Control power of a high-dimensional controlled nonlocal quantum computation

Neng-Fei Gong,[1] Tie-Jun Wang,[1,2,*] and Shohini Ghose[2,3,†]

[1] *School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2] *Department of Physics and Computer Science, Wilfrid Laurier University, Waterloo, Ontario N2L 3C5, Canada*
[3] *Institute for Quantum Computing, University of Waterloo, Ontario N2L 3G1, Canada*

(Received 21 January 2021; accepted 12 April 2021; published 4 May 2021)

We propose a scheme for a high-dimensional nonlocal controlled quantum computation network. A client with limited quantum technology can control a distributed computation between two quantum servers in a secure manner, such that the client's computational information remains private. We define a measure to quantify the client's control power when performing nonlocal quantum gates. We find that, given the same channel resources, the client's control power over nonlocal quantum gate operations between quantum servers is much greater than that of quantum state transfer between quantum servers. Our scheme prevents quantum servers in the network from stealing each other's information or jointly stealing the client's information. Our protocol provides new avenues for building quantum computing networks and methods to develop the resource theory of quantum channels.

DOI: 10.1103/PhysRevA.103.052601

I. INTRODUCTION

Networked or distributed quantum computing [1,2] composed of less powerful quantum computers can improve computing potential and solve large and complex quantum computing tasks. Quantum entanglement [3–5] between nodes of the network can link nonlocal quantum processors over large distances in a hierarchical and secure fashion. It can be used to realize basic components of nonlocal quantum computing, such as two-qubit controlled gates that have numerous applications [6–9]. In 2000, Eisert *et al.* [10] investigated the minimal resources for implementing a nonlocal CNOT gate. Guo *et al.* [11] proposed a scheme for a nonlocal swap operation and a nonlocal gate using cavity quantum electrodynamics [12]. Since then, a large number of theoretical schemes have been proposed to construct various nonlocal quantum gates [13–15], and much effort has been devoted to the implementation of nonlocal gates with less entanglement resources [16–18]. Nonlocal CNOT gate was experimentally realized on photonic qubits [19] and in other physical systems [19,20]. In 2017, the world record for quantum entanglement distribution over a distance of 1200 kilometers [21] was achieved, and subsequently in 2018, the first intercontinental quantum key distribution was completed [22]. These advances are stepping stones toward the future construction of entanglement-based large-scale quantum computing networks.

A practical quantum computing network would allow ordinary clients to connect to distributed networks using classical or quantum communication technologies. Quantum networks with third parties were first discussed for communication schemes such as quantum secret sharing [23] and controlled state teleportation [24]. In these applications, the third party ensures the security of communication. A third party controller can permit or restrict successful quantum state transfer from the sender to the receiver but is not the owner of the information transferred. However, in a quantum computing network, the third party (the client) is the owner and sender of calculation information, i.e., algorithm information and initial computing states. Given the client's dual identity (sender and controller) in the quantum computing network, there are two measures that can be used to assess the performance of the network based on the client's needs. The first measure is the security of the client's information; when uploading calculation information to the computing network, the client can either encrypt the initial computing state, or encrypt the algorithm. The second measure is the control power of the client, when the client is either controlling quantum state transfer or controlling quantum operations between two quantum servers.

To satisfy the security requirement, the client should have the ability to prevent any subserver in the quantum computing network from stealing the information of other servers, or all quantum servers in the network jointly from stealing the client's confidential quantum algorithm information. One of the most remarkable achievements in this field is blind quantum computation (BQC) [25–29]. This is an effective method for a client who has limited quantum (or completely classical) computational power or memory to delegate the computation to remote quantum servers without leaking any information about the client's input and computational task [25]. In the field of secure quantum computation with multiple parties, Elham [30] proposed the secure multiplayer quantum computation based on the BQC protocol. In 2020, Dulek *et al.* [31] generalized the multiparty quantum computation protocol for k players, against $k-1$ colluding players. BQC has been demonstrated in an optical experiment [20] using Bell states shared by two servers [32]. In this case, the client can be totally classical as long as the quantum servers do not

[*] wangtiejun@bupt.edu.cn
[†] sghose@wlu.ca

communicate with each other through classical channels [25,29,32]. However, it is unrealistic to prevent two powerful quantum servers from communicating. In 2014, Li *et al.* proposed a three-server BQC scheme that satisfies the client's computing and security needs even with communication between the servers [33], but the cost of this scheme is that at least three quantum servers are needed with quantum channels.

