Science in China Series G: Physics, Mechanics & Astronomy

www.scichina.com
phys.scichina.com
www.springerlink.com

Controlled remote implementation of partially unknown quantum operation

FAN QiuBo† & LIU DongDong

College of Mathematics and Physics, Xuzhou Institute of Technology, Xuzhou 221008, China

A protocol for controlled remote implementation of a partially unknown operation on an arbitrary quantum state is proposed. In this protocol, a task can be performed using a GHZ state shared among three distant parties: Alice, Bob and the controller Charlie. This protocol is also generalized to the multi-party control system based on sharing an *N*-qubit GHZ state.

remote implementation, GHZ state, Hadamard operation

Quantum teleportation and remote state preparation (RSP) are two ingenious applications in the quantum information field. The quantum teleportation process, originally proposed by Bennett et al.[1], may transmit an unknown quantum state from a sender to a spatially distant receiver via a quantum channel with the help of some classical information[2−7]. Two bits of forward classical communication and one ebit of entanglement (a maximally entangled pair of qubits) per teleported qubit are both necessary and sufficient, and neither resource can be traded off against the other. RSP[8−18] is an interesting new method to transmit known pure quantum states using a prior shared entanglement and some classical communication when the sender completely knows the transmitted state. In RSP, the goal is the same as that of quantum teleportation—for the receiver to end up with a single specimen of a state—but here the sender starts with complete classical knowledge of the state.

Teleportation of a quantum operation may be understood as an unknown quantum operation being transferred from a local system to a remote system without physically sending the device. Taking into account quantum teleportation, RSP, and the action of a quantum operation, one can denote it as "remote implementation of operation" (RIO). In recent years, RIO has attracted a lot of attention[19−22]. For example, Wang[19] proposed the protocol of remote implementations of partially unknown quantum operations of multiqubits belonging to the restricted sets. In this protocol, the quantum operation to be remotely implemented belongs to one of the two restricted sets defined by

Received January 5, 2008; accepted March 31, 2008; published online September 1, 2008
doi: 10.1007/s11433-008-0163-x
†Corresponding author (email: fanqiubo@xzit.edu.cn)
Supported by the Natural Science Youth Teacher Foundation of Xuzhou Institute of Technology, China (Grant No. XKY2007317)

$$U_0 = \begin{bmatrix} u_{00} & 0 \\ 0 & u_{11} \end{bmatrix}, \quad U_1 = \begin{bmatrix} 0 & u_{00} \\ u_{11} & 0 \end{bmatrix}. \tag{1}$$

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. Then, Wang[22] proposed a protocol to realize controlled and combined remote implementations of partially unknown quantum operations of multiqubits using N GHZ states.

Recently, the remote application of operators of the form

$$V = \mathrm{e}^{\mathrm{i}\phi_A \boldsymbol{n}_B \cdot \boldsymbol{\sigma}} \tag{2}$$

has been considered[23], where Φ_A is an angle known to Alice, σ a vector with three components $\{\sigma_x, \sigma_y, \sigma_z\}$, and n_{B} the unit vector along a direction known to Bob. The specific feature of the operator V is a splitting of its structure into two parts, and the angle σ is managed by Alice, but the direction n_{B} is governed by Bob. Consequently, Alice can by no means implement V locally by herself. In other words, bidirectional quantum state teleportation (BQST) turns out to be useless in this case.

An interesting protocol of remote application of hidden operators was presented in ref. [21]. In this protocol, Alice and Bob were two distant parties. The remote application was dealt with on Bob's arbitrary quantum state of an operator which was immersed in a lump operator given to Alice. It was shown that the task may be performed using a GHZ state shared between Alice and Bob, and a quantum protocol was proposed to control the task by a number of the third parties on sharing a multipartite GHZ state[24−26].

Here, to enhance security in managing the task, we propose a controlled remote implementation of a partially unknown quantum operation protocol. First, we put forward a protocol for implementation of the partially unknown quantum operation with one controller. Then, we generalize the protocol to the multi-party controlled system.

