

Probabilistic quantum teleportation of shared quantum secret

Hengji Li(李恒吉), Jian Li(李剑), and Xiubo Chen(陈秀波)

Citation: Chin. Phys. B, 2022, 31 (**9**): 090303. DOI: 10.1088/1674-1056/ac67c0
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

---

teering quantum nonlocalities of quantum dot system suffering from decoherence

Huan Yang(杨欢), Ling-Ling Xing(邢玲玲), Zhi-Yong Ding(丁智勇), Gang Zhang(张刚), and Liu Ye(叶柳)
Chin. Phys. B, 2022, 31 (**9**): 090302. DOI: 10.1088/1674-1056/ac615a

Direct measurement of two-qubit phononic entangled states via optomechanical interactions

A-Peng Liu(刘阿鹏), Liu-Yong Cheng(程留永), Qi Guo(郭奇), Shi-Lei Su(苏石磊), Hong-Fu Wang(王洪福), and Shou Zhang(张寿)
Chin. Phys. B, 2022, 31 (**8**): 080307. DOI: 10.1088/1674-1056/ac5d2f

Finite-key analysis of practical time-bin high-dimensional quantum key distribution with afterpulse effect

Yu Zhou(周雨), Chun Zhou(周淳), Yang Wang(汪洋), Yi-Fei Lu(陆宜飞), Mu-Sheng Jiang(江木生), Xiao-Xu Zhang(张晓旭), and Wan-Su Bao(鲍皖苏)
Chin. Phys. B, 2022, 31 (**8**): 080303. DOI: 10.1088/1674-1056/ac6017

Practical security analysis of continuous-variable quantum key distribution with an unbalanced heterodyne detector

Lingzhi Kong(孔令志), Weiqi Liu(刘维琪), Fan Jing(荆凡), and Chen He(贺晨)
Chin. Phys. B, 2022, 31 (**7**): 070303. DOI: 10.1088/1674-1056/ac4102

Coherence migration in high-dimensional bipartite systems

Zhi-Yong Ding(丁智勇), Pan-Feng Zhou(周攀峰), Xiao-Gang Fan(范小刚),Cheng-Cheng Liu(刘程程), Juan He(何娟), and Liu Ye(叶柳)
Chin. Phys. B, 2022, 31 (**6**): 060308. DOI: 10.1088/1674-1056/ac48f8

Probabilistic quantum teleportation of shared quantum secret

Hengji Li(李恒吉)[1,4], Jian Li(李剑)[2,3,†], and Xiubo Chen(陈秀波)[2]

[1] *School of Artificial Intelligence, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*
[2] *School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*
[3] *The Laboratory of Cryptography of Zhejiang Province, Hangzhou* 311121, *China*
[4] *Quantum Technology Laboratory and Applied Mechanics Group, University of Milan, Milan* 20133, *Italy*

(Received 17 January 2022; revised manuscript received 4 March 2022; accepted manuscript online 18 April 2022)

Very recently, Lee *et al.* proposed a secure quantum teleportation protocol to transfer shared quantum secret between multiple parties in a network [*Phys. Rev. Lett.* **124** 060501 (2020)]. This quantum network is encoded with a maximally entangled GHZ state. In this paper, we consider a partially entangled GHZ state as the entanglement channel, where it can achieve, probabilistically, unity fidelity transfer of the state. Two kinds of strategies are given. One arises when an auxiliary particle is introduced and a general evolution at any receiver's location is then adopted. The other one involves performing a single generalized Bell-state measurement at the location of any sender. This could allow the receivers to recover the transmitted state with a certain probability, in which only the local Pauli operators are performed, instead of introducing an auxiliary particle. In addition, the successful probability is provided, which is determined by the degree of entanglement of the partially multipartite entangled state. Moreover, the proposed protocol is robust against the bit and phase flip noise.

Keywords: probabilistic quantum teleportation, shared quantum secret, partially entangled GHZ state

PACS: 03.67.–a, 03.67.Hk, 03.65.Ud **DOI:** 10.1088/1674-1056/ac67c0

1. Introduction

Quantum teleportation[1] uses a pre-shared quantum channel to faithfully transfer an unknown quantum state between distant nodes within a network. Nowadays, it has played a pivotal role in various quantum information technologies such as measurement-based quantum computation,[2] quantum network[3,4] and a possible further quantum Internet.[5,6] Experimentally, the teleportation of arbitrary quantum states from a two-dimensional qubit[7] to a high-dimensional qudit[8] has been realized.

To realize versatile quantum networks, the incorporation of multiple participants needs to be further considered. Controlled teleportation has been proposed which can split quantum information from one sender to multiple receivers.[9–12] Teleportations of multiparty states have also been demonstrated and studied,[13,14] in which the multipartite entanglement state could be teleported. Besides quantum teleportation, controlled remote state preparation is presented,[15,16] where the goal can only be achieved with the control of the agents. A distributed quantum computation with the control of the controller[17] is proposed. Moreover, there are other typical quantum communication protocols that could facilitate the construction of versatile quantum networks.[18–25] Various kinds of quantum cryptography protocols, such as quantum key distribution,[18,19] quantum secure direct communication[20] and quantum secret sharing,[21,22] could generate a secure communication channel. In such a way, it is impossible in principle to eavesdrop without a high probability of disturbing the transmission, which will be detected. Considering a real situation, for obtaining deterministically maximally entangled pure states, quantum entanglement concentration and purification schemes are proposed,[23–25] which are very important elements for long-distance quantum communication.

