, σ_z, σ_x, $\sigma_x\sigma_z$ for i =0, 1, 2, 3 respectively. Then equation (A.1) can be written as,

$$\begin{aligned} &|\xi\rangle_A^I \otimes |B\rangle_{A_1,B_1}^{(i)} \\ &= \tfrac{1}{2} \sum_{r=0}^{3} \sum_{j,k,l=0}^{1} a_j |B\rangle_{A,A_1}^{(r)} {}_A\langle l| \otimes_{A_1} \langle l|\sigma_{A_1}^{(r)\dagger}|j\rangle_A \\ &\qquad \otimes |k\rangle_{A_1} \otimes \sigma_{B_1}^{(i)} |k\rangle_{B_1} \\ &= \tfrac{1}{2} \sum_{r=0}^{3} \sum_{j,k=0}^{1} a_j \sigma_{B_1}^{(i)} |B\rangle_{A,A_1}^{(r)} {}_{A_1}\langle j|\sigma_{A_1}^{(r)\dagger}|k\rangle_{A_1} \otimes |k\rangle_{B_1}, \end{aligned} \quad \text{(A.2)}$$

using ${}_A\langle l|j\rangle_A = \delta_{lj}$.

Since,

$$\begin{aligned} {}_{A_1}\langle j|\sigma_{A_1}^{(r)\dagger}|k\rangle_{A_1} &= {}_{B_1}\langle j|\sigma_{B_1}^{(r)\dagger}|k\rangle_{B_1} = {}_{B_1}\langle k|\sigma_{B_1}^{(r)*}|j\rangle_{B_1}, \\ &= {}_{B_1}\langle k|\sigma_{B_1}^{(r)}|j\rangle_{B_1} \end{aligned}$$

equation (A.2) becomes,

$$\begin{aligned} &|\xi\rangle_A^I \otimes |B\rangle_{A_1,B_1}^{(i)} \\ &= \tfrac{1}{2} \sum_{r=0}^{3} \sum_{j=0}^{1} a_j \sigma_{B_1}^{(i)} |B\rangle_{A,A_1}^{(r)} {}_{A_1} \otimes \sigma_{B_1}^{(r)} |j\rangle_{B_1} \\ &= \tfrac{1}{2} \sum_{r=0}^{3} |B\rangle_{A,A_1}^{(r)} \otimes \sigma_{B_1}^{(i)} \sigma_{B_1}^{(r)} |\xi\rangle_{B_1}^I . \end{aligned} \quad \text{(A.3)}$$

Similarly, for the state $|\eta\rangle_B^I \otimes |B\rangle_{B_2,A_2}^{(i)}$, one can write directly using equation (A.3),

$$|\eta\rangle_B^I \otimes |B\rangle_{B_2,A_2}^{(i)} = \tfrac{1}{2}\left[\sum_{s=0}^{3} |B\rangle_{B,B_2}^{(s)} \otimes (\sigma_{A_2}^{(i)} \sigma_{A_2}^{(s)}) |\eta\rangle_{A_2}^I\right]. \quad \text{(A.4)}$$

Appendix B

We can write the state $|\xi\rangle_{\{A\}}^I \otimes |E\rangle_{\{A'\},\{B'\}}^{(i')}$ as,

$$\begin{aligned} &|\xi\rangle_{\{A\}}^I \otimes |E\rangle_{\{A'\},\{B'\}}^{(i')} \\ &= \sum_{r=0}^{2^{2m}-1} |E\rangle_{\{A\},\{A'\}}^{(r)} {}^{(r)}\langle E| \left(|\xi\rangle_{\{A\}}^I \otimes |E\rangle_{\{A'\},\{B'\}}^{(i')}\right) \end{aligned} . \quad \text{(B.1)}$$

Using equation (9) and (10), equation (B.1) can be written as,

$$\begin{aligned}\left|\xi\right\rangle_{\{A\}}^{I}\otimes\left|E\right\rangle_{\{A'\},\{B'\}}^{(i')} &= \frac{1}{2^m}\sum_{r=0}^{2^{2m}-1}\sum_{j,k,l=0}^{M} a_j\, U_{\{B'\}}^{(i')}\left|E\right\rangle_{\{A\},\{A'\}}^{(r)} \\ &\left\{{}_{\{A\}}\left\langle\tilde{l}\right|\otimes{}_{\{A'\}}\left\langle\tilde{l}\right|(U_{\{A'\}}^{(r)})^{\dagger}\right\}\left|\tilde{j}\right\rangle_{\{A\}}\otimes\left\{\left|\tilde{k}\right\rangle_{\{A'\}}\otimes\left|\tilde{k}\right\rangle_{\{B'\}}\right\} \\ &= \frac{1}{2^m}\sum_{r=0}^{2^{2m}-1}\sum_{j,k=0}^{M} a_j\, U_{\{B'\}}^{(i')}\left|E\right\rangle_{\{A\},\{A'\}}^{(r)} \\ &\left\{{}_{\{A'\}}\left\langle\tilde{j}\right|(U_{\{A'\}}^{(r)})^{\dagger}\right\}\left|\tilde{k}\right\rangle_{\{A'\}}\otimes\left|\tilde{k}\right\rangle_{\{B'\}},\end{aligned} \tag{B.2}$$

using ${}_{\{A\}}\left\langle\tilde{l}\right|\left.\tilde{j}\right\rangle_{\{A\}}=\delta_{lj}$.