Assuming that security can be guaranteed, the control power of the remote controllable quantum computing operation must also be assessed. In quantum communication, there have been many studies of the control power of the third party for quantum state transfer between two quantum servers [34–40]. To our knowledge, there has been no quantitative analysis of the control capabilities of clients in quantum computing networks. In this paper, we propose a method for clients to remotely control quantum gate operations between two quantum servers while ensuring security of the protocol as well as providing the client with control power to supervise the entire computing process.

We describe a scheme for the client to securely implement a nonlocal quantum gate between two remote servers using a tripartite entangled quantum state. To analyze the client's supervision capabilities more clearly, we introduce the concept of control power in controlled nonlocal gate operations. We find that, in higher dimensions, using the same channel resources, the client's control of nonlocal quantum gates between quantum servers is much greater than that of quantum state transfer between the quantum servers. This means that, when clients connect into distributed computing networks, encrypting the algorithm can be more effective for control than encrypting the initial state. In addition, through a security-checking strategy, the client can prevent quantum servers in the network from stealing each other's information or jointly stealing the algorithm information. Furthermore, we do not need to assume that classical communication is forbidden between servers. The cost of the security is that the client must have the ability to perform single-qudit measurements, but any additional quantum computational power or quantum memory is not necessary.

II. ARBITRARY DIMENSIONAL PERFECT NONLOCAL CONTROLLED PHASE GATE

We first construct a client-controlled nonlocal controlled phase gate scheme between two quantum servers. We choose the nonlocal controlled phase (CP) gate because the CP gate is a symmetrical gate in which quantum computing servers implement the same gate operations. This makes it useful for analyzing the relation between the channel parameters and gate fidelities. Moreover, it is a basic quantum logic operation unit of quantum computing, an arbitrary quantum circuit can be decomposed into CP gates and single qubit operations, allowing universal quantum computation in d-level systems [41].

The scheme for the nonlocal CP gate controlled by a client is shown in Fig. 1. Two remote quantum servers, Alice and Bob, have the qudits A and B, respectively. The initial state of qudits AB is set as $|\psi\rangle^{in} = \sum_{p=0}^{d-1} \alpha_p |p\rangle_A \otimes \sum_{p'=0}^{d-1} \beta_{p'} |p'\rangle_B$. The third party Charlie, as a client, wants to nonlocally perform a d-dimensional CP gate on qudit A and B, which is written as $U_{CP}^{AB}|\psi\rangle^{in} = \sum_{p,p'=0}^{d-1} \alpha_p \beta_{p'} e^{\frac{2\pi}{d} i(n_1 p + n_2 p' - pp')} |pp'\rangle_{AB}$. Here, n_1 (or n_2) is the private algorithm information encoded by Charlie. For selective implementation of such a nonlocal d-dimensional CP gate between two remote quantum servers, the client Charlie should share a three-qudit (abc) entangled quantum channel $|\psi_0\rangle_{abc}$ with them (with the qudit a distributed to Alice, b to Bob, and c to Charlie). For convenience and without loss of generality, we write such a channel state as

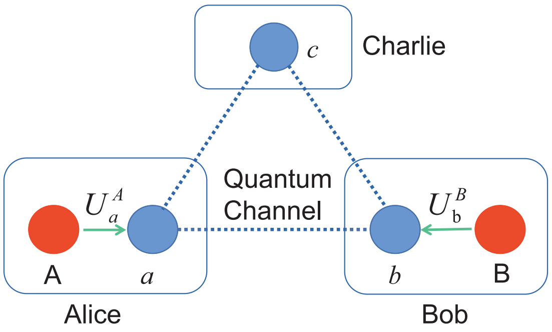


FIG. 1. Diagram showing client's (Charlie's) controlled participation in nonlocal quantum gates. Alice and Bob are two quantum servers with quantum computers, and they can execute local two-qudit unitary operation on their qudits. The three blue discs connected with dotted lines represent the tripartite (abc) entangled quantum channel. Alice and Bob can also send and receive classical information through classical channels. Qudits A and B represent the quantum memory units which can perform quantum computing.

$$|\psi_0\rangle_{abc} = \frac{1}{d\sqrt{d'}} \sum_{k=0}^{d'-1} |k\rangle_c \sum_{l,m=0}^{d-1} (\sigma_{a,z})^{\nu(k)} \times \otimes (\sigma_{b,z})^{\nu'(k)} e^{\frac{2i\pi}{d} lm} |lm\rangle_{ab}, \tag{1}$$

where d is the dimension of the qudit a or b, and $d' \geqslant d$ is the dimension of the qudit c. Here, $\sigma_{K,z}^n = \sum_{j=0}^{d-1} e^{\frac{2\pi i}{d} jn} |j\rangle_K \langle j|$, $K = a,\ b,\ c,\ A$, or B.

