IJCAT International Journal of Computing and Technology, Volume 1, Issue 6, July 2014
ISSN : 2348 - 6090
www.IJCAT.org

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

[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 paper, we present a generalization of our original secure quantum information exchange (SQIE) protocol [J. Phys. B: At. Mol. Opt. Phys. 44 (2011) 115504], for the secure exchange of two single qudit (an arbitrary *d*-level system) information states between the two legitimate users, Alice and Bob. Further we extend this result from single qudit to multi-qudits to obtain the secure exchange of the information states involving arbitrary number of qudits.

***Keywords* - Quantum entanglement, Quantum teleportation, Qudit, Quantum Information Exchange, Generalized Bell states.**

1. Introduction

Quantum teleportation (QT), first introduced by Bennett et al [1], is one way quantum communication between two users, Alice and Bob, in which an unknown information state is transferred from Alice (sender) to Bob (receiver) without physically sending it. After introduction of the idea of QT, a number of theoretical studies [2-3] on QT have been done. Also several experiments [4-6] demonstrating QT have been done. In some studies on QT [7-9], a third party is included between the two users, Alice and Bob. This third party controls the whole process of QT with Alice due to which the security of QT increases. Thus, this process is termed as controlled QT.
Many authors extended the original scheme of QT to teleport arbitrary 2-qubit information state [10-12] and further, to teleport arbitrary *n*-qubit information state [11, 13-16]. Arbitrary 2-qubit information state can be teleported using generalized Bell states, which are tensor products of two standard bipartite Bell states [11], while arbitrary *n*-qubit information state can be teleported using generalized Bell states of 2*n*-qubits, which are tensor product of *n*-standard bi-partite Bell states [11, 13]. To increase the security of these QT schemes, some authors [15-16] proposed the controlled QT of unknown information states of multi-qubits by introducing a third observer or a number of observers between two legitimate observers, Alice and Bob. In all the above studies on QT are based on qubits, i.e., two level systems. For the systems of arbitrary d-levels (qudits), many authors have extended the above studies on QT and presented the QT schemes to teleport single qudit information states [17, 18] and also to teleport arbitrary *n*-qudit information states [19]. Further, some authors have proposed the controlled QT of information states involving multi qudits [20-25].
The aim of above studies on QT is to send unknown information states from Alice to Bob, i.e., one way quantum communication. In a very recent paper [26], the authors presented a new idea called secure quantum information exchange (SQIE) that allows two-way quantum communication between Alice and Bob. Initially, if each of Alice and Bob has single qubit information state, the SQIE protocol gives the simultaneous exchange of information states from Alice to Bob and Bob to Alice via a special kind of six-qubit entangled (SSE) state and a third party, Charlie. This protocol has the security that either both, Alice and Bob successfully exchange their information states or in case of failure of this exchange process, no-one among them gets correct information states. For experimental realization of this protocol, the authors proposed an efficient scheme to generate the SSE states using interaction between Λ-type three-level atoms and optical coherent fields.

Further, the authors [27] generalized their original SQIE protocol to accomplish the secure exchange of the information states involving multi-qubits. For this purpose, they have generalized the SSE states. Another interesting point about original SQIE is the security of this protocol. The authors [27] have discussed the security of original and generalized SQIE protocols against the number of qubits with the controller, Charlie. They have concluded

that unity is the upper bound for insecurity in the quantum network in the original SQIE process, while one-sixteenth is the lower bound for insecurity in the quantum network in the original SQIE process. For generalized SQIE protocol, if Alice and Bob has to send m and n qubit states respectively, $2^{-2(m+n)}$ is the lower bound for insecurity in the quantum network.

In the real world, there may need of exchanging a large amount of information encoded in single qudit and also in multi qudit states. For this, in this paper, we extend the SQIE protocol from qubits to qudits to attain the secure exchange of information states encoded in single qudit and also in multi qudits.

2. Generalization of SQIE Protocol for Two Unknown Single Qudit Information States

In this section, we extend the original idea of SQIE for secure exchange of two unknown single qubit states to secure exchange of two unknown single qudit states between Alice and Bob. Let Alice want to send single qudit information state,

$$|\xi\rangle_A^I = [a_0|0\rangle + a_1|1\rangle + \ldots\ldots\ldots\ldots + a_{d-1}|d-1\rangle]_A , \quad (1)$$

to Bob and Bob want to send single qudit information state,

$$|\eta\rangle_B^I = [b_0|0\rangle + b_1|1\rangle + \ldots\ldots\ldots\ldots + b_{d-1}|d-1\rangle]_B , \quad (2)$$

to Alice. This information exchange process must have security that both, Alice and Bob, get their required information states. In case of failure of this, none of them get the required information state. Here, $|0\rangle,|1\rangle,\ldots\ldots,|d-1\rangle$ are orthogonal d-states in the computational basis of a d-level quantum system (qudit). Superscripts I refer to information states.