Here,

$$U_{\{A'\}}^{(r)}=(\sigma_{A_1'}^{r_1}\otimes\sigma_{A_2'}^{r_2}\otimes.....\otimes\sigma_{A_m'}^{r_m}), \tag{B.3}$$

and $(r_1r_2.....r_m)$ is the quaternary representation of the decimal number r. Since

$$\begin{aligned}{}_{\{A'\}}\left\langle\tilde{j}\right|(U_{\{A'\}}^{(r)})^{\dagger}\left|\tilde{k}\right\rangle_{\{A'\}} &= {}_{\{B'\}}\left\langle\tilde{j}\right|(U_{\{B'\}}^{(r)})^{\dagger}\left|\tilde{k}\right\rangle_{\{B'\}} \\ &= {}_{\{B'\}}\left\langle\tilde{k}\right|(U_{\{B'\}}^{(r)})^{*}\left|\tilde{j}\right\rangle_{\{B'\}} = {}_{\{B'\}}\left\langle\tilde{k}\right|(U_{\{B'\}}^{(r)})\left|\tilde{j}\right\rangle_{\{B'\}},\end{aligned}$$

equation (B.2) becomes,

$$\begin{aligned}&\left|\xi\right\rangle_{\{A\}}^{I}\otimes\left|E\right\rangle_{\{A'\},\{B'\}}^{(i')} \\ &= \frac{1}{2^m}\sum_{r=0}^{2^{2m}-1}\sum_{j=0}^{M} a_j\, U_{\{B'\}}^{(i')}\left|E\right\rangle_{\{A\},\{A'\}}^{(r)}\otimes(U_{\{B'\}}^{(r)})\left|\tilde{j}\right\rangle_{\{B'\}} \\ &= \frac{1}{2^m}\sum_{r=0}^{2^{2m}-1}\left|E\right\rangle_{\{A\},\{A'\}}^{(r)}\otimes U_{\{B'\}}^{(i')}U_{\{B'\}}^{(r)}\left|\xi\right\rangle_{\{B'\}}^{I}.\end{aligned} \tag{B.4}$$

Similarly, for the state $\left|E\right\rangle_{\{B''\},\{A''\}}^{(i'')}\otimes\left|\eta\right\rangle_{\{B\}}^{I}$, one can write directly using equation (B.4),

$$\begin{aligned}&\left|E\right\rangle_{\{B''\},\{A''\}}^{(i'')}\otimes\left|\eta\right\rangle_{\{B\}}^{I} \\ &= \frac{1}{2^n}\sum_{s=0}^{2^{2n}-1}\left|E\right\rangle_{\{B\},\{B''\}}^{(s)}\otimes U_{\{A''\}}^{(i'')}U_{\{A''\}}^{(s)}\left|\xi\right\rangle_{\{A''\}}^{I},\end{aligned} \tag{B.5}$$

where

$$\begin{aligned}U_{\{A''\}}^{(i'')} &= \sigma_{A_1''}^{i_1''}\otimes\sigma_{A_2''}^{i_2''}\otimes.....\otimes\sigma_{A_n''}^{i_n''}, \\ U_{\{A''\}}^{(s)} &= \sigma_{A_1''}^{s_1}\otimes\sigma_{A_2''}^{s_2}\otimes.....\otimes\sigma_{A_n''}^{s_n},\end{aligned} \tag{B.6}$$

and $(s_1s_2.....s_n)$ is the quaternary representation of the decimal number s.

References

[1] C.H. Bennett and G. Brassard, Proc. IEEE Inter. Conf. Computers, Systems, and Signal Processing, Bangalore, (1984) 175; A.K. Ekert, Phys. Rev. Lett. 67 (1991) 661; N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74 (2002) 145; V. Scarani, S. Iblisdir and N. Gisin, Rev. Mod. Phys. 77 (2005) 1225.

[2] C.H. Bennett and S.J. Wiesner, Phys. Rev. Lett. 69 (1992) 2881; H. Lee, D. Ahn and S.W. Hwang, Phys. Rev. A 66 (2002) 024304.

[3] C.H. Bennett, H.G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W.K. Wootters Phys. Rev. Lett. 70 (1993) 1895.

[4] G. Rigolin, Phys. Rev. A 71 (2005) 032303; F.-G. Deng, Phys. Rev. A 72, 036301 (2005); Y. Yeo and W.K. Chua, Phys. Rev. Lett. 96 (2006) 060502.

[5] P.-X. Chen, S.-Y. Zhu and G.-C. Guo, Phys Rev A 74 (2006) 032324.

