PHYSICAL REVIEW A **75**, 062323 (2007)

Combined and controlled remote implementations of partially unknown quantum operations of multiqubits using Greenberger-Horne-Zeilinger states

An Min Wang[*]

Quantum Theory Group, Department of Modern Physics, University of Science and Technology of China, Hefei, 230026, People's Republic of China

(Received 13 October 2006; published 19 June 2007)

We propose and prove protocols of combined and controlled remote implementations of partially unknown quantum operations belonging to the restricted sets [A. M. Wang, Phys. Rev. A **74**, 032317 (2006)] using Greenberger-Horne-Zeilinger (GHZ) states. We present the protocols in detail in the cases of one qubit, with two senders and with one controller, respectively. Then we study the variations of protocols with many senders, or with many controllers, or with both many senders and controllers using a multipartite GHZ state. Furthermore, we extend these protocols to the cases of multiqubits. Because our protocols have to request that the senders work together and transfer the information in turn or receive the repertoire of extra supercontrollers, or/and the controller(s) open the quantum channel and distribute the passwords in different ways, they definitely have the strong security in remote quantum information processing and communications. Moreover, the combined protocol with many senders is helpful to arrive at the power of remote implementations of quantum operations to the utmost extent in theory, since the different senders may have different operational resources and different operational rights in practice, and the controlled protocol with many controllers is able to enhance security and increase applications of remote implementations of quantum operations in engineering, since it has some common features in a controlled process.

DOI: 10.1103/PhysRevA.75.062323 PACS number(s): 03.67.Lx, 03.67.Hk, 03.65.Ud

I. INTRODUCTION

Quantum teleportation [1] is one of the most striking developments in quantum theory. It indicates that a quantum state can be remotely transferred in a completely different way compared with a classical state. Thus, one would like to know whether and how a quantum operation can also be remotely transferred in a completely different way compared with a classical operation. This problem is called the remote implementation of quantum operation (RIO), which was studied successfully by Huelga, Plenio, and Vaccaro (HPV) [2,3] for the case of one qubit. Recently, we proposed and proved a protocol of remote implementations of partially unknown quantum operations of multiqubits via deducing the general restricted sets of quantum operations and finding the unified recovery operations [4]. Specifically, our restricted sets of operations are not reducible to a direct product of two restricted sets of one-qubit operations, and our recovery operations have general and unified forms. Hence our protocol can be thought of as a development of the HPV protocol but not a simple extension of the HPV protocol to the cases of multiqubits systems. At the same time, we have considered its experimental implementation scheme in the cavity QED [5].

Remote implementation of a quantum operation means that this quantum operation performed on a local system (sender's) is teleported and then it acts on an unknown state belonging to a remote system (receiver's) [2–4]. Here, a sender is a person who transfers a quantum operation, and a receiver is a person whose system receives this quantum operation and this quantum operation acts on an unknown state belonging to his or her system. Obviously, the RIO is different from simple teleportation of quantum operation without action, and it is also not an implementation of nonlocal quantum operation [6,7], although there are closed connections among these tasks. Actually, all of them play important roles in distributed quantum computation [6,7], quantum program [8,9], and the other remote quantum information processing and communication tasks. At present, a series of works on the remote implementations of quantum operations have appeared and made some interesting progress both in theory [2–4,10] and in experiment [5,11–13].

Both HPVs and our recent protocols of RIOs use Bell states as a quantum channel. However, it is well known that Greenberger-Horne-Zeilinger (GHZ) states [14] are also a very important quantum resource in quantum information processing and communications (QIPC). Motivated by the scheme of teleportation of quantum states using a GHZ state [15–17] and the fact that it has been successfully applied to quantum secret sharing [18], we would like to investigate the remote implementations of quantum operations using GHZ state(s). Specifically, using the GHZ state(s) in our RIO protocols can enhance security, increase variety, extend applications, as well as advance efficiency via fetching in many senders and many controllers. Our results indicate that GHZ states are powerful and important resources in QIPC.

It is useful and interesting to investigate the remote implementations of partially unknown quantum operations because they consume less overall resources than the ones of the completely unknown quantum operations do, and such RIOs can satisfy the requirements of some practical applications. Here, the "partially unknown" quantum operations are thought of as those belonging to some restricted sets that satisfy some given restricted conditions. Note that the restricted sets of quantum operations are still very large sets of

[*] Electronic address: anmwang@ustc.edu.cn

(unitary) transformations because their unknown elements take continuous values, which had been seen in Refs. [2–4]. In the simplest case of one qubit, two kinds of restricted sets of quantum operations are, respectively, a set of diagonal operations and a set of off-diagonal operations [3]. For the case of multiqubits, the general forms of restricted sets of quantum operations were obtained by our recent work [4] and every row and every column of these operations have only one nonvanishing element.

It must be emphasized that the main feature of using GHZ states in the RIO protocols is to provide the ability for fetching in more than one sender or/and (many) controller(s). When there is more than one sender, we called this RIO protocol a combined one, when there is (are) the controller(s), we call this RIO protocol the controlled one, and when there are both many senders and controllers, we called this RIO protocol a combined-controlled one. A combined RIO protocol has to have the senders' cooperation, a controlled RIO protocol has to have the controllers' actions, and a combined-controlled RIO protocol has to have both senders' cooperation and controllers' action. Otherwise, the corresponding RIOs cannot be faithfully and determinedly completed.

In the combined RIO protocol, the later sender has to obtain the classical information from all former senders in the sending sequence of protocols so that the later sender can correctly choose his or her operation. Therefore the combined RIO protocol has a strong security mechanism. Note that the feature of this strong security mechanism is actualized in the classical sense, and it can be called "sequential multiple-safety." This concept can be understood and illustrated by a classical example of opening a safe-deposit box. For simplicity, let us only consider the case of sequential double-safety, whose example is how to open a safe-deposit box with two locks and every lock has a set of various keys. Suppose that the set of keys of the first lock is $k_1^A, k_1^B, \ldots$, and the set of keys of the second lock is $k_2^A, k_2^B, \ldots$. Opening the safe-deposit box requires one to use the sequential and paired keys (k_1^A, k_2^A), or $(k_1^B, k_2^B), \ldots$ to complete it. Otherwise the safe-deposit box cannot be opened. In other words, two guardians (corresponding to two senders) have to cooperate with each other via transferring information in turn. When the first guardian opens the first lock using some given key k_1^C (corresponding to a quantum operation belonging to some given restricted set), he or she has to tell the second guardian of his or her using key C so that the second guardian can correctly use k_2^C to open the safe-deposit box. Moreover, the combined RIO protocol can accept the arrangement of a single or several extra supercontrollers. The different senders receive different repertoire distributed by these supercontrollers, and the variations of repertoire will result in remote implementations of different operations in general. This implies that the final operation to be remotely implemented is determined by the supercontrollers, and then there exist more means to enhance security. If the receiver expects to gain an operation belonging to a given restricted set, he or she can play a supercontroller to distribute the repertoire that can determine this given restricted set to the senders. It is interesting that the combined RIO protocol with many senders is helpful to arrive at the power of RIOs to the utmost extent in theory. Actually, since it is possible that different senders have different operational resources and different operational rights in practice, their cooperations can combine more or more suitable and applicable operations, and thus the combined protocol with many senders has a higher practical power of RIOs than one with only one sender.

While in the controlled RIO protocol, not only does a controller play such a role that the quantum channel between sender and receiver is opened by his or her operations, but also the controller's measurement (classical information) affects the form of the sender's operations or the receiver's operations. This implies that the controller's action contains two aspects of "start up" and "authorization" so that the RIOs can be faithfully and determinedly completed. Based on this fact, we can say the controlled RIO protocol definitely enhances the security of remote quantum information processing and communications. Startup of the quantum channel in the controlled RIO protocol is easy to understand. However, from our point of view, the necessity of the authorization from controllers and the variations of its ways in the controlled RIO protocol, that is, why, how, and when to distribute the passwords (carry out authorization), by the controllers need to be carefully studied in order to faithfully and determinedly complete the protocol in the different cases and for the different purposes of RIOs. It will be seen that they are not trivial or simple, and they have practical significance and applications in engineering. For example, if the controller trusts in the sender or is easy to communicate with the sender, he or she authorizes the sender; if the controller trusts in the receiver or is easy to communicate with the receiver he or she authorizes the receiver; if the controller hopes to "say the last words," he or she authorizes the receiver at a chosen stage of the protocols. In addition, it should be pointed out that a controller has only a qubit here. When there are many controllers, they can form one or several controlled parties. Every controlled party is made of m controllers, and then the length of its distributing password will be to m c-bits.

As to the combined-controlled RIO protocol, it includes the above features and advantages of both the combined and controlled RIO protocols. However, it requires one to use the multipartite GHZ states. If we only use three partite GHZ states in our protocols, we have at most two senders or one controller in the one-qubit RIO. In fact, the number of the senders and/or the number of controllers depend(s) on the partite number of GHZ states. Hence when using more than three partite GHZ states, we can further extend our protocols to the cases of more than two senders and many controllers, even to the cases of many senders and many controllers together. In addition, in the cases of RIO of many qubit systems, the possible number of controllers depends on the number of GHZ states.

Because the no-cloning-broadcast theorem [19,20] forbids one to faithfully transfer an unknown, even partially (un)known quantum operation to more than one location at the same time, we give up to consider such a scheme with more than one receiver. However, alternatively, we can construct a symmetric scheme among three parties (locations), in which two partners play as two senders and the other partner plays as a receiver in the combined RIO protocol, or every partner plays a role among sender, receiver, and controller in the controlled RIO protocol.

Besides Sec. I written as an introduction, this paper is organized as follows: in Sec. II, we simply recall the RIO protocols using Bell states and introduce our restricted sets of quantum operation of multiqubits; in Sec. III we propose and prove a protocol of combined remote implementations of partially unknown quantum operations of one qubit using one GHZ state; in Sec. IV we propose and prove protocols of controlled remote implementations of partially unknown quantum operations of one qubit using one GHZ state; in Sec. V we study the variations of protocol when using multipartite GHZ states; in Sec. VI, by aid of the explicit forms of our restricted sets of quantum operations of N qubits [4] and the general swapping transformations, we extend our protocols to the cases of multiqubits; in Sec. VII, we summarize and discuss our results; in the appendixes, we analyze and study the general swapping transformations used in this paper and provide the proofs of our protocols in detail for the cases of more than one qubit.

II. RIO PROTOCOL USING BELL STATES

In the HPV protocol [2,3], the joint system of Alice and Bob initially reads

$$|\Psi^{\text{ini}}_{ABY}\rangle = |\Phi^+\rangle_{AB} \otimes |\xi\rangle_Y, \tag{1}$$

where

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) \tag{2}$$

is one of four Bell states which is shared by Alice (the first qubit) and Bob (the second qubit), and the unknown state (the third qubit)

$$|\xi\rangle_Y = y_0|0\rangle_Y + y_1|1\rangle_Y \tag{3}$$

belongs to Bob. Note that the Dirac's vectors with the subscripts A, B, and Y in the above three equations indicate their bases, respectively, belonging to the qubits A, B, and Y.

The quantum operation to be remotely implemented belongs to one of the two restricted sets defined by

$$U(0,u) = \begin{pmatrix} u_0 & 0 \\ 0 & u_1 \end{pmatrix}, \quad U(1,u) = \begin{pmatrix} 0 & u_0 \\ u_1 & 0 \end{pmatrix}. \tag{4}$$

We can say that they are partially unknown in the sense that the values of their matrix elements are unknown, but their structures, that is, the positions of their nonzero matrix elements, are known. In our notation, a restricted set of one-qubit operations is denoted by $U(d,u)$, where $d=0$ or 1 indicates, respectively, this operation belonging to a diagonal or off-diagonal restricted set, while u is its argument (made of unknown elements).

The simplified HPV protocol can be expressed by five steps [4], which are Bob's preparing, the classical communication from Bob to Alice, Alice's sending, the classical communication from Alice to Bob, and Bob's recovering. The whole protocol can be illustrated by the quantum circuit (see Fig. 1).

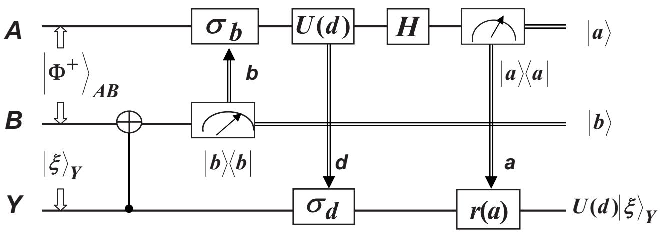

FIG. 1. Quantum circuit of the simplified HPV protocol, where $U(d)$ is a quantum operation to be remotely implemented and it is diagonal or off-diagonal, H is a Hadamard gate, σ_b, σ_d are identity matrices or NOT gates (σ_1) with respect to $b,d=0$ or $b,d=1$, respectively, and $r(a)=(1-a)\sigma_0+a\sigma_3$ is an identity matrix when $a=0$ or a phase gate (σ_3) when $a=1$. The measurements $|a\rangle\ \langle a|$ and $|b\rangle\ \langle b|$ are carried out in the computational basis ($a,b=0,1$). "⇒" (crewel with an arrow) indicates the transmission of classical communication to the location of the arrow direction.

In order to extend the RIO protocol to the cases of multiqubits, we first have to seek for the correct restricted sets of quantum operations of multiqubits that can be remotely implemented in a faithful and determined way. Actually, we have obtained their general and explicit forms in our recent works [4], that is, the restricted sets of quantum operations of N qubits have such forms that their every row and every column only has one nonzero element. Thus it is easy to know that there are $2^N!$ restricted sets of operations in the N-qubit systems. Denoting the xth restricted set by $T^r_N(x,t)$, and its nonzero element in the mth row by t_m, we have

$$T^r_N(x,t) = \sum_{m=1}^{2^N} t_m|m,D\rangle\langle p_m(x),D|. \tag{5}$$

Here, $x=1,2,\ldots,2^N$ and

$$p(x) = (p_1(x),p_2(x),\ldots,p_{2^N}(x)) \tag{6}$$

is an element belonging to the set of all permutations for the list $\{1,2,\ldots,2^N\}$. Moreover, when the requirement of the unitary condition is introduced, t_m will be taken as $e^{i\phi_m}$, and ϕ_m is real.

To remotely implement quantum operations belonging to the above restricted sets, the sender(s) needs a mapping table which provides one-to-one mapping from $T^r_N(x,t)$ to a classical information x ($x=1,2,\ldots,2^N!$), and the receiver knows a mapping table which gives out one-to-one mapping from a classical information x ($x=1,2,\ldots,2^N!$)to $R_N(x)$ with the following expression:

$$R_N(x) = T^r_N(x,0) = \sum_{m=1}^{2^N} |m,D\rangle\langle p_m(z),D|. \tag{7}$$

Obviously, it has the same structure as $T^r_N(x,t)$ to be remotely implemented, and it is an important part in the final recovery operation.

For simplicity, let us consider the case of two qubits. It is clear that there are 24 kinds of restricted sets of quantum operations that can be remotely implemented. In our RIO protocol, we use two Bell states $|\Phi^+\rangle_{A_1B_1}, |\Phi^+\rangle_{A_2B_2}$ as the quantum channel, where qubits A_1, A_2 belong to Alice and B_1, B_2 belong to Bob. Initially, an unknown state $|\xi\rangle_{Y_1Y_2}$ also belongs to Bob. Bob first performs two controlled-NOT (C^{NOT}) transformations by using Y_1, Y_2 as control qubits and B_1, B_2 as target qubits, respectively. Then he measures his qubits B_1 and B_2 in the computational basis $|b_1\rangle_{B_1}\langle b_1| \otimes |b_2\rangle_{B_2}\langle b_2|$, where $b_1, b_2 = 0, 1$ and sends the results to Alice. After receiving the two classical bits, Alice first carries out the quantum operations $\sigma_{b_1}^{A_1} \otimes \sigma_{b_2}^{A_2}$ on her two qubits A_1, A_2. Next Alice acts $T_2^r(x,t)$ on A_1A_2 and executes two Hadamard gate transformations $H_{A_1} \otimes H_{A_2}$. Then she measures her two qubits in the computational basis $|a_1\rangle_{A_1}\langle a_1| \otimes |a_2\rangle_{A_2}\langle a_2|$ ($a_1, a_2 = 0, 1$) and sends the results a_1a_2 and x to Bob. As we have mentioned, the transmission of x is to let Bob choose $R_2(x)$ correctly. With this information, Bob's recovery operations are taken as $[\mathfrak{r}^{Y_1}(a_1) \otimes \mathfrak{r}^{Y_2}(a_2)]\ R_2(x)$, where $\mathfrak{r}(y) = (1-y)\sigma_0 + y\sigma_3$. Finally, our protocol is completed faithfully and determinedly through the above five steps.