To complete this task, we generalize here the original special kind of six-qubit entangled (SSE) states [11] to special kind of six-qudit entangled states, which can be written as

$$|\psi\rangle^E_{A_1,B_1,B_2,A_2,C_1,C_2} = \frac{1}{d}[\sum_{u,v=0}^{d-1} |E\rangle^{(uv)}_{A_1,B_1} \otimes |E\rangle^{(uv)}_{B_2,A_2} \otimes |\phi\rangle^{(uv)}_{C_1,C_2}], \quad (3)$$

where the states $\{|E\rangle^{(uv)}_{A_1,B_1}\}$ and $\{|E\rangle^{(uv)}_{B_2,A_2}\}$ are maximally entangled states of two qudits and can written as

$$|E\rangle^{(uv)}_{A_1,B_1} = \frac{1}{\sqrt{d}}[\sum_{l=0}^{d-1} e^{2\pi i l u/d}|l\rangle_{A_1} \otimes |l\oplus v\rangle_{B_1}], \quad (4)$$

$$|E\rangle^{(uv)}_{B_2,A_2} = \frac{1}{\sqrt{d}}[\sum_{l=0}^{d-1} e^{2\pi i l u/d}|l\rangle_{B_2} \otimes |l\oplus v\rangle_{A_2}]. \quad (5)$$

For $u, v = 0, 1, \ldots\ldots, d-1$, both $\{|E\rangle^{(uv)}_{A_1,B_1}\}$ and $\{|E\rangle^{(uv)}_{B_2,A_2}\}$ form complete sets of orthogonal d^2-states in d^2-dimensional Hilbert space, $l \oplus v \equiv (l+v) \bmod d$. The states $\{|\phi\rangle^{(uv)}_{C_1,C_2}\}$ are different d^2-orthogonal states belonging to the computational basis $|00\rangle,|01\rangle,|02\rangle,\ldots\ldots,(|d-1\rangle \otimes |d-1\rangle)$. The states given by equation (3) form a set of $d^2!$ states.

Considering one state of the states given by equation (3) as entangled state,

$$|\psi\rangle^E_{A_1,B_1,B_2,A_2,C_1,C_2} = \frac{1}{d}[\sum_{u,v=0}^{d-1} |E\rangle^{(uv)}_{A_1,B_1} \otimes |E\rangle^{(uv)}_{B_2,A_2} \otimes |uv\rangle_{C_1,C_2}], \quad (6)$$

we can write the initial state of composite system as

$$|\psi\rangle_{A,A_1,B_1,B_2,A_2,C_1,C_2,B} = |\xi\rangle^I_A \otimes |\psi\rangle^E_{A_1,B_1,B_2,A_2,C_1,C_2} \otimes |\eta\rangle^I_B = \frac{1}{d}[\sum_{u,v=0}^{d-1} (|\xi\rangle^I_A \otimes |E\rangle^{(uv)}_{A_1,B_1}) \otimes (|E\rangle^{(uv)}_{B_2,A_2} \otimes |\eta\rangle^I_B) \otimes |uv\rangle_{C_1,C_2}]. \quad (7)$$

Here, qudits in modes A_1, A_2 are with Alice, qudits in modes B_1, B_2 are with Bob, while qudits in modes C_1, C_2 are with Charlie.

From Appendix **A**, we have

$$|\xi\rangle^I_A \otimes |E\rangle^{(uv)}_{A_1,B_1} = \frac{1}{d}[\sum_{r',s'=0}^{d-1} |E\rangle^{(r's')}_{A,A_1} \otimes U^{(uv)}_{B_1} (U^{(r's')}_{B_1})^* |\xi\rangle^I_{B_1}], \quad (8)$$

$$|\eta\rangle^I_B \otimes |E\rangle^{(uv)}_{B_2,A_2} = \frac{1}{d}[\sum_{r'',s''=0}^{d-1} |E\rangle^{(r''s'')}_{B,B_2} \otimes U^{(uv)}_{A_2} (U^{(r''s'')}_{A_2})^* |\eta\rangle^I_{A_2}], \quad (9)$$

where U's are unitary operations given by

$$U^{(uv)} = \sum_{l=0}^{d-1} e^{2\pi i l u/d} |l\oplus v\rangle\langle l| , \quad (10)$$

for $u, v = 0, 1, \ldots\ldots, d-1$. Using equations (8) and (9), equation (7) can be written as

$$|\psi\rangle_{A,A_1,B_1,B_2,A_2,C_1,C_2,B} = \frac{1}{d}[\sum_{u,v=0}^{d-1} \frac{1}{d}\{\sum_{r',s'=0}^{d-1} |E\rangle^{(r's')}_{A,A_1} \otimes U^{(uv)}_{B_1} (U^{(r's')}_{B_1})^* |\xi\rangle^I_{B_1}\} \otimes \frac{1}{d}\{\sum_{r'',s''=0}^{d-1} |E\rangle^{(r''s'')}_{B,B_2} \otimes U^{(uv)}_{A_2} (U^{(r''s'')}_{A_2})^* |\eta\rangle^I_{A_2}\} \otimes |uv\rangle_{C_1,C_2}]. \quad (11)$$