To achieve the nonlocal CP operation, simultaneously, Alice and Bob perform the two different d-dimensional controlled-flip operations $U(-)_a^A$ and $U(+)_b^B$ on qudit pairs Aa and Bb, respectively:

$$|p\rangle_A |l\rangle_a \xrightarrow{U(-)_a^A} |p\rangle_A |l-p\rangle_a, \quad |p'\rangle_B |m\rangle_b \xrightarrow{U(+)_b^B} |p'\rangle_B |m+p'\rangle_b. \tag{2}$$

To achieve the nonlocal CP operation, the quantum channel $|\psi\rangle_{abc}$ should be designed based on private algorithm information (n_1, n_2) desired by the client. Next we describe the specific implementation of the nonlocal controlled CP gate using three different channels.

A. Channel I

By setting $d = d'$, $k = l$, $\nu(k) = 0$, and $\nu'(k) = 0$, the channel is a d-dimensional GHZ-type state of the form

$$|\psi\rangle_{abc} = \frac{1}{d} \sum_{l,m=0}^{d-1} e^{\frac{2\pi i}{d} lm} |lml\rangle_{abc}. \tag{3}$$

This is easy to achieve by using an additional d-dimensional discrete Fourier transform operation ($|l\rangle \rightarrow \frac{1}{\sqrt{d}}\sum_{m=0}^{d-1} e^{\frac{2\pi i}{d}lm}|m\rangle$) on qudit b of a standard Greenberger-Horne-Zeilinger (GHZ) state $\frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}|lll\rangle_{abc}$.

To implement the nonlocal CP gate $U(n)$ (n is a d-dimensional private algorithm information encoded by Charlie) given by

$$U(n)|\psi\rangle^{in} \rightarrow \sum_{p,p'=0}^{d-1} e^{\frac{2\pi i}{d}(pn-pp')}\alpha_p|p\rangle_A\beta_{p'}|p'\rangle_B, \tag{4}$$

between qudits A and B, Alice and Bob simultaneously perform the two different d-dimensional controlled-flip operations $U(-)_a^A$ and $U(+)_b^B$ on qudit pairs Aa and Bb, respectively. Then Alice and Bob measure the qudits a and b in the z basis $\{|l'\rangle_a\}$ and $\{|m'\rangle_b\}$ (here, $l' = l - p$ and $m' = m + p'$) and they make the measurement outcome results public via a classical channel. If Alice and Bob's outcome is $|l'm'\rangle_{ab}$, the state of the system becomes

$$\begin{aligned}&\sum_{p,p'=0}^{d-1}\alpha_p\beta_{p'}|p\rangle_A|p'\rangle_B e^{\frac{2\pi}{d}i(l'+p)(m'-p')}|l'+p\rangle_c\\ &\quad= \sigma_{B,z}^{d-l'}\sigma_{A,z}^{m'}\sum_{p,p'=0}^{d-1} e^{\frac{2\pi i}{d}(m'l'-p'p)}\alpha_p\beta_{p'}|p\rangle_A|p'\rangle_B|l'+p\rangle_c,\end{aligned} \tag{5}$$

where $\sigma_{K,z}^{n} = \sum_{j=0}^{d-1} e^{\frac{2\pi i}{d}jn}|j\rangle_K\langle j|$. With these measurement results, Alice and Bob can rotate the state of the system ABc into the state $\sum_{p,p'=0}^{d-1} e^{-\frac{2\pi}{d}ip'p}\alpha_p\beta_{p'}|p\rangle_A|p'\rangle_B|l'+p\rangle_c$ via appropriate unitary operations according to Eq. (5). At the same time, Charlie measures qudit c in the x basis $\{|\tilde{k}\rangle_c^x\}$ ($|k\rangle_c = \frac{1}{\sqrt{d}}\sum_{\tilde{l}=0}^{d-1} e^{\frac{2\pi i}{d}k\tilde{k}}|\tilde{k}\rangle_c^x$). The state of the system ABc becomes

$$\sum_{p,p'=0}^{d-1} e^{-\frac{2\pi i}{d}p'p}\alpha_p\beta_{p'}|p\rangle_A|p'\rangle_B\frac{1}{\sqrt{d}}\sum_{\tilde{k}=0}^{d-1} e^{\frac{2\pi i}{d}(l'+p)\tilde{k}}|\tilde{k}\rangle_c^x. \tag{6}$$

If Charlie's outcome is $|\tilde{k}\rangle_c^x$, Alice and Bob will share a state of the form

$$e^{\frac{2\pi i}{d}\tilde{k}l'}\sum_{p=0}^{d-1} e^{\frac{2\pi i}{d}p\tilde{k}}\alpha_p|p\rangle_A\sum_{p'=0}^{d-1} e^{-\frac{2\pi i}{d}pp'}\beta_{p'}|p'\rangle_B. \tag{7}$$

By ignoring the overall phase and performing the single-qudit operation $\sigma_{A,z}^{d-\tilde{k}+n}$ on qudit A, the state of qubits AB can be transformed into Eq. (4), which is the standard form of a d-dimensional controlled phase gate.