III. COMBINED RIO PROTOCOL IN THE CASE OF ONE QUBIT USING ONE GHZ STATE

As is well known, Bell state and GHZ state are both important quantum resources in QIPC. It is interesting whether a task of QIPC that can be carried out by using Bell states can also be done by using less GHZ states too. It will be seen that this is true for the combined RIO. Actually, this problem is related to the essential feature of utilizable entanglement existing within them.

A quantum operation of N-qubits is a product of two parts $\mathcal{U}_2$ and $\mathcal{U}_1$, that is, $\mathcal{U} = \mathcal{U}_2\mathcal{U}_1$. Assuming $\mathcal{U}_1$ and $\mathcal{U}_2$ both belong to the restricted sets, we can denote them by $T_N^r(x_1, v_1)$ and $T_N^r(x_2, v_2)$, respectively, in our notation. Thus the remote implementation of $\mathcal{U}$ can be completed via sending $\mathcal{U}_1$ and $\mathcal{U}_2$ in turn by one sender in the known protocols [3,4], but $2N$ shared Bell pairs are needed. However, we find that this task can be faithfully and determinedly completed by two senders via N GHZ states. Moreover, such a combined RIO protocol has a strong security mechanism. More analysis about the security mechanism has been given in the Introduction.

A. Some notations

Without loss of generality, for the RIO protocols of one qubit using a GHZ state, we can write the initial state in a symmetric form of three partite subsystems:

$$|\Psi^{\mathrm{ini}}\rangle = |\mathrm{GHZ}_+\rangle_{ABC}|\chi\rangle_X|\xi\rangle_Y|\zeta\rangle_Z, \tag{8}$$

where the GHZ state has the form

$$|\mathrm{GHZ}_+\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \tag{9}$$

and it is shared by Alice, Bob, and Charlie. While $|\chi\rangle_X$, $|\xi\rangle_Y$, and $|\zeta\rangle_Z$ are all unknown states of one qubit system. The six qubits of the joint system are divided into three pairs, in which the qubits A and X belong to Alice, the qubits B and Y belong to Bob, and the qubits C and Z belong to Charlie. Obviously, their roles are initially symmetric for RIO of one qubit.

In order to clearly express our protocol and strictly prove it, we denote that the Hilbert space of the joint system is initially taken as a direct product of all qubit Hilbert spaces according to the following sequence:

$$H = H_A \otimes H_B \otimes H_C \otimes H_X \otimes H_Y \otimes H_Z. \tag{10}$$

We can simply call this direct-product "space structure" and denote it by a bit-string, for example, the space structure of the above Hilbert space is $ABCXYZ$. Note that the above space structure is only a notation rule used here, it is absolutely not a precondition of the protocols. If we would like to prove our protocols generally for the cases of multiqubits, such a kind of notation rule is convenient, as is shown in Appendix A. Obviously, since taking such a space structure, the subspaces belonging to Alice, or Bob, or Charlie are separated. This will lead to inconvenience in the whole-space expression of local operations, especially for the cases of multiqubits. Hence there is the requirement to change the space structure, and the change can be realized by a series of swapping transformations, which is studied in Appendix A.

In our protocols, despite that only local operations and classical communication are used, the problems we deal with are related with the whole system because there is entanglement among various partite subsystems. Thus knowing the space structure will be helpful for us to understand the effect of local operations, especially for multiqubits systems. In fact, our protocol in the multiqubit cases can be found partially due to the reasons that we clearly express an appropriate space structure and general swapping transformations. Hence in the following we want to keep the above sequence of direct products of qubit spaces via the whole-space expressions of our formula in the joint system.

From the symmetric initial state (8), any two parties can play as two senders and the other party is one receiver. We are always able to swap their positions in a given space structure among three partite subsystems using so-called general swapping transformations that are defined in Appendix A. Without loss of generality, as soon as two senders are chosen, we can rewrite the initial state space structure as

$$H_{\mathrm{Sender1}} \otimes H_{\mathrm{Sender2}} \otimes H_{\mathrm{Receiver}} \otimes H_{\mathrm{Unknown\ State}}. \tag{11}$$

This means that the first and second qubits belong, respectively, to sender 1 and sender 2, the third qubit is mastered by the receiver, and the fourth qubit is an unknown state in the receiver's hands. Obviously, the unknown states belonging to two senders are needless in the combined RIO protocol as soon as the roles of attendees are fixed.

B. Protocol steps

Without loss of generality, we set Alice and Bob as two senders, Alice first sends $U(d_1, u)$ and Bob then sends $U(d_2, v)$, which are defined by Eq. (4). Charlie plays a receiver. The initial state can be rewritten as

$$|\Psi^{\mathrm{ini}}\rangle = |\mathrm{GHZ}_+\rangle_{ABC}|\zeta\rangle_Z, \tag{12}$$

and the receiver's (Charlie's) unknown state is denoted by

$$|\zeta\rangle = z_0|0\rangle_Z + z_1|1\rangle_Z. \tag{13}$$

Our combined protocol is made of the following seven steps.

Step one: Charlie's preparing. As a receiver, Charlie first performs a controlled-NOT using his qubit occupied by the unknown state (to be the acted state) as a control, his shared part (the third qubit in the above initial state) of the GHZ state as a target, and then measures his shared part of the GHZ state in the computational basis $|c\rangle\ \langle c|$ $(c=0,1)$, that is

$$\mathcal{P}_C(c) = I_4 \otimes \{[(|c\rangle_C\langle c|) \otimes \sigma_0^Z][\sigma_0^C \otimes C^{\mathrm{NOT}}(2,1)]\}, \tag{14}$$

where σ_0 is the 2×2 identity matrix, σ_i $(i=1,2,3)$ are the Pauli matrices, I_m is a m dimensional identity matrix, and C^{NOT} is a controlled-NOT defined by

$$C^{\mathrm{NOT}}(2,1) = \sigma_0 \otimes (|0\rangle\langle 0|) + \sigma_1 \otimes (|1\rangle\langle 1|) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \tag{15}$$

while (2, 1), as the variable of C^{NOT}, indicates that the second qubit is a control and the first qubit is a target.

The purpose of this step is to let the unknown state be correlated with all senders' local qubits. This is a precondition that all senders are able to remotely implement a quantum operation belonging to the restricted sets.

Step two: First classical communication. Charlie sends the classical information c to Alice and Bob. The aim of this step is that the receiver tells Alice and Bob that he is ready to receive the remote operation, as well as his prepared way.

It must be emphasized that for the cases of one qubit, the receiver's preparing has two equivalent ways with respect to $c=0$ or 1, respectively. If the receiver first fixes the value of c and tells all senders before the beginning of protocol, this step can be saved. In particular, when c is just taken as 0, the sender does not need the transformation σ_c in the next steps, since σ_0 is trivial.

Step three: Alice's sending. Alice's operation includes four parts. After receiving Charlie's classical bit c, Alice first performs a prior transformation σ_c dependent on c, second, carries out the quantum operation $U(d_1,u)$ to be remotely implemented on her qubit (the first qubit), third, executes a Hadamard transformation

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{16}$$

and finally measures her qubit in the computational basis $|a\rangle_A\langle a|$ $(a=0,1)$. All of Alice's local operations and measurement are just

$$\mathcal{S}_A(a,c;d_1,u) = \{(|a\rangle_A\langle a|)[H^A U(d_1,u)]\sigma_c^A\} \otimes I_8. \tag{17}$$

The action of the first part σ_c is to perfectly prepare the state of the joint system as such a superposition that the basis in the locally acted system (belonging to the sender's subsystem) of every component state is the same as its basis in the remotely operated system (belonging to the space of the unknown state in the receiver's subsystems) and the corresponding coefficients are ones of the unknown state. The second part of the sending step is an operation belonging to the restricted sets, which will be remotely implemented in the protocol. The third part of the sending step, the Hadamard gate, is often seen in quantum computation and quantum communication. Its action is similar to the cases in the teleportation of states. The fourth part of the sending step is a measurement on the computational basis whose aim is to project to the needed result.

Step four: Second classical communication. Alice sends the classical information d_1 to Bob and a,d_1 to Charlie.

The communication to Bob is that the first sender tells the second sender which kind of operations (denoted by d_1) has been transferred so that Bob can correctly chose his second sending operation. The communication to Charlie is that the first sender tells the receiver what measurement (denoted by a) has been done and which kind of operations (denoted by d_1) has been transferred. In the protocol, the sender has a one-to-one mapping table to indicate a kind of restricted set by a value of classical information. For the case of one qubit, it can be encoded by one c-bit, in which 0 denotes a restricted set of diagonal operations and 1 denotes a restricted set of off-diagonal operations. This communication is necessary in order to faithfully and determinedly finish the protocol.

Step five: Bob's sending. After receiving Alice's classical bit d_1, Bob first joins Charlie's classical bit c (replacing Charlie's transfer, this classical bit also can be sent by Alice), and performs a prior transformation $\sigma_{d_1}\sigma_c$, and then carries out the quantum operation $U(d_2,v)$ to be remotely implemented on his qubit (the second qubit). Finally, Bob executes a Hadamard transformation and measures his qubit in the computational basis $|b\rangle_A\langle b|$ $(b=0,1)$. All of Bob's local operations and measurement are expressed as

$$\mathcal{S}_B(b,c;d_1,d_2,v) = \sigma_0 \otimes \{(|b\rangle_B\langle b|)[H^B U(d_2,v)](\sigma_{d_1}^B\sigma_c^B)\} \otimes I_4. \tag{18}$$

Step six: Third classical communication. Bob sends the classical information b and d_2 to Charlie. The aim of this communication is to let Charlie know what measurement (denoted by b) has been done and which kinds of operations (denoted by d_2) are transferred by Bob, and then correctly build his recovery operations.

Step seven: Charlie's recovering. Based on four classical bits a,d_1 and b,d_2, respectively, from two senders Alice and Bob, Charlie first is required to do a recovery operation that consists of two parts. The first part is $\mathfrak{r}(a)\sigma_{d_1}$, where $\mathfrak{r}(a)$ is a diagonal phase gate with a parameter that is defined by

$$\mathfrak{r}(z) = (1-z)\sigma_0 + z\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1-2z \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & (-1)^z \end{pmatrix}. \tag{19}$$

Note that $z=0,1$, and then $(-1)^z=1-2z$. The two factors of the first part correspond, respectively, to a fixed form of a restricted set which has the same structure and the phase transformation in order to fix the phase. The second part is $\mathfrak{r}(b)\sigma_{d_2}$ so that the second part of the operation is recovered.

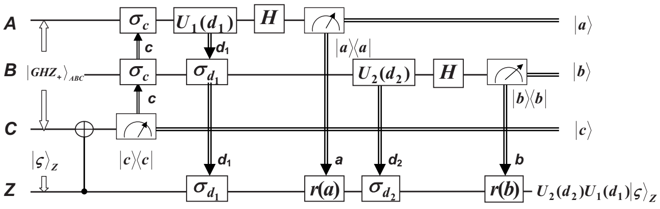

FIG. 2. Quantum circuit of the combined remote implementation of quantum operation with two senders Alice and Bob. Here, $U_1(d_1)$ and $U_2(d_2)$ are, respectively, a part of the quantum operation $U(d_1,d_2)=U_2(d_2)U_1(d_1)$ that is remotely implemented by combining Alice and Bob's actions, H is a Hadamard transformation, $\sigma_c,\sigma_{d_1},\sigma_{d_2}$ are identity matrices or NOT gates (σ_1) for $c,d_1,d_2=0$ or $c,d_1,d_2=1$, respectively, and $r(x)=(1-x)\sigma_0+x\sigma_3$ is an identity matrix if $x=0$ or a phase gate (σ_3) if $x=1$. The measurements $|a\rangle\langle a|$, $|b\rangle\langle b|$, and $|c\rangle\langle c|$ are carried out in the computational basis ($a,b,c=0,1$). "⇒" (crewel with an arrow) indicates the transmission of classical communication to the location of the arrow direction.

Note that for the cases of one qubit, the fixed forms of the restricted sets of diagonal and off-diagonal operations are, respectively, σ_0 and σ_1. Thus we obtain

$$\mathcal{R}_C(a,b;d_1,d_2)=I_4\otimes(\sigma_0^C\otimes\{[\mathfrak{r}(b)\sigma_{d_2}][\mathfrak{r}(a)\sigma_{d_1}]\}). \tag{20}$$

All of the operations and measurements in our above protocol can be jointly written as

$$\begin{aligned}\mathcal{I}_R&(a,b,c;d_1,d_2,u,v)\\&=[|a\rangle_A\langle a|H^AU(d_1,u)\sigma_c^A]\otimes[|b\rangle_B\langle b|H^BU(d_2,v)\sigma_{d_1}\sigma_c^A]\\&\quad\otimes\{[|c\rangle\langle c|\otimes\mathfrak{r}(b)\sigma_{d_2}\mathfrak{r}(a)\sigma_{d_1}]C^{\text{NOT}}(2,1)\}.\end{aligned}\tag{21}$$

Its acting on the initial state gives

$$\begin{aligned}|\Psi_C^{\text{final}}&(a,b,c;d_1,d_2,u,v)\rangle\\&=\mathcal{I}_R(a,b,c;d_1,d_2,u,v)|\Psi_C^{\text{ini}}\rangle\\&=\frac{1}{2\sqrt{2}}|abc\rangle_{ABC}\otimes U(d_2,v)U(d_1,u)|\zeta\rangle_Z,\end{aligned}\tag{22}$$

where $a,b,c=0,1$ denote the spin up or down, and $d_1,d_2=0$ and $d_1,d_2=1$, respectively, indicate the operations of diagonal and off-diagonal restricted sets. Therefore the remote implementations of the combination of two quantum operations belonging to restricted sets are faithfully and determinedly completed. It can be called the combined remote implementation of quantum operations which can be displayed by Fig. 2.

C. Protocol proof

Charlie's preparation gives

$$|\Psi^P(c)\rangle=\mathcal{P}_C(c)|\Psi_{ABCZ}^{\text{ini}}\rangle=\frac{1}{\sqrt{2}}(\sigma_c\otimes\sigma_c\otimes I_4)\sum_{k=0}^{1}z_k|kkck\rangle_{ABCY},\tag{23}$$

with the relation

$$\begin{aligned}\{I_4&\otimes[(|c\rangle c\otimes\sigma_0)C^{\text{NOT}}(2,1)]\}|\text{GHZ}_+\rangle|k\rangle\\&=\frac{1}{\sqrt{2}}(\sigma_c\otimes\sigma_c\otimes I_4)|kkck\rangle.\end{aligned}\tag{24}$$

Its proof needs to use $\sigma_c|c\rangle=|0\rangle$ and $\sigma_c|1-c\rangle=|1\rangle$ for $c=0,1$ [4]. After receiving the classical information c from Charlie (receiver), Alice supplements a σ_c transformation, and then performs the first sending operations, we have

$$\begin{aligned}|\Psi_1^S(a,c;d_1,u)\rangle&=\mathcal{S}_A(a,c,d_1,u)|\Psi^P(c)\rangle\\&=\frac{1}{\sqrt{2}}\sum_{k=0}^{1}z_k[|a\rangle_A\langle a|HU(d_1,u)|k\rangle](\sigma_c|k\rangle_B)|ck\rangle_{CY}.\end{aligned}\tag{25}$$

Alice then tells Bob d_1 and Charlie a,d_1. In succession, based on the classical information c (coming from Charlie) and d_1 (coming from Alice), Bob first carries out $\sigma_{d_1}\sigma_c$, and then performs the second sending operations:

$$\begin{aligned}|\Psi_2^S&(a,b,c;d_1,d_2,u,v)\rangle\\&=\mathcal{S}_B(b,c,d_2,v)|\Psi_1^S(a,c,d_1,u)\rangle\\&=\frac{1}{\sqrt{2}}\sum_{k=0}^{1}z_k[\langle a|HU(d_1,u)|k\rangle_A\langle b|HU(d_2,v)\sigma_{d_1}|k\rangle_B]\\&\quad\times|abck\rangle_{ABCY}.\end{aligned}\tag{26}$$

Finally, Bob's recovery operation gives

$$\begin{aligned}|\Psi^{\text{final}}&(a,b,c;d_1,d_2,u,v)\rangle\\&=\mathcal{R}_B(a,b,d_1,d_2)|\Psi_2^S(a,b,c,d_1,d_2,u,v)\rangle\\&=\frac{1}{\sqrt{2}}\sum_{k=0}^{1}z_k[\langle a|HU(d_1,u)|k\rangle\langle b|HU(d_2,v)\sigma_{d_1}|k\rangle]\\&\quad\times|abc\rangle_{ABC}[\mathfrak{r}(b)\sigma_{d_2}\mathfrak{r}(a)\sigma_{d_1}|k\rangle_Z].\end{aligned}\tag{27}$$