Very recently, Lee *et al.* proposed a teleportation protocol of shared quantum secret states among multiple senders and receivers.[4] It can teleport quantum information shared by an arbitrary number of senders to another arbitrary number of receivers, where neither any single- nor subparties of senders and receivers can fully access the secret quantum information. This indicates that we can relay quantum information over a network in an efficient and distributed manner without requiring fully trusted central or intermediate nodes.[26] In Lee *et al.*'s scheme,[4] a multipartite maximally entangled GHZ state and n times of standard Bell-state measurements are required. It can perfectly achieve the teleportation with unit probability.

Due to the fragility of the entanglement[27] and the inevitable effects of environmental noise,[28,29] a maximally entangled state could be degraded into a partially entangled state. On the one hand, employing entanglement concentration,[30,31] one can probabilistically obtain a maximally entangled state, but, for this to occur, a large ensemble of partially entangled states is required. On the other hand, probabilistic teleportation was proposed via direct utilization of a partially entangled state in the network channel. In Ref. [32], the sender still makes a standard Bell-state measurement, however, on reconstruction of the original state, the receiver needs to introduce an auxiliary particle and then perform a two-

†Corresponding author. E-mail: lijian@bupt.edu.cn

© 2022 Chinese Physical Society and IOP Publishing Ltd

particle unitary transformation. Considering the fact that there is one to one correspondence between the joint measurement result and the final state, the proper measurement result might lead the receiver to recover the target state. For example, generalized Bell-state[33] and GHZ measurements[14] have been introduced to probabilistically transfer the state without an auxiliary particle.

In this manuscript, we consider the partially entangled GHZ state as the network channel to achieve the teleportation of shared quantum secret. It is shown that the shared quantum secret can reach its destination with unity fidelity. However, the price we pay to achieve unity fidelity is that the successful probability is less than 1. Two kinds of approaches are given, inspired by prior work.[32,33] The first one involves performing n times of standard Bell-state measurements, however at the end of the protocol, introduction of an auxiliary qubit and adoption of a general evolution[32] is required at any receiver's location. The second possibility involves performing a generalized Bell-state measurement[33] at only one sender's location. Moreover, the successful probability is given, which is determined by the degree of the entanglement of the channel.

The paper is structured as follows. Firstly, the original protocols is shown in Section 2, and then we present two new proposals of probabilistic teleportation of the shared quantum secret in Section 3. In Section 4, we discuss our two schemes and Section 5 contains our conclusions.

2. The original protocol

First of all, let us recall the original scheme.[4] It can teleport the shared quantum secret from the senders $\{\boldsymbol{s}_1, \boldsymbol{s}_2, \ldots, \boldsymbol{s}_n\}$, i.e., a group of n parties to the receivers $\{\boldsymbol{r}_1, \boldsymbol{r}_2, \ldots, \boldsymbol{r}_m\}$, i.e., another group of m parties, connected in the quantum network. Suppose that a quantum secret in $|\varphi\rangle = \alpha|0\rangle_L + \beta|1\rangle_L$ with logical basis, $\{|0\rangle_L, |1\rangle_L\}$, is shared by separated n parties in quantum network. The shared secret state to be teleported can be written as $|\varphi\rangle_s^n = \alpha \otimes_{i=1}^n |0\rangle_{s_i} + \beta \otimes_{i=1}^n |1\rangle_{s_i}$, and the shared secret state that is obtained at the receivers' hands could be reconstructed as $|\varphi\rangle_r^m = \alpha \otimes_{j=1}^m |0\rangle_{r_j} + \beta \otimes_{j=1}^m |1\rangle_{r_j}$. To achieve this goal, the network channel utilized is $(n+m)$-particle GHZ state $|\varepsilon\rangle_{n+m} = \frac{1}{\sqrt{2}}\left(\otimes_{i=1}^n |0\rangle_{s_i'} \otimes_{j=1}^m |0\rangle_{r_j} + \otimes_{i=1}^n |1\rangle_{s_i'} \otimes_{j=1}^m |1\rangle_{r_j}\right)$. The teleportation protocol between multiple parties in a quantum network is presented below.

Firstly, each sender $\boldsymbol{s}_i$ performs the standard Bell-state measurement ($\boldsymbol{B}$) on two particles, one from $|\varphi\rangle_s^n$ and the other from the network channel. The Bell states are denoted as

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right), \tag{1a}$$

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right). \tag{1b}$$

Then they communicate the outcomes to the receivers $\boldsymbol{r}_j$. Conditioned on the results, the state of the channel at the receivers' locations is $|\varphi\rangle_r^m$ plus logical Pauli operators. Lastly, the receivers can reconstruct the target state $|\varphi\rangle_r^m$ by carrying out the local Pauli operators, according to the results of all the senders. Figure 1 shows the protocol, while taking $|\varepsilon\rangle_{n+m}$ as the network channel and $\mathcal{M}_1 = \cdots = \mathcal{M}_n = \boldsymbol{B}$.

