Wilfrid Laurier University

Scholars Commons @ Laurier

8-11-2014

"Multiparty Quantum Communication Using Multiqubit Entanglement and Teleportation"

Shohini Ghose
Wilfrid Laurier University, sghose@wlu.ca

Atul Kumar
Indian Institute of Technology - Jodhpur

Angele M. Hamel
Wilfrid Laurier University, ahamel@wlu.ca

Follow this and additional works at: https://scholars.wlu.ca/phys_faculty

Part of the Physics Commons

Recommended Citation

S. Ghose, A. Kumar, and A. M. Hamel, "Multiparty Quantum Communication Using Multiqubit Entanglement and Teleportation," Physics Research International, vol. 2014, Article ID 948750, 8 pages, 2014. doi:10.1155/2014/948750

Research Article

Multiparty Quantum Communication Using Multiqubit Entanglement and Teleportation

S. Ghose,[1,2] A. Kumar,[3] and A. M. Hamel[1]

[1] *Wilfrid Laurier University, Waterloo, ON, Canada N2L 3C5*
[2] *University of Waterloo, Waterloo, ON, Canada N2L 3G1*
[3] *Indian Institute of Technology Jodhpur, Rajasthan 342 011, India*

Correspondence should be addressed to S. Ghose; sghose@wlu.ca

We propose a $2N$ qubit entangled channel that can be used to teleport N qubits in a network to a single receiver. We describe the structure of this channel and explicitly demonstrate how the protocol works. The channel can be used to implement a scheme in which all parties have to participate in order for the teleportation to be successful. This can be advantageous in various scenarios and we discuss the potential application of this protocol to voting.

1. Introduction

Communication in a network of multiple parties is currently a vital area of research and discussion. Quantum protocols that harness the power of entanglement offer new avenues for efficient multipartite communication. For example, the pioneering protocol of Christandl and Wehner [1] allows one member of a group to send another member anonymous messages. However, their solution allows a malicious group member to alter the transmitted state undetected. Brassard et al. [2] offer an improved anonymous communication protocol that sets no limit on the number of malicious participants and aborts if they are active. Identifying quantum channels for novel communication protocols thus remains an active area of research [3–16]. Such channels have potential applications to tasks such as voting, where private messages go to a single receiver. Quantum voting protocols have been proposed that use entangled states distributed amongst participants in order to allow each participant to act independently and in secret [17–24]. Although the schemes ensure the anonymity of the senders, they require qubits/qudits to be physically sent to the receiver, which makes protocols vulnerable to eavesdropping or cheating.

In this paper we describe a protocol for communication using multiqubit entanglement and teleportation. We consider a network of N parties, where each person wants to send a qubit privately and anonymously to a receiver. In the context of voting, each qubit could be used to encode a yes/no vote of the sender. One simple option for sending N qubits to a receiver is for each member of the network to share an entangled Bell pair with the receiver and use this entangled channel to teleport his/her qubit to the receiver. Here, we describe the use of a $2N$ qubit entangled state to perform the teleportation. This $2N$ qubit state cannot be written as a product of N Bell pairs via local operations. By controlling access to the $2N$th qubit, we can develop a scheme that cannot be implemented with Bell pairs: we look at the case where all members in the network must participate or the protocol fails; that is, if any member does not send a qubit, then the receiver will not receive any of the qubits perfectly. Such an all-or-nothing scenario would be useful in certain voting schemes such as a jury or a committee, or in countries like Australia where all voters must participate. Furthermore, this protocol would be useful in cases where each transmitted qubit only encodes part of a message and the message is readable only if all parts are teleported. For example, the qubits could encode parts of the password to a joint bank account shared by all N parties that can only be accessed with the knowledge and participation of all members. Another possible application is in a spy network, where each spy in the network knows and transmits part

of a secret. Unlike other secret sharing schemes [25–29], the senders do not have to communicate with each other and do not have any common information at the end of the protocol.

We propose a $2N$ qubit entangled channel that can be used to teleport N qubits to a receiver. Unlike other schemes for N-qubit teleportation [8, 30–32], our protocol only requires single and two-qubit gates and measurements that are feasible in current experiments. Like other teleportation protocols, since the N qubits are teleported to the receiver by the senders, there is no physical transmission of qubits from the senders to the receiver and thus nothing for an adversary to steal or eavesdrop on. We describe how the structure of the entangled channel can also be used to ensure that the protocol succeeds when all N senders participate. The set up satisfies the general criteria for voting protocols established in the literature [18].

  (1) No one can determine the state of anyone else's qubit (vote) from the publicly broadcast information in the protocol.

  (2) The receiver will not be able to gain any information about the individual qubits from the publicly broadcast information in the protocol. The receiver does not need to know the state of each qubit to accurately receive each teleported qubit. Information labelling individual qubits (votes) can be discarded before measuring the state of each qubit to count votes.

  (3) A sender cannot prove to a third party what his/her teleported state was. For voting, this means that the vote is receipt-free; that is, the voter cannot prove to a third party how he/she voted.

  (4) A sender cannot transmit more than one qubit. In the context of voting, this means that each authorized voter can only vote once.

In order to ensure these conditions, our protocol requires some assumptions to be made:

  (1) The senders and the receiver verify that they share a perfect entangled channel using established techniques. Once the senders and the receiver verify that they share a perfect quantum channel, the protocol ensures that only authorized senders participate in the protocol.

  (2) All the senders and the receiver in the protocol are honest; that is, none of them tries to cheat during the protocol.

Under these assumptions, our protocol ensures teleportation of N independent qubits to the receiver with perfect fidelity and unit probability. We now proceed to discuss the protocol in detail.