Based on the forms of the restricted set of one qubit and the phase transformation $\mathfrak{r}(a)$, we rewrite them as

$$U(d_1,u)=U(0,u)\sigma_{d_1}=\sum_{j=0}^{1}u_j|j\rangle\langle j|\sigma_{d_1},\tag{28}$$

$$\mathfrak{r}(a)=\sum_{l=0}^{1}(-1)^{al}|l\rangle\langle l|,\tag{29}$$

and substitute them into the above expression of $|\Psi^{\text{final}}\rangle$. The result is

$$\begin{aligned}|\Psi^{\text{final}}&(a,b,c;d_1,d_2,u,v)\rangle\\&=\frac{1}{\sqrt{2}}\sum_{j=0}^{1}\sum_{k=0}^{1}\sum_{l=0}^{1}u_jy_k[\langle a|H|j\rangle\langle j|\sigma_{d_1}|k\rangle\langle b|HU(d_2,v)\sigma_{d_1}|k\rangle]\\&\quad\times|abc\rangle_{ABC}[\mathfrak{r}(b)\sigma_{d_2}(-1)^{al}|l\rangle_Y\langle l|\sigma_{d_1}|k\rangle].\end{aligned}\tag{30}$$

Because

$$\langle j|\sigma_d|k\rangle\langle l|\sigma_d|k\rangle=\langle j|\sigma_d|k\rangle\delta_{jl},\tag{31}$$

$$\langle a|H|j\rangle(-1)^{aj}=1/\sqrt{2}, \tag{32}$$

it further becomes

$$\begin{aligned}|\Psi^{\mathrm{final}}(a,b,c;d_1,d_2,u,v)\rangle &= \frac{1}{2}|abc\rangle_{AB}\left[\sum_{j=0}^{1}\sum_{k=0}^{1}u_j y_k[\langle b|HU(d_2,v)\sigma_{d_1}|k\rangle]\langle j|\sigma_{d_1}|k\rangle\right]\\ &\quad\times\mathfrak{r}(b)\sigma_{d_2}|j\rangle_Y.\end{aligned} \tag{33}$$

Again inserting the complete relation after $U(d_2)$ and using the above same skills, that is $U(d_2)=U(0,v)\sigma_{d_2}=\Sigma_{i=0}^{1}v_i|i\rangle\langle i|\sigma_{d_2}$ and $\mathfrak{r}(b)=\Sigma_{l=0}^{1}(-1)^{bl}|l\rangle\langle l|$, we obtain

$$\begin{aligned}|\Psi^{\mathrm{final}}(a,b,c;d_1,d_2,u,v)\rangle &= \frac{1}{2\sqrt{2}}|abc\rangle_{ABC}\left[\sum_{i=0}^{1}\sum_{j=0}^{1}\sum_{k=0}^{1}v_i u_j y_k\langle i|\sigma_{d_2}|j\rangle\langle j|\sigma_{d_1}|k\rangle\right]|i\rangle_Y\\ &= \frac{1}{2\sqrt{2}}|abc\rangle_{ABC}[U(d_2,v)U(d_1,u)|\xi\rangle_Y].\end{aligned} \tag{34}$$

The proof of our protocol with two senders using one GHZ state is finished.

IV. CONTROLLED RIO PROTOCOL IN CASES OF ONE QUBIT USING ONE GHZ STATE

Now, let us investigate the controlled remote implementations of quantum operations belonging to restricted sets of one qubit using one three-partite GHZ state. When a task in QIPC is done by the given number of the Bell states, more things can be done by the same number of the GHZ states because the utilizable entanglement within the GHZ state is more than one within the Bell state from our point of view. It will be seen that the controlled RIO protocol, as a good example in this aspect, obviously increases the variety of RIO and enhances the security of RIO. The controller's actions in the controlled RIO protocol include two aspects of startup and authorization. Since startup of the quantum channel is easy to understand, we will stress, here, the necessity of authorization and the variations of its ways, that is, why, how, and when to distribute the passwords, by the controller. It will be seen that these problems are not trivial and are worthy of studying due to their practical significance and applications in engineering. Concrete analysis is mentioned in the Introduction.

From the initial state Eq. (8), it is easy to find that any one partite subsystem of them plays a possible role among a sender, a receiver, and a controller in the protocol. In other words, when a controller is fixed to a given partite subsystem, the other two partite subsystems play as a sender and a receiver, respectively. In terms of general swapping transformation, as soon as a controller is chosen or dominated, we can rewrite the initial state space structure as

$$H_{\mathrm{Controller}}\otimes H_{\mathrm{Sender}}\otimes H_{\mathrm{Receiver}}\otimes H_{\mathrm{Unknown\ State}}. \tag{35}$$

This means that the first qubit belongs to the controller, the second qubit is in the sender's partite subsystem (the local subsystem), the third qubit is mastered by the receiver, and the fourth qubit is an unknown state in the receiver's hands. Obviously, the unknown states belonging to sender and controller are needless in the protocol as soon as the roles of attendees are fixed.

A. Protocol steps

When we introduce a controller, the protocol of controlled remote implementations of quantum operations belonging to the restricted sets is made up of seven steps, of which there are four steps of quantum operations including measurement and three of classical communications. Since the significance and actions of the most related operations have been explained in Sec. III, we do not intend to repeat them here. However, we still would like to emphasize the significance of the controller's role and the variations of the protocol.

Controlling step. This step is carried out by the controller:

$$\mathcal{C}(\gamma)=(|\gamma\rangle\langle\gamma|H)\otimes I_8, \tag{36}$$

This step is a key matter in the controlled RIO protocol. In fact, when the controller has not done it, there is no quantum entanglement between any two partite subsystems, so there are no feasible remote implementations of quantum operations. Only if a controller agrees or wishes that the other two partite subsystems implement the RIO protocol does he or she carry out this operation and measurement. Its action is to open the quantum channel between the sender and receiver that is necessary for the remote implementation of quantum operations belonging to the restricted sets.

Allowing step. This step still has to be completed by the controller, that is, he or she transfers one c-bit γ to the sender or the receiver, which is denoted by $C_{\mathrm{cs}}(\gamma)$ or $C_{\mathrm{cr}}(\gamma)$, respectively.

This allowing step as well as the above controlling step can be arranged at any time in the RIO process corresponding to the different requirements, however, the different arrangement will result in influences on the steps of this protocol. If the classical bit γ is arranged to transfer to the sender, this communication has to be done before the other parts of the sending operations. If the classical bit γ is chosen to transfer to the receiver, this communication is able to be done at the beginning (before the receiver's preparation), or in the middle (before the recovered operations), or at the end (after the standard recovered operations). In these cases, although the receiver can have the different choices to finish this protocol, we prefer to use a unified method for the one-qubit RIO, that is, we use the classical information γ before the end of the protocol.

This step can be understood figuratively as that the controller distributes the "password" γ to one of sender and receiver, or gives an authorization to one of them, or says the last word (to the receiver) in the protocol. This indicates that the role of the controller is very important and indispensable. In other words, this is not trivial in engineering because the above means are useful in the controlled process and imply potential applications in practice. Without the password distribution by the controller, the sender and receiver cannot faithfully and determinedly complete the RIO. This can be clearly seen in the following proof about this protocol.

Preparing step. This step is carried out by the receiver. There are two kinds of cases, respectively, based on whether the classical information from the controller is obtained by the receiver or not.

(a) Case one. The receiver does not obtain the classical information from the controller, his or her preparing is

$$\mathcal{P}(\beta) = I_4 \otimes [(|\beta\rangle\langle\beta|) \otimes \sigma_0]C^{\text{NOT}}(2,1). \qquad (37)$$

(b) Case two. The controlling step has happened and the receiver gets the classical bit γ from the controller, the preparing step has three different forms according to the time to obtain the classical bit γ in general.

(1) When the classical bit γ is known at the beginning of this step, the receiver has to add a prior operation,

$$\mathcal{P}^{\text{pre}}(\gamma) = I_4 \otimes \mathfrak{r}(\gamma) \otimes \sigma_0, \qquad (38)$$

before the above operation (37). Of course, since it commutes with the project measurement, it also can be inserted between the measurement and the controlled-NOT in the operation (37).

(2) When the classical bit γ is known after the operation (37) or before the next recovery operation, the receiver performs a supplementary operation

$$\mathcal{P}^{\text{aft}}(\gamma) = I_4 \otimes \mathfrak{r}(\gamma) \otimes \mathfrak{r}(\gamma), \qquad (39)$$

where we have used the fact that

$$[\mathfrak{r}(\gamma) \otimes \mathfrak{r}(\gamma)][(|\beta\rangle\langle\beta| \otimes \sigma_0)C^{\text{NOT}}(2,1)] \\ = [(|\beta\rangle\langle\beta| \otimes \sigma_0)C^{\text{NOT}}(2,1)][\mathfrak{r}(\gamma) \otimes \sigma_0]. \qquad (40)$$

(3) When the classical bit γ is known after the next recovery operation, this case is discussed in the following recovery step. It is clear that for the above two cases, the receiver always can delay using the classical information up to after the recovery operation. Therefore this case is more general. However, it will be seen that the delaying method is able to lead to the unexpected complication in the recovery step for the cases of multiqubits.

Classical communication from receiver to the sender. This step is that the receiver transfers a c-bit $\boldsymbol{\beta}$ to the sender, which is denoted by $C_{\text{rs}}(\beta)$.

Sending step. This step is carried out by the sender. There are two cases.

(1) Case one. There is no classical information transferred from the controller to the sender. Thus Alice's sending can be jointly written as

$$\mathcal{S}(\alpha,\beta;d,u) = \{\sigma_0 \otimes (|\alpha\rangle\langle\alpha|)[HU(d,u)\sigma_\beta] \otimes I_4\}. \qquad (41)$$

(2) Case two. The sender obtains the classical information γ from the controller, he or she has to add to a prior operation

$$\mathcal{S}^{\text{add}}(\gamma) = \sigma_0 \otimes \mathfrak{r}(\gamma) \otimes I_4 \qquad (42)$$

at the beginning of this step. This means that the sending step becomes

$$\mathcal{S}^{\text{all}}(\alpha,\beta,\gamma;d,u) = \mathcal{S}(\alpha,\beta;d,u)\mathcal{S}_A^{\text{add}}(\gamma). \qquad (43)$$

Classical communication from sender to receiver. This step is that the sender transfers the classical information α and d to the receiver, which is denoted by $C_{\text{sr}}(\alpha;d)$.

Recovery step. This step is carried out by the receiver. Therefore the receiver's recovery operations are written as

$$\mathcal{R}(\alpha;d) = I_8 \otimes [\mathfrak{r}(\alpha)\sigma_d], \qquad (44)$$

where $d=0$ or 1.

It must be emphasized that the above $\mathcal{R}(\alpha;d)$ can only guarantee that the operation $U(d,u)$ is faithfully and determinedly transferred, if the protocol sets that the controller transfers his or her classical bit γ before its action. Just as the statement above, if γ is transferred to the sender, the sender has a prior preparation part; when γ is sent to the receiver before his or her preparing step, he or she can add a supplementary part at the beginning, in the middle, or at the end of the preparing step. Obviously, the end of the preparing is just before the recovering, and so we can move this supplementary part here. However, if the receiver obtains γ from the controller after the above $\mathcal{R}(\alpha;d)$ action, the receiver has to perform an additional recovery part

$$\mathcal{R}^{\text{aft}}(\gamma;d) = (-1)^{\gamma d} I_4 \otimes \mathfrak{r}(\gamma) \otimes \mathfrak{r}(\gamma), \qquad (45)$$

where $\mathfrak{r}(z)$ is defined in Eq. (19). Note that $\mathfrak{r}(\gamma)|\beta\rangle\langle\beta| = (-1)^{\gamma\beta}|\beta\rangle\langle\beta|$, we obtain its other form,

$$\mathcal{R}^{\text{aft}}(\beta,\gamma;d) = (-1)^{\gamma(d+\beta)} I_8 \otimes \mathfrak{r}(\gamma). \qquad (46)$$

It is clear that when the protocol sets that the controller transfers his or her classical bit γ to the receiver, we always can delay using the classical information γ. In other words, in order to standardize the protocol in the cases of one qubit, we do not add any $\mathcal{P}^{\text{pre}}$ and $\mathcal{P}^{\text{aft}}$ in the preparing step, but we always use the above $\mathcal{R}^{\text{aft}}$ at the end of the protocol. Thus the whole recovery operations are

$$\mathcal{R}^{\text{all}}(\alpha,\gamma,d) = \mathcal{R}^{\text{aft}}(\gamma;d)\mathcal{R}(\alpha;d). \qquad (47)$$

However, for the case of multiqubits, it is not so simple. Generally, we put the additional recovery operations before the standard recovery operations (44), even before the preparing step in order to have the simplest additional operations for the cases of multiqubits. Of course, if we persist in putting the additional recovery operation last, we will pay the price that it gets a little complicated to express.

In summary, when there is a controller, we have proposed four kinds of protocols for controlled remote implementation of operations belonging to the restricted sets. (1) The sender obtains the password; (2)–(4) the receiver obtains the password, respectively, before the preparing, after the preparing (before the recovering), and after the recovering. The second, third, and fourth kinds of our protocols can be unitedly expressed without obvious difficulty in the case of one qubit. If the controller transfers his classical bit γ to the sender, the sequence of the above steps in our protocol will become

$$\mathcal{C}(\gamma) \to C_{\text{cs}}(\gamma) \to \mathcal{P}(\beta) \to C_{\text{rs}}(\beta) \to \mathcal{S}^{\text{all}}(\alpha,\beta,\gamma;d) \\ \to C_{\text{sr}}(\alpha;d) \to \mathcal{R}(\alpha;d), \qquad (48)$$

if the controller transfers his classical bit γ to the receiver, the sequence of the above steps in our protocol is

$$\mathcal{C}(\gamma) \rightarrow C_{\mathrm{cr}}(\gamma) \rightarrow \mathcal{P}(\beta) \rightarrow C_{\mathrm{rs}}(\beta) \rightarrow \mathcal{S}(\alpha,\beta;d) \rightarrow C_{\mathrm{sr}}(\alpha;d) \rightarrow \mathcal{R}^{\mathrm{all}}(\alpha,\gamma;d). \tag{49}$$

It is clear that transferring γ to the sender or the receiver can be figuratively understood as distributing a "password," especially while transferring γ to the receiver at the end of protocol, it can be figuratively understood as "saying the last word." They are both important controlled means. Besides the password distributing, the controller owns the right to open the quantum channel. All of these are some main features of a controlled process. Therefore we called the above process a controlled remote implementations of operations.

Now, as an example, we fix the controller as Charlie, Alice as a sender, and Bob as a receiver without loss of generality. Thus the initial state is simplified as

$$|\Psi^{\mathrm{ini}}_{ABCY}\rangle = F_4^{-1}(1,3)[|\mathrm{GHZ}_+\rangle_{CAB}|\xi\rangle_Y], \tag{50}$$

where $F_4(1,3)$ is a forward rearrangement made of two swapping transformations between the neighbor qubits, and it is defined in Appendix A. Similarly, we can discuss the other choices of the controller, sender, and receiver, but we do not intend to discuss them here.

If we set that Charlie (the controller) transfers the password to the sender, it is the first of our protocols. All of the operations and measurements in our protocol can be jointly written as

$$\begin{aligned}\mathcal{I}_R(a,b,c;d) = F_4^{-1}(1,3)((|c\rangle_C\langle c|H^C)\\ \otimes [|a\rangle_A\langle a|H^A U(d,u)\sigma_b^A \mathfrak{r}(c)]\\ \otimes \{[\sigma_0 \otimes \mathfrak{r}(a)]C^{\mathrm{NOT}}\})F_4(1,3).\end{aligned} \tag{51}$$

Note that the operations with the superscripts A,C denote their Hilbert spaces belonging, respectively, to the spaces of qubits A,C. Sometimes, if there is no confusion, we omit these superscripts. This whole space form of our protocol has covered up the sequence of operations and steps of classical communication, but its advantage is clear. Its action on the initial state (50) yields

$$\begin{aligned}|\Psi^{\mathrm{final}}_{ABCY}(a,b,c;d)\rangle = \mathcal{I}_R(a,b,c;d)|\Psi^{\mathrm{ini}}_{ABCY}\rangle\\ = \frac{1}{2\sqrt{2}}|abc\rangle_{ABC} \otimes U(d,u)|\xi\rangle_Y.\end{aligned} \tag{52}$$

The unknown state to be remotely implemented is just $|\xi\rangle_Y$ in Bob's partite subsystem defined by Eq. (3). Our protocol is then determinedly and faithfully completed.