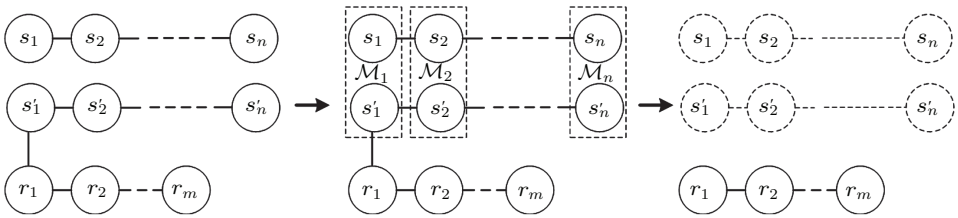


Fig. 1. The $(n+m)$-particle entangled state ($\{s_1', s_2', \ldots, s_n'\}$ and $\{r_1, r_2, \ldots, r_m\}$), as the network channel is utilized to teleport a quantum secret $|\varphi\rangle_s^n$ ($\{s_1, s_2, \ldots, s_n\}$) between n senders and m receivers. After performing n joint measurements (the dotted frame), denoted as $\mathcal{M}_i$, the receivers can reconstruct the shared secret.

3. Teleportation with a partial multipartite entanglement state

Instead of sharing a GHZ state, the senders and the receivers may initially share a non-maximally entangled state of the form

$$\begin{aligned}|\varepsilon'\rangle_{n+m} = P\big(&\otimes_{i=1}^n |0\rangle_{s_i'} \otimes_{j=1}^m |0\rangle_{r_j} \\ &+ p \otimes_{i=1}^n |1\rangle_{s_i'} \otimes_{j=1}^m |1\rangle_{r_j}\big),\end{aligned} \tag{2}$$

where $P = \frac{1}{\sqrt{|p|^2+1}}$ and $|p| \leq 1$. Next, two approaches are presented for the successful implementation of teleportation of a shared secret with unit fidelity, denoted respectively as protocols 1 and 2.

3.1. Teleportation based on n times of standard Bell state measurements

In this subsection, we present our simple scheme, where n times of $\boldsymbol{B}$s are still performed at every sender's location. Figure 1 shows the protocol, while taking $|\varepsilon'\rangle_{n+m}$ as the network channel and $\mathcal{M}_1 = \cdots = \mathcal{M}_n = \boldsymbol{B}$. It is shown here that the shared quantum secret can be recovered with unit fidelity, however, a proper generalized revolution is needed. First of all, write the initial composite system as

$$
\begin{aligned}
|\varphi\rangle_s^n|\varepsilon'\rangle_{n+m} =\ & P(\alpha\otimes_{i=1}^n|0\rangle_{s_i}+\beta\otimes_{i=1}^n|1\rangle_{s_i})\left(\otimes_{i=1}^n|0\rangle_{s_i'}\otimes_{j=1}^m|0\rangle_{r_j}+p\otimes_{i=1}^n|1\rangle_{s_i'}\otimes_{j=1}^m|1\rangle_{r_j}\right)\\
&\times\frac{\sqrt{2}}{2}P\Big[|\Phi_n^+\rangle_{s_1,\ldots,s_n,s_1',\ldots,s_n'}(\alpha\otimes_{j=1}^m|0\rangle_{r_j}+p\beta\otimes_{j=1}^m|1\rangle_{r_j})+|\Phi_n^-\rangle_{s_1,\ldots,s_n,s_1',\ldots,s_n'}(\alpha\otimes_{j=1}^m|0\rangle_{r_j}-p\beta\otimes_{j=1}^m|1\rangle_{r_j})\\
&+|\Psi_n^+\rangle_{s_1,\ldots,s_n,s_1',\ldots,s_n'}(p\alpha\otimes_{j=1}^m|1\rangle_{r_j}+\beta\otimes_{j=1}^m|0\rangle_{r_j})+|\Psi_n^-\rangle_{s_1,\ldots,s_n,s_1',\ldots,s_n'}(p\alpha\otimes_{j=1}^m|1\rangle_{r_j}-\beta\otimes_{j=1}^m|0\rangle_{r_j})\Big],
\end{aligned}
\tag{3}
$$

with

$$
\begin{aligned}
|\Phi_n^\pm\rangle_{s_1,\ldots,s_n,s_1',\ldots,s_n'} &= \frac{1}{\sqrt{2}}\left(\otimes_{i=1}^n|0\rangle_{s_i}\otimes_{i=1}^n|0\rangle_{s_i'}\pm\otimes_{i=1}^n|1\rangle_{s_i}\otimes_{i=1}^n|1\rangle_{s_i'}\right),\\
|\Psi_n^\pm\rangle_{s_1,\ldots,s_n,s_1',\ldots,s_n'} &= \frac{1}{\sqrt{2}}\left(\otimes_{i=1}^n|0\rangle_{s_i}\otimes_{i=1}^n|1\rangle_{s_i'}\pm\otimes_{i=1}^n|1\rangle_{s_i}\otimes_{i=1}^n|0\rangle_{s_i'}\right).
\end{aligned}
\tag{4a}
$$