During the entire process of nonlocal gating, Charlie does not disclose his measurement results $\tilde{k}$ to Alice and Bob. He only tells Alice the operation $\sigma_{A,z}^{d-\tilde{k}+n}$. With information about $(d-\tilde{k}+n)$ and the information in any one person's possession, neither Alice nor Bob can know the value of n. That is, only Charlie knows what kind of CP gate operation Alice and Bob are implementing. But if Alice and Bob work together to jointly measure the state they have, they can know what kind of CP gate operation (the value of n) is finally implemented. Therefore, Charlie needs to introduce a security checking process to find out whether whether Alice and Bob are jointly stealing the algorithm. We will describe this step in Sec. IV.

B. Channel II

By setting $d = d'$, and $\nu(k) = \nu'(k) = k$, the channel is a d-dimensional GHZ-type state of the form

$$|\psi'\rangle_{abc} = \frac{1}{d}\sum_{m,l'=0}^{d-1} e^{\frac{2\pi i}{d}(mk)}|mk\rangle_{bc}\frac{1}{\sqrt{d}}\sum_{l=0}^{d-1} e^{\frac{2\pi i}{d}l(k+m)}|l\rangle_a. \tag{8}$$

By using the inverse change of d-dimensional discrete Fourier transform operation ($\frac{1}{\sqrt{d}}\sum_{m=0}^{d-1} e^{\frac{2\pi i}{d}lm}|m\rangle \rightarrow |l\rangle$) on qudit a, the state of $|\psi'\rangle_{abc}$ becomes

$$|\psi_x'\rangle_{abc} = \frac{1}{\sqrt{d}}\sum_{l'=0}^{d-1}|B(k,k)\rangle_{ba}|k\rangle_c, \tag{9}$$

where $|B(u,v)\rangle = \frac{1}{\sqrt{d}}\sum_{m=0}^{d-1} e^{\frac{2\pi i}{d}mu}|m\rangle_b \otimes |m+v\rangle_a$ is the d-dimensional Bell state. Here, $v = 0, 1, 2, \ldots, d-1$ (where $m+v$ must be taken modulo d) denotes the bit information of the two-particle state and $u = 0, 1, 2, \ldots, d-1$ represents the relative phase information.

To implement the nonlocal CP gate $U(n_1, n_2)$ (n_1, n_2 are the d-dimensional private algorithm information encoded by Charlie) given by

$$U(n_1,n_2)|\psi\rangle^{in} \rightarrow \sum_{p,p'=0}^{d-1} e^{\frac{2\pi i}{d}(pn_1+p'n_2-pp')}\alpha_p|p\rangle_A\beta_{p'}|p'\rangle_B, \tag{10}$$

between qudits A and B, Alice and Bob simultaneously perform the two different d-dimensional controlled-flip operations $U(+)_a^A$ and $U(-)_b^B$ on qudit-pairs Aa and Bb, respectively. Then Alice and Bob measure the qudits a and b in the z basis $\{|l'\rangle_a\}$ and $\{|m'\rangle_b\}$, and they make the measurement outcome results public via a classical channel.

If the measurement result of qudits ab is $|00\rangle_{ab}$, the state of the three-qudit system ABc becomes

$$\begin{aligned}&\sum_{p'=0}^{d-1}\beta_{p'}|p'\rangle_B\sum_{p=0}^{d-1} e^{-\frac{2\pi i}{d}(p+p')p'}\alpha_p|p\rangle_A|d-p-p'\rangle_c\\ &\quad= \sum_{p'=0}^{d-1}\beta_{p'}e^{-\frac{2\pi i}{d}p'^2}|p'\rangle_B\sum_{p=0}^{d-1} e^{-\frac{2\pi i}{d}pp'}\alpha_p|p\rangle_A|d-p-p'\rangle_c.\end{aligned} \tag{11}$$