2. $2N$ Qubit Entangled Quantum Channel

Before describing our $2N$ qubit entangled channel, we first review the properties of a standard quantum channel composed of the direct product of N Bell pairs $|\phi\rangle^{+} = (1/\sqrt{2})[|00\rangle + |11\rangle]$; that is,

$$
\begin{aligned}
|\Phi\rangle_{12\cdots(2N-1)(2N)} = {} & |\phi\rangle^{+}_{(1)(N+1)} \otimes |\phi\rangle^{+}_{(2)(N+2)} \cdots \\
& \otimes |\phi\rangle^{+}_{(N-1)(2N-1)} \otimes |\phi\rangle^{+}_{(N)(2N)},
\end{aligned}
\tag{1}
$$

where the 1st qubit is entangled with the $(N + 1)$th qubit, 2nd qubit is entangled with the $(N + 2)$th qubit, and so on. The $2N$ qubit channel in (1) has the property that the value (0 or 1) of the first N qubits is exactly the same as that of the last N qubits. For example, the four- and six-qubit quantum channels corresponding to the direct product of two and three Bell pairs can be written as

$$
\begin{aligned}
|\Phi\rangle_{1234} & = |\phi\rangle^{+}_{13} \otimes |\phi\rangle^{+}_{24} \\
& = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]_{13} \otimes \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]_{24} \\
& = \frac{1}{2}[|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle]_{1234},
\end{aligned}
\tag{2}
$$

$$
\begin{aligned}
|\Phi\rangle_{123456} & = |\phi\rangle^{+}_{14} \otimes |\phi\rangle^{+}_{25} \otimes |\phi\rangle^{+}_{36} \\
& = \frac{1}{2}[|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle]_{1245} \\
& \quad \otimes \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]_{36} \\
& = \frac{1}{2\sqrt{2}}[|000000\rangle + |001001\rangle + |010010\rangle \\
& \qquad + |011011\rangle + |100100\rangle + |101101\rangle \\
& \qquad + |110110\rangle + |111111\rangle]_{123456},
\end{aligned}
\tag{3}
$$

respectively. Notice that the first 2 qubits in each term in (2) are identical to the last 2 qubits and the first 3 qubits in (3) are identical to the last 3 qubits in each term. This property allows us to analyze the characteristics of the $2N$ qubit entangled quantum state used as a resource in this paper.

The $2N$ qubit entangled channel we propose $|\Psi\rangle_{12\cdots(2N-1)(2N)}$ can be written as

$$
\begin{aligned}
& |\Psi\rangle_{12\cdots(2N-1)2N} \\
& = \frac{1}{\sqrt{2^{N-1}}} \\
& \times \left[\sum_{i} \left\{ |\psi_{i}\rangle_{1\cdots(N-1)} |\psi_{i}\rangle_{(N+1)\cdots(2N-1)} \right\} |\phi\rangle^{+}_{N(2N)} \right. \\
& \left. \quad + \sum_{j} \left\{ |\psi_{j}\rangle_{1\cdots(N-1)} |\psi_{j}\rangle_{(N+1)\cdots(2N-1)} \right\} |\psi\rangle^{+}_{N(2N)} \right],
\end{aligned}
\tag{4}
$$

where the state $|\psi_i\rangle$ contains half of the basis states corresponding to $(N-1)$ qubits with even number of $|1\rangle$'s and the state $|\psi_j\rangle$ contains other half of the basis states with odd number of $|1\rangle$'s. This state cannot be transformed into the product state of N Bell pairs (1), via local unitary operations. For each term of the $2N$ qubit entangled state $|\Psi\rangle_{12\cdots(2N-1)(2N)}$, the value (0 or 1) of the $2N$th qubit is exactly the same as that of the Nth qubit if the number of $|1\rangle$'s from the qubits $1, 2, \ldots, (N-1)$ is even; else the value of the $2N$th qubit is opposite to that of the Nth qubit. For example, the states $|\psi_i\rangle$ and $|\psi_j\rangle$ for a four-qubit quantum channel would be $|\psi_i\rangle_1 = |\psi_i\rangle_3 = |0\rangle$ and $|\psi_j\rangle_1 = |\psi_j\rangle_3 = |1\rangle$. Similarly for a six-qubit quantum channel, the states $|\psi_i\rangle$ and $|\psi_j\rangle$ are $|\psi_i\rangle_{12} = |\psi_i\rangle_{45} = |00\rangle, |11\rangle$ and $|\psi_j\rangle_{12} = |\psi_j\rangle_{45} = |01\rangle, |10\rangle$, respectively. Hence, the four- and six-qubit entangled channels would be

$$
\begin{aligned}
|\Psi\rangle_{1234} &= \frac{1}{2}\left[|00\rangle_{13} \otimes \frac{1}{\sqrt{2}}\{|00\rangle + |11\rangle\}_{24} \right.\\
&\quad \left. + |11\rangle_{13} \otimes \frac{1}{\sqrt{2}}\{|01\rangle + |10\rangle\}_{24} \right]\\
&= \frac{1}{2}[|0000\rangle + |0101\rangle + |1011\rangle + |1110\rangle]_{1234},
\end{aligned}
\tag{5a}
$$

$$
\begin{aligned}
|\Psi\rangle_{123456} &= \frac{1}{2}\left[\{|0000\rangle + |1111\rangle\}_{1245} \right.\\
&\quad \otimes \frac{1}{\sqrt{2}}\{|00\rangle + |11\rangle\}_{36}\\
&\quad + \{|0101\rangle + |1010\rangle\}_{1245}\\
&\quad \left. \otimes \frac{1}{\sqrt{2}}\{|01\rangle + |10\rangle\}_{36} \right]\\
&= \frac{1}{2\sqrt{2}}[|000000\rangle + |001001\rangle + |010011\rangle\\
&\quad + |011010\rangle + |100101\rangle + |101100\rangle\\
&\quad + |110110\rangle + |111111\rangle]_{123456}.
\end{aligned}
\tag{5b}
$$

Notice that, in each term, the fourth qubit (sixth qubit) in (5a) (see (5b)) is exactly the same as the second qubit (third qubit) if the number of $|1\rangle$'s in the individual terms $|0\rangle, |1\rangle$ ($|00\rangle, |01\rangle, |10\rangle, |11\rangle$) of the state $|\psi\rangle_1/_3$ ($|\psi\rangle_{12}/_{45}$) is even; else the fourth (sixth) qubit is the opposite of the second (third) qubit. Note also that the first N qubits each has nonzero concurrence with the $2N$th qubit, where concurrence is a measure of two-qubit entanglement [33]. This entanglement with the $2N$th qubit can be used for the teleportation scheme as described below.