Adjust the order of $2n$ particles from $(s_1,\ldots,s_n,s_1',\ldots,s_n')$ to $(s_1,s_1',s_2,s_2',\ldots,s_n,s_n')$ and we have (for brevity, the subscripts are omitted)

$$
\begin{aligned}
|\Phi_n^+\rangle &= \frac{1}{\sqrt{2^{n-1}}}\sum_{k=\text{even}\le n}N\big[|\phi^-\rangle^k|\phi^+\rangle^{n-k}\big],\\
|\Phi_n^-\rangle &= \frac{1}{\sqrt{2^{n-1}}}\sum_{k=\text{odd}\le n}N\big[|\phi^-\rangle^k|\phi^+\rangle^{n-k}\big],
\end{aligned}
\tag{5a}
$$

$$
\begin{aligned}
|\Psi_n^+\rangle &= \frac{1}{\sqrt{2^{n-1}}}\sum_{k=\text{even}\le n}N\big[|\psi^-\rangle^k|\psi^+\rangle^{n-k}\big],\\
|\Psi_n^-\rangle &= \frac{1}{\sqrt{2^{n-1}}}\sum_{k=\text{odd}\le n}N\big[|\psi^-\rangle^k|\psi^+\rangle^{n-k}\big],
\end{aligned}
\tag{5b}
$$

where $N[\cdot]$ represents the sum of all possible permutation, for instance,

$$
\begin{aligned}
&N\big[|\psi^-\rangle^{\otimes3}|\psi^+\rangle\big]\\
=\ &|\psi^+\rangle|\psi^-\rangle|\psi^-\rangle|\psi^-\rangle+|\psi^-\rangle|\psi^+\rangle|\psi^-\rangle|\psi^-\rangle\\
&+|\psi^-\rangle|\psi^-\rangle|\psi^+\rangle|\psi^-\rangle+|\psi^-\rangle|\psi^-\rangle|\psi^-\rangle|\psi^+\rangle.
\end{aligned}
$$

After performing n times of $\boldsymbol{B}$s, they inform the receivers of the results via the classical channels. Define the measurement result of the sender $\boldsymbol{s}_i$ as z_ix_i and let the classical bits $\{00,10,01,11\}$ correspond to $\{|\phi^+\rangle,|\phi^-\rangle,|\psi^+\rangle,|\psi^-\rangle\}$.

If the result is $|\Phi_n^+\rangle$ or $|\Phi_n^-\rangle$, at any receiver's location, he carries out the local Pauli operator $\sigma_z^Z(Z=(\sum_{i=1}^n z_i)\bmod 2)$, and the state will be

$$
|\varphi_1'\rangle_r^m=\frac{1}{\sqrt{|\alpha|^2+|p\beta|^2}}\left(\alpha\otimes_{j=1}^m|0\rangle_{r_j}+p\beta\otimes_{j=1}^m|1\rangle_{r_j}\right). \tag{6}
$$

For reconstructing the initial state with unity fidelity, an auxiliary qubit with the original state $|0\rangle_{\text{aux}}$ is required to be introduced. Due to the symmetry of $|\varphi_1'\rangle_r^m$, the auxiliary qubit can be held by any receiver $\boldsymbol{r}_j$. Without loss of generality, we can assume that the last receiver $\boldsymbol{r}_m$ holds the auxiliary qubit and then performs a collective unitary operator

$$
U_{|\Phi^\pm\rangle}=\begin{pmatrix}p & \sqrt{1-|p|^2} & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ \sqrt{1-|p|^2} & -p & 0 & 0\end{pmatrix}, \tag{7}
$$

under the basis $\{|0\rangle_{r_j}|0\rangle_{\text{aux}},|0\rangle_{r_j}|1\rangle_{\text{aux}},|1\rangle_{r_j}|0\rangle_{\text{aux}},|1\rangle_{r_j}|1\rangle_{\text{aux}}\}$. It will transform the product state $|\varphi_1'\rangle_r^m\otimes|0\rangle_{\text{aux}}$ to

$$
\begin{aligned}
|\varphi_1''\rangle_r^m =\ & \frac{1}{\sqrt{|\alpha|^2+|p\beta|^2}}\big[p|\varphi\rangle_r^m|0\rangle_{\text{aux}}\\
&+\alpha\sqrt{1-|p|^2}\otimes_{j=1}^m|1\rangle_{r_j}|1\rangle_{\text{aux}}\big].
\end{aligned}
\tag{8}
$$

Then he implements a Z-basis measurement on the auxiliary qubit which is a projective measurement on the basis $\{|0\rangle,|1\rangle\}$. If the result is $|0\rangle_{\text{aux}}$, the teleportation is successfully accessed with fidelity 1, while whenthe result is $|1\rangle_{\text{aux}}$, the teleportation fails with no information about the target state provided. The optimal successful probability is $|Pp|^2$, in which "optimal" means the introduction of an auxiliary qubit.

When the result is $\{|\Psi_n^+\rangle,|\Psi_n^-\rangle\}$, anyone of the receivers carries out the local Pauli operator $\sigma_x^X\sigma_z^Z(X=(\sum_{i=1}^n x_i)\bmod 2)$ and the other receivers respectively perform the operator σ_x^X, which will make the state owned by the receivers become

$$
|\varphi_2'\rangle_r^m=\frac{1}{\sqrt{|\alpha p|^2+|\beta|^2}}\left(\alpha p\otimes_{j=1}^m|0\rangle_{r_j}+\beta\otimes_{j=1}^m|1\rangle_{r_j}\right). \tag{9}
$$

Similarly, an auxiliary qubit with the original state $|0\rangle_{\text{aux}}$ is introduced at the location of the last receiver $\boldsymbol{r}_m$, and the corresponding collective unitary operator is

$$
U_{|\Psi^\pm\rangle}=\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & p & \sqrt{1-|p|^2}\\ 0 & 0 & \sqrt{1-|p|^2} & -p\end{pmatrix}, \tag{10}
$$

which will transform the product state $|\varphi_2'\rangle_r^m\otimes|0\rangle_{\text{aux}}$ to

$$
\begin{aligned}
|\varphi_2''\rangle_r^m =\ & \frac{1}{\sqrt{|\alpha p|^2+|\beta|^2}}\big[p|\varphi\rangle_r^m|0\rangle_{\text{aux}}\\
&+\beta\sqrt{1-|p|^2}\otimes_{j=1}^m|1\rangle_{r_j}|1\rangle_{\text{aux}}\big].
\end{aligned}
\tag{11}
$$

Next, he implements a Z-measurement on the auxiliary qubit. When the result is $|0\rangle_{\text{aux}}$, the target state can be recovered with the probability $|Pp|^2$. Adding up both the contributions, the optimal probability of successful teleportation is obtained as $Q_1=2|Pp|^2$.

