Remote implementations of partially unknown quantum operations of multiqubits

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 28 October 2005; revised manuscript received 1 June 2006; published 15 September 2006)

We propose and prove the protocol of remote implementations of partially unknown quantum operations of multiqubits belonging to the restricted sets. Moreover, we obtain the general and explicit forms of restricted sets and present evidence of their uniqueness and optimization. In addition, our protocol has universal recovery operations that can enhance the power of remote implementations of quantum operations.

DOI: 10.1103/PhysRevA.74.032317 PACS number(s): 03.67.Lx, 03.65.−w, 03.67.Hk

I. INTRODUCTION

Teleportation of a quantum state [1] means this unknown state is being transferred from a local system to a remote system without physically sending the particle. Thus, teleportation of a quantum operation may be understood as this unknown quantum operation being transferred from a local system to a remote system without physically sending the device. However, in the historical literature, it is more interesting that an unknown quantum operation acting on the local system (the sender's) is teleported and acts on an unknown state belonging to the remote system (the receiver's) [2]. Taking both teleportation and the action of a quantum operation into account, one can denote it as "remote implementation of operation" (RIO).

If not only a receiver's quantum state (belonging to the remote system) but also a sender's quantum operation (performing on the local system) are completely unknown (arbitrary) at the beginning, the required resource of RIO will be maximum [2]. Moreover, if there is a protocol of RIO, then it will be of significance only when the resource cost of RIO is less than twice the required resource of teleportation, because that can always be completed via so-called bidirectional quantum state teleportation (BQST). Here, BQST contains three steps, that is, the receiver first teleports an unknown target state to the sender, then the sender performs an unknown operation (to be remotely implemented) on the received state to obtain an acted state, and finally the sender teleports this acted state back to the receiver.

Usually, when a teleported state is partially unknown or partially known (even completely known), this state transmission process from a local system to a remote system is called "remote state preparation" [3,4], while when a teleported operation is partially unknown or partially known, this operation transmission process from a local system to a remote system is called "remote control of states" [5]. So-called "partially unknown" or "partially known" quantum operations refer to those belonging to some restricted sets that satisfy some given restricted conditions. In Ref. [5], the authors presented two kinds of restricted sets of quantum operations in the case of one qubit, that is, one set consists of diagonal operations and the other set consists of antidiagonal operations. It is clear that the restricted sets of quantum operations still include a very large amount of unitary transformations [5]. Actually, the remote implementations of quantum operations belonging to the restricted sets will consume fewer overall resources than one of completely unknown quantum operations, and they can satisfy the requirements of some practical applications. Moreover, the remote implementations of quantum operations are closely related with nonlocal quantum operations via local implementations. They both play important roles in distributed quantum computation [6,7], quantum programs [8,9], and other tasks of remote quantum-information processing and communication. Recently, a series of works on the remote implementations of quantum operations appeared and made some interesting progress both in theory [2,5,10] and in experiment [11–13]. Therefore, from our point of view, it is very important and useful to investigate the extension of remote implementations of quantum operations to the cases of multiqubits.

To this end, we have to solve some key problems in the cases of multiqubits, such as how to determine and classify the restricted sets of quantum operations, how to obtain and express the explicit form of restricted sets, and finally to present the protocol of remote implementation of partially unknown quantum operations belonging to the restricted sets. This paper will focus on these problems. It must be emphasized that for the cases of N qubits, the protocol proposed by us only uses N Bell pairs that is half of the overall quantum resources of the BQST scheme. In addition, there are universal recovery operations performed by the receiver in this protocol. This implies that the quantum operations that can be remotely implemented are extended from within a given restricted set to all of the restricted sets. One of its advantages is to enhance the power of remote implementations of quantum operations. This is useful because one can design the universal recovery quantum circuits that can be used to the remote implementations of quantum operations belonging to our restricted sets in the near future. Because the explicit forms of our restricted sets of multiqubit quantum operations are not reducible to the direct products of two restricted sets of one-qubit quantum operations, our protocol can be thought of as a development of the scheme of Huelga, Plenio, and Vaccaro's (HPV) [5].

This paper is organized as follows. In Sec. II, we first recall HPV protocol and point out its simplification; in Sec. III, we obtain the general and explicit form of restricted sets of N qubit operations, and present evidence of their uniqueness and optimization in our protocol; in Sec. IV, we propose the protocol of remote implementations of two-qubit opera-

*Email address: anmwang@ustc.edu.cn

tions belonging to our restricted sets; in Sec. V, we extend our protocol to the cases of N qubits; in Sec. VI, we summarize our conclusions and discuss some problems; in the Appendixes, we explain some notation in this paper, introduce general swapping transformations, and prove our protocol of remote implementations of N-qubit operations belonging to our restricted sets.

II. SIMPLIFIED HPV PROTOCOL

The remote implementation of a quantum operation within some given restricted set was proposed by Huelga, Plenio, and Vaccaro (HPV) [5]. In HPV's protocol, Alice is set as a sender and Bob is set as a receiver. Thus, the initial state in the joint system of Alice and Bob reads

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

where

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

is one of four Bell states that are 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 Dirac's vectors with the subscripts A,B,Y indicate their bases, respectively, belonging to the qubits A,B,Y.

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

$$U(0) = \begin{pmatrix} u_{00} & 0 \\ 0 & u_{11} \end{pmatrix}, \quad U(1) = \begin{pmatrix} 0 & u_{01} \\ u_{10} & 0 \end{pmatrix}. \tag{4}$$

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. Thus, HPV's protocol and its simplification can be expressed as the following steps.

Step one: Bob's preparation. In the original HPV protocol, in order to receive the remote control, Bob first performs a controlled-NOT using his shared part of the e-bit as a control, and then measures his second qubit (the third qubit in the joint system of Alice and Bob) in the computational bases $|b\rangle_Y\langle b|(b=0,1)$. So, Bob's preparation can be written as

$$\mathcal{P}_B^{\text{original}}(b) = (\sigma_b^B \otimes \sigma_0^Y)(\sigma_0^B \otimes |b\rangle_Y\langle b|)(|0\rangle_B\langle 0| \otimes \sigma_0^Y + |1\rangle_B\langle 1| \otimes \sigma_1^Y), \tag{5}$$

where σ_0 is a 2×2 identity matrix and σ_i $(i=1,2,3)$ are the Pauli matrices. Note that the matrices with the superscripts A,B,Y denote their Hilbert spaces belonging, respectively, to the spaces of qubits A,B,Y. Obviously, the reduced space of Alice or Bob is easy to obtain by partial tracing.

In fact, the first step in the original HPV protocol can be simplified by changing Bob's preparation as [13]

$$\mathcal{P}_B(b) = (|b\rangle_B\langle b| \otimes \sigma_0^Y)(\sigma_0^B \otimes |0\rangle_Y\langle 0| + \sigma_1^B \otimes |1\rangle_Y\langle 1|), \tag{6}$$

that is, Bob first performs a controlled-NOT using his second qubit (the third qubit in the joint system of Alice and Bob) as a control, and then measures his first qubit in the computational bases $|b\rangle_B\langle b|(b=0,1)$. This change is very simple but it is nontrivial because it saves a NOT gate performed by Bob; moreover, an additional swapping gate at the end of the original HPV protocol becomes redundant.

Step two: Classical communication from Bob to Alice. After finishing his measurement on the computational basis $|b\rangle\langle b|(b=0,1)$, Bob transfers a classical bit b to Alice. This step is necessary so that Alice can determine her operation.