When setting that Charlie's information transfers to Alice, the whole process of controlled remote implementation of quantum operations belonging to the restricted sets is shown in Fig. 3.

Here, we only express the full operations for the first of our protocols, and provide a figure of its quantum circuit. For the other three kinds of our protocols, the full operations and the figures of quantum circuits are similar. In addition, we should note that the controller cannot choose who is a sender and who is a receiver in the other two partite subsystems. In other words, when Charlie is a controller, either Alice or Bob can be chosen as a sender and the other one partite subsystem plays as a receiver.

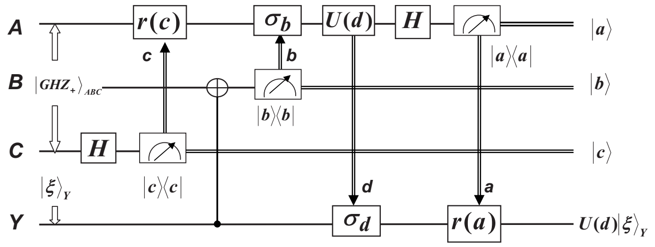

FIG. 3. Quantum circuit of the controlled remote implementations of quantum operations with a controller Charlie. Here, $U(d)$ belonging to the restricted sets is a quantum operation to be remotely implemented, H is a Hadamard transformation, σ_b, σ_d are identity matrices or NOT gates (σ_1) for $b,d=0$ or $b,d=1$, respectively, and $r(x)=(1-x)\sigma_0+x\sigma_3$ is equal to an identity matrix if $x=0$ or a phase gate if $x=1$. The measurements $|a\rangle\langle a|$, $|b\rangle\langle b|$, and $|c\rangle\langle c|$ are carried out in the computational basis $(a,b,c=0,1)$. "⇒" (crewel with an arrow) indicates the transmission of classical communication to the location of the arrow direction.

B. Protocol proof

In this section, let us prove the controlled RIO protocol in detail. For simplicity, we only consider the cases that Alice is a sender, Bob is taken as a receiver, and Charlie is a controller. Initially, the joint system is in the state (50). Charlie's action gives

$$\begin{aligned}|\Psi^{C}_{ABCY}(c)\rangle = F_4^{-1}(1,3)\mathcal{C}(c)F_4(1,3)|\Psi^{\mathrm{ini}}_{ABCY}\rangle\\ = \frac{1}{2}F_4^{-1}(1,3)[\sigma_0 \otimes \mathfrak{r}(c) \otimes I_4]\\ \times[|c\rangle_C \otimes (|00\rangle_{AB} + |11\rangle_{AB}) \otimes |\xi\rangle_Y]\end{aligned} \tag{53}$$

$$\begin{aligned}= \frac{1}{2}F_4^{-1}(1,3)[I_4 \otimes \mathfrak{r}(c) \otimes \sigma_0]\\ \times[|c\rangle_C \otimes (|00\rangle_{AB} + |11\rangle_{AB}) \otimes |\xi\rangle_Y],\end{aligned} \tag{54}$$

where we have used the definition of $\mathfrak{r}(y)$ in Eq. (19). Thus Alice and Bob now share a Bell state, and they can carry out the protocol of RIO. However, because HPV protocol is dependent on the type of Bell state, Charlie has to send the "password" c to Alice or Bob. Actually, this indicates that Charlie has his control right. We need to consider such two cases.

The first case is that the protocol sets Charlie to transfer his classical information c to Alice. Using $\mathcal{P}(b)$, Bob prepares his state as

$$\begin{aligned}|\Psi^{P}_{ABCY}(b,c)\rangle = F_4^{-1}(1,3)\mathcal{P}(b)F_4(1,3)|\Psi^{C}_{ABCY}\rangle\\ = \frac{1}{2}\{F_4^{-1}(2,4)[\mathfrak{r}(c)\sigma_b \otimes I_8]\}\\ \times[(y_0|00\rangle_{AY} + y_1|11\rangle_{AY}) \otimes |bc\rangle_{BC}],\end{aligned} \tag{55}$$

Alice starts with a supplementary operation $\mathfrak{r}(c)$ on her qubit [that is, Eq. (42) in the whole space] so that the state of joint system is perfectly ready, and then begins sending. The result is

$$|\Psi^S(a,b,c;d)\rangle = F_4^{-1}(1,3)\mathcal{S}^{\text{all}}(a,b,c,d)\mathcal{S}_A^{\text{add}}(c)F_4(1,3)|\Psi_{ABCY}^P\rangle$$

$$= \frac{1}{2}F_4^{-1}(2,4)\left[\left(\sum_k^1 y_k\langle a|HU(d,u)|k\rangle|a\rangle_A|k\rangle_Y\right)\right.$$

$$\left.\otimes|bc\rangle_{BC}\right]. \tag{56}$$

The second case is that the protocol sets Charlie to transfer his classical information c to Bob. If Bob chooses to first perform $\mathcal{P}^{\text{pre}}$, then the result is the same. Therefore when Alice finishes the sending operation, we also obtain Eq. (56). Noting that $\mathcal{P}^{\text{aft}}(c)\mathcal{P}(b)=\mathcal{P}(b)\mathcal{P}^{\text{pre}}(c)$, we can, after $\mathcal{P}(b)$ acts, use $\mathcal{P}^{\text{aft}}(c)$. From $\mathcal{R}(a;d)\mathcal{P}^{\text{aft}}(c)=(-1)^{cd}\mathcal{P}^{\text{aft}}(c)\mathcal{R}(a;d)$, this also means that Bob can delay the additional recovery operation to the end. It is clear that the results of three kinds of procedures are the same.

Now, Bob performs recovery operation (44). Similar to the proof of Eq. (34) by using the relations (28), (29), (31), and (32), we can obtain

$$|\Psi^{\text{final}}(a,b,c;d)\rangle = F_4^{-1}(1,3)\mathcal{R}(a,d)F_4(1,3)|\Psi_{ABCY}^S\rangle$$

$$= \frac{1}{2\sqrt{2}}|a\rangle_A \otimes F_3^{-1}(1,3)$$

$$\times\left[\left(\sum_{j=0}^1\sum_{k=0}^1 u_j y_k\langle j|\sigma_d|k\rangle|j\rangle_Y\right)\otimes|bc\rangle_{BC}\right]$$

$$= \frac{1}{2\sqrt{2}}|abc\rangle_{ABC}\otimes U(d,u)|\xi\rangle_Y. \tag{57}$$

This is the conclusion (52) of our protocol. Therefore we finish the proof our protocols of controlled RIO with a controller in the cases of one qubit.

V. VARIATIONS OF PROTOCOLS USING MULTIPARTITE GHZ STATES

In Secs. III and IV, we limit ourselves to using a three partite GHZ state. If we use a many partite GHZ state, there will be more variations among our RIO protocols. The variations can include the RIO protocols with more than two senders, or with many controllers, or with both many senders and controllers. For simplicity, we only consider the four partite GHZ state, and the initial state is taken as

$$|\Psi_{A_1A_2A_3BY}\rangle = \frac{1}{\sqrt{2}}(|0000\rangle_{A_1A_2A_3B} + |1111\rangle_{A_1A_2A_3B})$$

$$\otimes (y_0|0\rangle_Y + y_1|1\rangle_Y). \tag{58}$$

Our RIO protocols can have, respectively, three senders, two controllers, and two senders adding one controller. In the following, we only present the operation and measurement steps, and all classical communications are omitted.

Three senders. Set Alice1, Alice2, and Alice3 as senders. After Bob's preparing

$$\mathcal{P}_B(b) = I_8 \otimes [(|b\rangle\langle b| \otimes \sigma_0)C^{\text{NOT}}(2,1)], \tag{59}$$

all senders' sending operations read

$$\mathcal{S}_{A_1A_2A_3}(a_1,a_2,a_3;d_1,d_2,d_3;v_1,v_2,v_3;)$$

$$= [|a_1\rangle\langle a_1|H^{A_1}U(d_1,v_1)\sigma_b]$$

$$\otimes [|a_2\rangle\langle a_2|H^{A_2}U(d_2,v_2)\sigma_{d_1}\sigma_b]$$

$$\otimes [|a_3\rangle\langle a_3|H^{A_3}U(d_3,v_3)\sigma_{d_2}\sigma_{d_1}\sigma_b] \otimes I_4. \tag{60}$$

In practice, $\Pi_{i=1}^n\sigma_{d_i}$ can be simplified as $\sigma_{\Sigma_{i=1}^n d_i \bmod 2}$ since $d_i=0,1$ for any i, while Bob's recovering becomes

$$\mathcal{R}_B(a_1,a_2,a_3,d_1,d_2,d_3) = I_{16} \otimes [\mathfrak{r}(a_3)\sigma_{d_3}\mathfrak{r}(a_2)\sigma_{d_2}\mathfrak{r}(a_1)\sigma_{d_1}]. \tag{61}$$

Two controllers. Set Alice1 and Alice2 as two controllers and Alice3 as one sender. Two controllers both perform a Hadamard transformation and then measure their individual qubit

$$C(a_1,a_2) = (|a_1\rangle\langle a_1|H) \otimes (|a_2\rangle\langle a_2|H) \otimes I_4. \tag{62}$$

It is clear that

$$C(a_1,a_2)|\Psi_{A_1A_2A_3BY}\rangle = \frac{1}{2\sqrt{2}}|a_1a_2\rangle \otimes \{[\sigma_0 \otimes \mathfrak{r}(a_2)\mathfrak{r}(a_1)]$$

$$\times(|00\rangle_{A_3B} + |11\rangle_{A_3B})\}$$

$$\otimes (y_0|0\rangle_Y + y_1|1\rangle_Y) \tag{63}$$

$$= \frac{1}{2\sqrt{2}}|a_1a_2\rangle \otimes \{[\mathfrak{r}(a_2)\mathfrak{r}(a_1) \otimes \sigma_0]$$

$$\times(|00\rangle_{A_3B} + |11\rangle_{A_3B})\}$$

$$\otimes (y_0|0\rangle_Y + y_1|1\rangle_Y). \tag{64}$$

In practice, $\mathfrak{r}(a_1)\mathfrak{r}(a_2)=\mathfrak{r}(a_2)\mathfrak{r}(a_1)$ can be simplified as $\mathfrak{r}(a_1+a_2)$ since $a_1,a_2=0,1$. Besides the fact that an extra supplementary operation $\mathfrak{r}(a_2)$ is needed in the beginning of the recovery step, the remaining steps are similar to the case of one controller. It is clear that security can be enhanced via increasing the number of controllers because the faithful and determined implementation of this protocol requires that all the controllers cooperate and are authorized. If Alice1 and Alice2 are actually one compound subsystem (or called one controlled party), the enhancement of security then comes from increasing the "password" length (complication).

Two senders and one controller. Set Alice1 as one controller and Alice2 and Alice3 as two senders. Alice1's controlling step will result in

$$C_{A_1}(a_1)|\Psi_{A_1A_2A_3BY}\rangle = \frac{1}{2}|a_1\rangle \otimes \{[\mathfrak{r}(a_1)_{A_3} \otimes I_4](|000\rangle_{A_2A_3B}$$

$$+ |111\rangle_{A_2A_3B})\} \otimes (y_0|0\rangle_Y + y_1|1\rangle_Y) \tag{65}$$

$$
\begin{aligned}
&=\frac{1}{2}|a_1\rangle \otimes \{[I_2 \otimes \mathfrak{r}(a_1)_{A_3} \otimes I_2]\\
&\quad\times(|000\rangle_{A_2A_3B} + |111\rangle_{A_2A_3B})\}\\
&\quad\otimes (y_0|0\rangle_Y + y_1|1\rangle_Y) \qquad (66)
\end{aligned}
$$

$$
\begin{aligned}
&=\frac{1}{2}|a_1\rangle \otimes \{[I_4 \otimes \mathfrak{r}(a_1)_{B_1}]\\
&\quad\times(|000\rangle_{A_2A_3B} + |111\rangle_{A_2A_3B})\}\\
&\quad\otimes (y_0|0\rangle_Y + y_1|1\rangle_Y). \qquad (67)
\end{aligned}
$$

Besides the fact that an extra supplementary $\mathfrak{r}(a_1)$ is needed to be added to the beginning of the sending step by one of the senders (Alice2 or Alice3), or the recovery operation by the receiver (Bob), the remaining steps are similar to the RIO protocol with two senders.

These variations of the RIO protocols can be proved in a similar way in Secs. III and IV, and we do not intend to present them here. It is clear that the summation of the senders number and the controllers number is m when we use an $(m+1)$-partite shared GHZ state in the RIO protocols of one qubit.

VI. EXTENSION OF PROTOCOLS TO CASES OF N QUBITS

We have seen that when a new sender or controller is fetched in the protocols for the case of one qubit, the entanglement resource actually used for the remote transferring operation is still one Bell pair, despite the fact that our protocols are carried out via one GHZ state. In other words, the design of a new sender or/and adding a controller will use a part of the entanglement resource of GHZ states, the remaining entanglement is finally used for the rest of the transfer of quantum operations. For the cases of more than one qubit using GHZ states, the process of RIO utilizes the entanglement in a similar way, and hence our restricted sets [4] are still suitable for our combined and controlled RIOs.

By comparing with the cases of one qubit, we can extend the combined and controlled RIO protocols to the cases of N qubits in terms of our restricted sets. However, we find that the variety of protocols is more obvious, and the expressions and proofs of the protocols get a little complicated. Our protocols are still made up of seven steps for combined and controlled remote implementations of N-qubit quantum operations belonging to the restricted sets.

A. Some notations

Usually, in order to avoid possible errors, we need to denote the sequential structure of the direct product space of qubits, or a sequence of direct products of qubit space basis vectors in the multiqubit systems. For Alice's space, we set its sequential structure as $A_1A_2\cdots A_N$, in other words, its basis vector has the form $|a_1\rangle_{A_1}|a_2\rangle_{A_2}\cdots|a_N\rangle_{A_N}$ (or $|a_1a_2\cdots a_N\rangle_{A_1A_2\cdots A_N}$). Similarly, we set the sequential structure of Bob's space as $B_1B_2\cdots B_NY_1Y_2\cdots Y_N$, in other words, its basis vector has the form $|b_1\rangle_{B_1}|b_2\rangle_{B_2}\cdots|b_N\rangle_{B_N}|k_1\rangle_{Y_1}|k_2\rangle_{Y_2}\cdots|k_N\rangle_{Y_N}$. It is clear that for an N-qubit system, its space structure can be represented by a bit-string with the length of N.

Without loss of generality, we denote that the initial state with the shared GHZ state(s) between the senders and receiver, or between the controller(s) and the receiver, or among the the senders, controller(s), and receiver, has the following form:

$$|\Psi_N^{\mathrm{ini}}\rangle = \left(\bigotimes_{i=1}^{N}|\mathrm{GHZ}^{+}(m_i+1)\rangle\right)\otimes|\xi\rangle_{Y_1Y_2\cdots Y_N}, \qquad (68)$$

where the (m_i+1)-partite GHZ state is defined by

$$|\mathrm{GHZ}^{+}(m_i+1)\rangle = \frac{1}{\sqrt{2}}\left[\left(\prod_{\alpha_i=1}^{m_i}|0\rangle_{A_{\alpha_i}}\right)\otimes|0\rangle_{B_i} + \left(\prod_{\alpha_i=1}^{m_i}|1\rangle_{A_{\alpha_i}}\right)\otimes|1\rangle_{B_i}\right] \qquad (69)$$

and $m_i > 1$. Especially, when some m_i is taken as 1, this state will reduce to the Bell state. $|\xi\rangle_{y_1y_2\cdots y_N}$ is an arbitrary (unknown) pure state in the N-qubit systems, that is,

$$|\xi\rangle_{Y_1\cdots Y_N} = \sum_{k_1,\ldots,k_N=0}^{1} y_{k_1\cdots k_N}|k_1k_2\cdots k_N\rangle. \qquad (70)$$

Hence we know that the space structures are initially

$$\left[\prod_{i=1}^{N}\left(\prod_{\alpha_i=1}^{m_i}A_i\right)B_i\right]\prod_{t=1}^{N}Y_t. \qquad (71)$$

It must be emphasized that if the total system is initially in the state (68), our task is to remotely implement a quantum operation of N qubits, and Bob is a receiver, then the allowing number of senders is, at most, $\min[m_i,(i=1,2,\ldots,N)]$ and the allowing number of controllers is, at most, $\Sigma_{i=1}^{N}(m_i-1)$. When the number of senders is taken as n $(1\leqslant n\leqslant\min[m_i,(i=1,2,\ldots,N)])$, the maximal number of controllers is equal to $\Sigma_{i=1}^{N}m_i-nN$. Obviously, for a given j, if $m_j<1$, there is no sender since $\min[m_i,(i=1,2,\ldots,N)]\leqslant 0$. This implies that there is no RIO protocol of N-qubit systems. When $m_i=1$ for any i, the shared entangled states are all Bell states. Hence there is no controller since $\Sigma_{i=1}^{N}m_i|_{m_i=1}-nN\leqslant 0$, and there is only one sender.