3.2. Teleportation based on a single generalized Bell state measurement

In the subsection above, for teleporting the initial state with unity fidelity, an auxiliary qubit needs to be introduced and a two-particle collective transformation is then performed. Here, we show that it is possible for the receivers to recover the target state without the auxiliary qubit, though not with unit probability. To fulfill this, instead of performing n $\boldsymbol{B}$s, a single generalized Bell state measurement ($\boldsymbol{B}_{\rm G}$) is required. Firstly, define the generalized Bell basis[33]

$$|\phi_h^+\rangle = H\left(|00\rangle + h|11\rangle\right),\ \ |\phi_h^-\rangle = H\left(h^*|00\rangle - |11\rangle\right), \tag{12a}$$

$$|\psi_g^+\rangle = G\left(|01\rangle + g|10\rangle\right),\ \ |\psi_g^-\rangle = G\left(g^*|01\rangle - |10\rangle\right), \tag{12b}$$

where h and g are complex numbers, and $H = \frac{1}{\sqrt{|h|^2+1}}$, $G = \frac{1}{\sqrt{|g|^2+1}}$. We can invert the transformations (12a) and (12b), and it will yield

$$\begin{aligned} |00\rangle &= H\left(|\phi_h^+\rangle + h|\phi_h^-\rangle\right), \\ |11\rangle &= H\left(h^*|\phi_h^+\rangle - |\phi_h^-\rangle\right), \end{aligned} \tag{13a}$$

$$\begin{aligned} |01\rangle &= G\left(|\psi_g^+\rangle + g|\psi_g^-\rangle\right), \\ |11\rangle &= G\left(g^*|\psi_g^+\rangle - |\psi_g^-\rangle\right). \end{aligned} \tag{13b}$$

Adjust the order and rewrite the composite system as

$$\begin{aligned} |\varphi\rangle_s^n|\varepsilon'\rangle_{n+m} = P\Big[& |\phi_h^+\rangle_{s_1,s_1'}|\Phi_{n-1}^+\rangle_{s_2,s_2',\ldots,s_n,s_n'} H\left(\alpha\otimes_{j=1}^m|0\rangle_{r_j} + ph^*\beta\otimes_{j=1}^m|1\rangle_{r_j}\right) \\ & + |\phi_h^+\rangle_{s_1,s_1'}|\Phi_{n-1}^-\rangle_{s_2,s_2',\ldots,s_n,s_n'} H\left(\alpha\otimes_{j=1}^m|0\rangle_{r_j} - ph^*\beta\otimes_{j=1}^m|1\rangle_{r_j}\right) \\ & + |\phi_h^-\rangle_{s_1,s_1'}|\Phi_{n-1}^+\rangle_{s_2,s_2',\ldots,s_n,s_n'} H\left(h\alpha\otimes_{j=1}^m|0\rangle_{r_j} - p\beta\otimes_{j=1}^m|1\rangle_{r_j}\right) \\ & + |\phi_h^-\rangle_{s_1,s_1'}|\Phi_{n-1}^-\rangle_{s_2,s_2',\ldots,s_n,s_n'} H\left(h\alpha\otimes_{j=1}^m|0\rangle_{r_j} + p\beta\otimes_{j=1}^m|1\rangle_{r_j}\right) \\ & + |\psi_g^+\rangle_{s_1,s_1'}|\Psi_{n-1}^+\rangle_{s_2,s_2',\ldots,s_n,s_n'} G\left(p\alpha\otimes_{j=1}^m|1\rangle_{r_j} + g^*\beta\otimes_{j=1}^m|0\rangle_{r_j}\right) \\ & + |\psi_g^+\rangle_{s_1,s_1'}|\Psi_{n-1}^-\rangle_{s_2,s_2',\ldots,s_n,s_n'} G\left(p\alpha\otimes_{j=1}^m|1\rangle_{r_j} - g^*\beta\otimes_{j=1}^m|0\rangle_{r_j}\right) \\ & + |\psi_g^-\rangle_{s_1,s_1'}|\Psi_{n-1}^+\rangle_{s_2,s_2',\ldots,s_n,s_n'} G\left(pg\alpha\otimes_{j=1}^m|1\rangle_{r_j} - \beta\otimes_{j=1}^m|0\rangle_{r_j}\right) \\ & + |\psi_g^-\rangle_{s_1,s_1'}|\Psi_{n-1}^-\rangle_{s_2,s_2',\ldots,s_n,s_n'} G\left(pg\alpha\otimes_{j=1}^m|1\rangle_{r_j} + \beta\otimes_{j=1}^m|0\rangle_{r_j}\right)\Big], \end{aligned} \tag{14}$$