By performing the single-qudit operation $\sigma_{B,z}^{s} = \sum_{j=0}^{d-1} e^{\frac{2\pi i}{d}j^2}|j\rangle_B\langle j|$ on qudit B, the state of qudits ABc can be transformed into

$$\sum_{p,p'=0}^{d-1} e^{-\frac{2\pi i}{d}pp'}\beta_{p'}|p'\rangle_B\alpha_p|p\rangle_A|d-p-p'\rangle_c. \tag{12}$$

At same time, Charlie measures qudit c in the x basis $\{|\tilde{k}\rangle_c^x\}$. The state shared by Alice and Bob becomes

$$\begin{aligned}&\sum_{p'=0}^{d-1}\beta_{p'}|p'\rangle_B\sum_{p=0}^{d-1}e^{-\frac{2\pi i}{d}pp'}\alpha_p|p\rangle_A\frac{1}{\sqrt{d}}\sum_{\tilde{l}=0}^{d-1}e^{-\frac{2\pi i}{d}(p+p')\tilde{k}}|\tilde{k}\rangle_c^x\\&=\frac{1}{\sqrt{d}}\sum_{\tilde{k}=0}^{d-1}|\tilde{k}\rangle_c^x\sigma_{A,z}^{d-\tilde{k}}\sigma_{B,z}^{d-\tilde{k}}\left(\sum_{p,p'=0}^{d-1}e^{-\frac{2\pi i}{d}pp'}\alpha_p\beta_{p'}|p\rangle_A|p'\rangle_B\right).\end{aligned}\tag{13}$$

If Charlie's outcome is $|\tilde{k}\rangle$, Alice and Bob will share the state

$$\sigma_{A,z}^{d-\tilde{k}}\sigma_{B,z}^{d-\tilde{k}}\sum_{p'=0}^{d-1}\beta_{p'}|p'\rangle_B\sum_{p=0}^{d-1}e^{-\frac{2\pi i}{d}pp'}\alpha_p|p\rangle_A.\tag{14}$$

By asking Alice and Bob to perform the single-qudit operation $\sigma_{A,z}^{\tilde{k}+n_1}\sigma_{B,z}^{\tilde{k}+n_2}$ on qudits AB, the state of qubits AB can be transformed into Eq. (10). If the measurement results of qudits ab is $|l'm'\rangle_{ab}$, Alice should perform $\sigma_{A,z}^{m'}$ on qudit A, and Bob should perform the $\sigma_{B,z}^{s}\sigma_{B,z}^{m'-l'}$ on qudit B. After Charlie measures his qudit c in the x basis, he asks Alice and Bob to perform the single-qudit operations $\sigma_{A,z}^{\tilde{k}+n_1}\sigma_{B,z}^{\tilde{k}+n_2}$ on qudits AB, and the system ABc is collapsed into the state Eq. (10) with overall phase $e^{\frac{2\pi i}{d}(m'+\tilde{k})(l'-m')}$.

During the process, Charlie does not disclose his measurement results $\tilde{k}$ to Alice and Bob, and only tells Alice and Bob the corresponding operations $\sigma_{A,z}^{\tilde{k}+n_2}$ and $\sigma_{B,z}^{\tilde{k}+n_1}$, respectively. Without the information of $\tilde{k}$, Alice or Bob cannot know the value of n_1, n_2, or n_1+n_2 with only the information in any one person's possession. That is, only Charlie will know what kind of CP gate operation Alice and Bob are implementing. But if Alice and Bob work together to measure jointly the state in their hands, they can know what kind of CP gate operation (the value of n_1+n_2) is finally implemented. Therefore, as in the previous case, Charlie must introduce an additional security checking process, as described in Sec. IV.

C. Channel III

By setting $d'=d^2$, the basis state of qudit c is $|k_1'\rangle_{c_1}\otimes|k_2'\rangle_{c_2}$, $\nu(k_1)=k_1$, and $\nu'(k_2)=k_2$, the channel is a d-dimensional GHZ-type state of the form

$$\begin{aligned}|\psi''\rangle_{abc}&=\frac{1}{d^2}\sum_{l,m,k_1,k_2=0}^{d-1}e^{\frac{2\pi i}{d}lm}e^{\frac{2\pi i}{d}k_1l}e^{\frac{2\pi i}{d}k_2m}|lmk_1k_2\rangle_{abc_1c_2}\\&=\frac{1}{d^2}\sum_{l,m,k_1,k_2=0}^{d-1}e^{\frac{2\pi i}{d}lm}\sigma_{a,z}^{k_1}\sigma_{b,z}^{k_2}|lmk_1k_2\rangle_{abc_1c_2}.\end{aligned}\tag{15}$$