It must be emphasized that Bob's preparation can be done in two equivalent ways with respect to $b=0$ and 1, respectively. Bob can fix his measurement as $|0\rangle\langle 0|$ and tells Alice before the beginning of the protocol, this communication step can be saved, and then Alice's next sending step will not need a first σ_b $(=\sigma_0)$ transformation. Similarly, if Bob takes $b=1$ and tells Alice before the beginning of the protocol, this step can be saved also, but Alice's next sending step still needs a prior transformation σ_1. In the above sense, the protocol may be able to save a classical bit, even a NOT gate.

Step three: Alice's sending. After receiving Bob's classical bit b, Alice first performs a prior transformation σ_b dependent on b, and then carries out the quantum operation $U(d)$ to be remotely implemented on her qubit (the first qubit). Finally, Alice executes a Hadamard transformation and 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

$$\mathcal{S}_A(a,b;d) = (|a\rangle_A\langle a|)[H^A U(d)\sigma_b^A], \tag{7}$$

where the Hadamard transformation H is defined by

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{8}$$

$U(d)$, defined by Eq. (4), belongs to diagonal or antidiagonal restricted sets, respectively, when $d=0$ or 1, and σ_b is taken as σ_0- or σ_1-dependent on the received classical information $b=0$ or 1.

Step four: Classical communication from Alice to Bob. After finishing her measurement on the computational basis $|a\rangle_A\langle a|(a=0,1)$, Alice transfers a classical bit a to Bob. Moreover, Alice also needs to transfer an additional classical information $d=0$ or 1 in order to tell Bob whether the transferred operation is diagonal or antidiagonal, unless they have prescribed the transferred operation belonging to a given restricted set before the beginning of the protocol.

Step five: Bob's recovery. In order to obtain the remote implementation of this quantum operation in a faithful and determined way, Bob has to preform his recovery operation in general. In the original HPV protocol, this operation is

$$\mathcal{R}_B^{\text{original}}(a;d) = \{[(1-a)\sigma_0^B + a\sigma_3^B]\sigma_d^B\} \otimes \sigma_0^Y. \tag{9}$$

In the simplified HPV protocol, Bob's recovery operation becomes

$$\mathcal{R}_B(a;d) = \sigma_0^B \otimes \{[(1-a)\sigma_0^Y + a\sigma_3^Y]\sigma_d^Y\}. \tag{10}$$

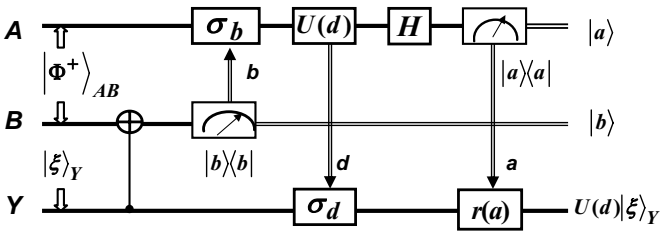

FIG. 1. Quantum circuit of the simplified HPV protocol, where $U(d)$ is a quantum operation to be remotely implemented and it is diagonal or antidiagonal, H is a Hadamard gate, σ_b, σ_d are identity matrices or NOT gates (σ_1) with respect to $b,d=0$ or $b,d=1$, respectively, and $r(a)=(1-a)\sigma_0+a\sigma_3$ 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 ($a,b=0,1$). $\Rightarrow$ indicates the transmission of classical communication to the location of the arrow direction.

It is clear that the original HPV protocol will result in $U(d)(y_0|0\rangle_B+y_1|1\rangle_B)$ in the second qubit of the joint system. One cannot help to perform an additional swapping operation between the second qubit and the third qubit defined by

$$\mathcal{B}_{\text{swap}}^{\text{original}}=\begin{pmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{pmatrix}. \tag{11}$$

However, in terms of the simplified HPV protocol, after carrying out the above steps from one to five, we can directly obtain $U(d)(y_0|0\rangle_Y+y_1|1\rangle_Y)$ in the third qubit of the joint system. This means that an additional swapping step has been saved.

All of the operations including measurements in the simplified HPV protocol can be jointly written as

$$\begin{aligned}\mathcal{I}_R(a,b;d)=&[\sigma_0^A\otimes\mathcal{R}_B(a;d)][\mathcal{S}_A(a,b;d)\\&\otimes\sigma_0^B\otimes\sigma_0^Y][\sigma_0^A\otimes\mathcal{P}_B(b)].\end{aligned} \tag{12}$$

Its action on the initial state (1) gives

$$|\Psi_{ABY}^{\text{final}}(a,b;d)\rangle=\mathcal{I}_R(a,b;d)|\Psi_{ABY}^{\text{ini}}\rangle=\frac{1}{2}|ab\rangle_{AB}\otimes U(d)|\xi\rangle_Y, \tag{13}$$

where $a,b=0$ or 1 denotes the spin up or spin down, and $d=0$ or 1 indicates the diagonal operation or antidiagonal operation, respectively. Therefore, the remote implementations of one-qubit quantum operations belonging to two restricted sets are faithfully and determinedly completed.

It is easy to plot the quantum circuit of the simplified HPV protocol; see Fig. 1.

III. RESTRICTED SETS OF QUANTUM OPERATIONS

We have described the simplified HPV protocol of remote implementations of one-qubit quantum operations in detail. For our purpose, to extend it to the cases of multiqubits, we first seek the restricted sets of multiqubit quantum operations that can be remotely implemented in a faithful and determined way. Here, through analyzing and discussing the cases of one- and two-qubit operations, we can exhibit our method to obtain the general and explicit forms of restricted sets of multiqubit quantum operations.

Let us start with the analysis of HPV's protocol for one qubit. From our point of view, the purpose of Bob's preparation is to lead to the first qubit (locally acted qubit in Alice's subsystem) being correlated with the third qubit (remotely operated or controlled qubit in Bob's subsystem) in such a superposition that for its every orthogonal component state, the first qubit and the third qubit are always located at the same computational bases. Bob arrives at this aim with two possible ways via quantum entanglement resource between the first qubit and the second qubit (in Bob's subsystem). When Bob uses $b=0$, then this aim has been achieved, but if Bob takes $b=1$, Alice has to supplement a σ_1 transformation for this aim. It is clear that such a superposition state has at most two orthogonal component states that are equal to the dimension of Hilbert's space of an unknown state. This implies that we can, at most, transfer two unknown complex numbers from the first qubit to the third qubit. We think that this is a really physical reason why we can only remotely implement a quantum operation belonging to the restricted sets. Without using additional correlation (entanglement), we cannot change this physical fact. However, using additional entanglement will destroy our attempt to save quantum resources.

In the second step, the communication from Bob to Alice is to tell Alice which preparing way Bob has used. In order to include all contributions of operation on the first qubit and transfer them to the third qubit, we need a Hadamard gate acting on the transformed qubit so that Alice's project measurement on a given computational basis does not lead to losing the actions on the other computational bases, because the first qubit and the third qubit are correlated in the above way. However, the action of the Hadamard gate will result in an algebraic addition of all of matrix elements in some row or column of this operation arising in front of some computation bases. Its advantage is that we are able to transfer the whole effect of operation to the third qubit, but its disadvantage is that we are not able to redivide the algebraic addition of matrix elements in some row or column of this operation because these elements are unknown. A uniquely choice way is to set only one nonzero element in every row or every column of this operation. In fact, this choice is also optimal since it allows the maximal numbers that can be transferred and also includes the unitary operations with such forms. This requirement yields the limitations to the structures of operations that can be remotely implemented, that is, so-called restricted sets of quantum operations. In the case of one qubit, it is easy to see that two restricted sets of quantum operations are made from a kind of diagonal operation and a kind of antidiagonal operation.