1 The protocol for implementation of partially unknown quantum operation with one controller

Firstly, for concreteness, suppose the operators U_d (d = 0; 1) (Alice does not know the two operators U_d (d = 0; 1)) that Alice can locally manipulate have the form

$$U_0 = \begin{bmatrix} \mathrm{e}^{\mathrm{i}\phi} & 0 \\ 0 & \mathrm{e}^{-\mathrm{i}\phi} \end{bmatrix}, \quad U_1 = \begin{bmatrix} 0 & \mathrm{e}^{\mathrm{i}\phi} \\ -\mathrm{e}^{-\mathrm{i}\phi} & 0 \end{bmatrix}, \tag{3}$$

with arbitrary real Φ and θ. We 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. The task is to let Alice remotely apply U_d on Bob's qubit $b(\Psi)$ with the controller Charlie. Since U_d is unknown to the sender Alice, we refer to this kind of task as a remote application of the partially unknown quantum operation.

For the sake of clearness, we first consider the three-party case. Alice is set as a sender, Bob as a receiver, and Charlie as a controller. The role of the controller is that Charlie takes the responsibility to decide whether or not and when the task should be done. If for some reasons the controller does not agree on the task, Alice and Bob are unable to start it. In this paper, we present a quantum scheme in which Alice and Bob could go only when all the controllers agree. Thus, the initial state in the joint system composed of qubits controlled by Alice, Bob, and Charlie is as follows:

$$|\chi\rangle_{ABCb} = |GHZ\rangle_{ABC} \otimes |\psi\rangle_b, \tag{4}$$

where

$$|GHZ\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ABC}. \tag{5}$$

Qubit A is held by Alice, qubit B by Bob, and qubit C by Charlie. Bob's qubit b is in an unknown state Ψ (all partners do not know the state of b):

$$|\psi\rangle_b = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1. \tag{6}$$

(i) Step one: Charlie's operation. If Alice and Bob want to do remote implementation of a partially unknown quantum operation, they ask Charlie to carry out a Hadamard operation on C. If Charlie wants Alice and Bob to do remote implementation of the partially unknown quantum operation, he carries out a Hadamard (H) operation on his qubit C; whereas, he does nothing. Suppose Charlie would like to help Alice and Bob, he carries out a Hadamard operation. The Hadamard operation has the form:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{7}$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{8}$$

which transforms the state shown in eq. (4) into

$$|\zeta\rangle_{ABCb} = \frac{1}{\sqrt{2}}[(|00\rangle + |11\rangle)_{AB}|\psi\rangle_b \otimes |0\rangle_C + (|00\rangle - |11\rangle)_{AB}|\psi\rangle_b \otimes |1\rangle_C]. \tag{9}$$

Charlie measures qubit C, and if the outcome is $|0\rangle$ ($|1\rangle$), he will record it as $\kappa = 0(1)$. If he obtains the outcome $|0\rangle_C$, qubits (A; B; b) will collapse into the state

$$|\zeta_0\rangle = \frac{1}{2}(|00\rangle + |11\rangle)_{AB} \otimes |\psi\rangle_b; \tag{10}$$

otherwise, we propose that the state of qubits (A; B; b) be

$$|\zeta_1\rangle = \frac{1}{2}(|00\rangle - |11\rangle)_{AB} \otimes |\psi\rangle_b. \tag{11}$$

After measuring qubit C, Charlie informs Alice and Bob of his measurement results κ (1 classical bit).

(ii) Step two: Bob's preparation. In order to receive the remote control, Bob performs some operations as

$$\omega_B(\eta) = (|\eta\rangle_B\langle\eta| \otimes \sigma_0^b)(\sigma_0^B \otimes |0\rangle_b\langle 0| + \sigma_1^B \otimes |1\rangle_b\langle 1|), \tag{12}$$

that is, Bob sends qubits b and B through a controlled-NOT with b as the control qubit and B the target one. Then Bob measures qubit B in the computational bases $|\eta\rangle_b\langle\eta|$, where $\eta = 0, 1$. If the outcome is $|0\rangle$ ($|1\rangle$), then he will record it as $\eta = 0$ (1), and each occurs with a probability of 1/2. He sends the outcome η to Alice (1 classical bit).