From equation (11), it is clear that if Alice and Bob perform 2-qudit Bell state measurement (BSM) on their two qudits in modes A, A_1 and B, B_2 and convey their BSM results $(r's')$ and $(r''s'')$ to Charlie through classical

channels respectively, then Charlie measures his two qudits in modes C_1, C_2 in the computational basis $\{|00\rangle,|01\rangle,|02\rangle,.....,(|d-1\rangle\otimes|d-1\rangle)\}$ and, depending on his own measurement result uv and BSM results received, Charlie transmits classical information to each of Alice and Bob. Now according to the classical information received from Charlie, Alice performs unitary transformation $(U_{A_2}^{(uv)}(U_{A_2}^{(r''s'')})^*)^\dagger$ on her qudit in modes A_2 and Bob performs unitary transformation $(U_{B_1}^{(uv)}(U_{B_1}^{(r's')})^*)^\dagger$ on her qudit in modes B_2 in order to get the exact replicas of the required quantum information states. This completes the SQIE process.

Also if any of Alice and Bob withholds the classical information from Charlie, then Charlie cancels the exchange process and none of Alice and Bob gets correct information state.

3. Secure Quantum Information Exchange of the Information States Involving Arbitrary Number of Qudits

In this section, we generalize the result of Section **2** to get the secure exchange of information states of arbitrary number of qudits between Alice and Bob. Let Alice require to send arbitrary m-qudit information state in modes $\{A\}\equiv(A_1,A_2,....,A_m)$,

$$|\xi\rangle_{\{A\}}^{I}=[a_0|\tilde{0}\rangle+a_1|\tilde{1}\rangle+a_2|\tilde{2}\rangle+.....+a_M|\tilde{M}\rangle]_{\{A\}}, \quad (12)$$

to Bob and Bob require to send arbitrary n-qudit information state in modes $\{B\}\equiv(B_1,B_2,....,B_n)$,

$$|\eta\rangle_{\{B\}}^{I}=[b_0|\tilde{0}\rangle+b_1|\tilde{1}\rangle+b_2|\tilde{2}\rangle+.....+b_N|\tilde{N}\rangle]_{\{B\}}, \quad (13)$$

to Alice. The security of this process is similar to the SQIE protocol discussed in Section **2**. Here, $M\equiv d^m-1$, $N\equiv d^n-1$ and $|\tilde{0}\rangle,|\tilde{1}\rangle,|\tilde{2}\rangle,.....,|\tilde{M}\rangle$ $(|\tilde{0}\rangle,|\tilde{1}\rangle,|\tilde{2}\rangle,.....,|\tilde{N}\rangle)$ are orthogonal d^m (d^n)-state in the computational basis $|00..^m...0\rangle$, $|00..^m...1\rangle$, $|00..^m...2\rangle$, ….., $|(d-1)(d-1)..^m...(d-1)\rangle$ $(|00..^n...0\rangle$, $|00..^n...1\rangle$, $|00..^n...2\rangle$, ….., $|(d-1)(d-1)..^n...(d-1)\rangle)$ of d^m (d^n)-dimensional Hilbert space.

To complete this task, we need to generalize the special kind of six-qudit entangled states given by equation (3). If we take $p=\max\{m,n\}$, then we give $2p$-qudits to Charlie and $2p$-qudits of Charlie requires d^{2p} terms in the generalized state. Now we consider the d-dimensional generalized Bell states (d-GBS) of $2m$ and $2n$-qudits. For d-GBS of $2m$-qudits encoded in the modes $\{A'\}\equiv(A_1',A_2',....,A_m')$ and $\{B'\}\equiv(B_1',B_2',....,B_m')$, one can have d^{2m} d-GBS in which one of the states can be expressed as

$$|E\rangle_{\{A'\},\{B'\}}^{(00)}=\frac{1}{d^{m/2}}\sum_{k=0}^{M}|\tilde{k}\rangle_{\{A'\}}\otimes|\tilde{k}\rangle_{\{B'\}}. \quad (14)$$