For the cases of two qubits, the above analyses are still feasible and valid. Because the unique nonzero element in the first row has four possible positions, the unique nonzero element in the second row has three possible positions, the unique nonzero element in the third row has two possible positions, and the unique nonzero element in the fourth row has one possible position, the restricted sets of operations are made of $4!=24$ kinds of operations.

It is easy to write the set of all of permutations for the list {1,2,3,4},

$$\begin{aligned}\mathbb{P}_4 = \{&(1,2,3,4),(1,2,4,3),(1,3,2,4),(1,3,4,2),(1,4,2,3),(1,4,3,2),\\ &(2,1,3,4),(2,1,4,3),(2,3,1,4),(2,3,4,1),(2,4,1,3),(2,4,3,1),(3,1,2,4),(3,1,4,2),\\ &(3,2,1,4),(3,2,4,1),(3,4,1,2),(3,4,2,1),(4,1,2,3),(4,1,3,2),(4,2,1,3),(4,2,3,1),(4,3,1,2),(4,3,2,1)\}. \end{aligned} \tag{14}$$

Denoting the xth element in this set by

$$p(x) = (p_1(x), p_2(x), p_3(x), p_4(x)), \tag{15}$$

for example $p(1)=(1,2,3,4)$, $p(2)=(1,2,4,3)$, and so on, we can obtain 24 restricted sets of two-qubit operations as follows:

$$T_2^r(x,t) = \sum_{m=1}^{4} t_m |m,D\rangle\langle p_m(x),D|, \tag{16}$$

where we have defined $|1,D\rangle=|00\rangle$, $|2,D\rangle=|01\rangle$, $|3,D\rangle=|10\rangle$, $|4,D\rangle=|11\rangle$. Here, the label D indicates the decimal system.

It is easy to verify that

$$T_2^r(x,t)[T_2^r(x,t)]^\dagger = \sum_{m=1}^{4} t_m t_m^* |m,D\rangle\langle m,D|, \tag{17}$$

$$[T_2^r(x)]^\dagger T_2^r(x) = \sum_{m=1}^{4} t_i t_m^* |p_m(x),D\rangle\langle p_m(x),D|. \tag{18}$$

Therefore, in terms of the requirement of the unitary condition for quantum operations, the only nonzero element t_m in the mth row of quantum operations belonging to the restricted sets should be taken as $e^{i\phi_m}$, and ϕ_m is real.

The above analyses and discussions have provided evidence of unique forms of restricted sets of two-qubit operations in a kind of protocol of RIO such as ours. In fact, this kind of protocol uses the Hadamard gates to transfer the whole effect of operation to the different qubits, but does not use the extra correlation doing it. Therefore, the forms of restricted sets are uniquely determined. Otherwise, the operation cannot be remotely implemented by using such a kind of protocol.

To remotely implement quantum operations belonging to the above restricted sets, Bob needs a mapping table that provides one-to-one mapping from a classical information x ($x=1,2,\ldots,24$) to a part of his recovery operation $R_2(x)$ defined by

$$R_2(x) = T_2^r(x,0) = \sum_{m=1}^{4} |m,D\rangle\langle p_m(z),D|. \tag{19}$$

Obviously, it has the same structure as $T_2^r(x,t)$ to be remotely implemented.

It is easy to see that the controlled kinds of operations,

$$U_C(1) = T_2^r(2,t)|_{t_1=t_2=1} = \begin{pmatrix}1&0\\0&0\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix} + \begin{pmatrix}0&0\\0&1\end{pmatrix}\otimes\begin{pmatrix}0&t_3\\t_4&0\end{pmatrix}, \tag{20}$$

$$U_C(2) = T_2^r(6,t)|_{t_1=t_3=1} = \begin{pmatrix}1&0\\0&1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&0\end{pmatrix} + \begin{pmatrix}0&t_2\\t_4&0\end{pmatrix}\otimes\begin{pmatrix}0&0\\0&1\end{pmatrix}, \tag{21}$$

$$U_C(3) = T_2^r(7,t)|_{t_1=t_2=1} = \begin{pmatrix}1&0\\0&0\end{pmatrix}\otimes\begin{pmatrix}0&t_3\\t_4&0\end{pmatrix} + \begin{pmatrix}0&0\\0&1\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix}, \tag{22}$$

$$U_C(4) = T_2^r(15,t)|_{t_2=t_4=1} = \begin{pmatrix}0&t_1\\t_3&0\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&0\end{pmatrix} + \begin{pmatrix}1&0\\0&1\end{pmatrix}\otimes\begin{pmatrix}0&0\\0&1\end{pmatrix} \tag{23}$$

belong to the restricted set. They are important operations in quantum-information processing.

Based on the same reasons stated above, any restricted set of N-qubit operations has such a structure that every row and every column of its operations only has one nonzero element, and we denote this nonzero element in the mth row by t_m, that is, the members of $2^N!$ restricted sets of N-qubit operations have the forms

$$T_N^r(x,t) = \sum_{m=1}^{2^N} t_m |m,D\rangle\langle p_m(x),D|, \tag{24}$$

where $x=1,2,\ldots,2^N!$ and

$$p(x) = (p_1(x), p_2(x), \ldots, p_{2^N}(x)) \tag{25}$$

is an element belonging to the set of all permutations for the list $\{1,2,\ldots,2^N\}$. All of the restricted sets of N-qubit operations are denoted by $\mathbb{T}_N^r$.

For the cases of N-qubit operations, we can take all nonzero elements of $T_N^r(x,t)$ as 1 and obtain its fixed form $R_N(x)$, that is,

$$R_N(x) = T_N^r(x,0) = \sum_{m=1}^{2^N} |m,D\rangle\langle p_m(x),D|. \tag{26}$$

It will be used in Bob's recovery operation of our protocol.

It must be emphasized that we usually study the cases in which $T_N^r(x,t)$ is unitary, although it does not affect our protocol. Before the beginning of the protocol, we need to build

two mapping tables: one provides one-to-one mapping from $T_N^r(x,t) \in \mathbb{T}_N^r$ to the classical information x, which is known as Alice, and another provides one-to-one mapping from a classical information x to $R_N(x)$, which is known as Bob.

It is clear that our explicit restricted sets of multiqubit operations are not reducible to the simple direct product of two restricted sets of one-qubit operations. Thus, in this sense, our protocol can be thought of as a development of HPV's protocol to the cases of multiqubits.

IV. PROTOCOL IN THE CASE OF TWO QUBITS

Now let us propose the protocol of remote implementations of two-qubit quantum operations belonging to 24 restricted sets in detail.

Assume the initial state of the joint system to be

$$|\Psi^{\text{ini}}_{A_1B_1A_2B_2Y_1Y_2}\rangle = |\Phi^+\rangle_{A_1B_1} \otimes |\Phi^+\rangle_{A_2B_2} |\xi\rangle_{Y_1Y_2}, \tag{27}$$

where the unknown state of two qubits is

$$|\xi\rangle_{Y_1Y_2} = \sum_{j_1,j_2=0}^{1} y_{j_1j_2} |j_1j_2\rangle_{Y_1Y_2}, \tag{28}$$

the qubits A_1, A_2 belong to Alice, the other four qubits B_1, B_2, Y_1, Y_2 are owned by Bob. It is clear that Alice and Bob share initially two Bell states.