3. N-Qubit Communication Protocol

We first review the original teleportation protocol proposed by Bennett et al. [34] in order to provide an insight into our scheme. If a sender wants to communicate a single qubit state $|\phi\rangle_1 = [a|0\rangle + b|1\rangle]_1$ to a receiver, then the sender and the receiver must share one of the Bell states, that is,

$$
\begin{aligned}
|\psi\rangle_{23}^{\pm} &= \frac{1}{\sqrt{2}}[|01\rangle \pm |10\rangle]_{23},\\
|\phi\rangle_{23}^{\pm} &= \frac{1}{\sqrt{2}}[|00\rangle \pm |11\rangle]_{23},
\end{aligned}
\tag{6}
$$

where the qubit 2 is assigned to the sender and the qubit 3 is assigned to the receiver. If the shared entangled resource is $|\phi\rangle_{23}^{+}$ then the joint state of the three qubits can be written as

$$
\begin{aligned}
|\psi\rangle_{234} &= |\phi\rangle_1 \otimes |\phi\rangle_{23}^{+}\\
&= \frac{|\phi\rangle_{12}^{+}}{2}[a|0\rangle + b|1\rangle]_3 + \frac{|\phi\rangle_{12}^{-}}{2}[a|0\rangle - b|1\rangle]_3\\
&\quad + \frac{|\psi\rangle_{12}^{+}}{2}[a|1\rangle + b|0\rangle]_3 + \frac{|\psi\rangle_{12}^{-}}{2}[a|1\rangle - b|0\rangle]_3.
\end{aligned}
\tag{7}
$$

If the sender performs any measurement on the qubits 1 and 2 in the Bell basis, then the state of receiver's qubit will be projected onto one of the four possible states as shown in (7) with equal probability of $1/4$. For example, if the sender's measurement outcome is $|\phi\rangle_{12}^{+}$, then the receiver's qubit will be projected onto the desired teleported state. However, in all the other measurement outcomes of the sender, the receiver would need to perform a single qubit unitary transformation on the qubit 3 to recover the teleported state.

The direct product state of N Bell pairs $|\phi\rangle_{ij}^{+}$ in (1) can also be used as a resource for the teleportation of N single qubit states in a similar fashion. For example, if the $2N$ qubit channel in (1) is shared between the N senders and a receiver, then the first N qubits can be assigned to the N senders and the last N qubits can be assigned to the receiver. Each sender wants to teleport a single-qubit state to the receiver and thus measures his/her qubits in the Bell basis and sends the measurement result to the receiver. The receiver would then be able to recover the state of all the qubits by performing single-qubit unitary transformations on his/her qubits depending on the measurement outcomes of the senders. Notice that, similar to the single qubit teleportation protocol, the measurement outcomes $|\phi\rangle_{ij}^{+}$, $|\phi\rangle_{ij}^{-}$, $|\psi\rangle_{ij}^{+}$, and $|\psi\rangle_{ij}^{-}$ would always correspond to the states $[a|0\rangle + b|1\rangle]$, $[a|0\rangle - b|1\rangle]$, $[a|1\rangle + b|0\rangle]$, and $[a|1\rangle - b|0\rangle]$, respectively.

We now proceed to describe the teleportation protocol using our state (4) as an entangled channel, instead of the standard channel of N Bell pairs described above. For our protocol, the first N qubits in the shared entangled state are with the senders and the last N qubits are with the receiver. Each sender wants to teleport the state $|\phi\rangle_{A_i} = [a_{A_i}|0\rangle_{A_i} + b_{A_i}|1_{A_i}\rangle]$ to the receiver. Thus, the joint state of $3N$ qubits,

TABLE 1: 2-qubit teleportation: unitary transformations required for the receiver to recover two qubits depending on the measurement outcomes of the two senders.

First sender's measurements	Second sender's measurements	Unitary transformations required to obtain the correct votes corresponding to the measurement outcomes $(++, +-, -+, --)$
$\lvert\phi\rangle^{\pm}_{A_1 1}$	$\lvert\phi\rangle^{\pm}_{A_2 2}$	$I, \sigma_z^4, \sigma_z^3, \sigma_z^3\sigma_z^4$
$\lvert\phi\rangle^{\pm}_{A_1 1}$	$\lvert\psi\rangle^{\pm}_{A_2 2}$	$\sigma_x^4, \sigma_y^4, \sigma_z^3\sigma_x^4, \sigma_z^3\sigma_y^4$
$\lvert\psi\rangle^{\pm}_{A_1 1}$	$\lvert\phi\rangle^{\pm}_{A_2 2}$	$\sigma_x^3, \sigma_x^3\sigma_z^4, \sigma_y^3, \sigma_y^3\sigma_z^4$
$\lvert\psi\rangle^{\pm}_{A_1 1}$	$\lvert\psi\rangle^{\pm}_{A_2 2}$	$\sigma_x^3\sigma_x^4, \sigma_x^3\sigma_y^4, \sigma_y^3\sigma_x^4, \sigma_y^3\sigma_y^4$

composed of N votes and $2N$ qubit entangled channel can be expressed as

$$
\begin{aligned}
&\lvert\psi\rangle_{12\cdots(3N-1)3N} \\
&= \prod_i \left[a_{A_i}\lvert 0\rangle_{A_i} + b_{A_i}\lvert 1\rangle_{A_i}\right] \otimes \lvert\psi\rangle_{12\cdots(2N-1)2N}.
\end{aligned}
\tag{8}
$$

Each sender performs a Bell measurement on his/her qubit to be teleported and the shared entangled qubit in the $2N$ qubit entangled state. The joint state of $3N$ qubits in (8) can be rewritten in terms of the measurement basis of all the senders as

$$
\begin{aligned}
\lvert\psi\rangle = \frac{1}{2^N}\Big[&\big\{\lvert\phi\rangle^+_{A_1 1}\otimes\lvert\phi\rangle^+_{A_2 2}\otimes\cdots \\
&\otimes\lvert\phi\rangle^+_{A_{N-1}(N-1)}\otimes\lvert\phi\rangle^+_{A_N N}\big\} \\
&\otimes\lvert\chi\rangle^{(1)}_{(N+1)(N+2)\cdots(2N-1)2N} \\
&+\big\{\lvert\phi\rangle^+_{A_1 1}\otimes\lvert\phi\rangle^+_{A_2 2}\otimes\cdots \\
&\otimes\lvert\phi\rangle^+_{A_{N-1}(N-1)}\otimes\lvert\phi\rangle^-_{A_N N}\big\} \\
&\otimes\lvert\chi\rangle^{(2)}_{(N+1)(N+2)\cdots(2N-1)2N}+\cdots \\
&+\big\{\lvert\psi\rangle^-_{A_1 1}\otimes\lvert\psi\rangle^-_{A_2 2}\otimes\cdots \\
&\otimes\lvert\psi\rangle^-_{A_{N-1}(N-1)}\otimes\lvert\psi\rangle^+_{A_N N}\big\} \\
&\otimes\lvert\chi\rangle^{(4^N-1)}_{(N+1)(N+2)\cdots(2N-1)2N} \\
&+\big\{\lvert\psi\rangle^-_{A_1 1}\otimes\lvert\psi\rangle^-_{A_2 2}\otimes\cdots \\
&\otimes\lvert\psi\rangle^-_{A_{N-1}(N-1)}\otimes\lvert\psi\rangle^-_{A_N N}\big\} \\
&\otimes\lvert\chi\rangle^{(4^N)}_{(N+1)(N+2)\cdots(2N-1)2N}\Big],
\end{aligned}
\tag{9}
$$