In order to complete the set of d^{2m} d-GBS, we can consider a set of d^{2m} unitary operations acting on modes $\{B'\}$ in this state, given by

$$U_{\{B'\}}^{(u'v')}\equiv(U_{B_1'}^{(u_1'v_1')})\otimes(U_{B_2'}^{(u_2'v_2')})\otimes.....\otimes(U_{B_m'}^{(u_m'v_m')}), \quad (15)$$

for $(u',v')=0, 1, 2, ….., M$. Here u' and v' are decimal equivalents of d-dimensional numbers $(u_1'u_2'.....u_m')$ and $(v_1'v_2'.....v_m')$ respectively and each of u_α' and v_α' takes values 0, 1, 2, …., (d-1). Each unitary operation $U_{B_\alpha'}^{(u_\alpha'v_\alpha')}$ is given by equation (10) and

$$|E\rangle_{\{A'\},\{B'\}}^{(u'v')}=(U_{\{B'\}}^{(u'v')})|E\rangle_{\{A'\},\{B'\}}^{(00)}. \quad (16)$$

Similarly, the d-GBS of $2n$-qudits encoded in the modes $\{B''\}\equiv(B_1'',B_2'',....,B_n'')$ and $\{A''\}\equiv(A_1'',A_2'',....,A_n'')$, for $(u'',v'')=0, 1, 2, …., N$, can be written as

$$\begin{aligned}|E\rangle_{\{A''\},\{B''\}}^{(u''v'')}&=\frac{1}{d^{n/2}}(U_{\{B''\}}^{(u''v'')})|E\rangle_{\{A''\},\{B''\}}^{(00)}\\&=\frac{1}{d^{n/2}}(U_{\{B''\}}^{(u''v'')})\sum_{k=0}^{N}|\tilde{k}\rangle_{\{A''\}}\otimes|\tilde{k}\rangle_{\{B''\}},\end{aligned} \quad (17)$$

where

$$U_{\{B''\}}^{(u''v'')}\equiv(U_{B_1''}^{(u_1''v_1'')})\otimes(U_{B_2''}^{(u_2''v_2'')})\otimes.....\otimes(U_{B_n''}^{(u_n''v_n'')}), \quad (18)$$

each unitary operation $U_{B_\alpha''}^{(u_\alpha''v_\alpha'')}$ is given by equation (10) for $u_\alpha'',v_\alpha''=0, 1, 2,…., (d-1)$ and u'' and v'' are decimal equivalents of d-dimensional numbers $(u_1''u_2''.....u_n'')$ and $(v_1''v_2''.....v_n'')$ respectively.

We have only d^{2m} and d^{2n} d-GBS of $2m$ and $2n$ qudits respectively and only one of these two families gives a family of d^{2p} states. If $m>n$, $d^{2m}=d^{2p}$ but d^{2n} becomes smaller than d^{2p} and if $n>m$, $d^{2n}=d^{2p}$ but d^{2m} becomes smaller than d^{2p}. This problem can be avoided by repeating the members of smaller family of states till d^{2p} states are obtained. Thus if indices u and v takes values 0, 1, ….., d^p-1, we can define indices $u'\equiv u\ (\mathrm{mod}\ d^m)$, $v'\equiv v\ (\mathrm{mod}\ d^m)$, $u''\equiv u\ (\mathrm{mod}\ d^n)$ and $v''\equiv v\ (\mathrm{mod}\ d^n)$ and write the d-GBS,

$|E\rangle_{\{A'\},\{B'\}}^{(uv)}=|E\rangle_{\{A'\},\{B'\}}^{(u'v')}$ and $|E\rangle_{\{B''\},\{A''\}}^{(uv)}=|E\rangle_{\{B''\},\{A''\}}^{(u''v'')}$.

The entangled state corresponding to special kind of six-qudit entangled state (3) can be written as

$$\left|\psi\right\rangle^{E}_{\{A'\},\{B'\},\{B''\},\{A''\},\{C\}} = \frac{1}{d^{p}}\Big[\sum_{u,v=0}^{d^{p}-1}\left|E\right\rangle^{(uv)}_{\{A'\},\{B'\}}\otimes\left|E\right\rangle^{(uv)}_{\{B''\},\{A''\}}\otimes\left|\phi\right\rangle^{(uv)}_{\{C\}}\Big], \quad (19)$$

where modes $\{C\}\equiv(C_1,C_2,.....,C_{2p})$ and $\left\{\left|\phi\right\rangle^{(uv)}_{\{C\}}\right\}$ are different orthogonal d^{2p}-states belonging to the computational basis $\left\{\left|\tilde{0}\right\rangle,\left|\tilde{1}\right\rangle,.....,\left|\tilde{P}\right\rangle\right\}$, $(P\equiv d^{2p}-1)$ in d^{2p} -dimensional Hilbert space. Superscript E refers to entangled state.