Note that the Hilbert space of the joint system is initially taken as a series of direct products of Hilbert spaces of all qubits according to the following sequence:

$$H = H_{A_1} \otimes H_{B_1} \otimes H_{A_2} \otimes H_{B_2} \otimes H_{Y_1} \otimes H_{Y_2}. \tag{29}$$

We can simply call this sequence "space structure" and denote it by a bit-string; for example, the space structure of the above Hilbert space is $A_1B_1A_2B_2Y_1Y_2$. Obviously, taking such a space structure, the subspace belonging to Alice or Bob is separated. It will lead to inconvenience in the expression of local operations acting on their full subspaces and in the proof of the protocol of multiqubits. Therefore, there is a need to change the space structure. This can be realized by a series of swapping transformations, which are studied in Appendix A.

In terms of the general swapping transformations defined in Appendix A, we can change the initial space structure, for example,

$$|a_1b_1a_2b_2y_1y_2\rangle_{A_1B_1A_2B_2Y_1Y_2} = \Upsilon^{-1}(3,2)(|a_1b_1y_1\rangle_{A_1B_1Y_1} \otimes |a_2b_2y_2\rangle_{A_2B_2Y_2}), \tag{30}$$

$$|a_1b_1a_2b_2y_1y_2\rangle_{A_1B_1A_2B_2Y_1Y_2} = [\Lambda^{-1}(2,2) \otimes I_4](|a_1a_2\rangle_{A_1A_2} \otimes |b_1b_2\rangle_{B_1B_2} \otimes |y_1y_2\rangle_{Y_1Y_2}), \tag{31}$$

$$|a_1b_1a_2b_2y_1y_2\rangle_{A_1B_1A_2B_2Y_1Y_2} = \Gamma^{-1}(3,2)(|a_1a_2\rangle_{A_1A_2} \otimes |y_1y_2\rangle_{Y_1Y_2} \otimes |b_1b_2\rangle_{B_1B_2}). \tag{32}$$

Thus, we can express our formula compactly and clearly in the whole space, and can finally prove our protocol conveniently and strictly. Our notations in the whole space will be helpful for in understanding the problems even if a little complication in expressions is induced. It will be seen that such notations are more useful for the extension to the cases of multiqubits. However, it must be emphasized that these swapping transformations in the following formula do not really exist in the practical process.

Step one: Bob's preparation. Our protocol begins from this step. Bob first performs two controlled-NOT using, respectively, his qubits Y_1 and Y_2 as two control qubits, B_1 and B_2 as two target qubits, and then measures his two qubits B_1 and B_2 in the computational basis $|b_1\rangle_{B_1}\langle b_1| \otimes |b_2\rangle_{B_2}\langle b_2|(b_1,b_2=0,1)$. Therefore, Bob's preparation reads

$$\mathcal{P}_B(b_1,b_2) = \Upsilon^{-1}(3,2)\left\{ \bigotimes_{m=1}^{2} \sigma_0^{A_m} \otimes [(|b_m\rangle_{B_m}\langle b_m| \otimes \sigma_0^{Y_m}) C^{\text{not}}(0,1)] \right\} \Upsilon(3,2), \tag{33}$$

where $\Upsilon(3,N)$ is defined in Appendix A. Note that this expression is written in the whole joint system so that we can prove our protocol more conveniently in Appendix B.

If we do not use the swapping transformations, the form of Bob's preparation becomes

$$\begin{aligned}\mathcal{P}_B(b_1,b_2) = {} & (\sigma_0^{A_1} \otimes |b_1\rangle_{B_1}\langle b_1| \otimes \sigma_0^{A_2} \otimes |b_2\rangle_{B_2}\langle b_2| \otimes \sigma_0^{Y_1} \\ & \otimes \sigma_0^{Y_2})[\sigma_0^{A_1} s C_2^{\text{not}}(0,1) \otimes \sigma_0^{Y_2}] \\ & \times (\sigma_0^{A_1} \otimes \sigma_0^{B_1} \otimes \sigma_0^{A_2} \otimes C_1^{\text{not}}(0,1))\end{aligned} \tag{34}$$

Here, C_M^{not} can be called the separated controlled-NOT since its control and target are separated by M qubits, that is, its definition is

$$\begin{aligned}C_M^{\text{not}}(0,1) = {} & \sigma_0 \otimes \left(\bigotimes_{m=1}^{M} \sigma_0 \right) \otimes (|0\rangle\langle 0|) \\ & + \sigma_1 \otimes \left(\bigotimes_{m=1}^{M} \sigma_0 \right) \otimes (|1\rangle\langle 1|),\end{aligned} \tag{35}$$

while (0,1) indicates that the last qubit is a control and the first qubit is a target and is flipped when the control qubit is $|1\rangle$. If $M=0$, it comes back to the usual controlled-NOT. It is clear that using the general swapping transformations can simplify the expressions of formula in form.

Step two: Classical communication from Bob to Alice. After finishing his measurement on the computational basis, Bob transfers two classical bits b_1, b_2 to Alice. This step is necessary so that Alice can determine her sending operations.

It must be emphasized that Bob's preparation step has four equivalent ways corresponding, respectively, to b_1b_2 taking 00, 01, 10, 11 in order to carry out the protocol. If Bob first fixes the value of b_1b_2 and tells Alice before the beginning of the protocol, this step can be saved. In particular, when b_1b_2 is just taken as 00, Alice also does not need the transformation $\sigma_{b_1} \otimes \sigma_{b_2}$ in the next step, since $\sigma_0 \otimes \sigma_0$ is trivial.

Step three: Alice's sending. After receiving Bob's classical bits b_1b_2, Alice, on her two qubits (the qubits A_1A_2), first performs $\sigma_{b_1}^{A_1}\otimes\sigma_{b_2}^{A_2}$, secondly acts $T_2^r(x,t)$ to be remotely implemented, then carries out two Hadamard transformations, and finally measures her two qubits in the computational basis $|a_1\rangle_{A_1}\langle a_1|\otimes|a_2\rangle_{A_2}\langle a_2|(a_1,a_2=0,1)$. Since the basis vector of Alice's space has the structure $|a_1a_2\rangle_{A_1A_2}$, all of Alice's local operations and measurement are just

$$\mathcal{S}_A(a_1,b_1,a_2,b_2;x,t)=[\Lambda^{-1}(2,2)\otimes I_4]\{[(|a_1a_2\rangle_{A_1A_2}\langle a_1a_2|)\times(H^{A_1}\otimes H^{A_2})T_2^r(x,t)(\sigma_{b_1}^{A_1}\otimes\sigma_{b_2}^{A_2})]\otimes I_{16}\}[\Lambda(2,2)\otimes I_4], \quad (36)$$

where $\Lambda(2,2)$ is defined in Appendix A and I_m is an m-dimensional identity matrix.

Step four: Classical communication from Alice to Bob. After finishing her measurement on the computational basis $|a_1\rangle_{A_1}\langle a_1|\otimes|a_2\rangle_{A_2}\langle a_2|(a_1,a_2=0,1)$, Alice transfers two classical bits a_1,a_2 to Bob. Moreover, Alice also needs to transfer x (which can be encoded by five classical bits) to Bob in order to let him know the transferred operation $T_2^r(x,t)$ belonging to which restricted set, unless they prescribed the transferred operation $T_2^r(x,t)$ belonging to a given restricted set before the beginning of the protocol. All of the classical information is necessary for Bob so that he can determine his recovery operations.

Step five: Bob's recovering. In order to obtain the remote implementations of quantum operations in a faithful and determined way, Bob performs his recovery operation,

$$\mathcal{R}_B(a_1,a_2;x)=I_{16}\otimes\{[r^{Y_1}(a_1)\otimes r^{Y_2}(a_2)]R_2(x)\}, \quad (37)$$

where $r(y)$ is defined by

$$r(y)=(1-y)\sigma_0+y\sigma_3 \quad (38)$$

while $R_2(x)$ is obtained by the mapping table from the classical information x to $R_2(x)$. For example, Bob receives 1 (which can be encoded by 00000), thus he knows $R(1)$ is an identity matrix; Bob receives 2 (which can be encoded by 00001), thus he knows

$$R_2(2)=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix} \quad (39)$$

and so on. The mapping between x and $R_2(x)$ is given in advance before the protocol beginning.