where $|\Phi_{n-1}^+\rangle$, $|\Phi_{n-1}^-\rangle$, $|\Psi_{n-1}^+\rangle$ and $|\Psi_{n-1}^-\rangle$ are defined by Eqs. (5a) and (5b). Here, the sender s_1 performs the $\boldsymbol{B}_{\rm G}$. Indeed, anyone of all the senders can implement the $\boldsymbol{B}_{\rm G}$, because of the symmetry of the initial state $|\varphi\rangle_s^n$ and the network channel $|\varepsilon'\rangle_{n+m}$, which will yield the same result. Without loss of generality, assume that the first sender is assigned to do this. Figure 1 shows the protocol, while taking $|\varepsilon'\rangle_{n+m}$ as the network channel and $\mathcal{M}_1 = \boldsymbol{B}_{\rm G}$, $\mathcal{M}_2 = \cdots = \mathcal{M}_n = \boldsymbol{B}$. It also indicates that the outcome is irrespective of the order of performed the joint measurements. There are four choices $p = \frac{1}{h^*} = g^*$, $p = \frac{1}{h^*} = \frac{1}{g}$, $p = h = g^*$ and $p = h = \frac{1}{g}$, which can achieve the teleportation with unity fidelity. Next, we take $p = \frac{1}{h^*} = g^*$ as an example to analyze it.

If the outcome is $|\phi_h^+\rangle|\Phi_{n-1}^\pm\rangle$, the state at the receivers' hands will be $\alpha\otimes_{j=1}^m|0\rangle_{r_j} \pm \beta\otimes_{j=1}^m|1\rangle_{r_j}$, and when the outcome is $|\psi_g^+\rangle|\Psi_{n-1}^\pm\rangle$, the state will be $\alpha\otimes_{j=1}^m|1\rangle_{r_j} \pm \beta\otimes_{j=1}^m|0\rangle_{r_j}$. In both of these two cases, one can recover the target state by performing the proper local Pauli operator. Correspondingly, the successful probability is $Q_2^{\rm s} = 2|P^2p|^2$, where $Q_2^{\rm s}$ means the successful probability without introducing an additional qubit.

If the outcomes are $|\phi_h^-\rangle|\Phi_{n-1}^\pm\rangle$ or $|\psi_g^-\rangle|\Psi_{n-1}^\pm\rangle$, the unnormalized state will be $\alpha|0\rangle \pm |p|^2\beta|1\rangle$ or $|p|^2\alpha|1\rangle \pm \beta|0\rangle$, respectively. Similar to protocol 1 in subsection 3.1, the receivers can obtain the target state by introducing the auxiliary state and the corresponding general evolution respectively is found by replacing p with $|p|^2$ in Eqs. (7) and (10). Consequently, the optimal successful probability is $Q_2^{\rm o} = 2|Pp|^4$, where $Q_2^{\rm o}$ represents the successful probability with introducing an additional qubit.

Thereby, the total successful probability is $Q_2 = Q_2^{\rm s} + Q_2^{\rm o} = 2|Pp|^2 = Q_1$. For the remaining three choices, it can be analyzed similarly and all of the four possible measurement results can achieve the reliable teleportation. Moreover, the successful probability is the same as the case given above.

4. Analysis

The access information in the probabilistic teleportation of shared secret state can be shown by the same methods presented in Ref. [4]. Any subparties can not fully access the quantum secret during the teleportation procedures. Note that n times of $\boldsymbol{B}$s are not necessary. Actually, only one Bell-state measurement is sufficient for implementing the protocol. Rewrite Eqs. (5a) and (5b) as (without normalized)

$$\begin{aligned} |\Phi_n^+\rangle = {} & |\phi^+\rangle \sum_{k=\text{even}\le n} N\left[|-\rangle^k|+\rangle^{2(n-1)-k}\right] + |\phi^-\rangle \\ & \times \sum_{k=\text{odd}\le n} N\left[|-\rangle^k|+\rangle^{2(n-1)-k}\right], \end{aligned} \tag{15a}$$

$$|\Phi_n^-\rangle = |\phi^+\rangle \sum_{k=\text{odd}\le n} N\left[|-\rangle^k|+\rangle^{2(n-1)-k}\right] + |\phi^-\rangle$$

$$\times \sum_{k=\text{even}\le n} N\left[|-\rangle^k|+\rangle^{2(n-1)-k}\right], \tag{15b}$$

$$|\Psi_n^+\rangle = |\psi^+\rangle \sum_{k=\text{even}\le n} N\left[|-\rangle^k|+\rangle^{2(n-1)-k}\right] + |\psi^-\rangle \times \sum_{k=\text{odd}\le n} N\left[|-\rangle^k|+\rangle^{2(n-1)-k}\right], \tag{15c}$$

$$|\Psi_n^-\rangle = |\psi^+\rangle \sum_{k=\text{odd}\le n} N\left[|-\rangle^k|+\rangle^{2(n-1)-k}\right] + |\psi^-\rangle \times \sum_{k=\text{even}\le n} N\left[|-\rangle^k|+\rangle^{2(n-1)-k}\right], \tag{15d}$$

implying that performing one $\boldsymbol{B}$ and $2(n-1)$ times of X-basis measurements is equivalent to n times of $\boldsymbol{B}$s, where the X-basis measurement is a projective measurement on the basis $\{|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}\}$. Because performing twice single-particle measurement is much more experimentally feasible than a two-particle joint measurement, it seems that we should choose the latter one, in which only one $\boldsymbol{B}$ is performed. However, only two of the Bell states $|\phi^-\rangle$ and $|\psi^-\rangle$, can be unambiguously identified, meaning the success probability of one $\boldsymbol{B}$ is limited to $1/2$.[34,35] Therefore, for Eqs. (5a) and (5b), while performing n $\boldsymbol{B}$s, it fails only when the result is $|\phi^+\rangle^{\otimes n}$ or $|\psi^+\rangle^{\otimes n}$. Consequently, the successful probability increases to $1-2^{-n}$, indicating that increasing n boosts the probability to successfully discriminate the logical Bell states.[36]