Using equations (12), (13) and (19), the initial state of composite system can be written as

$$\begin{aligned}\left|\psi\right\rangle_{\{A\},\{A'\},\{B'\},\{B''\},\{A''\},\{C\},\{B\}} &= \left|\xi\right\rangle^{I}_{\{A\}}\otimes\left|\psi\right\rangle^{E}_{\{A'\},\{B'\},\{B''\},\{A''\},\{C\}}\otimes\left|\eta\right\rangle^{I}_{\{B\}}\\ &= \frac{1}{d^{p}}\Big[\sum_{u,v=0}^{d^{p}-1}\big(\left|\xi\right\rangle^{I}_{\{A\}}\otimes\left|E\right\rangle^{(uv)}_{\{A'\},\{B'\}}\big)\\ &\quad\otimes\big(\left|E\right\rangle^{(uv)}_{\{B''\},\{A''\}}\otimes\left|\eta\right\rangle^{I}_{\{B\}}\big)\otimes\left|\phi\right\rangle^{(uv)}_{\{C\}}\Big]\end{aligned}. \quad (20)$$

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

From Appendix **B**, we find that the states, $\left|\xi\right\rangle^{I}_{\{A\}}\otimes\left|E\right\rangle^{(uv)}_{\{A'\},\{B'\}}$ and $\left|E\right\rangle^{(uv)}_{\{B''\},\{A''\}}\otimes\left|\eta\right\rangle^{I}_{\{B\}}$, in equation (20), can be rewritten as

$$\left|\xi\right\rangle^{I}_{\{A\}}\otimes\left|E\right\rangle^{(uv)}_{\{A'\},\{B'\}} = \frac{1}{d^{m}}\sum_{r',s'=0}^{M}\left|E\right\rangle^{(r's')}_{\{A\},\{A'\}}\otimes U^{(uv)}_{\{B'\}}(U^{(r's')}_{\{B'\}})^{*}\left|\xi\right\rangle^{I}_{\{B'\}}, \quad (21)$$

$$\left|E\right\rangle^{(uv)}_{\{B''\},\{A''\}}\otimes\left|\eta\right\rangle^{I}_{\{B\}} = \frac{1}{d^{n}}\sum_{r'',s''=0}^{N}\left|E\right\rangle^{(r''s'')}_{\{B\},\{B''\}}\otimes U^{(uv)}_{\{A''\}}(U^{(r''s'')}_{\{A''\}})^{*}\left|\xi\right\rangle^{I}_{\{A''\}}, \quad (22)$$

where the d-GBS $\left|E\right\rangle^{(r's')}_{\{A\},\{A'\}}$ and $\left|E\right\rangle^{(r''s'')}_{\{B\},\{B''\}}$ are given by equations (16) and (17) respectively, unitary operations $U^{(uv)}_{\{B'\}}$, $U^{(uv)}_{\{A''\}}$, $U^{(r's')}_{\{B'\}}$ and $U^{(r''s'')}_{\{A''\}}$ are given by equations (15), (18), (5B.3) and (5B.6) respectively. Using equations (21) and (22), equation (20) can be written as

$$\begin{aligned}\left|\psi\right\rangle_{\{A\},\{A'\},\{B'\},\{B''\},\{A''\},\{C\},\{B\}} &= \frac{1}{d^{p}}\Big[\sum_{u,v=0}^{d^{p}-1}\Big\{\frac{1}{d^{m}}\sum_{r',s'=0}^{M}\left|E\right\rangle^{(r's')}_{\{A\},\{A'\}}\otimes U^{(uv)}_{\{B'\}}(U^{(r's')}_{\{B'\}})^{*}\left|\xi\right\rangle^{I}_{\{B'\}}\Big\}\\ &\otimes\Big\{\frac{1}{d^{n}}\sum_{r'',s''=0}^{N}\left|E\right\rangle^{(r''s'')}_{\{B\},\{B''\}}\otimes U^{(uv)}_{\{A''\}}(U^{(r''s'')}_{\{A''\}})^{*}\left|\xi\right\rangle^{I}_{\{A''\}}\Big\}\otimes\left|\phi\right\rangle^{(uv)}_{\{C\}}\Big].\end{aligned} \quad (23)$$

Now Alice performs $2m$-qudit Bell state measurement (BSM) on her qudits in modes $\{A\},\{A'\}$ and Bob performs $2n$-qudit BSM on his qudits in modes $\{B\},\{B''\}$, while Charlie measures his qudits in modes $\{C\}$ in the computational basis $\left\{\left|\tilde{0}\right\rangle,\left|\tilde{1}\right\rangle,.....,\left|\tilde{P}\right\rangle\right\}$. Alice and Bob, both, convey their BSM results $(r's')$ and $(r''s'')$ to Charlie through classical channels. Charlie, on the basis of BSM results obtained by Alice and Bob and his own measurement result, decides about the classical information to be conveyed to each of Alice and Bob. Depending on these classical information conveyed by Charlie, Alice and Bob perform the required unitary transformations on their qudits in modes $\{A''\}$ and $\{B'\}$ respectively, in order to generate exact replicas of the required quantum information states. From equation (23), it is clear that if result of Charlie's measurement is (uv), then Alice performs unitary transformation $\big(U^{(uv)}_{\{A''\}}(U^{(r''s'')}_{\{A''\}})^{*}\big)^{\dagger}$ and Bob performs unitary transformation $\big(U^{(uv)}_{\{B'\}}(U^{(r's')}_{\{B'\}})^{*}\big)^{\dagger}$ on their particles for the Bob's BSM result $(r''s'')$ and Alice's BSM result $(r's')$ respectively.