Finally, all of the operations including measurements in the whole space for the remote implementations of quantum operations of two qubit can be written jointly as

$$\mathcal{I}_R(a_1,b_1,a_2,b_2;x,t)=\mathcal{R}_B(a_1,a_2;x)\mathcal{S}_A(a_1,b_1,a_2,b_2;x,t)\times\mathcal{P}_B(b_1,b_2). \quad (40)$$

Its action on the initial state gives the remote implementations of two-qubit quantum operations belonging to the above 24 restricted sets, that is, the final state becomes

$$|\Psi^{\text{final}}_{A_1B_1A_2B_2Y_1Y_2}(a_1,b_1,a_2,b_2;x,t)\rangle=\mathcal{I}_R(a_1,b_1,a_2,b_2;x)|\Psi^{\text{ini}}_{A_1B_1A_2B_2Y_1Y_2}\rangle \quad (41)$$

$$=\frac{1}{4}|a_1b_1a_2b_2\rangle_{A_1B_1A_2B_2}\otimes T_2^r(x,t)|\xi\rangle_{Y_1Y_2}, \quad (42)$$

where $a_m,b_n=0,1$; $m,n=1,2$. Therefore, our protocol completes faithfully and determinedly the remote implementations of quantum operations $T_2^r(x,t)$ belonging to 24 restricted sets. Its proof is found in Appendix B when $N=2$.

V. EXTENSION TO THE CASES OF N QUBITS

Based on our above protocol of remote implementations of two-qubit operations belonging to our restricted sets, we can extend it to the cases of more than two qubits without obvious difficulty. Our protocol consists of five steps for the remote implementations of N-qubit operations belonging to our restricted sets. Set the initial state as

$$|\Psi_N^{\text{ini}}\rangle=\left(\bigotimes_{m=1}^{N}|\Phi^+\rangle_{A_mB_m}\right)\otimes|\xi\rangle_{Y_1Y_2\cdots Y_N}, \quad (43)$$

where $|\xi\rangle_{Y_1Y_2\cdots Y_N}$ is an arbitrary (unknown) pure state in an N-qubit system, that is,

$$|\xi\rangle_{Y_1Y_2\cdots Y_N}=\sum_{k_1,k_2,\ldots,k_N=0}^{1}y_{k_1k_2\cdots k_N}|k_1k_2\cdots k_N\rangle. \quad (44)$$

It is clear that the space structure is initially

$$\prod_{m=1}^{N}(A_mB_m)\prod_{n=1}^{N}Y_n. \quad (45)$$

Usually, in order to avoid possible errors and provide convenience in the proof, we need to set the sequential structure of 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 $|b_1\rangle_{B_1}|b_2\rangle_{B_2}\cdots|b_N\rangle_{B_N}|y_1\rangle_{Y_1}|y_2\rangle_{Y_2}\cdots|y_N\rangle_{Y_N}$. It is clear that for an N-qubit system, its space structure can be represented by a bit-string with the length of N.

Now, let us describe our protocol in a concise way.

Step one: Bob's preparation.

$$\mathcal{P}_B(b_1,b_2,\ldots,b_N)=\Upsilon^{-1}(3,N)\left\{\bigotimes_{m=1}^{N}\sigma_0^{A_m}\otimes[(|b_m\rangle\langle b_m|\otimes\sigma_0)C^{\text{not}}(0,1)]\right\}\Upsilon_N(3,N), \quad (46)$$

where $\Upsilon(3,N)$ is defined in Appendix A. It must be emphasized that $\Upsilon(3,N)$ does not appear in the practical process, it is only required to express our steps clearly and compactly.

Step two: Classical communication from Bob to Alice. Alice transfers a classical bit-string $b_1b_2\cdots b_N$ to Bob unless Bob and Alice have an arrangement about Bob's preparing method (that is, $b_1b_2\cdots b_N$ to be determined by Bob and known by Alice) before the beginning of the protocol.

Step three: Alice's sending.

$$\mathcal{S}_A(a_1,b_1,a_2,b_2,\ldots,a_N,b_N;x,t)=[\Lambda^{-1}(2,N)\otimes I_{2^N}]\left[\left(\bigotimes_{m=1}^{N}|a_m\rangle_{A_m}\langle a_m|\right)\left(\bigotimes_{m=1}^{N}H^{A_m}\right)\times T_N^r(x,t)\left(\bigotimes_{m=1}^{N}\sigma_{b_m}^{A_m}\right)\otimes I_{4^N}\right][\Lambda(2,N)\otimes I_{2^N}], \quad (47)$$

where $\Lambda_N(2,N)$ is defined in Appendix A.

Step four: Classical communication from Alice to Bob. Alice transfers a classical bit-string $a_1a_2\cdots a_N$ and a classical information x (which can be encoded by $[\log_2(2^N!)]+1$ c-bit string, where $[\cdots]$ means taking the integer part) corresponding to the quantum operation $T_N^r(x,t)$ to be remotely implemented in her mapping table.

Step five: Bob's recovering.

$$\mathcal{R}_B(a_1,a_2\cdots a_N;x)=I_{4^N}\otimes\left\{\left(\bigotimes_{m=1}^{N}r(a_m)\right)R_N(x)\right\}, \quad (48)$$

where $R_N(x)$ is determined by Bob's mapping table.

Thus, all of the operations including measurements in the extension of remote implementations of quantum operations to the case of N qubits can be written as

$$\mathcal{I}_R(a_1,b_1,a_2,b_2;\ldots,a_N,b_N;x,t)=\mathcal{R}_B(a_1,a_2,\ldots,a_N;x)\times\mathcal{S}_A(a_1,b_1,a_2,b_2,\ldots,a_N,b_N;x,t)\times\mathcal{P}_B(b_1,b_2,\ldots,b_N). \quad (49)$$

The final state becomes

$$|\Psi_N^{\text{final}}(a_1,b_1,a_2,b_2,\ldots,a_N,b_N;x)\rangle=\mathcal{I}_R(a_1,b_1,a_2,b_2;\ldots,a_N,b_N;x,t)|\Psi_N^{\text{ini}}\rangle \quad (50)$$

$$=\frac{1}{2^N}\left(\bigotimes_{i=1}^{N}|a_ib_i\rangle_{A_iB_i}\right)\otimes T_N^r(x,t)|\xi\rangle_{Y_1Y_2\cdots Y_N}, \quad (51)$$

where $a_m,b_n=0,1$; $m,n=1,2,\ldots,N$.

It is easy to see that our restricted sets of three-qubit operations include the interesting controlled-controlled-$U(d)$ gate with the form

$$U^{\text{cc}}(d)=(|00\rangle\langle 00|+|01\rangle\langle 01|+|10\rangle\langle 10|)\otimes\sigma_0+|11\rangle\langle 11|\otimes U(d), \quad (52)$$

where $U(d)$ is a diagonal or antidiagonal operation of one-qubit systems. Just as well known, it, together with the operations (20)–(23), can be used to construct a universal gate.

The protocol proof of remote implementations of N-qubit operations belonging to our restricted sets is given in Appendix B.