After performing $n_1 (1 \le n_1 \le n)$ times of $\boldsymbol{B}$s and $2(n-n_1)$ times of X-basis measurements, the shared secret could be tepeported with the probability $1-2^{-n_1}$, under the assumption that $|+\rangle$ and $|-\rangle$ can be perfectly discriminated. Therefore, the optimal probability of successful teleportation in protocol 1 is $Q_1(1-2^{-n_1})$. To achieve the teleportation with probability τ, it should meet the requirement $n_1 \ge \log_2^{\omega(\tau,p)}$ with $\omega(\tau,p) = \frac{2|Pp|^2}{2|Pp|^2-\tau}$. It can be analyzed similarly in protocol 2, where one $\boldsymbol{B}_\text{G}$ is necessary, with $n_2 (0 \le n_2 \le n)$ times of $\boldsymbol{B}$s and $2(n-1-n_2)$ X-basis measurements.

The successful probability in both two protocols is $2|Pp|^2$, depending on the entropy of the network channel $|\varepsilon'\rangle_{n+m}$. The corresponding von Neumann entropy is $E(p) = -P^2\log_2 P^2 - P^2|p|^2\log_2 P^2|p|^2$.[30] To explain it more clearly, we use another definition of the degree of entanglement, which of a bipartite pure quantum state can be represented by the concurrence defined by $C = \sqrt{2[1-\text{Tr}(w^2)]}$, where $\text{Tr}(w^2)$ is the purity of the associated reduced density matrix.[36,37] For a pure state of multiple subsystems, one can accordingly define the concurrence across every bipartition.[39] Therefore, for the channel $|\varepsilon'\rangle_{n+m}$, the concurrence is $c(p) = \frac{2|p|}{1+|p|^2}$, which is a monotonically increasing function of $|p|$. Then, we can rewrite the total successful probability as $Q_2 = Q_1 = |p|c(p)$, the successful probability without the introduction of an auxiliary qubit $Q_2^\text{s} = c^2(p)/2$, and the successful probability with the introduction of an auxiliary qubit $Q_2^\text{o} = |p|^2c^2(p)/2$.

Figure 2 shows the result intuitively. The total successful probability Q_2 increases from 0 to 1 with $|p|$ increasing. When $|p| = 1$, $|\varepsilon'\rangle_{n+m}$ becomes the maximally entangled state and correspondingly the maximum value is obtained. The range of values for both Q_2^s and Q_2^o are $[0,1/2)$ with $|p| \in [0,1)$. Note that when $|p| = 1$, $Q_2^\text{s} = 1$ whereas $Q_2^\text{o} = 0$. Because for the other four possible outcomes $|\phi_h^-\rangle|\Phi_{n-1}^\pm\rangle$ and $|\psi_g^-\rangle|\Psi_{n-1}^\pm\rangle$ in the formula (14), one can also recover the target state without the auxiliary qubit. Interestingly, Q_2^s is always bigger than Q_2^o and when $|p| \le 0.3$, $Q_2^\text{s} \approx Q_2$ with $Q_2^\text{o} \approx 0$.

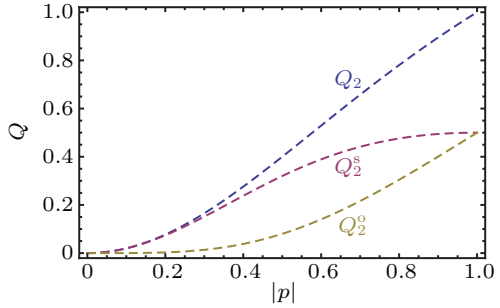


Fig. 2. The successful probability Q_2, Q_2^s and Q_2^o.

In general, decoherence and noise degrade the entanglement of the channel in a rather complicated way. For example, the initial two-qubit network channel might evolve into a mixed state (Werner state),[40] which is non unitary. A quantum state can not be teleported via the channel with unit fidelity, even if the successful probability is less than unit.[41] Here, we focus on the question whether the teleportation can be achieved with unit fidelity. Therefore, we consider the case that a maximally entangled pure channel still evolves to a pure partially entangled one. Note that for some kinds of unitary noises,[42] such as bit and phase flip noise, the degree of the entanglement of the channel remains unchanged. In this case, the receivers can easily overcome it by performing the proper local Pauli operations at the end of the protocol. For example, while a phase flip noise occurs at any sender's location in the network channel, any receiver could carry out an extra σ_z gate to retrieve the teleported state.

5. Conclusion

In summary, in this work, we describe two optimal methods for teleporting a shared quantum secret via a non-maximally multipartite GHZ state in a quantum network. The unit fidelity transfer of the initial state can be achieved with a calculable probability, which is determined by the degree of entanglement of the channel. For reconstructing the state, an auxiliary qubit is required to be introduced at anyone of the receivers in the first strategy. However, in the second approach, after any sender performs the generalized Bell-state measurement, the state can be recovered with a certain probability without the need for an auxiliary qubit. We will discuss

the case that the network channel degrades in a rather complicated way in our future work.