(iii) Step three: Alice's sending. After receiving Bob's (η) and Charlie's (κ) classical bits, Alice first applies the corresponding operation

$$\sigma_u(\sigma_0 = I, \sigma_1 = \sigma_x, \sigma_2 = \mathrm{i}\sigma_y, \sigma_3 = \sigma_z)$$

on her qubit A dependent on $\kappa \oplus \eta$, where $\oplus$ denotes an addition mod 2. As a consequence, the state that Alice and Bob share becomes

$$\left|\zeta^1\right\rangle = (\alpha\left|00\right\rangle + \beta\left|11\right\rangle)_{Ab}. \tag{13}$$

The unknown coefficients α, β of Bob's state are now "visible" to Alice. Next, Alice carries out the quantum operation U_d (i.e. U_0) on qubit A, which transforms $\left|\zeta^1\right\rangle$ to

$$\left|\zeta^2\right\rangle = \frac{1}{\sqrt{2}}(\alpha \mathrm{e}^{\mathrm{i}\phi}\left|00\right\rangle + \beta \mathrm{e}^{-\mathrm{i}\phi}\left|11\right\rangle)_{Ab}. \tag{14}$$

Finally, Alice executes the Hadamard transformation H and measures her qubit on the computational basis $\left|\upsilon\right\rangle_A \left\langle\upsilon\right|$, where $\upsilon = 0, 1$. If she obtains the outcome $\left|0\right\rangle_A$, qubit (b) will collapse into the state

$$\left|\zeta_0^2\right\rangle = \alpha \mathrm{e}^{\mathrm{i}\phi}\left|0\right\rangle_b + \beta \mathrm{e}^{-\mathrm{i}\phi}\left|1\right\rangle_b; \tag{15}$$

otherwise, the state of qubit (b) will be

$$\left|\zeta_1^2\right\rangle = \alpha \mathrm{e}^{\mathrm{i}\phi}\left|0\right\rangle_b - \beta \mathrm{e}^{-\mathrm{i}\phi}\left|1\right\rangle_b. \tag{16}$$

After measuring qubit A, Alice informs Bob of her measurement result υ (1 classical bit[27,28]). If the outcome is $\left|0\right\rangle$ ($\left|1\right\rangle$), recorded by her as $\upsilon = 0(1)$, all of Alice's local operations and measurement are just

$$S_A = \left|\eta\right\rangle_A \left\langle\eta\right|[H^A U_d U_k^A]. \tag{17}$$

(iv) Step four: Bob's recovery. In order to obtain the remote implementation of this quantum operation in a faithful and determined way, Bob has to perform his recovery operation in general. That is, if Alice's measurement result is $\left|0\right\rangle$, then Bob performs a σ_0 operation on qubit b; if Alice's measurement result is $\left|1\right\rangle$, then Bob performs a σ_3 operation on qubit b.

After carrying out the above steps from one to four, we directly obtain U_d $(\alpha\left|0\right\rangle + \beta\left|1\right\rangle)$ in the qubit b of the joint system. The controlled remote implementation of an unknown quantum operation has been successfully completed.

2 The protocol for implementation of partially unknown quantum operation with a multi-party controlled system

This protocol may also be generalized to a multi-party control system. The quantum resource required for that purpose is a $(N + 2)$-qubit GHZ state of the form

$$\frac{1}{\sqrt{2}}\sum_{n=0}^{1}\left|n\right\rangle_B \left|n\right\rangle_A \bigotimes_{p=1}^{N}\left|n\right\rangle_{c_p}, \tag{18}$$

and Bob's qubit b is in

$$\left|\psi\right\rangle_b = \sum_{m=0}^{1}\alpha_m\left|m\right\rangle_b, \tag{19}$$

where $\alpha_0 = \alpha$ and $\beta_1 = \beta$. So the initial state of all the qubits involved reads

$$\frac{1}{\sqrt{2}}\sum_{n,m=0}^{1}\alpha_m\left|n\right\rangle_B \left|n\right\rangle_A \left|m\right\rangle_b \bigotimes_{p=1}^{N}\left|n\right\rangle_{c_p}. \tag{20}$$

If all controllers agree to help Alice and Bob to do remote implementation of the partially unknown quantum operation, C_1, C_2, ..., C_N respectively carry out an H operation on his/her qubit. Then all controllers measure his/her qubit on the basis (0, 1) with the result $|0\rangle$ ($k_p = 0$) or $|1\rangle$ ($k_p = 1$). The initial state eq. (20) is rewritten in the form:

$$\frac{1}{\sqrt{2}} \sum_{n,m=0}^{1} \alpha_m |n\rangle_B |n\rangle_A |m\rangle_b . \tag{21}$$