VI. DISCUSSION AND CONCLUSION

In summary, we propose and prove the protocol of remote implementations of partially unknown quantum operations of multiqubits belonging to the restricted sets, and we obtain the general and explicit forms of these restricted sets, that is, every row and every column of an arbitrary member of operations belonging to the restricted sets only has one nonzero element. Our protocol is based on the simplified HPV scheme, but it can be thought of as a development of HPV's scheme to the cases of multiqubit systems since our restricted sets of multiqubit operations are not simply reducible to the direct products of HPV's restricted sets of one-qubit operations. Moreover, we have given evidence of the uniqueness and optimization of our restricted sets based on the precondition that our protocol only uses N Bell's pairs. In order to show our protocol in the above several aspects, we investigate in detail the cases of two qubits. Note that those quantum operations with the clearly physical significance and practical applications are included in our restricted sets, which can be implemented remotely. It should be pointed out that the universal recovery operations found by us are useful because they will be helpful for the design of universal recovery quantum circuits in the near future. This implies that the quantum operations that can be remotely implemented are extended from only belonging to a given restricted set to belonging to all of the restricted sets in our protocol. Its advantage is obviously that the power of remote implementations of quantum operations is enhanced. Of course, the universal recovery operations need two mapping tables that are known, respectively, as Alice and Bob before the beginning of the protocol.

In the area of resource consumption, the remote implementations of quantum operations belonging to two restricted sets of one-qubit operations need one e-bit which is shared by the sender and receiver and three c-bits (or two when Bob fixes his preparing way), from which one c-bit is transferred from the receiver to the sender and two c-bits are transferred from the sender to the receiver. In our protocol, we can see that the remote implementations of quantum operations belonging to 24 restricted sets of two-qubit operations need two e-bits and nine c-bits (or seven c-bits when Bob fixes his preparing way), where two e-bits are shared by the sender and the receiver, respectively, and two of nine c-bits are transferred from the receiver to the sender while the other seven c-bits are transferred from the sender to the receiver. For the case of N qubit operations, since the number of restricted sets that can be remotely implemented is $2^N!$, their remote implementations need N e-bits and $2N+[\ln_2(2^N!)]+1$ c-bits (or $N+[\ln_2(2^N!)]+1$ c-bits when Bob fixes his preparing way), where N e-bits are shared by the sender and the receiver, and N c-bits are transferred from the receiver to the sender while the other $N+[\ln_2(2^N!)]+1$ c-bits are transferred from the sender to the receiver. Here, "$[x]$" means taking the integer part of x. In addition, the fixed local operations $R_N(x)$ need to be used, and two mapping tables from $T_N^r(x,t)$ to a classical information x and from a classical information x to $R_N(x)$ need to be built before the beginning of the protocol. Usually, the number of interesting restricted

sets that can be remotely implemented is small, and the classical resource can be correspondingly decreased. However, this will pay the price that the power of protocol of remote implementations of quantum operations is reduced. It should be pointed out that the implementations of nonlocal quantum operations are different from the remote implementations of the quantum operations. Therefore, the resource used by them may be different in general.

Similar to the conclusion provided by Refs. [2,5], we have not found a faithful scheme without using maximum entanglement [14]. Actually, this is partially because there is no obvious physical significance when a unitary operation belonging to the restricted sets acts on a density matrix of a diagonal state, and such an action is equivalent to the known one that will be used in the recovery operation. For example, a phase gate on one qubit acting on a density matrix of a diagonal state gives nothing; an antidiagonal unitary transformation on one qubit acting on a density matrix of a diagonal state is just a flip gate. Of course, the study of the possible tradeoffs between the entanglement and classical communication will still be important in the near future.

Furthermore, we can investigate the controlled remote implementations of partially unknown quantum operations belonging to the restricted sets of one and multiqubits. Similar to the controlled teleportation of a quantum state via the GHZ states, the controlled remote implementations of partially unknown quantum operations can use the GHZ states, which are a very important quantum information resource [15]. In our view, the controlled remote implementations of quantum operations should have some remarkable applications in the remote quantum-information processing and communication, including the future quantum internet. Here, a quantum internet is a counterpart to the classical one, but it connects some quantum computers that are located at different places together and is used for the remote communication of quantum information and remote implementations of quantum operations. The relevant conclusions are studied in [16].

ACKNOWLEDGMENTS

We acknowledge all the collaborators of our quantum theory group at the Institute for Theoretical Physics of our university. In particular, we are grateful to Ning Bo Zhao, Xiao San Ma, Bo Sheng Zhang, Cheng Zhao, and Dong Zheng for their suggestive discussions. 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

Here, we study the general swapping transformations, which are combinations of a series of usual swapping transformations. They are used in our protocol in order to express our formula clearly and compactly, and prove our protocol easily and strictly.

Note that a swapping transformation of two neighbor qubits (2×2 matrix) 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 forward to the site i $(i<j)$ in the qubit string, where $P_N(j,k)$ extracts out the spin-state of site j, and backwards rearranges it backwards to the site k $(k>j)$ in the qubit string. Note that "$\leftarrow$" means that the factors are arranged from right to left corresponding to α, β from small to large. Now, in terms of $P(j,k)$, we can introduce two general swapping transformations with the forms

$$\Lambda(2,N) = \prod_{i=1\leftarrow}^{N-1} P_{2N}(2(N-i), 2N-i) \quad (N \geqslant 2), \tag{A6}$$

$$\Omega(2,N) = \prod_{i=1\leftarrow}^{N} P_{2N}(1,2N) \quad (N \geqslant 2). \tag{A7}$$

Thus,

$$\Lambda(2,N)\left(\bigotimes_{i=1}^{N}|a_i b_i\rangle\right) = \left(\bigotimes_{i=1}^{N}|a_i\rangle\right) \otimes \left(\bigotimes_{j=1}^{N}|b_j\rangle\right), \tag{A8}$$

$$\Lambda(2,N)\left(\bigotimes_{k=1}^{N}(M_{\alpha_i}^{A_i} \otimes M_{\beta_i}^{B_i})\right)\Lambda^{-1}(2,N) = \left(\bigotimes_{i=1}^{N} M_{\alpha_i}^{A_i}\right) \otimes \left(\bigotimes_{j=1}^{N} M_{\beta_j}^{B_j}\right), \tag{A9}$$

$$\Omega(2,N)\left[\left(\bigotimes_{i=1}^{N}|a_i\rangle\right) \otimes \left(\bigotimes_{j=1}^{N}|b_j\rangle\right)\right] = \left(\bigotimes_{i=1}^{N}|b_i\rangle\right) \otimes \left(\bigotimes_{j=1}^{N}|a_j\rangle\right), \tag{A10}$$

$$\Omega(2,N)\left[\left(\overset{N}{\underset{i=1}{\otimes}} M_{\alpha_i}^{A_i}\right)\left(\overset{N}{\underset{i=1}{\otimes}} M_{\beta_i}^{B_i}\right)\right]\Omega^{-1}(2,N) = \left(\overset{N}{\underset{i=1}{\otimes}} M_{\beta_i}^{B_i}\right)\otimes\left(\overset{N}{\underset{j=1}{\otimes}} M_{\alpha_j}^{A_j}\right). \quad \text{(A11)}$$

Similarly, we can introduce

$$\Upsilon(3,N) = \prod_{i=1\leftarrow}^{N-1} F_{3N}(3i,2N+i) \quad (N \geqslant 2). \quad \text{(A12)}$$

$$\Gamma(3,N) = [I_{2^N}\otimes\Omega(2,N)][\Lambda(2,N)\otimes I_{2^N}]. \quad \text{(A13)}$$