This state is also a perfect channel for the client to perform a nonlocal controlled CP gate between Alice and Bob. To implement the nonlocal CP gate $U(n_1,n_2)$ between qudits A and B, Alice and Bob simultaneously perform the two different d-dimensional controlled-flip operations $U(-)_a^A$ and $U(+)_b^B$ on qudit pairs Aa and Bb, respectively. Then the state of the whole system $ABabc$ becomes

$$\begin{aligned}&\frac{1}{d^2}\sum_{p,p',l',m',k_1,k_2=0}^{d-1}e^{\frac{2\pi i}{d}(l'+p)(m'-p')}e^{\frac{2\pi i}{d}k_1(l'+p)}\\&\quad\times\otimes e^{\frac{2\pi}{d}k_2(m'-p')}\alpha_p|p\rangle_A\beta_{p'}|p'\rangle_B|l'm'k_1k_2\rangle_{abc_1c_2}\\&=\frac{1}{d^2}\sum_{p,p',l',m',k_1,k_2=0}^{d-1}e^{\frac{2\pi i}{d}(l'm'+k_1l'+k_2m')}\sigma_{A,z}^{(m'+k_1)}\\&\quad\times\otimes\sigma_{B,z}^{(d-l'-k_2)}\alpha_p|p\rangle_A\beta_{p'}e^{-\frac{2\pi i}{d}pp'}|p'\rangle_B|l'm'k_1k_2\rangle_{abc_1c_2},\end{aligned}\tag{16}$$

where $m'=m+p'$ and $l'=l-p$. Alice and Bob measure the qudits a and b in the z basis $\{|l'\rangle_a\}$ and $\{|m'\rangle_b\}$, and they make the measurement outcomes public via a classical channel.

If the measurement result of qudits ab is $|00\rangle_{ab}$, the state of the three-qudit system ABc becomes

$$\begin{aligned}|\phi''\rangle_{ABc}=\frac{1}{d}\sum_{p,p',k_1,k_2=0}^{d-1}&e^{\frac{2\pi i}{d}(k_1p-k_2p'-pp')}\alpha_p\beta_{p'}|p\rangle_A\\&\times\otimes|p'\rangle_B|k_1k_2\rangle_{c_1c_2}.\end{aligned}\tag{17}$$

At the same time, Charlie measures qudit c_1 in the z basis $\{|k_1\rangle_{c_1}\}$ and qudit c_2 in the z basis $\{|k_2\rangle_{c_2}\}$. If Charlie's outcome is $|k_1\rangle_{c_1}|k_2\rangle_{c_2}$, Alice and Bob will share a state in the form

$$\sigma_{A,z}^{k_1}\sigma_{B,z}^{d-k_2}\left(\sum_{p,p'=0}^{d-1}e^{-\frac{2\pi i}{d}pp'}\alpha_p\beta_{p'}|p\rangle_A|p'\rangle_B\right).\tag{18}$$

By performing the single qudit operations $\sigma_{A,z}^{d-k_1+n_1}\sigma_{B,z}^{k_2+n_2}$ on qudits AB, the state of qubits AB can be transformed into Eq. (10). If the measurement results of qudits ab is $|l'm'\rangle_{ab}$, Alice and Bob can rotate the state of the system AB into the state Eq. (10) with an overall phase of $e^{\frac{2\pi i}{d}(l'm'+k_1l'+k_2m')}$ by using appropriate unitary operations according to their measurement results and Charlie's instructions.

In the entire process, Charlie does not disclose his measurement results k_1 and k_2 to Alice and Bob but only tells them the corresponding operations $\sigma_{A,z}^{d-k_1+n_1}$ and $\sigma_{B,z}^{k_2+n_2}$, respectively. Without the information of k_1 and k_2, Alice or Bob cannot know the value of n_1 or n_2 using just their individual information. Only Charlie will know what kind of CP gate operation Alice and Bob are implementing. But if Alice and Bob work together to jointly measure the state, they can know what kind of CP gate operation (the value of n_1 and n_2) is implemented. Hence, Charlie needs to perform security checking as described in Sec. IV.