where $\lvert\chi\rangle^{(1)}_{(N+1)(N+2)\cdots(2N-1)2N} - \lvert\chi\rangle^{(4^N)}_{(N+1)(N+2)\cdots(2N-1)2N}$ are the states of receiver's qubits depending on the measurement outcomes of all the senders and contains all the information about the individual qubits (votes). For example, if we consider a four-qubit entangled resource, then the $\lvert\chi\rangle^{(1)}_{34}$

state corresponding to the measurement outcomes $\lvert\phi\rangle^+_{A_1 1}$ and $\lvert\phi\rangle^+_{A_2 2}$ would be

$$
\begin{aligned}
\lvert\chi\rangle^{(1)}_{34} = \big[&a_{A_1}a_{A_2}\lvert 00\rangle_{34} + a_{A_1}b_{A_2}\lvert 01\rangle_{34} \\
&+ b_{A_1}a_{A_2}\lvert 11\rangle_{34} + b_{A_1}b_{A_2}\lvert 10\rangle_{34}\big].
\end{aligned}
\tag{10}
$$

The receiver at this stage would not be able to separate the exact qubits teleported by the senders as the joint state of receiver's qubit cannot be written as the direct product state of the individual qubits. However, if he/she performs a CNOT operation with qubit 3 as the control and qubit 4 as the target, then the joint state of the receiver's qubits can be reexpressed as

$$
\begin{aligned}
\lvert\chi\rangle^{(1)}_{34} &= \big[a_{A_1}a_{A_2}\lvert 00\rangle_{34} + a_{A_1}b_{A_2}\lvert 01\rangle_{34} \\
&\quad + b_{A_1}a_{A_2}\lvert 10\rangle_{34} + b_{A_1}b_{A_2}\lvert 11\rangle_{34}\big] \\
&= \big[a_{A_1}\lvert 0\rangle_3 + b_{A_1}\lvert 1_3\rangle\big]\otimes\big[a_{A_2}\lvert 0\rangle_4 + b_{A_2}\lvert 1_4\rangle\big],
\end{aligned}
\tag{11}
$$

respectively. Thus, the receiver can successfully separate the qubits teleported by the senders. However, for all the other measurement outcomes of the senders, the receiver would need to perform single qubit unitary operations in addition to the CNOT transformations. The required single-qubit unitary transformations for the use of the four qubit entangled channel are summarized in Table 1. For this protocol to be successful, the receiver must know the distribution of entangled qubits so that he/she can apply the correct unitary transformations to recover the teleported qubits accurately. The multiqubit state teleported to the receiver could be used as an input for another computation or communication protocol without the receiver having to know the state of the qubits.

For the case of a $2N$ qubit entangled channel, the state $\lvert\chi\rangle^{(1)}_{(N+1)(N+2)\cdots(2N-1)2N}$ corresponding to the measurement outcomes $\lvert\phi\rangle^+_{A_1 1}, \lvert\phi\rangle^+_{A_2 2}, \ldots, \lvert\phi\rangle^+_{A_{N-1}(N-1)}$ and $\lvert\phi\rangle^+_{A_N(N)}$ can be either written as

$$
\begin{aligned}
&\lvert\chi\rangle^{(1)}_{(N+1)(N+2)\cdots(2N-1)2N} \\
&= \big[a_{A_1}a_{A_2}\cdots a_{A_{N-1}}a_{A_N}\lvert 00\cdots 00\rangle_{(N+1)(N+2)\cdots(2N-1)2N} \\
&\quad + a_{A_1}a_{A_2}\cdots a_{A_{N-1}}b_{A_N}\lvert 00\cdots 01\rangle_{(N+1)(N+2)\cdots(2N-1)2N} \\
&\quad + a_{A_1}a_{A_2}\cdots b_{A_{N-1}}a_{A_N}\lvert 00\cdots 11\rangle_{(N+1)(N+2)\cdots(2N-1)2N}
\end{aligned}
$$

$$+ a_{A_1} a_{A_2} \cdots b_{A_{N-1}} b_{A_N} |00\cdots10\rangle_{(N+1)(N+2)\cdots(2N-1)2N}$$

$$+ \cdots$$

$$+ b_{A_1} b_{A_2} \cdots a_{A_{N-1}} a_{A_N} |11\cdots00\rangle_{(N+1)(N+2)\cdots(2N-1)2N}$$

$$+ b_{A_1} b_{A_2} \cdots a_{A_{N-1}} b_{A_N} |11\cdots01\rangle_{(N+1)(N+2)\cdots(2N-1)2N}$$

$$+ b_{A_1} b_{A_2} \cdots b_{A_{N-1}} a_{A_N} |11\cdots11\rangle_{(N+1)(N+2)\cdots(2N-1)2N}$$

$$+ b_{A_1} b_{A_2} \cdots b_{A_{N-1}} b_{A_N} |11\cdots10\rangle_{(N+1)(N+2)\cdots(2N-1)2N} \big]$$
$$(12)$$

if N is even or

$$|\chi\rangle^{(1)}_{(N+1)(N+2)\cdots(2N-1)2N}$$

$$= \big[a_{A_1} a_{A_2} \cdots a_{A_{N-1}} a_{A_N} |00\cdots00\rangle_{(N+1)(N+2)\cdots(2N-1)2N}$$

$$+ a_{A_1} a_{A_2} \cdots a_{A_{N-1}} b_{A_N} |00\cdots01\rangle_{(N+1)(N+2)\cdots(2N-1)2N}$$

$$+ a_{A_1} a_{A_2} \cdots b_{A_{N-1}} a_{A_N} |00\cdots11\rangle_{(N+1)(N+2)\cdots(2N-1)2N}$$

$$+ a_{A_1} a_{A_2} \cdots b_{A_{N-1}} b_{A_N} |00\cdots10\rangle_{(N+1)(N+2)\cdots(2N-1)2N}$$

$$+ \cdots$$

$$+ b_{A_1} b_{A_2} \cdots a_{A_{N-1}} a_{A_N} |11\cdots01\rangle_{(N+1)(N+2)\cdots(2N-1)2N}$$

$$+ b_{A_1} b_{A_2} \cdots a_{A_{N-1}} b_{A_N} |11\cdots00\rangle_{(N+1)(N+2)\cdots(2N-1)2N}$$

$$+ b_{A_1} b_{A_2} \cdots b_{A_{N-1}} a_{A_N} |11\cdots10\rangle_{(N+1)(N+2)\cdots(2N-1)2N}$$

$$+ b_{A_1} b_{A_2} \cdots b_{A_{N-1}} b_{A_N} |11\cdots11\rangle_{(N+1)(N+2)\cdots(2N-1)2N} \big]$$
$$(13)$$

if N is odd. In order to recover the teleported qubits, the receiver performs $(N-1)$ CNOT operations on the joint state of N qubits by always using the $2N$th qubit as the target and the qubits $(N+1), (N+2), \ldots (2N-2), (2N-1)$ as controls, respectively. The CNOT operations transform the states in (12) and (13) to the form

$$|\chi\rangle^{(1)}_{(N+1)(N+2)\cdots(2N-1)2N} = \prod_i \left(a_{A_i} |0\rangle_{N+i} + b_{A_i} |1\rangle_{N+i} \right).$$
$$(14)$$