Thus,

$$\Upsilon(3,N)\left(\overset{N}{\underset{i=1}{\otimes}}|a_i b_i\rangle\right)\otimes\left(\overset{N}{\underset{j=1}{\otimes}}|y_j\rangle\right) = \overset{N}{\underset{i=1}{\otimes}}|a_i b_i y_i\rangle, \quad \text{(A14)}$$

$$\Upsilon(3,N)\left[\overset{N}{\underset{k=1}{\otimes}}(M_{\alpha_i}^{A_i}\otimes M_{\beta_i}^{B_i})\right]\left(\overset{N}{\underset{j=1}{\otimes}} M_{\gamma_j}^{Y_j}\right)\Upsilon^{-1}(3,N) = \overset{N}{\underset{i=1}{\otimes}} M_{\alpha_i}^{A_i}\otimes M_{\beta_i}^{B_i}\otimes M_{\gamma_i}^{Y_i}, \quad \text{(A15)}$$

$$\Gamma(3,N)\left(\overset{N}{\underset{i=1}{\otimes}}|a_i b_i\rangle\right)\otimes\left(\overset{N}{\underset{j=1}{\otimes}}|y_j\rangle\right) = \left(\overset{N}{\underset{i=1}{\otimes}}|a_i\rangle\right)\otimes\left(\overset{N}{\underset{j=1}{\otimes}}|y_j\rangle\right)\otimes\left(\overset{N}{\underset{k=1}{\otimes}}|b_k\rangle\right), \quad \text{(A16)}$$

$$\Gamma(3,N)\left[\overset{N}{\underset{k=1}{\otimes}}(M_{\alpha_i}^{A_i}\otimes M_{\beta_i}^{B_i})\right]\left(\overset{N}{\underset{j=1}{\otimes}} M_{\gamma_j}^{Y_j}\right)\Upsilon^{-1}(3,N) = \left(\overset{N}{\underset{i=1}{\otimes}} M_{\alpha_i}^{A_i}\right)\otimes\left(\overset{N}{\underset{j=1}{\otimes}}\otimes M_{\gamma_j}^{Y_j}\right)\otimes\left(\overset{N}{\underset{k=1}{\otimes}} M_{\beta_k}^{B_k}\right). \quad \text{(A17)}$$

More generally, consider the set $\mathbb{Q}_N$ to be a whole permutation of the bit-string $a_1a_2\cdots a_N$, and denote the zth element with a bit-string form $Q(z)=q_1(z)q_2(z)\cdots q_N(z)$. We can always 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 $\mathbb{Q}_N$. That is, we can write a given general swapping transformation $W_N[a_1a_2\cdots a_N\rightarrow q_1(z)q_2(z)\cdots q_N(z)]$,

$$W_N[a_1a_2\cdots a_N\rightarrow q_1(z)q_2(z)\cdots q_N(z)]|a_1a_2\cdots a_N\rangle = |q_1(z)q_2(z)\cdots q_N(z)\rangle. \quad \text{(A18)}$$

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

$$W_N^{-1}[a_1a_2\cdots a_N\rightarrow q_1(z)q_2(z)\cdots q_N(z)]\left(\prod_{i=1}^{N} M^{A_i}\right)\times W_N[a_1a_2\cdots a_N\rightarrow q_1(z)q_2(z)\cdots q_N(z)] = \left(\prod_{i=1}^{N} M^{A_{q_i(z)}}\right). \quad \text{(A19)}$$

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

Here, we would like to prove our protocol of remote implementations of quantum operations belonging to our restricted sets in the cases with more than one qubit.

By using the swapping transformation Υ, we can rewrite the initial state

$$|\Psi_N^{\text{ini}}\rangle = \frac{1}{\sqrt{2^N}}\Upsilon^{-1}(3,N)\sum_{k_1,\ldots,k_N=0}^{1} y_{k_1\cdots k_N}\overset{N}{\underset{m=1}{\otimes}}(|00k_m\rangle+|11k_m\rangle). \quad \text{(B1)}$$

From Bob's preparation, it follows that

$$\begin{aligned}|\Psi^P(b_1,\ldots,b_N)\rangle &= \mathcal{P}_B(b_1,b_2,\ldots,b_N)|\Psi_N^{\text{ini}}\rangle \\ &= \frac{1}{\sqrt{2^N}}\Upsilon^{-1}(3,N)\sum_{k_1,\ldots,k_N=0}^{1} y_{k_1\cdots k_N}\overset{N}{\underset{m=1}{\otimes}}\{\sigma_0 \\ &\quad\otimes[(|b_m\rangle\langle b_m|)C^{\text{not}}(0,1)]\}[(|00k_m\rangle \\ &\quad+|11k_m\rangle)]. \end{aligned} \quad \text{(B2)}$$

Note that

$$\begin{aligned}&\{\sigma_0\otimes[(|b\rangle\langle b|)C^{\text{not}}(0,1)]\}[(|00k\rangle+|11k\rangle)] \\ &= [\sigma_0\otimes(|b\rangle\langle b|)\otimes\sigma_0]\{(|000\rangle+|110\rangle)\delta_{k0}+(|011\rangle \\ &\quad+|101\rangle)\delta_{k1}\} \\ &= (|0b0\rangle\delta_{b0}+|1b0\rangle\delta_{b1})\delta_{k0}+(|0b1\rangle\delta_{b1}+|1b1\rangle\delta_{b0})\delta_{k1} \\ &= [|bb0\rangle(\delta_{b0}+\delta_{b1})\delta_{k0}+|(1-b)b1\rangle(\delta_{b1}+\delta_{b0})\delta_{k1}] \\ &= (\sigma_b\otimes I_4)(\delta_{k0}|0b0\rangle+\delta_{k1}|1b1\rangle) \\ &= (\sigma_b\otimes I_4)(\delta_{k0}+\delta_{k1})|kbk\rangle = (\sigma_b\otimes I_4)|kbk\rangle, \end{aligned} \quad \text{(B3)}$$

where we have used the facts that $\sigma_b|b\rangle=|0\rangle$ and $\sigma_b|1-b\rangle=|1\rangle$ for $b=0,1$. This results in

$$|\Psi^P(b_1,\ldots,b_N)\rangle = \frac{1}{\sqrt{2^N}}\Upsilon^{-1}(3,N)\sum_{k_1,\ldots,k_N=0}^{1} y_{k_1\cdots k_N}\bigotimes_{m=1}^{N}(\sigma_{b_m}\otimes\sigma_0\otimes\sigma_0)|k_m b_m k_m\rangle$$
$$= \frac{1}{\sqrt{2^N}}\left[\bigotimes_{m=1}^{N}(\sigma_{b_m}\otimes\sigma_0)\otimes I_{2^N}\right]\times\sum_{k_1,\ldots,k_N=0}^{1} y_{k_1\cdots k_N}\bigotimes_{m=1}^{N}|k_m b_m k_m\rangle\otimes\bigotimes_{m=1}^{N}|k_m\rangle$$
$$= \frac{1}{\sqrt{2^N}}\left[\bigotimes_{m=1}^{N}(\sigma_{b_m}\otimes\sigma_0)\otimes I_{2^N}\right]\Gamma_N^{-1}\times\sum_{k_1,\ldots,k_N=0}^{1} y_{k_1\cdots k_N}\bigotimes_{m=1}^{N}|k_m\rangle\otimes\bigotimes_{m=1}^{N}|k_m\rangle\otimes\bigotimes_{m=1}^{N}|b_m\rangle, \tag{B4}$$

where Γ_N is defined by

$$\Gamma_N = [I_{2^N}\otimes\Omega(2,N)][\Lambda(2,N)\otimes I_{2^N}] \tag{B5}$$

while $\Lambda(2,N)$ and $\Omega(2,N)$ are defined in Appendix A.