Bob carries out a CNOT_{bB} (b is the control qubit and B is the target one) to transform the state in eq. (21) to

$$\frac{1}{\sqrt{2}} \sum_{n,m=0}^{1} \alpha_m |n \oplus m\rangle_B |n\rangle_A |m\rangle_b . \tag{22}$$

After the above operation, Bob measures qubit B on the z-basis $(|0\rangle, |1\rangle)$. The state of the two qubits b and A collapses into

$$\sum_{n=0}^{1} \mathrm{e}^{-\mathrm{i}\pi nk} \alpha_{l \oplus n} |l \oplus n\rangle_b |n\rangle_A . \tag{23}$$

At this moment, if all the controllers agree on the task, they tell their measurement results k_p to Alice and Bob. Then Alice calculates the value of k, where

$$k = k_1 \oplus k_2 \oplus \cdots \oplus k_N = \bigoplus_{p=1}^{N} k_p . \tag{24}$$

Bob tells his measurement outcome l to Alice, too. The key point of controlling the task by all the controllers is that Bob needs to know the value of k to decide whether or not to apply σ_z on his qubit b. If one of the controllers refuses to cooperate, the task cannot be started because the value of k is determined by the value of all k_p.

For any possible values of l and k, Alice and Bob are able to establish with certainty the necessary shared state eq. (13) by the operation $(\sigma_z^k \otimes \sigma_z^l)$. So Alice and Bob may also realize controlled remote implementation of the partially unknown operation. The working scheme of the controlled remote application of the partially unknown quantum operation is illustrated in Figure 1.

3 Discussion and conclusions

In conclusion, we proposed a protocol for controlled remote implementation of a partially unknown operation on an arbitrary quantum state with local operation and classical communication. The main differences between controlled RIO and controlled teleportation (quantum state sharing) are: (1) The goal is different. The purpose of controlled RIO is to let the sender do remote implementation of the unknown operation on an arbitrary quantum state with the help of the controller, while in controlled teleportation (quantum state sharing) Alice sends an unknown quantum state to the receiver with the help of the controller. (2) In controlled RIO, Alice need not know the operation that she carries out remote implementation, while in controlled teleportation (quantum state sharing) Alice must own the teleported state. Compared with the previous protocol[22], the present one has some difference. That is, in our protocol, for a multi-party control system, we use one N-qubit GHZ state as a quantum channel. But in the protocol given in ref. [22], N GHZ states are needed. We can say that different quantum resources have different features in quantum information processing and communications. The obvious advantage in our protocol is that the sources are

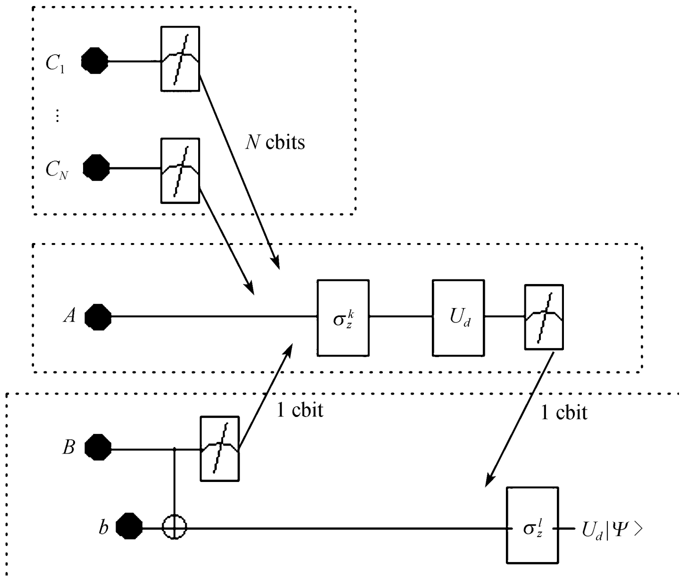

Figure 1 The quantum scheme for remote implementation of a partially unknown quantum operation.

saved. So, we hope that using the existing technology it is possible to realize the controlled remote implementation of a partially unknown quantum operation protocol with ease.

We would like to thank Drs. Xia Yan and Song Jie for useful discussions, and acknowledge the valuable suggestions from the peer reviewers.