4. Conclusion

We generalized the original SQIE protocol for the secure exchange of two single qudit information states between two users, Alice and Bob. We further generalized this result from single qudit to multi-qudits to achieve the secure exchange of the information states involving arbitrary number of qudits.

In reference [27], we discussed the security of SQIE protocol against the number of qubits with the controller, Charlie. This consideration can be done for the above two generalized SQIE protocols discussed in Sections **2** and **3**. For the SQIE protocol discussed in Section **2**, if Alice and Bob have to send two unknown single qudit states, the number of possible quantum channels between Alice and Bob is d^4. Thus if Charlie gets l qudits, for $l < 4$, the probability for insecurity is d^{-l} and for $l \geq 4$, it is d^{-4}.

For the SQIE protocol discussed in Section **3**, if Alice and Bob have to send m and n qudit states respectively, then the number of possible quantum channels between Alice and Bob is $d^{2(m+n)}$. Thus if Charlie gets l qubits, for $l < 2(m+n)$, the probability for insecurity is d^{-l} and for $l \geq 2(m+n)$, it is $d^{-2(m+n)}$.

Appendix A

The state $|\xi\rangle_A^I \otimes |E\rangle_{A_1,B_1}^{(uv)}$ can be written as

$$|\xi\rangle_A^I \otimes |E\rangle_{A_1,B_1}^{(uv)} = \sum_{r',s'=0}^{d-1} |E\rangle_{A,A_1}^{(r's')} {}^{(r's')}\langle E| \left(|\xi\rangle_A^I \otimes |E\rangle_{A_1,B_1}^{(uv)}\right). \tag{A.1}$$

Since

$$|E\rangle_{A_1,B_1}^{(uv)} = \frac{1}{\sqrt{d}}[\sum_{l=0}^{d-1} e^{2\pi ilu/d}|l\rangle_{A_1} \otimes |l\oplus v\rangle_{B_1}]$$
$$= \frac{1}{\sqrt{d}} U_{B_1}^{(uv)}[\sum_{l=0}^{d-1}|l\rangle_{A_1} \otimes |l\rangle_{B_1}],$$

where $U_{B_1}^{(uv)}$ is unitary operation given by equation (10). Then equation (A.1) takes the form,

$$|\xi\rangle_A^I \otimes |E\rangle_{A_1,B_1}^{(uv)} = \frac{1}{d}[\sum_{r',s'=0}^{d-1}\sum_{j,k,l=0}^{d-1} a_j |E\rangle_{A,A_1}^{(r's')} \left({}_A\langle l| \otimes {}_{A_1}\langle l|U_{A_1}^{(r's')^\dagger}\right) \left(|j\rangle_A^I \otimes |k\rangle_{A_1} \otimes U_{B_1}^{(uv)}|k\rangle_{B_1}\right)]$$
$$= \frac{1}{d}[\sum_{r',s'=0}^{d-1}\sum_{j,k=0}^{d-1} a_j |E\rangle_{A,A_1}^{(r's')} {}_{A_1}\langle j|U_{A_1}^{(r's')^\dagger}|k\rangle_{A_1} \otimes U_{B_1}^{(uv)}|k\rangle_{B_1}]. \tag{A.2}$$

Since

$${}_{A_1}\langle j|U_{A_1}^{(r's')^\dagger}|k\rangle_{A_1} = {}_{B_1}\langle j|U_{B_1}^{(r's')^\dagger}|k\rangle_{B_1} = {}_{B_1}\langle k|(U_{B_1}^{(r's')})^*|j\rangle_{B_1}.$$

Then equation (A.2) becomes

$$|\xi\rangle_A^I \otimes |E\rangle_{A_1,B_1}^{(uv)} = \frac{1}{d}[\sum_{r',s'=0}^{d-1}\sum_{j=0}^{d-1} a_j |E\rangle_{A,A_1}^{(r's')} \otimes U_{B_1}^{(uv)}(U_{B_1}^{(r's')})^*|j\rangle_{B_1}]$$
$$= \frac{1}{d}[\sum_{r',s'=0}^{d-1} |E\rangle_{A,A_1}^{(r's')} \otimes U_{B_1}^{(uv)}(U_{B_1}^{(r's')})^*|\xi\rangle_{B_1}^I]. \tag{A.3}$$