Acknowledgements

Project supported by the Open Fund of Advanced Cryptography and System Security Key Laboratory of Sichuan Province, China (Grant No. SKLACSS-202108), the Open Research Fund of Key Laboratory of Cryptography of Zhejiang Province, China (Grant No. ZCL21006), the National Natural Science Foundation of China (Grant Nos. U1636106, 92046001, 61671087, 61962009, and 61170272), the BUPT Excellent Ph.D. Students Foundation (Grant No. CX2020310), Natural Science Foundation of Beijing Municipality, China (Grant No. 4182006), and the Fundamental Research Funds for the Central Universities, China (Grant No. 2019XD-A02).

References

[1] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895
[2] Raussendorf R, Browne D E and Briegel H J 2003 *Phys. Rev. A* **68** 022312
[3] Pirandola S, Eisert J, Weedbrook C, Furusawa A and Braunstein S L 2015 *Nat. Photon.* **9** 641
[4] Lee S M, Lee S W, Jeong H and Park H S 2020 *Phys. Rev. Lett.* **124** 060501
[5] Kimble H J 2008 *Nature* **453** 1023
[6] Cacciapuoti A S, Caleffi M, Meter R V and Hanzo L 2020 *IEEE Transact. Commu.* **68** 3808
[7] Pfaff W, Hensen B J, Bernien H, Dam S B, Blok M S, Taminiau T H, Tiggelman M J, Schouten R N, Markham M, Twitchen D J and Hanson R 2014 *Science* **345** 532
[8] Luo Y H, Zhong H S, Erhard M, Wang X L, Peng L C, Krenn M, Jiang X, Li L, Liu N L, Lu C Y, Zeilinger A and Pan J W 2019 *Phys. Rev. Lett.* **123** 070505
[9] Karlsson A and Bourennane M 1998 *Phys. Rev. A* **58** 4394
[10] Cleve R, Gottesman D and Lo H K 1999 *Phys. Rev. Lett.* **83** 648
[11] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[12] Dou Z, Xu G, Chen X B, Liu X and Y Y X 2018 *Sci. China Inf. Sci.* **61** 022501
[13] Lee J Y and Kim M S 2000 *Phys. Rev. Lett.* **84** 4236
[14] Ghosh S, Kar G, Roy A, Sarkar D and Sen U 2002 *New J. Phys.* **4** 48
[15] Li Y H, He L M and Zhou P 2021 *Int. J. Theor. Phys.* **60** 1635
[16] Wang C, Zeng Z and Li X H 2015 *Quantum Information Proc.* **14** 1077
[17] Gong N F, Wang T J and Ghose S 2021 *Phys. Rev. A* **103** 052601
[18] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[19] Zhou C, Wang X Y, Zhang Z G, Yu S, Chen Z Y and Guo H 2021 *Sci. China Phys. Mech. Astron.* **64** 1
[20] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302
[21] Gao Z K, Li T and Li Z H 2020 *Sci. China Phys., Mech. Astron.* **63** 1
[22] Yang Y G, Wang Y C, Yang Y L, Chen X B, Li Dan, Zhou Y H and Shi W M 2021 *Sci. China Phys., Mech. Astron.* **64** 1
[23] Sheng Y B, Deng F G and Zhou H Y 2008 *Phys. Rev. A* **77** 042308
[24] Sheng Y B and Deng F G 2010 *Phys. Rev. A* **81** 032307
[25] Ren B C, Wang H, Alzahrani F, Hobiny A and Deng F G 2017 *Ann. Phys.* **385** 86
[26] Pant M, Krovi H, Towsley D, Tassiulas L, Jiang L, Basu P, Englund D and Guha S 2019 *npj Quantum Inf.* **5** 1
[27] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 *Rev. Modern Phys.* **81** 865
[28] Schlosshauer M 2019 *Phys. Rep.* **831** 1
[29] Lipinska V, Murta G and Wehner S 2018 *Phys. Rev. A* **98** 052320
[30] Bennett C H, Bernstein H J, Popescu S and Schumacher B 1996 *Phys. Rev. A* **53** 2046
[31] Bose S, Vedral V and Knight P L 1999 *Phys. Rev. A* **60** 194
[32] Li W L, Li C F and Guo G C 2000 *Phys. Rev. A* **61** 034301
[33] Agrawal P and Pati A K 2002 *Phys. Lett. A* **305** 12
[34] Lütkenhaus N, Calsamiglia J and Suominen K A 1999 *Phys. Rev. A* **59** 3295
[35] Calsamiglia J and Lütkenhaus N 2001 *Appl. Phys. B* **72** 67
[36] Lee S W, Park K, Ralph T C and Jeong H 2015 *Phys. Rev. Lett.* **114** 113603
[37] Wootters W K 1998 *Phys. Rev. Lett.* **80** 2245
[38] Rungta P, Bužek V, Caves C M, Hillery M and Milburn G J 2001 *Phys. Rev. A* **64** 042315
[39] Bandyopadhyay S and Sanders B C 2006 *Phys. Rev. A* **74** 032310
[40] Werner R F 1989 *Phys. Rev. A* **40** 4277
[41] Horodecki M, Horodecki P and Horodecki R 1999 *Phys. Rev. A* **60** 1888
[42] Shapira D, Mozes S and Biham O 2003 *Phys. Rev. A* **67** 042301