1 Bennett C H, Brassard G, Crepeau C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys Rev Lett, 1993, 70(13): 1895—1899
2 Xia Y, Fu C B, Zhang S, et al. Probabilistic teleportation of an arbitrary three-particle state via a partial entangled four-particle state and a three-particle GHZ state. J Korean Phys Soc, 2005, 46(2): 388—392
3 Xia Y, Song J, Song H S. Quantum dialogue using non-maximally entangled states based on entanglement swapping. Phys Scr, 2007, 76: 363—369
4 Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A, 2003, 68(4): 042317-1—4
5 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69(5): 052319-1—4
6 Wang C, Deng F G, Li Y S, et al. Quantum secure direct communication with high-dimension quantum superdense coding. Phys Rev A, 2005, 71: 044305-1—4
7 Wang C, Deng F G, Long G L. Multi-step quantum secure direct communication using multiparticle Greenberger-Horne-Zeeilinger state. Opt Commun, 2005, 253(1): 15—20
8 Lo H K. Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity. Phys Rev A, 2000, 62(1): 012313-1—4
9 Pati A K. Minimum classical bit for remote preparation and measurement of a qubit. Phys Rev A, 2001, 63(1): 014302
10 Bennett C H, DiVincenzo D P, Shor P W, et al. Remote state preparation. Phys Rev Lett, 2001, 87(7): 077902-1—4
11 Ye M Y, Zhang Y S, Guo G C. Faithful remote state preparation using unite classical bits and a nonmaximally entangled state. Phys Rev A, 2004, 69(2): 022310-1—5
12 Dai H Y, Chen P X, Liang L M, et al. Classical communication cost and remote preparation of the four-particle GHZ class state. Phys Lett A, 2006, 355(4-5): 285—288
13 Xia Y, Song J, Song H S. Multiparty remote state preparation. J Phys B: At Mol Opt Phys, 2007, 40: 3719—3724
14 Yu C S, Song H S, Wang Y H. Remote preparation of a qudit using maximally entangled states of qubits. Phys Rev A, 2006, 73: 022340-1—4

15 Zeng B, Zhang P. Remote-state preparation in higher dimension and the parallelizable manifold S^{n-1}. Phys Rev A, 2001, 65(2): 022316-1－4

16 Wang D, Liu Y M, Zhang Z J. Remote preparation of a class of three-qubit states. Opt Commun, 2007, 281(4): 871－875

17 Xiang G Y, Li J, Bo Y, et al. Remote preparation of mixed states via noisy entanglement. Phys Rev A, 2005, 72: 012315-1－4

18 Liu W T, Wu W, Ou B Q, et al. Experimental remote preparation of arbitrary photon polarization states. Phys Rev A, 2007, 76: 022308-1－4

19 Wang A M. Remote implementations of partially unknown quantum operations of multiqubits. Phys Rev A, 2006, 74: 032317-1－6

20 Zhao N B, Wang A M. Hybrid protocol of remote implementations of quantum operations. Phys Rev A, 2007, 76: 062317-1－7

21 An N B. Remote application of hidden operators. Phys Lett A, 2007, 364(3-4): 198－202

22 Wang A M. Controlled and combined remote implementations of partially unknown quantum operations of multiqubits using GHZ states. arXiv: quant-ph/0510210

23 Groisman B, Reznik B. Implementing nonlocal gates with nonmaximally entangled states. Phys Rev A, 2005, 71: 032322-1－4

24 Xia Y, Song J, Song H S. Linear optical protocol for preparation of N-Photon Greenberger-Horne-Zeeilinger state with conventional detectors. Appl Phys Lett, 2008, 92: 021127-1－3

25 Xia Y, Song H S. Controlled quantum secure direct communication using a non-symmetric quantum channel with quantum superdense coding. Phys Lett A, 2007, 364: 117－122

26 Su X L, Jia X J, Xie C D, et al. Generation of GHZ-like and cluster-like quadripartite entangled states for continuous variable using a set of quadrature squeezed states. Sci China Ser G-Phys Mech Astron, 2008, 51(1): 1－13

27 Yang Y G, Wen Q Y. Threshold quantum secure direct communication without entanglement. Sci China Ser G-Phys Mech Astron, 2008, 51(2): 176－183

28 Ye M Y, Zhang Y S, Guo G C. Quantum entanglement and quantum operation. Sci China Ser G-Phys Mech Astron, 2008, 51(1): 14－21