[6] G. Gordon and G. Rigolin, Phys. Rev. A 73 (2006) 042309; H. Prakash, N. Chandra, R. Prakash and A. Dixit, Mod. Phys. Lett. B 21 (2007) 2019; X.H. Zhang, Z.Y. Yang and P.P. Xu, Sci. in China Series G: Phys. Mech. Ast. 52 (2009) 1034.

[7] G.J. Milburn and S.L. Braunstein, Phys. Rev. A 60, 937 (1999); G. Pires, N.G. de Ameida, A.T. Avelar and B. Baseia, Phys. Rev. A 70 (2004) 025803.

[8] D. Vitali, M. Fortunato and P. Tombesi, Phys. Rev. Lett. 85 (2000) 445.

[9] Enk S J and Hirota O, Phys. Rev. A 64 (2001) 022313; X. Wang, Phys. Rev. A 64 (2001) 022302; H. Jeong, M.S. Kim and J. Lee, Phys. Rev. A 64 (2001) 052308; J.Q. Liao, and L.M. Kuang, J. Phys. B: At. Mol. Opt. Phys.40 (2007) 1183.

[10] H. Prakash, N. Chandra, R. Prakash and Shivani, Phys. Rev. A 75 (2007) 044305; J. Phys. B: At. Mol. Opt. Phys. 40 (2007) 1613; Int. J. Quan. Inf. 6 (2008) 1077; Int. J. Mod. Phys. B 23 (2009) 585; Int. J. Mod. Phys. B 23 (2009) 2083; H.N. Phien and N.B. An, Phys. Lett. A 372 (2008) 2825; N.B. An, Phys. Lett A 373 (2009) 1701; M.K. Mishra and H. Prakash, J. Phys. B: At. Mol. Opt. Phys.43 (2010) 185501; H. Prakash and M.K. Mishra, e-print quant-ph/1107.2533v1.

[11] L. Davidovich, A. Maali, M. Brune, J.M. Raimond and S. Haroche, Phys. Rev. Lett. 71 (1993) 2360; J.I. Cirac and A.S. Parkins, Phys. Rev. A 50 (1994) R4441; S. Bose, P.L. Knight, M.B. Plenio and V. Vedral, Phys. Rev. Lett. 83 (1999) 5158.

[12] S.B. Zheng and G.C. Guo, Phys. Lett. A 232 (1997) 171; S.B. Zheng and G.C. Guo, Phys. Rev. A 63 (2001) 044302; S.B. Zheng, Phys. Rev A 69 (2004) 064302; G. Chimczak and R. Tanas, Phys. Rev. A 79 (2009) 042311.

[13] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, A. Zeilinger, Nature 390 (1997) 575; D. Boschi, S. Branca, F.D. Martini, L. Hardy and S. Popescu, Phys. Rev. Lett. 80 (1998) 1121.

[14] M.A. Nielsen, E. Knill and R. Laflamme, Nature 396 (1998) 52.

[15] M. Riebe, H. Häffner, C.F. Roos, W. Hänsel, M. Ruth, J. Benhelm, G.P.T. Lancaster, T.W. Körber, C. Becher, F. Schmidt-Kaler, D.F.V. James, R. Blatt, Nature 429 (2004) 734; M.D. Barrett, J. Chiaverini, T. Schaetz, J. Britton, W.M. Itano, J.D. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri, D.J. Wineland, Nature 429 (2004) 737.

[16] S. Olmschenk, D.N. Matsukevich, P. Maunz, D. Hayes, L.-M. Duan, and C. Monroe, Science 323, 486 (2009).

[17] M. Hillery, V. Buzek and A. Berthiaume, Phys. Rev. A 59 (1999) 1829.

[18] A. Karlsson and M. Bourennane, Phys. Rev. A 58 (1998) 4394.

[19] B. Aoun and M. Tarifi, e-print quant-ph/0401076.

[20] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A 54 (1996) 2651; P.D. Townsend, Nature 385 (1997) 47; S. Bose, V. Vedral, and P.L. Knight, Phys. Rev. A 57 (1998) 822.

[21] H. Prakash and A.K. Maurya, Opt. Commun. 284 (2011) 5024.

[22] B.S. Shi and A. Tomita, Phys. Lett. A 296 (2002) 161; J. Joo, Y.J. Park, S. Oh and J. Kim, New J. of Phys. 5 (2003) 136; Z.L. Cao and M. Yang, Physica A 337 (2004) 132.

[23] C.-P. Yang, S.-I. Chu and S. Han, Phys. Rev. A 70 (2004) 022329; Z.-J. Zhang, Phys. Lett. A 352 (2006) 55; Z.-X. Man, Y.-J. Xia and N.B. An, Phys. Rev. A 75 (2007) 052306; Z.-X. Man, Y.-J. Xia and N.B. An, J. Phys. B: At. Mol. Opt. Phys. 40 (2007) 1767.

[24] M.K. Mishra, A.K. Maurya and H. Prakash, J. Phys. B: At. Mol. Opt. Phys. 44 (2011) 115504.