For simplicity, in the following, we consider the combined RIO protocol of N-qubit systems with n senders by using N n-partite GHZ states and the controlled RIO protocol of N-qubit systems with n controllers by using n three partite GHZ states and $N-n$ Bell states. The variations of the protocols including the cases of both many senders and many controllers can be described in similar ways, and so they are omitted to save space. Moreover, we only present the operations and measurements and omit the steps of classical communications. Of course, we have to remember the implementing sequence of them. In addition, the significance and action of every step will not be stressed in detail as they can be understood from the corresponding cases of one qubit.

B. With n senders by using $Nn+1$-partite GHZ states

The combined RIO protocol of N-qubit systems with n senders requires the N shared $n+1$-partite GHZ states, and the initial state can be taken as

$$|\Psi_N^{\mathrm{ini}}\rangle = \left(\bigotimes_{m=1}^{N} |\mathrm{GHZ}_+(n+1)\rangle_{A_{m1}A_{m2}\cdots A_{mn}B_m}\right) \otimes |\xi\rangle_{Y_1Y_2\cdots Y_N}. \tag{72}$$

Let us set Bob as a receiver, Alice1, Alice2, up to Alice$n$ the first, second, up to the nth senders, and send, respectively, $T_N^r(x_1,v_1)$, $T_N^r(x_2,v_2)$, up to $T_N^r(x_n,v_n)$. This implies that the quantum operator to be remotely implemented has the form

$$U_N(n) = T_N^r(x_n,v_n)T_N^r(x_{n-1},v_{n-1})\cdots T_N^r(x_1,v_1). \tag{73}$$

Here, every $T_N^r(x_k,v_k)$ belongs to our restricted sets of N-qubit quantum operations [4].

In order to write our formula compactly and clearly, then prove our protocols more conveniently, we need to introduce two general swapping transformations

$$\Upsilon_A(n) = \prod_{i=1\leftarrow}^{n-1} [\urcorner(n+2-i,n+2-i,N) \otimes I_{2^{iN}}], \tag{74}$$

$$\Upsilon_B(n) = [I_{2^{nN}} \otimes \digamma^{-1}(1,2,N)][\urcorner(n+1,n+1,N) \otimes I_{2^N}], \tag{75}$$

where $\digamma(\alpha,n,N)$ and $\urcorner(\alpha,n,N)$ are defined in Appendix A and "←" means that the factors are arranged from right to left corresponding to the index i from small to large. It is easy to obtain

$$\Upsilon_A(n)\left[\left(\bigotimes_{m=1}^{N}|a_{m1}a_{m2}\cdots a_{mn}b_m\rangle_{A_{m1}A_{m2}\cdots A_{mn}B_m}\right)\left(\bigotimes_{m=1}^{N}|k_m\rangle_{Y_m}\right)\right]$$
$$= \left[\bigotimes_{i=1}^{n}\left(\bigotimes_{m=1}^{N}|a_{mi}\rangle_{A_{mi}}\right)\right]\left(\bigotimes_{m=1}^{N}|b_m\rangle_{B_m}\right)\left(\bigotimes_{m=1}^{N}|k_m\rangle_{Y_m}\right), \tag{76}$$

$$\Upsilon_B(n)\left[\left(\bigotimes_{m=1}^{N}|a_{m1}a_{m2}\cdots a_{mn}b_m\rangle_{A_{m1}A_{m2}\cdots A_{mn}B_m}\right)\left(\bigotimes_{m=1}^{N}|k_m\rangle_{Y_m}\right)\right]$$
$$= \left(\bigotimes_{m=1}^{N}|a_{m1}a_{m2}\cdots a_{mn}b_m\rangle_{A_{m1}A_{m2}\cdots A_{mn}}\right)\left(\bigotimes_{m=1}^{N}|b_mk_m\rangle_{B_mY_m}\right), \tag{77}$$

$$\Upsilon_A(n)\left\{\left[\bigotimes_{m=1}^{N}\left(\bigotimes_{\alpha=1}^{n}M_{a_{m\alpha}}^{A_{a_m\alpha}}\right)\otimes M_{b_m}^{B_m}\right]\otimes\left(\bigotimes_{m=1}^{N}M_{k_m}^{Y_m}\right)\right\}\Upsilon_A^{-1}(n)$$
$$= \left[\bigotimes_{\alpha=1}^{n}\left(\bigotimes_{m=1}^{N}M_{a_{m\alpha}}^{A_{m\alpha}}\right)\right]\otimes\left(\bigotimes_{m=1}^{N}M_{b_m}^{B_m}\right)\otimes\left(\bigotimes_{m=1}^{N}M_{k_m}^{Y_m}\right), \tag{78}$$

$$\Upsilon_B(n)\left\{\left[\bigotimes_{m=1}^{N}\left(\bigotimes_{\alpha=1}^{n}M_{a_{m\alpha}}^{A_{a_m\alpha}}\right)\otimes M_{b_m}^{B_m}\right]\otimes\left(\bigotimes_{m=1}^{N}M_{k_m}^{Y_m}\right)\right\}\Upsilon_B^{-1}(n)$$
$$= \left[\bigotimes_{m=1}^{N}\left(\bigotimes_{\alpha=1}^{n}M_{a_{m\alpha}}^{A_{a_m\alpha}}\right)\right]\otimes\left(\bigotimes_{m=1}^{N}M_{b_m}^{B_m}\otimes M_{k_m}^{Y_m}\right). \tag{79}$$

Hence Bob's preparing is written as

$$\mathcal{P}_B(b_1,b_2,\ldots,b_N) = \Upsilon_B^{-1}(n)\left[I_{2^{nN}}\otimes\left(\bigotimes_{m=1}^{N}(|b_m\rangle_{B_m}\langle b_m| \otimes \sigma_0^{Y_m})C^{\mathrm{NOT}}(2,1)\right)\right]\Upsilon_B(n) \tag{80}$$

$$= \urcorner^{-1}(n+2,n+2,N)\left(\bigotimes_{m=1}^{N}I_{2^n}\otimes(|b_m\rangle_{B_m}\langle b_m| \otimes \sigma_0^{Y_m})C^{\mathrm{NOT}}(2,1)\right)\urcorner(n+2,n+2,N). \tag{81}$$

When there are many senders, our protocol is actually the combination of remote implementations in turn. However, after the former operation is transferred remotely, the next sender's local system loses perfect correlation with the remote system to be operated. Since we use the GHZ states as a quantum channel, the former transfers have not exhausted all of the correlation in the joint system. Recalling the cases of one qubit, we can obtain the method to rebuild their correlation through replacing all σ_{d_i} by the corresponding fixed forms of the former operations. Hence the kth Alice's sending is

$$S_{A_k}(a_{mk},x_1,x_2,\ldots,x_k,v_k,b_1,b_2,\ldots,b_m)$$
$$= \Upsilon_A^{-1}(n)\left\{I_{2^{(k-1)N}}\otimes\left[\left(\bigotimes_{m=1}^{N}|a_{mk}\rangle_{A_{mk}}\langle a_{mk}|\right)\left(\bigotimes_{m=1}^{N}H^{A_{mk}}\right)\right.\right.$$
$$\left.\left.\times T_N^r(x_k,v_k)\left(\prod_{j=1\leftarrow}^{k-1}R_N(x_j)\right)\left(\bigotimes_{m=1}^{N}\sigma_{b_m}^{B_m}\right)\right]\otimes I_{2^{(n-k+2)N}}\right\}$$
$$\times\Upsilon_A(n), \tag{82}$$

where $R_N(x_j)$ is the fixed form $T_N^r(x_j,v_j)$ when all components of v_j take 1.

Bob's recovery operation is

$$\mathcal{R}_B(a_{11},\ldots,a_{1N};\ldots;a_{n1},\ldots,a_{nN};x_1,\ldots,x_n)$$
$$= I_{2^{3N}}\otimes\prod_{j=1\leftarrow}^{n}\left[\left(\bigotimes_{m=1}^{N}\mathfrak{r}^{Y_m}(a_{mj})\right)R_N(x_j)\right], \tag{83}$$

where $\mathfrak{r}(x_j)$ is defined by Eq. (19).

It must be pointed out that the classical communications are, respectively, listed as the following. First, Bob transfers N c-bits $b_1b_2\cdots b_N$ to all of the senders. Second, Alice1 transfers $[\log_2(2^N!)]+1$ classical c-bits (x_1) to Alice2, and $N+[\log_2(2^N!)]+1$ classical c-bits $(\{a_{11}a_{21}\cdots a_{N1};x_1\})$ to Bob, where $[\cdots]$ means to take the integer part and $[\log_2(2^N!)]+1$ comes from encoding length for the number of the restricted sets. This process continues in turn and the kth Alice transfers $k([\log_2(2^N!)]+1)$ classical c-bits $(\{x_1,x_2,\ldots,x_k\})$ to the $(k+1)$th Alice, and $N+[\log_2(2^N!)]+1$ classical c-bits $(\{a_{1k}a_{2k}\cdots a_{Nk};x_k\})$ to Bob. Up to the $(n-1)$th Alice transfers $(n-1)([\log_2(2^N!)]+1)$ classical c-bits $(\{x_1,x_2,\ldots,x_{n-1}\})$ to the last sender, that is, the nth Alice, and $N+[\log_2(2^N!)]+1$

classical c-bits $(\{a_{1(n-1)}a_{2(n-1)}\cdots a_{N(n-1)};x_{n-1}\})$ to Bob. Finally, the last sender only transfers $N+[\log_2(2^N!)]+1$ classical c-bits $(\{a_{1n}a_{2n}\cdots a_{Nn};x_k\})$ to Bob.

Obviously, the whole operations and measurements can be jointly written as

$$\mathcal{I}_R=\mathcal{R}_B\left(\prod_{j=1\leftarrow}^{n}\mathcal{S}_{A_j}\right)\mathcal{P}_B. \tag{84}$$

The proof of this protocol is put in Appendix B.

At the end of this section, we would like to point out that the combined RIO protocol can be carried out under one or several extra supercontrollers' commands. In this situation, the transferring information among the senders in turn is replaced by the supercontrollers. That is, based on the decomposition of the operation to be remotely implemented [Eq. (73)], the supercontrollers build a repertoire $\{x_1,x_2,\ldots,x_n\}$ and then distribute, respectively, $\{x_1,x_2,\ldots,x_k\}$ to the kth sender and make the senders build their own sending operations. This implies that the final operation to be remotely implemented is decided by the supercontrollers, and then there exist more means to enhance security. It is clear that the main steps of the above protocol do not change.

C. With *n* controllers by using *n* three-partite GHZ states and *N*−*n* Bell states

For the cases with n controllers, we set Charlie as controllers, Alice as a sender, and Bob as a receiver. The initial state with n shared three-partite GHZ states and $N-n$ shared Bell states reads

$$|\Psi_N^{\text{ini}}\rangle=\left(\bigotimes_{m=1}^{n}|\text{GHZ}^+\rangle_{C_mA_mB_m}\right)\otimes\left(\bigotimes_{s=n+1}^{N}|\Phi^+\rangle_{A_sB_s}\right)\otimes|\xi\rangle_{Y_1Y_2\cdots Y_N}. \tag{85}$$

Its space structure is

$$\prod_{m=1}^{n}C_mA_mB_m\prod_{s=n+1}^{N}A_sB_s\prod_{t=1}^{N}Y_t. \tag{86}$$

Here, Charlie's subsystem is written at the front for simplicity.

In order to write out our formula compactly and clearly, and then prove our protocols more conveniently, we need to introduce several general swapping transformations

$$\Theta_A(n)=[I_{2^n}\otimes\digamma(1,2,N)\otimes I_{2^N}][\digamma(1,3,n)\otimes I_{2^{3N-2n}}], \tag{87}$$

$$\Theta_B(n)=\left[I_{2^n}\otimes\neg^{-1}(3,3,N)\right][\digamma(1,3,n)\otimes I_{2^{3N-2n}}], \tag{88}$$

$$\Theta_C(n)=\digamma(1,3,n)\otimes I_{2^{3N-2n}}, \tag{89}$$

where $\digamma(\alpha,n,N)$ and $\neg(\alpha,n,N)$ are defined in Appendix A, and we have

$$\Theta_A(n)\left[\left(\bigotimes_{m=1}^{n}|c_ma_mb_m\rangle_{C_mA_mB_m}\right)\left(\bigotimes_{s=n+1}^{N}|a_sb_s\rangle_{A_sB_s}\right)\left(\bigotimes_{t=1}^{N}|k_t\rangle_{Y_t}\right)\right]$$
$$=\left(\bigotimes_{m=1}^{n}|c_m\rangle_{C_m}\right)\left(\bigotimes_{s=n+1}^{N}|a_s\rangle_{A_s}\right)\left(\bigotimes_{t=1}^{N}|b_t\rangle_{B_t}\right)\left(\bigotimes_{t=1}^{N}|k_t\rangle_{Y_t}\right), \tag{90}$$

$$\Theta_B(n)\left[\left(\bigotimes_{m=1}^{n}|c_ma_mb_m\rangle_{C_mA_mB_m}\right)\left(\bigotimes_{s=n+1}^{N}|a_sb_s\rangle_{A_sB_s}\right)\left(\bigotimes_{t=1}^{N}|k_t\rangle_{Y_t}\right)\right]$$
$$=\left(\bigotimes_{m=1}^{n}|c_m\rangle_{C_m}\right)\left(\bigotimes_{s=1}^{N}|a_sb_sk_s\rangle_{A_sB_sY_s}\right), \tag{91}$$

$$\Theta_C(n)\left[\left(\bigotimes_{m=1}^{n}|c_ma_mb_m\rangle_{C_mA_mB_m}\right)\left(\bigotimes_{s=n+1}^{N}|a_sb_s\rangle_{A_sB_s}\right)\otimes\left(\bigotimes_{t=1}^{N}|k_t\rangle_{Y_t}\right)\right]$$
$$=\left(\bigotimes_{m=1}^{n}|c_m\rangle_{C_m}\right)\left(\bigotimes_{s=1}^{N}|a_sb_s\rangle_{A_sB_s}\right)\otimes\left(\bigotimes_{t=1}^{N}|k_t\rangle_{Y_t}\right). \tag{92}$$

Similarly, we can obtain the transformed relations acting on the operations (or matrices):

$$\Theta_A(n)\left[\left(\bigotimes_{m=1}^{n}M_{c_m}^{C_m}\otimes M_{a_m}^{A_m}\otimes M_{m}^{B_m}\right)\right.$$
$$\left.\otimes\left(\bigotimes_{s=n+1}^{N}M_{a_s}^{A_s}\otimes M_{b_s}^{B_s}\right)\otimes\left(\bigotimes_{t=1}^{N}M_{y_t}^{Y_t}\right)\right]\Theta_A^{-1}(n)$$
$$=\left(\bigotimes_{m=1}^{n}M_{c_m}^{C_m}\right)\otimes\left(\bigotimes_{s=n+1}^{N}M_{a_s}^{A_s}\right)\otimes\left(\bigotimes_{m=1}^{N}M_{b_m}^{B_m}\right)\otimes\left(\bigotimes_{m=1}^{N}M_{y_m}^{Y_m}\right), \tag{93}$$

$$\Theta_B(n)\left[\left(\bigotimes_{m=1}^{n}M_{c_m}^{C_m}\otimes M_{a_m}^{A_m}\otimes M_{b_m}^{B_m}\right)\otimes\left(\bigotimes_{s=n+1}^{N}M_{a_s}^{A_s}\otimes M_{b_s}^{B_s}\right)\right.$$
$$\left.\otimes\left(\bigotimes_{t=1}^{N}M_{y_t}^{Y_t}\right)\right]\Theta_B^{-1}(n)$$
$$=\left(\bigotimes_{m=1}^{n}M_{c_m}^{C_m}\right)\otimes\left(\bigotimes_{s=1}^{N}M_{a_s}^{A_s}\otimes M_{b_s}^{B_s}\otimes M^{Y_s}\right), \tag{94}$$

$$\Theta_C(n)\left[\left(\bigotimes_{m=1}^{n}M_{c_m}^{C_m}\otimes M_{a_m}^{A_m}\otimes M_{b_m}^{B_m}\right)\right.$$
$$\left.\otimes\left(\bigotimes_{s=n+1}^{N}M_{a_s}^{A_s}\otimes M_{b_s}^{B_s}\right)\otimes\left(\bigotimes_{t=1}^{N}M_{y_t}^{Y_t}\right)\right]\Theta_C^{-1}(n)$$
$$=\left(\bigotimes_{m=1}^{n}M_{c_m}^{C_m}\right)\otimes\left(\bigotimes_{s=1}^{N}M_{a_s}^{A_s}\otimes M_{b_s}^{B_s}\right)\otimes\left(\bigotimes_{t=1}^{N}M_{y_t}^{Y_t}\right). \tag{95}$$