In this specific case, the receiver does not need to perform any single-qubit unitary transformations. However, for all other sets of measurement outcomes, the receiver would need to apply single-qubit transformations to his/her qubits conditioned on the senders' measurement outcomes to exactly recover the teleported qubits. Notice that the measurement outcomes $|\phi\rangle^+_{A_i i}$, $|\phi\rangle^-_{A_i i}$, $|\psi\rangle^+_{A_i i}$, and $|\psi\rangle^-_{A_i i}$ correspond to the states $[a_{A_i}|0\rangle_{N+i} + b_{A_i}|1\rangle_{N+i}]$, $[a_{A_i}|0\rangle_{N+i} - b_{A_i}|1\rangle_{N+i}]$, $[a_{A_i}|1\rangle_{N+i} + b_{A_i}|0\rangle_{N+i}]$, and $[a_{A_i}|1\rangle_{N+i} - b_{A_i}|0\rangle_{N+i}]$, respectively. For example, if the measurement outcomes of all the senders are $|\psi\rangle^-_{A_i i}$ then in addition to the $(N-1)$ CNOT operations, the receiver needs to apply σ^i_y operations to all the qubits. Similarly, for all other sets of measurement outcomes,

the receiver has to apply the appropriate unitary to each qubit in order to recover all the teleported qubits accurately.

Note that the all the receiver's CNOT operations use the $2N$th qubit as a target. The channel is not symmetric so it is important for the $2N$th qubit to be the target qubit. Thus, if the receiver does not have access to the $2N$th qubit for performing the CNOT gates, then the protocol would not work. Thus by controlling the receiver's access to the $2N$th qubit one can ensure that the protocol is only successful when all the senders participate. In order to ensure that the receiver only performs all the CNOT operations when all the senders participate, one could require that the receiver only gets access to the $2N$th qubit after all the senders broadcast their measurement results. If one or more senders decide not to participate in the scheme and do not measure his/her qubit, then the receiver would not get access to the $2N$th qubit and would not be able to perform any of the CNOT operations. In comparison, for the standard teleportation using N Bell pairs, limiting the receiver's access to only the $2N$th qubit would not prevent the successful teleportation of the 1st $N-1$ qubits. Our protocol thus offers the possibility of a scheme that cannot be done with N Bell pairs. Securing access to the $2N$th qubit also has an additional benefit: if the other qubits on the receiver's end are compromised or stolen, the teleported state of the qubits cannot be recovered from the stolen qubits, since the $2N$th qubit is required as a target to perform the CNOT operations and recover the teleported state of the other qubits. Thus, by keeping the $2N$th qubit secure, the protocol's security is ensured. In comparison, for the standard teleportation using N Bell pairs, all the qubits have to be kept safe in order to ensure secure teleportation. In a network as the number of senders N grows larger, the benefit of our protocol increases.

The protocol described above can be used in a voting system, where each sender sends a yes/no vote encoded in the teleported qubit. The voters (senders) do not have to physically send their votes to the polling station, since their votes are teleported to the receiver at the polling station. When we vote with a traditional paper ballot system, a number of properties are either explicit or implicit, properties such as confidentiality, eligibility, and integrity. Electronic voting systems, including quantum based systems, attempt to accomplish similar goals in the digital domain. In particular, they strive to maintain integrity, ensure eligibility, preserve unlinkability, and allow verifiability. The classic text, *Applied Cryptography* [35], lists specific properties a voting system should have. A more recent work [36] describes an entire taxonomy providing a hierarchy of protection a voting system can provide. Quantum-based systems excel at certain aspects. For example, our system has no physical transfer of ballots, since the vote qubits are teleported, so there is nothing to physically steal. Also, thanks to the no-cloning theorem, our ballots cannot be duplicated (and, in fact, nonduplication is identified by [35] as one of the hardest requirements to meet).

A recent quantum paper [18] lists security properties that a quantum voting system should satisfy and here we compare our protocol against these properties and describe explicitly below how our protocol can be used in a manner that meets these rules.

(R1) *The vote of each voter should be kept secret from all other voters.* Like all teleportation schemes, since the only publicly broadcast messages are the measurement outcomes of each voter, the individual votes cannot be deterministically extracted from this public information. In fact this means that not just the other voters are ignorant of a particular vote, but any outside observer is similarly ignorant.

(R2) *The receiver should not be able to gain information about the voting of individual voters.* The receiver at the polling station does not need to first know the state of each qubit (the vote) in order to perform the transformations required to accurately receive each teleported vote qubit. Once the receiver at the polling station has performed the operations and all the qubits have been successfully teleported, the information regarding which qubit was teleported from which sender can be deleted before the vote qubits are sent for measurement in order to count the vote. Hence when the votes are counted, there is no information about the voting of individual voters.

(R3) *The votes should be receipt-free.* Each voter's Bell measurement destroys the original state that was to be teleported, so a voter cannot show his/her vote to a third party after the vote has been teleported. Furthermore, the voter cannot use the measurement outcomes to prove to a third party what his/her vote was.

(R4) *A voter should not vote more than once.* Once a sender performs a Bell measurement on his/her qubit from the entangled channel, it becomes disentangled from the rest of the system. Thus, the sender cannot teleport additional votes without having more qubits from the entangled qunatum channel. This ensures that a sender in a voting scheme cannot vote more than once.

Furthermore, we additionally meet the requirement that only authorized voters can vote. Here we assume that a standardized authorization scheme has been used to create a list of authorized voters. The entangled channel qubits are then only distributed to voters on this list. Without sharing a qubit from the entangled channel, a voter will not be able to teleport his/her vote. Unauthorized voters who are not on the list will not be a part of the entangled network and cannot vote.