III. CONTROL POWER OF THE CLIENT

The client's control power is an important measure of the degree of client's supervision and hence the effectiveness of our scheme. We learn from the definition of control power in controlled teleportation [34], and analogously define the control power P of the client as the difference between two different nonlocal CP gate fidelities [37],

$$P=f_{CQT}-f_{NC}.\tag{19}$$

Here f_{CQT} is the conditioned fidelity, which is the nonlocal gate fidelity with the client's complete involvement, and f_{NC} is the nonconditioned fidelity, which is the nonlocal gate fidelity without the client's involvement. In our scheme, f_{CQT} is equal to 1 when using the perfect three-qudit quantum channels described in the previous section. f_{NC} is calculated to be

$$f_{NC} = \frac{\int \langle\psi_t|\rho_{AB}^{out}|\psi_t\rangle d\sigma_A d\sigma_B}{\int d\sigma_A d\sigma_B}, \tag{20}$$

where $|\psi_t\rangle$ is the correct form of the target operation, and σ_A and σ_B are integral elements for the normalization coefficient α_p and $\beta_{p'}$, respectively. ρ_{AB}^{out} is the reduced density matrix of system after nonlocal gating operation by tracing over the control qudit c.

The initial system is a product of qudit A and B in state $|\psi_{AB}\rangle$, with an auxiliary two-qudit state $\rho_{ab} = tr_c[\rho_{abc}]$. ρ_{abc} is the density matrix of the quantum channel. Alice executes local $U(-)_a^A$ gate on Aa, and Bob executes local $U(+)_b^B$ gate on Bb. If the measurement result of qudits a and b is $|lm\rangle_{ab}$, leaving AB in state ρ_{AB}^{out},

$$\begin{aligned}\rho_{AB}^{out} &= d^2\langle lm|U(-)_a^A U(+)_b^B|\psi_{AB}\rangle\langle\psi_{AB}|\rho_{ab}\\ &\quad\times\otimes U(-)_a^{A\dagger} U(+)_b^{B\dagger}|lm\rangle.\end{aligned} \tag{21}$$

The elements of this matrix can be written as

$$\begin{aligned}\langle ij|\rho_{AB}^{out}|i'j'\rangle &= d^2\langle ij|\langle lm|U(-)_a^A U(+)_b^B|\psi_{AB}\rangle\langle\psi_{AB}|\rho_{ab}\otimes U(-)_a^{A\dagger} U(+)_b^{B\dagger}|lm\rangle|i'j'\rangle\\ &= d^2\langle ij|\langle(l-i)(m+j)|\psi_{AB}\rangle\langle\psi_{AB}|\rho_{ab}\otimes|(l-i')(m+j')\rangle|i'j'\rangle\\ &= d^2\langle ij|\psi_{AB}\rangle\langle\psi_{AB}|i'j'\rangle\otimes\langle(l-i)(m+j)||\rho_{ab}\otimes|(l-i')(m+j')\rangle.\end{aligned} \tag{22}$$

Here, $|ij\rangle$ and $|i'j'\rangle$ are the eigenstates of the two-qudit system AB. When $l=0, m=0$, $\langle ij|\rho_{AB}^{out}|i'j'\rangle = d^2\langle ij|\psi_{AB}\rangle\langle\psi_{AB}|i'j'\rangle\otimes\langle(d-i)j|\rho_{ab}|(d-i')j'\rangle$. For example, in the two-dimensional case, the form of matrix ρ_{AB}^{in} is

$$\rho_{AB}^{in} = \begin{pmatrix}\alpha_0^2\beta_0^2 & \alpha_0\beta_0\alpha_0^*\beta_1^* & \alpha_0\beta_0\alpha_1^*\beta_0^* & \alpha_0\beta_0\alpha_1^*\beta_1^*\\ \alpha_0\beta_1\alpha_0^*\beta_0^* & \alpha_0^2\beta_1^2 & \alpha_0\beta_1\alpha_1^*\beta_0^* & \alpha_0\beta_1\alpha_1^*\beta_1^*\\ \alpha_1\beta_0\alpha_0^*\beta_0^* & \alpha_1\beta_0\alpha_0^*\beta_1^* & \alpha_1^2\beta_0^2 & \alpha_1\beta_0\alpha_1^*\beta_1^*\\ \alpha_1\beta_1\alpha_0^*\beta_0^* & \alpha_1\beta_1\alpha_0^*\beta_1^* & \alpha_1\beta_1\alpha_1^*\beta_0^* & \alpha_1^2\beta_1^2\end{pmatrix}. \tag{23}$$

Using $|\psi\rangle_{abc} = \frac{1}{2}(|000\rangle + |010\rangle + |101\rangle - |111\rangle)_{abc}$ as the channel, we have

$$\rho_{ab} = \frac{1}{4}\begin{pmatrix}1 & 1 & 0 & 0\\ 1 & 1 & 0 & 0\\ 0 & 0 & 1 & -1\\ 0 & 0 & -1 & 1\end{pmatrix}. \tag{24}$$