Similarly, for the state $|\eta\rangle_B^I \otimes |E\rangle_{B_2,A_2}^{(uv)}$, we may write using equation (A.3),

$$|\eta\rangle_B^I \otimes |E\rangle_{B_2,A_2}^{(uv)} = \frac{1}{d}[\sum_{r'',s''=0}^{d-1} |E\rangle_{B,B_2}^{(r''s'')} \otimes U_{A_2}^{(uv)}(U_{A_2}^{(r''s'')})^*|\xi\rangle_{A_2}^I]. \tag{A.4}$$

Appendix B

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

$$|\xi\rangle_{\{A\}}^I \otimes |E\rangle_{\{A'\},\{B'\}}^{(u'v')} = \sum_{r',s'=0}^{M} |E\rangle_{\{A\},\{A'\}}^{(r's')} {}^{(r's')}\langle E| \left(|\xi\rangle_{\{A\}}^I \otimes |E\rangle_{\{A'\},\{B'\}}^{(u'v')}\right). \tag{B.1}$$

Using equations (15) and (16), equation (B.1) can be written as

$$|\xi\rangle_{\{A\}}^I \otimes |E\rangle_{\{A'\},\{B'\}}^{(u'v')} = \frac{1}{d^m}\sum_{r',s'=0}^{M}\sum_{j,k,l=0}^{M} a_j U_{\{B'\}}^{(u'v')}|E\rangle_{\{A\},\{A'\}}^{(r's')}$$
$$\{{}_{\{A\}}\langle\tilde{l}| \otimes {}_{\{A'\}}\langle\tilde{l}|(U_{\{A'\}}^{(r's')})^\dagger\}|\tilde{j}\rangle_{\{A\}} \otimes \{|\tilde{k}\rangle_{\{A'\}} \otimes |\tilde{k}\rangle_{\{B'\}}\}$$
$$= \frac{1}{d^m}\sum_{r',s'=0}^{M}\sum_{j,k=0}^{M} a_j U_{\{B'\}}^{(u'v')}|E\rangle_{\{A\},\{A'\}}^{(r's')}$$
$$\{{}_{\{A'\}}\langle\tilde{j}|(U_{\{A'\}}^{(r's')})^\dagger\}|\tilde{k}\rangle_{\{A'\}} \otimes |\tilde{k}\rangle_{\{B'\}}, \tag{B.2}$$

where

$$U_{\{A'\}}^{(r's')} \equiv (U_{A_1'}^{(r_1's_1')}) \otimes (U_{A_2'}^{(r_2's_2')}) \otimes .....\otimes (U_{A_m'}^{(r_m's_m')}), \tag{B.3}$$

and r' and s' are the decimal conversions of d-dimensional numbers $(r_1'r_2'.....r_m')$ and $(s_1's_2'.....s_m')$. Since

$${}_{\{A'\}}\langle\tilde{j}|(U_{\{A'\}}^{(r's')})^\dagger|\tilde{k}\rangle_{\{A'\}} = {}_{\{B'\}}\langle\tilde{j}|(U_{\{B'\}}^{(r's')})^\dagger|\tilde{k}\rangle_{\{B'\}}$$
$$= {}_{\{B'\}}\langle\tilde{k}|(U_{\{B'\}}^{(r's')})^*|\tilde{j}\rangle_{\{B'\}}.$$

Then equation (B.2) becomes

$$|\xi\rangle_{\{A\}}^I \otimes |E\rangle_{\{A'\},\{B'\}}^{(u'v')} = \frac{1}{d^m}\sum_{r',s'=0}^{M}\sum_{j=0}^{M} a_j U_{\{B'\}}^{(u'v')}|E\rangle_{\{A\},\{A'\}}^{(r's')} \otimes (U_{\{B'\}}^{(r's')})^*|\tilde{j}\rangle_{\{B'\}}$$
$$= \frac{1}{d^m}\sum_{r',s'=0}^{M}|E\rangle_{\{A\},\{A'\}}^{(r's')} \otimes U_{\{B'\}}^{(u'v')}(U_{\{B'\}}^{(r's')})^*|\xi\rangle_{\{B'\}}^I. \tag{B.4}$$

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

$$|E\rangle_{\{B''\},\{A''\}}^{(u''v'')} \otimes |\eta\rangle_{\{B\}}^I = \frac{1}{d^n}\sum_{r'',s''=0}^{N}|E\rangle_{\{B\},\{B''\}}^{(r''s'')} \otimes U_{\{A''\}}^{(u''v'')}(U_{\{A''\}}^{(r''s'')})^*|\xi\rangle_{\{A''\}}^I, \tag{B.5}$$

where

$$U_{\{A''\}}^{(u''v'')} \equiv (U_{A_1''}^{(u_1''v_1'')}) \otimes (U_{A_2''}^{(u_2''v_2'')}) \otimes .....\otimes (U_{A_n''}^{(u_n''v_n'')}),$$
$$U_{\{A''\}}^{(r''s'')} \equiv (U_{A_1''}^{(r_1''s_1'')}) \otimes (U_{A_2''}^{(r_2''s_2'')}) \otimes .....\otimes (U_{A_n''}^{(r_n''s_n'')}). \tag{B.6}$$

and r'' and s'' are the decimal forms of d-dimensional numbers $(r_1''r_2''.....r_n'')$ and $(s_1''s_2''.....s_n'')$.