4. Conclusion

The development of resources for quantum communication and computation lies at the heart of quantum information theory. We have described a $2N$ qubit entangled channel that can be used to teleport N independent qubits in a network to a single receiver. We have discussed the structure of this channel and demonstrated how the protocol can be used for teleporting N qubits using only single and 2-qubit operations. We have shown the explicit operations required for 2- and 3-qubit teleportation and described the general

N-qubit teleportation scheme. The structure of the channel constructed allows the design of a teleportation protocol in which all authorized parties that have a qubit from the entangled channel have to participate in the protocol. This can be advantageous in situations where we demand all parties to participate. As an example, we have discussed the potential application of this protocol in a voting scheme. This scheme ensures that all voters must participate, that only authorized voters can vote, that each voter can only vote once, and that the vote is receipt-free. Unlike other quantum voting schemes, a third party cannot intercept or steal the votes, since the votes are teleported rather than physically sent. Assuming that the locations of the voters are isolated from each other, then the votes are private since the individual votes cannot be extracted perfectly from the publicly broadcast measurement outcomes. Our results thus demonstrate the potential of using multiqubit entanglement for communication tasks tailored to specific needs. We hope to extend this idea to develop other novel schemes in the future.

Appendix

We explicitly demonstrate our protocol for the case of 3-qubit teleportation, using a six-qubit entangled channel. The joint state of $3N$ qubits in (9) can be rewritten in terms of the measurement basis of all the senders as

$$
\begin{aligned}
|\psi\rangle = \frac{1}{2^N} \Big[& \big\{ |\phi\rangle^+_{A_1 1} \otimes |\phi\rangle^+_{A_2 2} \otimes \cdots \\
& \otimes |\phi\rangle^+_{A_{N-1}(N-1)} \otimes |\phi\rangle^+_{A_N N} \big\} \\
& \otimes |\chi\rangle^{(1)}_{(N+1)(N+2)\cdots(2N-1)2N} \\
& + \big\{ |\phi\rangle^+_{A_1 1} \otimes |\phi\rangle^+_{A_2 2} \otimes \cdots \\
& \otimes |\phi\rangle^+_{A_{N-1}(N-1)} \otimes |\phi\rangle^-_{A_N N} \big\} \\
& \otimes |\chi\rangle^{(2)}_{(N+1)(N+2)\cdots(2N-1)2N} \\
& + \cdots \\
& + \big\{ |\psi\rangle^-_{A_1 1} \otimes |\psi\rangle^-_{A_2 2} \otimes \cdots \\
& \otimes |\psi\rangle^-_{A_{N-1}(N-1)} \otimes |\psi\rangle^+_{A_N N} \big\} \\
& \otimes |\chi\rangle^{(4^N-1)}_{(N+1)(N+2)\cdots(2N-1)2N} \\
& + \big\{ |\psi\rangle^-_{A_1 1} \otimes |\psi\rangle^-_{A_2 2} \otimes \cdots \\
& \otimes |\psi\rangle^-_{A_{N-1}(N-1)} \otimes |\psi\rangle^-_{A_N N} \big\} \\
& \otimes |\chi\rangle^{(4^N)}_{(N+1)(N+2)\cdots(2N-1)2N} \Big],
\end{aligned}
$$

$$(A.1)$$

where $|\chi\rangle^{(1)}_{(N+1)(N+2)\cdots(2N-1)2N} - |\chi\rangle^{(4^N)}_{(N+1)(N+2)\cdots(2N-1)2N}$ are the states of the receiver's qubits depending on the measurement outcomes of all the senders and contain all the information about the senders' individual qubits. If a six-qubit entangled resource is used then the $|\chi\rangle^{(1)}_{456}$ state corresponding to

TABLE 2: 3-qubit teleportation: unitary transformations required for the receiver to recover the 3-qubit teleported states depending on the measurement outcomes of the three senders.

First sender's measurement outcomes	Second sender's measurement outcomes	Third sender's measurement outcomes	Unitary transformations required to obtain the correct votes corresponding to the measurement outcomes $+++, ++-, +-+, +--, -++, \ -+-, \ --+, \ ---$
$\lvert\phi\rangle^{\pm}_{A_1 1}$	$\lvert\phi\rangle^{\pm}_{A_2 2}$	$\lvert\phi\rangle^{\pm}_{A_3 3}$	$I, \sigma_z^6, \sigma_z^5, \sigma_z^5\sigma_z^6$ $\sigma_z^4, \sigma_z^4\sigma_z^6, \sigma_z^4\sigma_z^5, \sigma_z^4\sigma_z^5\sigma_z^6$
$\lvert\phi\rangle^{\pm}_{A_1 1}$	$\lvert\phi\rangle^{\pm}_{A_2 2}$	$\lvert\psi\rangle^{\pm}_{A_3 3}$	$\sigma_x^6, \sigma_y^6, \sigma_z^5\sigma_x^6, \sigma_z^5\sigma_y^6$ $\sigma_z^4\sigma_x^6, \sigma_z^4\sigma_y^6, \sigma_z^4\sigma_z^5\sigma_x^6, \sigma_z^4\sigma_z^5\sigma_y^6$
$\lvert\phi\rangle^{\pm}_{A_1 1}$	$\lvert\psi\rangle^{\pm}_{A_2 2}$	$\lvert\phi\rangle^{\pm}_{A_3 3}$	$\sigma_x^5, \sigma_x^5\sigma_z^6, \sigma_y^5, \sigma_y^5\sigma_z^6$ $\sigma_z^4\sigma_x^5, \sigma_z^4\sigma_x^5\sigma_z^6, \sigma_z^4\sigma_y^5, \sigma_z^4\sigma_y^5\sigma_z^6$
$\lvert\phi\rangle^{\pm}_{A_1 1}$	$\lvert\psi\rangle^{\pm}_{A_2 2}$	$\lvert\psi\rangle^{\pm}_{A_3 3}$	$\sigma_x^5\sigma_x^6, \sigma_x^5\sigma_y^6, \sigma_y^5\sigma_x^6, \sigma_y^5\sigma_y^6$ $\sigma_z^4\sigma_x^5\sigma_x^6, \sigma_z^4\sigma_x^5\sigma_y^6, \sigma_z^4\sigma_y^5\sigma_x^6, \sigma_z^4\sigma_y^5\sigma_y^6$
$\lvert\psi\rangle^{\pm}_{A_1 1}$	$\lvert\phi\rangle^{\pm}_{A_2 2}$	$\lvert\phi\rangle^{\pm}_{m_3 3}$	$\sigma_x^4, \sigma_x^4\sigma_z^6, \sigma_x^4\sigma_z^5, \sigma_x^4\sigma_z^5\sigma_z^6$ $\sigma_y^4, \sigma_y^4\sigma_z^6, \sigma_y^4\sigma_z^5, \sigma_y^4\sigma_z^5\sigma_z^6$
$\lvert\psi\rangle^{\pm}_{A_1 1}$	$\lvert\phi\rangle^{\pm}_{A_2 2}$	$\lvert\psi\rangle^{\pm}_{A_3 3}$	$\sigma_x^4\sigma_x^6, \sigma_x^4\sigma_y^6, \sigma_x^4\sigma_z^5\sigma_x^6, \sigma_x^4\sigma_z^5\sigma_y^6$ $\sigma_y^4\sigma_x^6, \sigma_y^4\sigma_y^6, \sigma_y^4\sigma_z^5\sigma_x^6, \sigma_y^4\sigma_z^5\sigma_y^6$
$\lvert\psi\rangle^{\pm}_{A_1 1}$	$\lvert\psi\rangle^{\pm}_{A_2 2}$	$\lvert\phi\rangle^{\pm}_{A_3 3}$	$\sigma_x^4\sigma_x^5, \sigma_x^4\sigma_x^5\sigma_z^6, \sigma_x^4\sigma_y^5, \sigma_x^4\sigma_y^5\sigma_z^6$ $\sigma_y^4\sigma_x^5, \sigma_y^4\sigma_x^5\sigma_z^6, \sigma_y^4\sigma_y^5, \sigma_y^4\sigma_y^5\sigma_z^6$
$\lvert\psi\rangle^{\pm}_{A_1 1}$	$\lvert\psi\rangle^{\pm}_{A_2 2}$	$\lvert\psi\rangle^{\pm}_{A_3 3}$	$\sigma_x^4\sigma_x^5\sigma_x^6, \sigma_x^4\sigma_x^5\sigma_y^6, \sigma_x^4\sigma_y^5\sigma_x^6, \sigma_x^4\sigma_y^5\sigma_y^6$ $\sigma_y^4\sigma_x^5\sigma_x^6, \sigma_y^4\sigma_x^5\sigma_y^6, \sigma_y^4\sigma_y^5\sigma_x^6, \sigma_y^4\sigma_y^5\sigma_y^6$