After Alice's sending and Bob's recovery operation, we have

$$|\Psi_N^{\text{final}}(x)\rangle = \frac{1}{\sqrt{2^N}}\Gamma_N^{-1}\sum_{k_1,\ldots,k_N=0}^{1} y_{k_1\cdots k_N}\left(\bigotimes_{m=1}^{N}|a_m\rangle_{A_m}\right)\times\left[\left(\bigotimes_{m=1}^{N}\langle a_m|\right)\left(\bigotimes_{m=1}^{N}H^{A_m}\right)T_N^r(x)\left(\bigotimes_{m=1}^{N}|k_m\rangle\right)\right]\otimes\left[\left(\bigotimes_{m=1}^{N}r(a_m)\right)R_N(x)\left(\bigotimes_{m=1}^{N}|k_m\rangle_{Y_m}\right)\right]\otimes\left(\bigotimes_{m=1}^{N}|b_m\rangle_{B_m}\right). \tag{B6}$$

Thus, Alice's sending step and Bob's recovery operations yield the final state in our interesting subsystem as

$$|\Psi_N^{\text{final}}(x)\rangle = \frac{1}{\sqrt{2^N}}\Gamma_N^{-1}\bigotimes_{m=1}^{N}|a_m\rangle_{A_m}\otimes\left\{\sum_{k_1,\ldots,k_N=0}^{1} y_{k_1\cdots k_N}\times\left[\left(\bigotimes_{m=1}^{N}\langle a_m|\right)\left(\bigotimes_{m=1}^{N}H\right)T_N^r(x,t)\left(\bigotimes_{n=1}^{N}|k_n\rangle\right)\right]\times\left(\bigotimes_{m=1}^{N}r^{Y_m}(a_m)\right)R_N(x)\left(\bigotimes_{m=1}^{N}|k_m\rangle_{Y_m}\right)\right\}\otimes\left(\bigotimes_{m=1}^{N}|b_m\rangle_{Y_m}\right). \tag{B7}$$

It is a key matter that we can prove the relation

$$T_N^r(1,t)R_N(x) = \sum_{m=1}^{2^N} t_m|m,D\rangle\langle m,D|\sum_{n=1}^{2^N}|n,D\rangle\langle p_n(x),D| = \sum_{m=1}^{2^N} t_m|m,D\rangle\langle p_m(x),D| = T_N^r(x,t). \tag{B8}$$

According to the translation from the binary system to the decimal system, we can rewrite t_m as $t_{j_1\cdots j_N}$. So, the diagonal $T_N^r(1,t)$ becomes

$$T_N^r(1) = \sum_{j_1,\ldots,j_N=0}^{1} t_{j_1 j_2\cdots j_N}|j_1 j_2\cdots j_N\rangle\langle j_1 j_2\cdots j_N|. \tag{B9}$$

In addition, we know

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

Substituting them into Eq. (B7), we have

$$|\Psi_N^{\text{final}}(x)\rangle = \frac{1}{\sqrt{2^N}}\Gamma_N^{-1}\bigotimes_{m=1}^{N}|a_m\rangle_{A_m}\otimes\left\{\sum_{j_1,\ldots,j_N=0}^{1}\sum_{k_1,\ldots,k_N=0}^{1}\sum_{l_1,\ldots,l_N} t_{j_1\cdots j_N}y_{k_1\cdots k_N}\times\left(\prod_{m=1}^{N}\langle a_m|H|j_m\rangle\right)\left[\left(\bigotimes_{i=1}^{N}\langle j_m|\right)R_N(x)\left(\bigotimes_{n=1}^{N}|k_n\rangle\right)\right]\times\left[\left(\bigotimes_{m=1}^{N}\langle l_m|\right)R_N(x)\left(\bigotimes_{n=1}^{N}|k_n\rangle\right)\right]\left(\prod_{m=1}^{N}(-1)^{a_m l_m}\right)\times\left(\bigotimes_{m=1}^{N}|l_m\rangle_{Y_m}\right)\otimes\left(\bigotimes_{m=1}^{N}|b_m\rangle_{B_m}\right)\right. . \tag{B11}$$

Because that $R_N(x)$ is such a matrix that its every row and every column only has one nonzero element and its value is 1, we can obtain

$$\left[\left(\bigotimes_{m=1}^{N}\langle j_m|\right)R_N(x)\left(\bigotimes_{m=1}^{N}|k_m\rangle\right)\right]\left[\left(\bigotimes_{m=1}^{N}\langle l_m|\right)R_N(x)\left(\bigotimes_{m=1}^{N}|k_m\rangle\right)\right] = \left(\prod_{m=1}^{N}\delta_{j_m l_m}\right)\left[\left(\bigotimes_{m=1}^{N}\langle j_m|\right)R_N(x)\left(\bigotimes_{m=1}^{N}|k_m\rangle\right)\right]. \tag{B12}$$

Again from

$$\langle a_m|H|j_m\rangle(-1)^{a_m j_m}=\frac{1}{\sqrt{2}} \tag{B13}$$

we can derive

$$\begin{aligned}|\Psi_N^{\text{final}}(x)\rangle=&\frac{1}{\sqrt{2^N}}\Gamma_N^{-1}\bigotimes_{m=1}^{N}|a_m\rangle_{A_m}\\&\otimes\left\{\sum_{j_1,\ldots,j_N}\sum_{k_1,\ldots,k_N=0}^{1}\sum_{l_1,\ldots,l_N}t_{j_1\cdots j_N}y_{k_1\cdots k_N}\right.\\&\left.\times\left[\left(\bigotimes_{m=1}^{N}\langle j_m|\right)R_N(x)\left(\bigotimes_{m=1}^{N}|k_m\rangle_{Y_m}\right)\right]\left(\bigotimes_{m=1}^{N}|j_m\rangle_{Y_m}\right)\right\}\\&\otimes\left(\bigotimes_{m=1}^{N}|b_m\rangle_{B_m}\right)\quad.\end{aligned} \tag{B14}$$

If we directly apply $T_N^r(x,t)$ to the unknown state, we have

$$\begin{aligned}T_N^r(x,t)|\xi\rangle_{k_1\cdots k_N}&=\sum_{k_1,\ldots,k_N=0}^{1}y_{k_1\cdots k_N}T_N^r(1,t)R(x)|k_1k_2\cdots k_n\rangle\\&=\sum_{j_1,\ldots,j_N=0}^{1}\sum_{k_1,\ldots,k_N=0}^{1}t_{j_1\cdots j_N}y_{k_1\cdots k_N}\\&\quad\times\langle j_1j_2\cdots j_N|R(x)|k_1k_2\cdots k_n\rangle\\&\quad\times|j_1j_2\cdots j_N\rangle.\end{aligned} \tag{B15}$$

This means that

$$|\Psi_N^{\text{final}}(x)\rangle=\frac{1}{\sqrt{2^N}}\bigotimes_{m=1}^{N}|a_mb_m\rangle_{A_mB_m}\otimes[T_N^r(x,t)|\xi\rangle_{Y_1\cdots Y_N}]. \tag{B16}$$

Here, we have restored the structure of Hilbert's space by dropping the swapping transformations. Therefore, we finish the proof of our protocol of remote implementations of N qubit operations belonging to our restricted sets.

[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] H. K. Lo, Phys. Rev. A **62**, 012313 (2000).

[4] A. K. Pati, Phys. Rev. A **63**, 014302 (2001).

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

[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. 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**, S384 (2005).

[14] An Min Wang, e-print quant-ph/0509164.

[15] 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).

[16] An Min Wang, e-print quant-ph/05010210.