The controllers's (all Alice2) startup is

$$\mathcal{C}(c_1,\ldots,c_n)=\Theta_C^{-1}(n)\left[\bigotimes_{m=1}^{n}(|c_m\rangle_{C_m}\langle c_m|H^{C_m})\otimes I_{2^{3N}}\right]\Theta_C(n). \tag{96}$$

Bob's prior preparation is

$$\mathcal{P}_B^{\text{add}}(c_1,\ldots,c_n)=\Theta_B^{-1}(n)\left\{I_{2^n}\otimes\left[\left(\bigotimes_{m=1}^{n}\sigma_0^{A_m}\otimes\mathfrak{r}^{B_m}(c_m)\otimes\sigma_0^{Y_m}\right)\otimes I_{2^{3(N-n)}}\right]\right\}\Theta_B(n). \tag{97}$$

Bob's preparing is

$$\mathcal{P}_B(b_1,b_2,\ldots,b_N)=\Theta_B^{-1}(n)\left[I_{2^n}\otimes\left(\bigotimes_{m=1}^{N}\sigma_0^{A_m}\otimes[(|b_m\rangle_{B_m}\langle b_m|\otimes\sigma_0^{Y_m})C^{\text{NOT}}(2,1)]\right)\right]\Theta_B(n). \tag{98}$$

Alice's prior sending is

$$\mathcal{S}_A^{\text{add}}(c_1,\ldots,c_n)=\Theta_A^{-1}(n)\left\{I_{2^n}\otimes\left[\left(\bigotimes_{m=1}^{n}\mathfrak{r}(c_m)\right)\otimes I_{2^{N-n}}\right]\otimes I_{4^N}\right\}\Theta_A(n). \tag{99}$$

Alice's sending is

$$\begin{aligned}\mathcal{S}_A(a_1,\ldots,a_N;b_1,\ldots,b_N;x,u)&=\Theta_A^{-1}(n)\left\{I_{2^n}\otimes\left[\left(\bigotimes_{m=1}^{N}|a_m\rangle_{A_m}\langle a_m|\right)\left(\bigotimes_{m=1}^{N}H^{A_m}\right)\right.\right.\\&\quad\left.\left.\times T_N^r(x,u)\left(\bigotimes_{m=1}^{N}\sigma_{b_m}^{A_m}\right)\right]\otimes I_{4^N}\right\}\Theta_A(n).\end{aligned} \tag{100}$$

Bob's supplementary recovering is

$$\mathcal{R}_B^{\text{add}}(c_1,\ldots,c_n)=\left(\bigotimes_{m=1}^{n}\sigma_0^{C_m}\otimes\sigma_0^{A_m}\otimes\mathfrak{r}^{B_m}(c_m)\right)\otimes I_{2^{2(N-n)}}\otimes\left[\left(\bigotimes_{m=1}^{n}\mathfrak{r}(c_m)^{Y_m}\right)\otimes I_{2^{N-n}}\right]. \tag{101}$$

Bob's recovering is

$$\mathcal{R}_B(a_1,a_2,\ldots,a_N;x)=I_{2^{(2N+n)}}\otimes\left(\bigotimes_{m=1}^{N}\mathfrak{r}(a_m)^{Y_m}\right)R_N(x). \tag{102}$$

In particular, since $R_N(x)\{[\otimes_{m=1}^{n}\mathfrak{r}(c_m)^{Y_m}]\otimes I_{2^{N-n}}\}R_N^{\dagger}(x)$ and $[\otimes_{m=1}^{N}\mathfrak{r}(a_m)^{Y_m}]$ are diagonal, they commute each other. Again from $R_N^{\dagger}(x)R_N(x)=I_{2^N}$, it follows that

$$\begin{aligned}&R_N(x)\left[\left(\bigotimes_{m=1}^{n}\mathfrak{r}(c_m)^{Y_m}\right)\otimes I_{2^{N-n}}\right]R_N^{\dagger}(x)\left[\left(\bigotimes_{m=1}^{N}\mathfrak{r}(a_m)^{Y_m}\right)R_N(x)\right]\\&=\left[\left(\bigotimes_{m=1}^{N}\mathfrak{r}(a_m)^{Y_m}\right)R_N(x)\right]\left[\left(\bigotimes_{m=1}^{n}\mathfrak{r}(c_m)^{Y_m}\right)\otimes I_{2^{N-n}}\right].\end{aligned} \tag{103}$$

Therefore we obtain a final recovery operation

$$\begin{aligned}&\mathcal{R}_B^{\text{aft}}(c_1,c_2,\ldots,c_n;x)\\&=\left(\bigotimes_{m=1}^{n}\sigma_0^{C_m}\otimes\sigma_0^{A_m}\otimes\mathfrak{r}^{B_m}(c_m)\right)\otimes I_{2^{2(N-n)}}\\&\quad\otimes\left\{R_N(x)\left[\left(\bigotimes_{m=1}^{n}\mathfrak{r}(c_m)^{Y_m}\right)\otimes I_{2^{N-n}}\right]R_N^{\dagger}(x)\right\}.\end{aligned} \tag{104}$$

Obviously, such a final additional recovery operation is complicated in form compared with the other additional operations. Perhaps it is not worth using in our protocols.

It must be pointed out that three ways of classical communication are, respectively, (1) Charlie (controllers) to Alice (sender) or Bob (receiver) n c-bits; (2) Bob to Alice N c-bits; and (3) Alice to Bob $N+[\log_2(2^N!)]+1$ c-bits. (x may be encoded by $[\log_2(2^N!)]+1$ c-bit string, where $[\cdots]$ means taking the integer part.)

Based on the kinds and time of the controllers distributing to the sender or receiver, we only can use one prior operation for Bob or Alice, which has been seen in the cases of one qubit. Except for the controlling step, the rest of the operations and measurements can be jointly written according to four cases (omitting arguments for simplicity):

(1) Alice (sender) obtains the password before her sending

$$\mathcal{I}_R(1)=\mathcal{R}_B\mathcal{S}_A\mathcal{S}_A^{\text{add}}\mathcal{P}_B; \tag{105}$$

(2) Bob (receiver) obtains the password before his preparation

$$\mathcal{I}_R(2)=\mathcal{R}_B\mathcal{S}_A\mathcal{P}_B\mathcal{P}_B^{\text{add}}; \tag{106}$$

(3) Bob (receiver) obtains the password after his preparation

$$\mathcal{I}_R(3)=\mathcal{R}_B\mathcal{R}_B^{\text{add}}\mathcal{S}_A\mathcal{P}_B;\ \text{and} \tag{107}$$

(4) Bob (receiver) obtains the password after his recovery operations

$$\mathcal{I}_R(4)=\mathcal{R}^{\text{aft}}\mathcal{R}_B\mathcal{S}_A\mathcal{P}_B. \tag{108}$$

Because the controlling step commutes with all the other operation steps, it only requires doing before the next operation needs the controller's classical information. The proofs of these protocols are put in Appendix B.

In the end of the section, we would like to point out that n controllers can form k controlled parties with, respectively, $n_1,n_2,\ldots,n_k$ controllers and $\Sigma_{i=1}^{k}n_i=n$. Thus the above protocols almost do not change, but the length of passwords distributed by the n_ith party is increased to n_i c-bits.

VII. DISCUSSION AND CONCLUSION

We have investigated the combined and controlled remote implementation of N-qubit quantum operations belonging to our restricted sets [4] using the GHZ states. The interest in theory to use the GHZ states as a quantum resource is to reveal and explore the difference between the existing utilizable entanglement within the GHZ state and that within the Bell state. The typical problems focus on two aspects: one is a similar task of QIPC such as how to finish the combined of the RIO by using a smaller number of the GHZ states than using one of the Bell states, and the other is that for a class of tasks of QIPC such as the RIO when it is done by using the same number of GHZ states as one of the Bell states, whose example is just the controlled RIO protocol. This will help us to understand the nature of quantum entanglement and sufficiently use the valuable quantum resources. The main reasons to use the GHZ states in our protocols are to enhance security, increase variety, extend applications, as well as advance efficiency via fetching in many senders or/and many controllers. Taking the important applications of the RIO in distributed quantum computation [6,7], quantum program [8,9], and the other remote quantum information processing tasks into account, we think that the significance of our results is obvious.

It is clear that knowing the forms of the restricted sets of quantum operations that can be remotely implemented is a key matter to successfully carry out the RIO protocols. In our recent work [4], we obtained their general and explicit forms. Moreover, we provided evidence of the uniqueness and optimization of our restricted sets based on the precondition that our protocol only uses N maximally entangled states. It must be emphasized that before the beginning of our protocols, we have to build two mapping tables: one of them provides one-to-one mapping from $T_N^r(x) \in \mathbb{T}_N^r$ to the classical information x which is known by the senders, and the other one provides one-to-one mapping from a classical information x to $R_N(x)$ which is known by the receiver. Since the unified recovery operations are able to be obtained, all of the quantum operations belonging to our restricted sets can be remotely implemented via our protocols in a faithful and determined way. In addition, although the important and interesting quantum operations belonging to the restricted sets should be unitary, this limitation does not affect the validity of our protocols.

It should be pointed out that the implementations of $R_N(x)$ are important in our protocols. It is a key to design recovery quantum circuits in the near future. In principle, we can construct $R_N(x)$ by using a series of universal gates [21]. Especially, we have found that $R_2(x)$ can be constructed by C^{not} and σ_1 [5]:

$$R_2(1) = I_{Y_1} \otimes I_{Y_2}, \tag{109}$$

$$R_2(2) = C^{\text{NOT}}(Y_1,Y_2), \tag{110}$$

$$R_2(3) = C^{\text{NOT}}(Y_2,Y_1)C^{\text{NOT}}(Y_1,Y_2)C^{\text{NOT}}(Y_2,Y_1), \tag{111}$$

$$R_2(4) = C^{\text{NOT}}(Y_2,Y_1)C^{\text{NOT}}(Y_1,Y_2), \tag{112}$$

$$R_2(5) = C^{\text{NOT}}(Y_1,Y_2)C^{\text{NOT}}(Y_2,Y_1), \tag{113}$$

$$R_2(6) = C^{\text{NOT}}(Y_2,Y_1), \tag{114}$$

$$R_2(7) = C^{\text{NOT}}(Y_1,Y_2)(I \otimes \sigma_1), \tag{115}$$

$$R_2(8) = (I \otimes \sigma_1), \tag{116}$$

$$R_2(9) = (\sigma_1 \otimes I)C^{\text{NOT}}(Y_1,Y_2)C^{\text{NOT}}(Y_2,Y_1), \tag{117}$$

$$R_2(10) = C^{\text{NOT}}(Y_2,Y_1)(I \otimes \sigma_1), \tag{118}$$

$$R_2(11) = C^{\text{NOT}}(Y_2,Y_1)(\sigma_1 \otimes I)C^{\text{NOT}}(Y_1,Y_2)C^{\text{NOT}}(Y_2,Y_1), \tag{119}$$

$$R_2(12) = C^{\text{NOT}}(Y_2,Y_1)C^{\text{NOT}}(Y_1,Y_2)(I \otimes \sigma_1), \tag{120}$$

$$R_2(13) = C^{\text{NOT}}(Y_2,Y_1)C^{\text{NOT}}(Y_1,Y_2)(\sigma_1 \otimes I), \tag{121}$$

$$R_2(14) = C^{\text{NOT}}(Y_2,Y_1)C^{\text{NOT}}(Y_1,Y_2)(\sigma_1 \otimes I)C^{\text{NOT}}(Y_2,Y_1), \tag{122}$$

$$R_2(15) = C^{\text{NOT}}(Y_2,Y_1)(\sigma_1 \otimes I), \tag{123}$$

$$R_2(16) = C^{\text{NOT}}(Y_1,Y_2)(\sigma_1 \otimes I)C^{\text{NOT}}(Y_2,Y_1), \tag{124}$$

$$R_2(17) = (\sigma_1 \otimes I), \tag{125}$$

$$R_2(18) = C^{\text{NOT}}(Y_1,Y_2)(\sigma_1 \otimes I), \tag{126}$$

$$R_2(19) = (I \otimes \sigma_1)C^{\text{NOT}}(Y_2,Y_1), \tag{127}$$

$$R_2(20) = C^{\text{NOT}}(Y_1,Y_2)(I \otimes \sigma_1)C^{\text{NOT}}(Y_2,Y_1), \tag{128}$$

$$R_2(21) = C^{\text{NOT}}(Y_2,Y_1)(\sigma_1 \otimes I)C^{\text{NOT}}(Y_1,Y_2), \tag{129}$$

$$R_2(22) = C^{\text{NOT}}(Y_2,Y_1)C^{\text{NOT}}(Y_1,Y_2)(I \otimes \sigma_1)C^{\text{NOT}}(Y_2,Y_1), \tag{130}$$

$$R_2(23) = (\sigma_1 \otimes I)C^{\text{NOT}}(Y_1,Y_2), \tag{131}$$

$$R_2(24) = (\sigma_1 \otimes \sigma_1), \tag{132}$$

where $C^{\text{NOT}}(Y_1,Y_2)$ means that we use qubit Y_1 as the control qubit, Y_2 as the target qubit to do the control-NOT transformation, and $C^{\text{NOT}}(Y_2,Y_1)$ means we use qubit Y_2 as the control qubit and qubit Y_1 as the target qubit. Furthermore, we are interested in the construction of a unified recovery quantum circuit, which will be studied in another paper. Using the above construction, we have considered the experimental implementation scheme in the cavity QED of our RIO protocol [5]. It is worth pointing out that the unified recovery operations in our protocols imply that quantum operations that can be remotely implemented can belong to all of the restricted sets but not only a kind of restricted set. This advantage obviously reveals that the power of remote implementations of quantum operations in our protocols is enhanced.

In this paper, we not only propose our protocols in detail, but also prove them strictly in the cases of one and more than one qubit. Through describing the cases with two or more than two senders as well as one or many controllers, we explain clearly their roles in our protocols.

For the combined remote implementation of quantum operations, we have shown that many senders complete the remote implementations of many parts of a quantum operation and then combine them together to obtain the finally remote implementation of the whole quantum operations via multipartite GHZ states. Because the next sender has to know the classical information from all of the former senders, the combination of many parts of operations has a sequence. This implies that the cooperation of all the senders is needed. In practice, it is possible that different senders have different operational resources and different operational rights. Therefore we can set a suitable combination of their resources and rights. This implies that the combined remote implementation can overcome the senders's possible shortcomings and help us to arrive at the power of our protocols to the utmost extent in theory. Moreover, the transferring information among the senders in turn can be replaced by distributing the repertoire from one or several extra supercontrollers to the senders. This makes the supercontrollers have their right to determine the final operation to be remotely implemented, and hence the enhancement of security of RIO can be obtained by new means. In addition, it is interesting theoretically to study the quantum resource cost in the RIO protocols with many senders by comparing the different schemes using GHZ states with using more Bell states.

From the controlled RIOs, we have seen that the controller(s) is (are) an (a group of) administrator(s) in our protocols. If the controllers (controller) accept(s) the application of remote implementations of operations from sender and receiver, or intend(s) to let sender(s) and receiver(s) carry out the RIO task, they (he or she) will perform the startup operation (controlling step) and then transfer the classical information as a "password" to the sender(s) or the receiver (allowing step) so that the protocols can begin and be faithfully completed. When controllers, a sender, and a receiver share N GHZ states, it does not mean that the sender and receiver can carry out RIO protocols due to the fact that the quantum channel between the sender and receiver has not been opened. The startup of the quantum channel is obtained by the controllers' operation. It is just one of the reasons why we use the name of controller(s). Then, the controller(s) transfers his or her classical information as a "password." However, as soon as the password is transferred, the controller has no means to stop the protocols. Therefore we suggest a scheme to delay this transmission (password distributing) and send the password(s) to the receiver until the finishing of the receiver's standard recovered step so that the controller(s) keeps his or hers interrupting right up to the end of the protocols, that is, "saying the last word." However, it is possible this may lead to a little complicated form of the receiver's recovery operation for the multiqubits cases, so we may give up this kind of scheme and put the additional recovery operation before the standard recovery operations.