the measurement outcomes $\lvert\phi\rangle^{+}_{A_1 1}$, $\lvert\phi\rangle^{+}_{A_2 2}$, and $\lvert\phi\rangle^{+}_{A_3 3}$ can be written as

$$\lvert\chi\rangle^{(1)}_{456} = \big[a_{A_1}a_{A_2}a_{A_3}\lvert000\rangle_{456} + a_{A_1}a_{A_2}b_{A_3}\lvert001\rangle_{456}$$
$$+ a_{A_1}b_{A_2}a_{A_3}\lvert011\rangle_{456} + a_{A_1}b_{A_2}b_{A_3}\lvert010\rangle_{456}$$
$$+ b_{A_1}a_{A_2}a_{A_3}\lvert101\rangle_{456} + b_{A_1}a_{A_2}b_{A_3}\lvert100\rangle_{456}$$
$$+ b_{A_1}b_{A_2}a_{A_3}\lvert110\rangle_{456} + b_{A_1}b_{A_2}b_{A_3}\lvert111\rangle_{456}\big].$$
$$(A.2)$$

As discussed above, the receiver would not be able to separate the exact votes sent by the senders as the joint state of receiver's qubit cannot be written as the direct product state of the individual qubits. However, if we apply two CNOT operations with qubits 4 and 5 as controls and qubit 6 as target then the joint state of receiver's qubits can be reexpressed as

$$\lvert\chi\rangle^{(1)}_{456} = \big[a_{A_1}a_{A_2}a_{A_3}\lvert000\rangle_{456} + a_{A_1}a_{A_2}b_{A_3}\lvert001\rangle_{456}$$
$$+ a_{A_1}b_{A_2}a_{A_3}\lvert010\rangle_{456} + a_{A_1}b_{A_2}b_{A_3}\lvert011\rangle_{456}$$
$$+ b_{A_1}a_{A_2}a_{A_3}\lvert100\rangle_{456} + b_{A_1}a_{A_2}b_{A_3}\lvert101\rangle_{456}$$
$$+ b_{A_1}b_{A_2}a_{A_3}\lvert110\rangle_{456} + b_{A_1}b_{A_2}b_{A_3}\lvert111\rangle_{456}\big]$$
$$= \big[a_{A_1}\lvert0\rangle_4 + b_{A_1}\lvert1_4\rangle\big] \otimes \big[a_{A_2}\lvert0\rangle_5 + b_{A_2}\lvert1_5\rangle\big]$$
$$\otimes \big[a_{A_3}\lvert0\rangle_6 + b_{A_3}\lvert1_6\rangle\big],$$
$$(A.3)$$

respectively. Thus, the receiver can successfully separate the exact qubits teleported by the senders. However, for all the other measurement outcomes of the senders, the receiver would need to perform single qubit unitary operations in addition to the CNOT transformations. For example, if a six-qubit quantum channel is used then, for the measurement outcomes $\lvert\phi\rangle^{+}_{A_1 1}$, $\lvert\phi\rangle^{+}_{A_2 2}$, and $\lvert\psi\rangle^{+}_{A_3 3}$ of the senders, the receiver needs to apply a σ_x^6 operation on the qubit 6. The protocol is successful for all the measurement outcomes of the senders. The required single-qubit unitary transformations for the use of six-qubit entangled channels is summarized in Table 2. For this protocol to be successful the receiver must know the distribution of entangled qubits so that he/she can apply the correct unitary transformations to recover the qubits exactly. However, this does not allow the receiver to gain any information about the individual qubits of the senders.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.
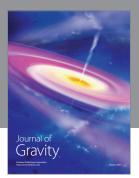
Acknowledgments
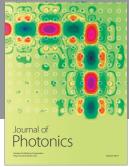
References

[1] M. Christandl and S. Wehner, "Quantum anonymous transmissions," in *Proceedings of the 11th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT '05)*, pp. 217–235, 2005.
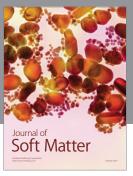
[2] G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, and A. Tapp, "Anonymous quantum communication," in *Advances in Cryptology—ASIACRYPT 2007*, vol. 4833 of *Lecture Notes in Computer Science*, pp. 460–473, Springer, Berlin, Germany, 2007.

[3] G. Rigolin, "Quantum teleportation of an arbitrary two-qubit state and its relation to multipartite entanglement," *Physical Review A*, vol. 71, Article ID 032303, 2005.

[4] F. G. Deng, "Temperature dependence of the velocity boundary condition for nanoscale fluid flows," *Physical Review A*, vol. 72, Article ID 036301, 2005.