References

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

[2] L. Vaidman, Phys. Rev. A 49, 1473 (1994); J. I. Cirac and A. S. Parkins, Phys. Rev. A 50, R4441 (1994); S. B. Zheng and G. C. Guo, Phys. Lett. A 232, 171 (1997), Phys. Rev. A 63, 04432 (2001).

[3] X. Wang, Phys. Rev. A 64, 022302 (2001); S. J. van Enk and O. Hirota, Phys. Rev. A 64, 022313 (2001); H. Prakash, N. Chandra, R. Prakash and Shivani, Phys.

Rev. A 75, 044305 (2007); 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, 185501 (2010); J. Opt. Soc. Am. B 29 (2012) 2915.

[4] D. Bouwmeester et al, Nature 390, 575 (1997); D. Boschi et al, Phys. Rev. Lett. 80, 1121 (1998).

[5] M. A. Nielsen, E. Knill and R. Laflamme, Nature 396 (1998) 52; I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden and N. Gisin, Nature, 421, 509 (2003).

[6] M. Riebe et al, Nature 429, 734-737 (2004); M. D. Barrett et al, Nature 429, 737 (2004); S. Olmschenk et al, Science 323, 486 (2009).

[7] A. Karlsson and M. Bourennane, Phys. Rev. A 58, 4394 (1998); M. Hillery, V. Buzek and A. Berthiaume, Phys. Rev. A 59 (1999) 1829.

[8] B. S. Shi and A. Tomita, Phys. Lett. A 296, 161 (2002); J. Joo and Y.-J. Park, Phys. Lett. A 296 (2002) 161; B. S. Shi and A. Tomita, Phys. Lett. A 300 (2002) 324.

[9] H. Prakash and A. K. Maurya, Opt. Commun. 284, 5024 (2011); J. Joo, Y. J. Park, S. Oh and J. Kim, New J. of Phys. 5, 136 (2003); Z. L. Cao and M. Yang, Physica A 337 132 (2004).

[10] C. P. Yang and G. C. Guo, Chin. Phys. Lett. 17, 162 (2000); J. Lee, H. Min, and S. D. Oh, Phys. Rev. A 66, 052318 (2002).

[11] G. Rigolin, Phys. Rev. A 71, 032303 (2005); F.-G. Deng, Phys. Rev. A 72, 036301 (2005).

[12] Y. Yeo and W. K. Chua, Phys. Rev. Lett. 96, 060502 (2006).

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

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

[15] C.-P. Yang, S.-I. Chu and S. Han, Phys. Rev. A 70, 022329 (2004); Z.-J. Zhang, Phys. Lett. A 352, 55 (2006).

[16] Z.-X. Man, Y.-J. Xia and N. B. An, Phys. Rev. A 75, 052306 (2007); Z.-X. Man, Y.-J. Xia and N. B. An, J. Phys. B: At. Mol. Opt. Phys. 40, 1767 (2007).

[17] Y.-B. Zhan, Chin. Phys. 16 2557 (2007).

[18] Y.-J. Tao, D.-P. Tian, M.-L. Hu and M. Qin, Chin. Phys. B 17, 624 (2008).

[19] Z. Zhang, Y. Liu and D. Wang, Phys. Lett. A 372, 28 (2007).

[20] X.-G. Zhan, H.-M. Li, H. Ji and H.-S. Zeng, Chin. Phys. 16 2880 (2007); H. Ji, X.-G. Zhan and H.-S. Zeng, Chin. Phys. Lett. 24 2724 (2007).

[21] J. Wang, K. Hou, H Yuan and S.-H. Shi, Phys. Scr. 80, 015004 (2009).

[22] X.-H. Li, F.-G. Deng and H.-Y. Zhou, Chin. Phys. Lett. 24, 1151 (2007).

[23] P. Zhou, X.-H. Li, F.-G. Deng and H.-Y. Zhou, J. Phys. A: Math. Theor. 40, 13121 (2007).

[24] J. Dong and J. F. Teng, Eur. Phys. J. D 49, 129 (2008).

[25] T.-J. Wang, H.-Y. Zhou and F.-G. Deng, Physica A 387, 4716 (2008).

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

[27] A. K. Maurya, M. K. Mishra and H. Prakash, Int. J. Comp. Tech. 1, 183 (2014).