It should be pointed out that when three partite subsystems share N GHZ states, their position and right are symmetric. Therefore any partite subsystem can be one of controller, sender, and receiver. The controller is determined by the other two parties' choice based on their requirement of RIO, and/or his or her own decision in order to authorize the other two partite subsystems carrying out RIO. If an advanced administrator nominates a controller, he or she can demand this controller open the quantum channel between the other two partite subsystems but keep the classical information in his or her hands as a controlled means. If the number of shared GHZ states is n less than N, only two partite subsystems will be symmetric and they can be chosen as either a sender and a receiver; the other one partite subsystem with n qubits only can play as the controllers.

Our protocols with more than two senders, or both many controllers and many senders, require the shared entangled states with more than three partite subsystems when we remotely implement N-qubit operations only using N GHZ states. In general, for the cases of RIO of N qubits, the initial states have the form (68). Note that $m_i \geqslant 1$ is necessary for any i. Otherwise, we do not have the sender. In other words, there is no N-qubit RIO protocol. If the number of senders is taken as n $(1 \leqslant n \leqslant \min[m_i, (i=1,2,\ldots,N)])$, the number of controllers is equal to $\sum_{i=1}^{N} m_i - nN$. Obviously, when initially shared entangled states contain the Bell states (that is, to allow some $m_j=1$), there is only one sender; when initially shared entangled states are all Bell states, the controller is not allowed and the number of senders is only 1; when initially shared entangled states are all three-partite GHZ states, the number of senders is, at most, 2, or there is one sender and N controllers. It is worth pointing out that many controllers can form one or several controlled parties, and the length of passwords distributed by a given controlled party made of m controllers increases to m c-bits. In this paper, we have studied the above different situations in the case of one-qubit. In order to save space, we only present the combined RIO protocol with n senders by using N $n+1$-partite GHZ states in the cases of N-qubits and controlled RIO protocol with n controllers by using n three-partite GHZ states and $N-n$ Bell states, because the variations of the protocols are direct extensions via jointly considering combined and controlled RIO protocols of N-qubit systems.

In summary, using GHZ states in the RIOs protocols indeed can enhance the security, increase the variety, extend the possible applications, and even advance the efficiency of the RIOs. Therefore our conclusions indicate that GHZ states are indeed powerful and important resources in quantum information processing and communications.

ACKNOWLEDGMENTS

We are grateful for all the collaborators of our quantum theory group at the Institute for Theoretical Physics of our university. This work was funded by the National Fundamental Research Program of China under Grant No. 2001CB309310 and partially supported by the National Natural Science Foundation of China under Grant No. 60573008.

APPENDIX A: SWAPPING TRANSFORMATION

In this appendix, we first study the general swapping transformations which are the combinations of a series of usual swapping transformations. They are used in our protocols in order to express our formulas clearly and compactly, and prove our protocols more conveniently and easily.

Note that a swapping transformation of two neighbor qubits is defined by

$$S_W = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{A1}$$

Its action is

$$S_W|\alpha_X\beta_Y\rangle = |\beta_Y\alpha_X\rangle, \quad S_W(M^X\otimes M^Y)S_W = M^Y\otimes M^X. \tag{A2}$$

This means that the swapping transformation changes the space structure $H_X\otimes H_Y$ into $H_Y\otimes H_X$.

For an N-qubit system, the swapping gate of the ith qubit and the $(i+1)$th qubit reads

$$S_N(i,i+1) = \sigma_0^{\otimes(i-1)}\otimes S_W\otimes\sigma_0^{\otimes(N-i-1)}. \tag{A3}$$

Two rearranged transformations are defined by

$$F_N(i,j) = \prod_{\alpha=1\leftarrow}^{j-i} S_N(j-\alpha, j+1-\alpha), \tag{A4}$$

$$P_N(j,k) = \prod_{\beta=j\leftarrow}^{k-1} S_N(\beta,\beta+1), \tag{A5}$$

where $F_N(i,j)$ extracts out the spin-state of site j and rearranges it forwards to the site i $(i<j)$ in the qubit-string, $P_N(j,k)$ extracts out the spin-state of site j and rearranges it backwards to the site k $(k>j)$ in the qubit-string. Note that "←" means that the factors are arranged from right to left corresponding to α,β from small to large.

In terms of $F(i,j)$ and $P(j,k)$, we can obtain the many general swapping transformations, and then change the space structure. For example, the initial space structure is

$$\prod_{i=1}^{N}\left(\prod_{\alpha=1}^{m} A_{i\alpha}\right), \tag{A6}$$

we would like to change it into

$$\left(\prod_{j=1}^{m} A_{j\beta}\right)\prod_{i=1}^{N}\left[\left(\prod_{\alpha=1}^{\beta-1} A_{i\alpha}\right)\left(\prod_{\alpha=1}^{\beta+1} A_{i\alpha}\right)\right], \tag{A7}$$

$$\prod_{i=1}^{N}\left[\left(\prod_{\alpha=1}^{\beta-1} A_{i\alpha}\right)\left(\prod_{\alpha=1}^{\beta+1} A_{i\alpha}\right)\right]\left(\prod_{j=1}^{m} A_{j\beta}\right). \tag{A8}$$

The corresponding general swapping transformations are, respectively, defined by

$$\digamma(\beta,m,N) = \prod_{i=1\leftarrow}^{N} F_{mN}[i, mi-(m-\beta)], \tag{A9}$$

$$\neg(\beta,m,N) = \prod_{i=1\leftarrow}^{N} P_{mN}[m(N-i)+\beta, mN-i+1], \tag{A10}$$

where $F[n,n]$ and $P[n,n]$ are thought of as the identity operator. Hence

$$\digamma(\beta,m,N)\prod_{i=1}^{N}|a_{i1}a_{i2}\cdots a_{im}\rangle = \left(\prod_{i=1}^{N}|a_{i\beta}\rangle\right)\otimes\prod_{i=1}^{N}|a_{i1}\cdots a_{i(\beta-1)}a_{i(\beta+1)}\cdots a_{im}\rangle, \tag{A11}$$

$$\digamma(\beta,m,N)\left[\prod_{i=1}^{N}(M_{a_{i1}}\otimes M_{a_{i2}}\otimes\cdots\otimes M_{a_{im}})\right]\digamma^{-1}(\beta,m,N) = \left(\prod_{i=1}^{N}M_{a_{i\beta}}\right)\otimes\prod_{i=1}^{N}(M_{a_{i1}}\otimes\cdots\otimes M_{a_{i(\beta-1)}}\otimes M_{a_{i(\beta+1)}} \otimes\cdots\otimes M_{a_{im}}), \tag{A12}$$

$$\neg(\beta,m,N)\prod_{i=1}^{N}|a_{i1}a_{i2}\cdots a_{im}\rangle = \prod_{i=1}^{N}|a_{i1}\cdots a_{i(\beta-1)}a_{i(\beta+1)}\cdots a_{im}\rangle\otimes\left(\prod_{i=1}^{N}|a_{i\beta}\rangle\right), \tag{A13}$$

$$\neg(\beta,m,N)\left[\prod_{i=1}^{N}(M_{a_{i1}}\otimes M_{a_{i2}}\otimes\cdots\otimes M_{a_{im}})\right]\neg^{-1}(\beta,m,N) = \left[\prod_{i=1}^{N}(M_{a_{i1}}\otimes\cdots\otimes M_{a_{i(\beta-1)}}\otimes M_{a_{i(\beta+1)}}\otimes\cdots\otimes M_{a_{im}})\right]\otimes\left(\prod_{i=1}^{N}M_{a_{i\beta}}\right). \tag{A14}$$

More generally, considering the set $\mathbb{Q}_N$ to be a whole permutation of the bit-string $a_1a_2\cdots a_N$, and denote the z element with a bit-string form $Q(z)=q_1(z)q_2(z)\cdots q_N(z)$, we always can obtain such a general swapping transformation W_N that a computational basis $|a_1a_2\cdots a_N\rangle$ of N-qubit systems can be swapped as another basis $|q_1(z)q_2(z)\cdots q_N(z)\rangle$ in which $q_1(z)q_2(z)\cdots q_N(z)$ is an arbitrary element of $\mathbb{Q}_N$. Thus we can write a given general swapping transformation $W_N[a_1a_2\cdots a_N\to q_1(z)q_2(z)\cdots q_N(z)]$,

$$W_N[a_1a_2\cdots a_N\to q_1(z)q_2(z)\cdots q_N(z)]|a_1a_2\cdots a_N\rangle = |q_1(z)q_2(z)\cdots q_N(z)\rangle. \tag{A15}$$

Furthermore, if we denote two-dimensional space A_i spanned by $|a_i\rangle$ $(a_i=0,1$ and $i=1,2,\ldots,N)$, and M^{A_i} is a matrix belonging to this space, we obviously have

$$
\begin{aligned}
&W_N^{-1}[a_1a_2\cdots a_N \to q_1(z)q_2(z)\cdots q_N(z)]\\
&\quad\times\left(\prod_{i=1}^{N} M^{A_i}\right)W_N[a_1a_2\cdots a_N \to q_1(z)q_2(z)\cdots q_N(z)]\\
&\quad=\left(\prod_{i=1}^{N} M^{A_{q_i(z)}}\right).
\end{aligned}\tag{A16}
$$

Therefore the general swapping transformation W_N defined above can be used to change the space structure of multiqubits systems.

APPENDIX B: PROOF OF OUR PROTOCOL IN CASES MORE THAN ONE QUBIT

Here, we would like to prove our protocols of controlled and combined RIO belonging to our restricted sets in the cases of more than one qubit.

First, let us prove the combined RIO of N-qubit systems with n senders. An important skill of the proof is to rewrite the initial state (72) as

$$
\begin{aligned}
|\Psi_N^{\text{ini}}\rangle &= \frac{1}{\sqrt{2^N}}\urcorner^{-1}(n+2,n+2,N)\left\{\sum_{k_1,\ldots,k_N=0}^{1} y_{k_1,\ldots,k_N}\right.\\
&\quad\times\left[\bigotimes_{m=1}^{N}\left(\left|\underbrace{0\cdots 0}_{n+1}k_m\right\rangle_{A_{m1}A_{m2}\cdots A_{mn}B_mY_m}\right.\right.\\
&\quad\left.\left.\left.+\left|\underbrace{1\cdots 1}_{n+1}k_m\right\rangle_{A_{m1}A_{m2}\cdots A_{mn}B_mY_m}\right)\right]\right\}.
\end{aligned}\tag{B1}
$$

Like Ref. [4], we have

$$
\begin{aligned}
&\{I_{2^n}\otimes[(|b_m\rangle\langle b_m|\otimes\sigma_0)C^{\text{NOT}}(2,1)]\}\\
&\quad\times\left(\left|\underbrace{0\cdots 0}_{n+1}k_m\right\rangle_{A_{m1}A_{m2}\cdots A_{mn}B_mY_m}\right.\\
&\quad\left.+\left|\underbrace{1\cdots 1}_{n+1}k_m\right\rangle_{A_{m1}A_{m2}\cdots A_{mn}B_mY_m}\right)\\
&\quad=[(\sigma_{b_m})^{\otimes n}\otimes I_4][|k_m\rangle^{\otimes n}|b_mk_m\rangle].
\end{aligned}\tag{B2}
$$

Thus Bob's preparing yields

$$
\begin{aligned}
|\Psi_N^P\rangle &= \mathcal{P}_B(b_1,\ldots,b_N)|\Psi_N^{\text{ini}}\rangle\\
&= \frac{1}{\sqrt{2^N}}\urcorner^{-1}(n+2,n+2,N)\\
&\quad\times\left\{\sum_{k_1,\ldots,k_N=0}^{1} y_{k_1,\ldots,k_N}\bigotimes_{m=1}^{N}[(\sigma_{b_m})^{\otimes n}\otimes I_4]\right.\\
&\quad\left.\times[|k_m\rangle^{\otimes n}|b_mk_m\rangle]\right\}\\
&= \frac{1}{\sqrt{2^N}}\Upsilon_A^{-1}(n)\left\{\sum_{k_1,\ldots,k_N=0}^{1} y_{k_1,\ldots,k_N}\left[\bigotimes_{\alpha=1}^{n}\left(\bigotimes_{m=1}^{N}\sigma_{b_m}^{A_{m\alpha}}|k_m\rangle_{A_{m\alpha}}\right)\right]\right.\\
&\quad\left.\times\left[\left(\bigotimes_{m=1}^{N}|b_m\rangle\right)\left(\bigotimes_{m=1}^{N}|k_m\rangle\right)\right]\right\}.
\end{aligned}\tag{B3}
$$

Omitting the swapping transformations as well as coefficient and keeping the relevant subspaces, we have

$$
|\psi_N^P\rangle \propto \sum_{k_1\cdots k_N=0}^{1} y_{k_1\cdots k_n}\left[\bigotimes_{\alpha=1}^{n}\left(\bigotimes_{m=1}^{N}\sigma_{b_m}^{A_{m\alpha}}|k_m\rangle_{A_{m\alpha}}\right)\right]\otimes\left(\bigotimes_{m=1}^{N}|k_m\rangle_{Y_m}\right).\tag{B4}
$$

Alice1's sending leads to

$$
\begin{aligned}
\mathcal{S}_{A_1}|\psi_N^P\rangle &\propto \sum_{k_1\cdots k_N=0}^{1} y_{k_1\cdots k_n}\left(\bigotimes_{m=1}^{N}|a_{m1}\rangle_{A_{m1}}\right)\\
&\quad\otimes\left[\left(\bigotimes_{m=1}^{N}\langle a_{m1}|\right)\left(\bigotimes_{m=1}^{N}H\right)T_N^r(x_1,v_1)\left(\bigotimes_{m=1}^{N}|k_m\rangle\right)\right]\\
&\quad\otimes\left[\bigotimes_{\alpha=2}^{n}\left(\bigotimes_{m=1}^{N}\sigma_{b_m}^{A_{m\alpha}}|k_m\rangle_{A_{m\alpha}}\right)\right]\otimes\left(\bigotimes_{m=1}^{N}|k_m\rangle_{Y_m}\right).
\end{aligned}\tag{B5}
$$

It is a key matter that we can prove the relation

$$
\begin{aligned}
T_N^r(1,v)R_N(x) &= \sum_{m=1}^{2^N} v^m|i,D\rangle\langle m,D|\sum_{n=1}^{2^N}|n,D\rangle\langle p_n(x),D|\\
&= \sum_{m=1}^{2^N} v^m|m,D\rangle\langle p_m(x),D| = T_N^r(x,v),
\end{aligned}\tag{B6}
$$

and we have known that

$$
T_N^r(1,v) = \sum_{j_1,\ldots,j_N=0}^{1} v^{j_1j_2\cdots j_N}|j_1j_2\cdots j_N\rangle\langle j_1j_2\cdots j_N|,\tag{B7}
$$

where m is a number in decimal system, but $j_1j_2\cdots j_N$ corresponds to its binary system form. Substituting them into Eq. (B5), we have

$$
\begin{aligned}
\mathcal{S}_{A_1}|\psi_N^P\rangle &\propto \left(\bigotimes_{m=1}^{N}|a_{m1}\rangle_{A_{m1}}\right)\sum_{k_1\cdots k_N=0}^{1} v_1^{j_1\cdots j_N}y_{k_1\cdots k_n}\\
&\quad\times\left(\prod_{m=1}^{N}\langle a_{m1}|H|j_{m1}\rangle\right)\left[\left(\bigotimes_{m=1}^{N}\langle j_{m1}|\right)R_N(x_1)\right.\\
&\quad\left.\times\left(\bigotimes_{m=1}^{N}|k_m\rangle\right)\right]\otimes\left[\bigotimes_{\alpha=2}^{n}\left(\bigotimes_{m=1}^{N}\sigma_{b_m}^{A_{m\alpha}}|k_m\rangle_{A_{m\alpha}}\right)\right]\\
&\quad\otimes\left(\bigotimes_{m=1}^{N}|k_m\rangle_{Y_m}\right).
\end{aligned}\tag{B8}
$$