[5] Z. X. Man, Y. J. Xia, and N. B. An, "Economical and feasible controlled teleportation of an arbitrary unknown *N*-qubit entangled state," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 40, no. 10, pp. 1767–1774, 2007.

[6] F. G. Deng, C. Y. Li, Y. S. Li, H. Y. Zhou, and Y. Wang, "Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement," *Physical Review A*, vol. 72, Article ID 022338, 2005.

[7] Y. Yeo and W. K. Chua, "Teleportation and dense coding with genuine multipartite entanglement," *Physical Review Letters*, vol. 96, Article ID 060502, 2006.

[8] P. X. Chen, S. Y. Zhu, and G. C. Guo, "General form of genuine multipartite entanglement quantum channels for teleportation," *Physical Review A*, vol. 74, Article ID 032324, 2006.

[9] Z. X. Man, Y. J. Xia, and N. B. An, "Genuine multiqubit entanglement and controlled teleportation," *Physical Review A*, vol. 75, no. 5, Article ID 052306, 5 pages, 2007.

[10] X. W. Wang, Y. G. Shan, L. X. Xia, and M. W. Lu, "Dense coding and teleportation with one-dimensional cluster states," *Physics Letters A*, vol. 364, no. 1, pp. 7–11, 2007.

[11] S. Muralidharan and P. K. Panigrahi, "Quantum-information splitting using multipartite cluster states," *Physical Review A*, vol. 78, Article ID 062333, 2008.

[12] N. Paul, J. V. Menon, S. Karumanchi, S. Muralidharan, and P. K. Panigrahi, "Quantum tasks using six qubit cluster states," *Quantum Information Processing*, vol. 10, no. 5, pp. 619–632, 2011.

[13] S. Muralidharan and P. K. Panigrahi, "Perfect teleportation, quantum-state sharing, and superdense coding through a genuinely entangled five-qubit state," *Physical Review A*, vol. 77, Article ID 032321, 2008.

[14] C. P. Yang, S.-I. Chu, and S. Han, "Efficient many-party controlled teleportation of multiqubit quantum information via entanglement," *Physical Review A*, vol. 70, Article ID 022329, 2004.

[15] S. Ghose, S. Debnath, N. Sinclair, and A. a. . Kabra, "Multiqubit nonlocality in families of 3- and 4-qubit entangled states," *Journal of Physics A: Mathematical and Theoretical*, vol. 43, no. 44, Article ID 445301, 16 pages, 2010.

[16] S. Ghose, N. Sinclair, S. Debnath, P. Rungta, and R. Stock, "Tripartite entanglement versus tripartite nonlocality in three-qubit greenberger-horne-zeilinger-class states," *Physical Review Letters*, vol. 102, Article ID 250404, 2009.

[17] M. Hillery, M. Ziman, V. Bužek, and M. Bieliková, "Towards quantum-based privacy and voting," *Physics Letters A*, vol. 349, no. 1–4, pp. 75–81, 2006.

[18] J. A. Vaccaro, J. Spring, and A. Chefles, "Quantum protocols for anonymous voting and surveying," *Physical Review A*, vol. 75, no. 1, Article ID 012333, 2007.

[19] S. Dolev, I. Pitowski, and B. Tamir, "A quantum secret ballot," http://arxiv.org/abs/quant-ph/0602087.

[20] D. Horoshko and S. Kilin, "Quantum anonymous voting with anonymity check," *Physics Letters A*, vol. 375, no. 8, pp. 1172–1175, 2011.

[21] M. Bonanome, V. Buzek, M. Hillery, and M. Ziman, "Toward protocols for quantum-ensured privacy and secure voting," *Physical Review A*, vol. 84, Article ID 022331, 2011.

[22] L. Jiang, G. He, D. Nie, J. Xiong, and G. Zeng, "Quantum anonymous voting for continuous variables," *Physical Review A: Atomic, Molecular, and Optical Physics*, vol. 85, no. 4, Article ID 042309, 2012.

[23] Y. Li and G. Zeng, "Anonymous quantum network voting scheme," *Optical Review*, vol. 19, no. 3, pp. 121–124, 2012.

[24] Y. Li and G. Zeng, "Quantum anonymous voting systems based on entangled state," *Optical Review*, vol. 15, no. 5, pp. 219–223, 2008.

[25] M. Hillery, V. Buzek, and A. Berthiaume, "Quantum secret sharing," *Physical Review A*, vol. 59, no. 3, pp. 1829–1834, 1999.

[26] A. Karlsson, M. Koashi, and N. Imoto, "Quantum entanglement for secret sharing and secret splitting," *Physical Review A: Atomic, Molecular, and Optical Physics*, vol. 59, article 162, no. 1, 1999.

[27] D. Gottesman, "Theory of quantum secret sharing," *Physical Review A*, vol. 61, no. 4, Article ID 042311, 8 pages, 2000.

[28] T. Tyc and B. C. Sanders, "How to share a continuous-variable quantum secret by optical interferometry," *Physics Letters A*, vol. 65, Article ID 042310, 2002.

[29] A. Karlsson and M. Bourennane, "Quantum teleportation using three-particle entanglement," *Physical Review A*, vol. 58, no. 6, pp. 4394–4400, 1998.

[30] C. Y. Cheung and Z. J. Zhang, "Criterion for faithful teleportation with an arbitrary multiparticle channel," *Physical Review A*, vol. 80, Article ID 022327, 2009.

[31] S. Muralidharan, S. Karumanchi, S. Jain, R. Srikanth, and P. K. Panigrahi, "2*N* qubit "mirror states" for optimal quantum communication," *The European Physical Journal D*, vol. 61, no. 3, pp. 757–763, 2011.

[32] M.-J. Zhao, Z.-G. Li, X. Li-Jost, and S. Fei, "Multiqubit quantum teleportation," *Journal of Physics A: Mathematical and Theoretical*, vol. 45, no. 40, Article ID 405303, 2012.

[33] W. K. Wootters, "Entanglement of formation of an arbitrary state of two qubits," *Physical Review Letters*, vol. 80, pp. 2245–2248, 1998.

[34] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters*, vol. 70, no. 13, pp. 1895–1899, 1993.

[35] B. Schneier, *Applied Cryptography*, John Wiley & Sons, New York, NY, USA, 2nd edition, 1996.

[36] L. Langer, A. Schmidt, J. Buchmann, and M. Volkamer, "A taxonomy refining the security requirements for electronic voting: Analyzing helios as a proof of concept," in *Proceedings of the 5th International Conference on Availability, Reliability, and Security (ARES '10)*, pp. 475–480, February 2010.