Similarly, considering all sending and recovering operations and again omitting unimportant subspaces, we obtain the final state:

$$\begin{aligned}|\psi_N^{\text{final}}\rangle \propto \sum_{k_1\cdots k_N=0}^{1} y_{k_1\cdots k_n}\left[\prod_{\alpha=0}^{n}\left(\sum_{l_{1\alpha}\cdots l_{N\alpha}=0}^{1}\right)\right] &\times\left[\prod_{\alpha=1}^{n}\left(\sum_{j_{1\alpha}\cdots j_{N\alpha}=0}^{1} v_1^{j_{1\alpha}\cdots j_{N\alpha}}\right)\right]\\ &\times\left[\prod_{\alpha=1}^{n}\left(\prod_{m=1}^{N}\langle a_{m\alpha}|H|j_{m\alpha}\rangle\right)\right]\\ &\times\left\{\prod_{\alpha=1}^{n}\left[\left(\bigotimes_{m=1}^{N}\langle j_{m\alpha}|\right)\prod_{k=1\leftarrow}^{\alpha} R_N(x_k)\left(\bigotimes_{m=1}^{N}|k_m\rangle\right)\right]\right\}\\ &\times\left\{\prod_{\alpha=1}^{n}\left(\bigotimes_{m=1}^{N}\langle l_{m\alpha}|\right)\left[\left(\bigotimes_{m=1}^{N}\mathfrak{r}(a_{m\alpha})\right)R_N(x_\alpha)\right]\right.\\ &\left.\times\left(\bigotimes_{m=1}^{N}|l_{m(\alpha-1)}\rangle\right)\right\}\left(\prod_{m=1}^{n}\delta_{k_m l_{m0}}\right)\left(\bigotimes_{m=1}^{N}|l_{mn}\rangle_{Y_m}\right).\end{aligned} \tag{B9}$$

By using the relations

$$\mathfrak{r}(a_m) = \sum_{l_m=0}^{1}(-1)^{a_m l_m}|l_m\rangle\langle l_m|, \tag{B10}$$

$$\langle a_m|H|j_m\rangle(-1)^{a_m j_m} = \frac{1}{\sqrt{2}}, \tag{B11}$$

and dropping unimportant coefficients, we can rewrite the final state as

$$\begin{aligned}|\psi_N^{\text{final}}\rangle \propto \sum_{k_1\cdots k_N=0}^{1} y_{k_1\cdots k_n}\left[\prod_{\alpha=0}^{n}\left(\sum_{l_{1\alpha}\cdots l_{N\alpha}=0}^{1}\right)\right] &\times\left[\prod_{\alpha=1}^{n}\left(\sum_{j_{1\alpha}\cdots j_{N\alpha}=0}^{1} v_1^{j_{1\alpha}\cdots j_{N\alpha}}\right)\right]\\ &\times\left[\prod_{\alpha=1}^{n}\prod_{m=1}^{N}(-1)^{a_{m\alpha}(j_{m\alpha}+l_{m\alpha})}\right]\\ &\times\left(\prod_{\alpha=1}^{n}\left\{\sum_{i_{10}^{\alpha}\cdots i_{N0}^{\alpha}=0}^{1}\left[\prod_{\beta=1}^{\alpha}\left(\sum_{i_{1\beta}^{\alpha}\cdots i_{N\beta}^{\alpha}=0}^{1}\right)\right.\right.\right.\\ &\left.\left.\left.\times\left(\bigotimes_{m=1}^{N}\langle i_{m\beta}^{\alpha}|\right)R_N(x_\beta)\left(\bigotimes_{m=1}^{N}|i_{m(\beta-1)}^{\alpha}\rangle\right)\right]\left(\prod_{m=1}^{N}\delta_{i_{m0}^{\alpha}k_m}\right)\right\}\right)\\ &\times\left[\prod_{\alpha=1}^{n}\left(\bigotimes_{m=1}^{N}\langle l_{m\alpha}|\right)R_N(x_\alpha)\left(\bigotimes_{m=1}^{N}|l_{m(\alpha-1)}\rangle\right)\right]\\ &\times\left(\prod_{\alpha=1}^{n}\prod_{m=1}^{N}\delta_{j_{m\alpha}i_{m\alpha}^{\alpha}}\right)\left(\prod_{m=1}^{N}\delta_{k_m l_{m0}}\right)\left(\bigotimes_{m=1}^{N}|l_{mn}\rangle_{Y_m}\right).\end{aligned} \tag{B12}$$

It is clear that the matrix elements related to $R_N(x_\beta)$ have $(n-\beta+2)$ factors. They read

$$\left[\prod_{\alpha=\beta}^{n}\left(\bigotimes_{m=1}^{N}\langle i_{m\beta}^{\alpha}|\right)R_N(x_\beta)\left(\bigotimes_{m=1}^{N}|i_{m(\beta-1)}^{\alpha}\rangle\right)\right]\left(\bigotimes_{m=1}^{N}\langle l_{m\beta}|\right)R_N(x_\beta)\times\left(\bigotimes_{m=1}^{N}|l_{m(\beta-1)}\rangle\right). \tag{B13}$$

Especially, when $\beta=1,2$, it becomes

$$\left[\prod_{\alpha=1}^{n}\left(\bigotimes_{m=1}^{N}\langle i_{m1}^{\alpha}|\right)R_N(x_1)\left(\bigotimes_{m=1}^{N}|i_{m0}^{\alpha}\rangle\right)\right]\left(\bigotimes_{m=1}^{N}\langle l_{m1}|\right)R_N(x_1)\times\left(\bigotimes_{m=1}^{N}|l_{m0}\rangle\right), \tag{B14}$$

$$\left[\prod_{\alpha=2}^{n}\left(\bigotimes_{m=1}^{N}\langle i_{m2}^{\alpha}|\right)R_N(x_2)\left(\bigotimes_{m=1}^{N}|i_{m1}^{\alpha}\rangle\right)\right]\left(\bigotimes_{m=1}^{N}\langle l_{m2}|\right)R_N(x_2)\times\left(\bigotimes_{m=1}^{N}|l_{m1}\rangle\right). \tag{B15}$$

Note that there are the δ factors $(\Pi_{m=1}^{N}\delta_{k_m l_{m0}})$ and $(\Pi_{\alpha=1}^{n}\Pi_{m=1}^{N}\delta_{i_{m0}^{\alpha}k_m})$ in the final state (B12), we can rewrite them as

$$\left(\prod_{m=1}^{N}\delta_{k_m l_{m0}}\right)\left(\prod_{\alpha=1}^{n}\prod_{m=1}^{N}\delta_{i_{m0}^{\alpha}l_{m0}}\right). \tag{B16}$$

Thus since $(\Pi_{\alpha=1}^{n}\Pi_{m=1}^{N}\delta_{i_{m0}^{\alpha}l_{m0}})$, the expression (B14) can be replaced by

$$\left(\prod_{\alpha=1}^{n}\prod_{m=1}^{N}\delta_{i_{m1}^{\alpha}l_{m1}}\right)\left(\bigotimes_{m=1}^{N}\langle l_{m1}|\right)R_N(x_1)\left(\bigotimes_{m=1}^{N}|l_{m0}\rangle\right). \tag{B17}$$

Here, we have continuously used the relation

$$\left[\left(\bigotimes_{m=1}^{N}\langle j_m|\right)R_N(x)\left(\bigotimes_{m=1}^{N}|k_m\rangle\right)\right]\left[\left(\bigotimes_{m=1}^{N}\langle l_m|\right)R_N(x)\left(\bigotimes_{m=1}^{N}|k_m\rangle\right)\right] = \left(\prod_{m=1}^{N}\delta_{j_m l_m}\right)\left[\left(\bigotimes_{m=1}^{N}\langle j_m|\right)R_N(x)\left(\bigotimes_{m=1}^{N}|k_m\rangle\right)\right]. \tag{B18}$$

This relation is obtained because every row or every column of $R_N(x)$ has only one nonvanishing element. Again based on $(\Pi_{\alpha=1}^{n}\Pi_{m=1}^{N}\delta_{i_{m1}^{\alpha}l_{m1}})$, the expression (B15) can be replaced by

$$\left(\prod_{\alpha=2}^{n}\prod_{m=1}^{N}\delta_{i_{m2}^{\alpha}l_{m2}}\right)\left(\bigotimes_{m=1}^{N}\langle l_{m2}|\right)R_N(x_2)\left(\bigotimes_{m=1}^{N}|l_{m1}\rangle\right). \tag{B19}$$

In turn, we can replace the expression (B13) by

$$\left(\prod_{\alpha=\beta}^{n}\prod_{m=1}^{N}\delta_{i_{m\beta}^{\alpha}l_{m\beta}}\right)\left(\bigotimes_{m=1}^{N}\langle l_{m\beta}|\right)R_N(x_\beta)\left(\bigotimes_{m=1}^{N}|l_{m(\beta-1)}\rangle\right) \tag{B20}$$

for β taking the values from 1 to n. Because the δ factors $(\Pi_{\alpha=1}^{n}\Pi_{m=1}^{N}\delta_{j_{m\alpha}i_{m\alpha}^{\alpha}})$ and $(\Pi_{\alpha=1}^{n}\Pi_{m=1}^{N}\delta_{i_{m\alpha}^{\alpha}l_{m\alpha}})$ appear in the final state, they make $j_{m\alpha}=l_{m\alpha}$. This means that the factor

$$\left[\prod_{\alpha=1}^{n}\prod_{m=1}^{N}(-1)^{a_{m\alpha}(j_{m\alpha}+l_{m\alpha})}\right] \tag{B21}$$

can be replaced by 1. Therefore by summation to eliminate δ functions, the final state is simplified as

$$\begin{aligned}|\psi_N^{\text{final}}\rangle \propto \sum_{k_1\cdots k_N=0}^{1} y_{k_1\cdots k_n}\left[\prod_{\alpha=1}^{n}\left(\sum_{j_{1\alpha}\cdots j_{N\alpha}=0}^{1} v_1^{j_{1\alpha}\cdots j_{N\alpha}}\right)\right]\\ \times\sum_{j_{10}\cdots j_{N0}=0}^{1}\left(\prod_{m=1}^{N}\delta_{j_{m0}k_m}\right)\\ \times\left[\prod_{\alpha=1}^{n}\left(\bigotimes_{m=1}^{N}\langle j_{m\alpha}|\right)R_N(x_\alpha)\left(\bigotimes_{m=1}^{N}|j_{m(\alpha-1)}\rangle\right)\right]\\ \times\left(\bigotimes_{m=1}^{N}|j_{mn}\rangle_{Y_m}\right)\end{aligned} \tag{B22}$$

$$=\left(\prod_{\alpha=0\leftarrow}^{n}T_N^r(x_\alpha,v_\alpha)\right)|\xi\rangle_{Y_1\cdots Y_N}. \tag{B23}$$

After restoring the coefficient, adding the other subspaces, and rearranging the space structure, we have

$$\begin{aligned}|\Psi_N^{\text{final}}\rangle = \frac{1}{\sqrt{2^{N+n}}}\left\{\bigotimes_{m=1}^{N}\left[\left(\bigotimes_{\alpha=1}^{n}|a_{m\alpha}\rangle_{A_{m\alpha}}\right)|b_m\rangle_{B_m}\right]\right\}U_N(n)\\ \times|\xi_N\rangle_{Y_1\cdots Y_N},\end{aligned} \tag{B24}$$

where $U_N(n)$ is defined by Eq. (73). Therefore we finish the proof of our combined RIO protocol with n senders in the cases of N qubits by using $(n+1)$-partite GHZ states.

Now, let us prove the controlled RIO protocol with n controllers. Since

$$\begin{aligned}[I_2\otimes(|c_m\rangle\langle c_m|H^{C_m})\otimes I_2]|\text{GHZ}_+\rangle\\ =\frac{1}{2}(S_W\otimes I_2)|c_m\rangle(|00\rangle+(-1)^{c_m}|11\rangle),\end{aligned} \tag{B25}$$

the initial state is transformed as

$$\begin{aligned}|\Psi_N^C\rangle = \mathcal{C}(c_1,c_2,\ldots,c_n)|\Psi_N^{\text{ini}}\rangle = \frac{1}{\sqrt{2^n}}\Theta_C^{-1}(n)\left[\left(\bigotimes_{m=1}^{n}|c_m\rangle\right)\right.\\ \left.\times\left(\bigotimes_{m=1}^{n}|\text{Bell}_{\text{c}_\text{m}}\rangle_{A_mB_m}\right)\left(\bigotimes_{s=n+1}^{N}|\text{Bell}_+\rangle_{A_sB_s}\right)\otimes|\xi\rangle_{y_1\cdots y_N}\right],\end{aligned} \tag{B26}$$

where $|\text{Bell}_+\rangle=|\Phi^+\rangle$ defined by Eq. (2) and

$$|\text{Bell}_{\text{c}_\text{m}}\rangle=\frac{1}{\sqrt{2}}[|00\rangle+(-1)^{c_m}|11\rangle]. \tag{B27}$$

From the transformation $\mathfrak{r}(x)$ defined by Eq. (19), it follows that

$$|\text{Bell}_{c_m}\rangle=[\sigma_0\otimes\mathfrak{r}(c_m)]|\text{Bell}_+\rangle=[\mathfrak{r}(c_{mc})\otimes\sigma_0]|\text{Bell}_+\rangle. \tag{B28}$$

Hence

$$\begin{aligned}|\Psi_N^C\rangle=\frac{1}{\sqrt{2^n}}\Theta_C^{-1}(n)\left(\left(\bigotimes_{m=1}^{n}|c_m\rangle\right)\left\{\left[\left(\bigotimes_{m=1}^{n}\sigma_{c_m}^{A_m}\otimes\sigma_0^{B_m}\right)\otimes I_{2^{2(N-n)}}\right]\right.\right.\\ \left.\left.\times\left(\bigotimes_{s=1}^{N}|\text{Bell}_+\rangle_{A_sB_s}\right)\right\}\otimes|\xi\rangle_{y_1\cdots y_N}\right)\end{aligned} \tag{B29}$$

$$\begin{aligned}=\frac{1}{\sqrt{2^n}}\Theta_C^{-1}(n)\left(\left(\bigotimes_{m=1}^{n}|c_m\rangle\right)\left\{\left[\left(\bigotimes_{m=1}^{n}\sigma_0^{A_m}\otimes\sigma_{c_m}^{B_m}\right)\otimes I_{2^{2(N-n)}}\right]\right.\right.\\ \left.\left.\times\left(\bigotimes_{s=1}^{N}|\text{Bell}_+\rangle_{A_sB_s}\right)\right\}\otimes|\xi\rangle_{y_1\cdots y_N}\right).\end{aligned} \tag{B30}$$

Note that $\mathfrak{r}(x)\mathfrak{r}(x)=I_2$; therefore whatever controllers (all of Charlie's) transfer their information to the sender (Alice) or the receiver (Bob), all factors $\mathfrak{r}(c_m)$ will be eliminated because the product of it and the prior transformation $\mathfrak{r}(c_m)$ becomes 1. If we delay the controllers' information to after the preparing, then we can similarly discuss in terms of Eq. (40). If we delay the controllers' information to the end of our protocols (that is, "say the last word") in the cases of multiqubits, we will pay the price that a more complicated additional recovery operation results in. For simplicity, we only need to prove the case that the controllers' information is transferred to Bob. It is clear that the further proof is the same as the RIO protocol of N-qubit systems using Bell states. This has been given in our paper [4], and thus it is omitted here.

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

[2] S. F. Huelga, J. A. Vaccaro, A. Chefles, and M. B. Plenio, Phys. Rev. A **63**, 042303 (2001).

[3] S. F. Huelga, M. B. Plenio, and J. A. Vaccaro, Phys. Rev. A **65**, 042316 (2002).

[4] An Min Wang, Phys. Rev. A **74**, 032317 (2006).

[5] Liang Qiu and An Min Wang, e-print arXiv:quant-ph/0701197.

[6] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello, Phys. Rev. A **59**, 4249 (1999).

[7] J. Eisert, K. Jacobs, P. Papadopoulos, and M. B. Plenio, Phys. Rev. A **62**, 052317 (2000).

[8] M. A. Nielsen and I. L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).

[9] A. S. Sørensen and K. Mølmer, Phys. Rev. A **58**, 2745 (1998).

[10] D. Collins, N. Linden, and S. Popescu, Phys. Rev. A **64**, 032302 (2001).

[11] Y.-F Huang, X.-F Ren, Y.-S. Zhang, L.-M. Duan, and G.-C Guo, Phys. Rev. Lett. **93**, 240501 (2004).

[12] G.-Y Xiang, J. Li, and G.-C. Guo, Phys. Rev. A **71**, 044304

(2005).

[13] S. F. Huelga, M. B. Plenio, G.-Y. Xiang, J. Li, and G.-C Guo, J. Opt. B: Quantum Semiclassical Opt. **7**, 5384 (2005).

[14] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bells Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht, 1989), pp. 73–76; D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).

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

[16] C.-P. Yang, Shih-I Chu, and S. Han, Phys. Rev. A **70**, 022329 (2004).

[17] F.-G. Deng, C.-Y. Li, Y. S. Li, H.-Y. Zhou, and Y. Wang, Phys. Rev. A **72**, 022338 (2005).

[18] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[19] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).

[20] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).

[21] M. A. Nielsen and I. I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).