Then, using our general derivation, we have

$$\rho_{AB}^{out} = \begin{pmatrix}\alpha_0^2\beta_0^2 & \alpha_0\beta_0\alpha_0^*\beta_1^* & 0 & 0\\ \alpha_0\beta_1\alpha_0^*\beta_0^* & \alpha_0^2\beta_1^2 & 0 & 0\\ 0 & 0 & \alpha_1^2\beta_0^2 & -\alpha_1\beta_0\alpha_1^*\beta_1^*\\ 0 & 0 & -\alpha_1\beta_1\alpha_1^*\beta_0^* & \alpha_1^2\beta_1^2\end{pmatrix}. \tag{25}$$

Thus, we get $\langle\psi_t|\rho_{AB}^{out}|\psi_t\rangle = |\alpha_0|^4 + |\alpha_1|^4$ where $|\psi_t\rangle$ follows from Eq. (7). For the d-dimensional case, $\langle\psi_t|\rho_{AB}^{out}|\psi_t\rangle = \Sigma_{p=0}^{d-1}|\alpha_p|^4$. One can easily see that the CP gate is symmetric between Alice and Bob, but the fidelity f_{NC} is related only to coefficients on Alice's side. This is because the state of the channel is Eq. (3) with ac symmetry. If the channel is in the form of bc symmetry, the corresponding $\langle\psi_t|\rho_{AB}^{out}|\psi_t\rangle$ is $\Sigma_{p=0}^{d-1}|\beta_{p'}|^4$. One can obtain $f_{NC} = \frac{2}{d+1}$ by simple integration [36]. This results in the control power $P = \frac{d-1}{d+1}$.

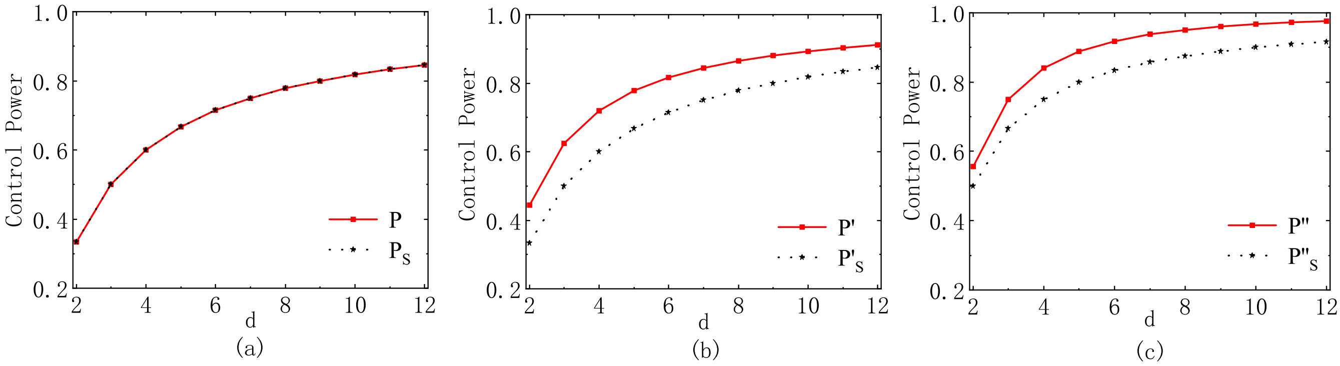
With the channel $|\psi'\rangle_{abc}$, we have $\langle\psi_t|\rho_{AB}^{out}|\psi_t\rangle = \sum_{j=0}^{d-1}(\sum_{i=0}^{d-1}|\alpha_i|^2|\beta_{i+j}|^2)^2$, and the corresponding $f'_{NC} = \frac{d+3}{(d+1)^2}$ for the d-dimensional case where $|\psi_t\rangle$ follows from Eq. (14). A higher control power than the channel in Eq. (2) is achieved while keeping the scheme perfect,

$$P' = 1 - \frac{d+3}{(d+1)^2}. \tag{26}$$

With the channel $|\psi''\rangle_{abc}$, we have $\langle\psi_t|\rho_{AB}^{out}|\psi_t\rangle = \sum_{m,n=0}^{d-1}|\alpha_m|^4|\beta_n|^4$ where $|\psi_t\rangle$ follows from Eq. (18). The corresponding unconditioned fidelity and control power are

$$f''_{NC} = \frac{4}{(d+1)^2}, \quad P'' = 1 - \frac{4}{(d+1)^2}. \tag{27}$$

To evaluate the performance of the control power P of the client, we numerically calculate P as a function of the dimension d of the controlled CP gate ($12 \geqslant d \geqslant 2$) in different quantum channels. The results are shown in Fig. 2. Here, P, P', and P'' are the control power of channels $|\psi\rangle_{abc}$, $|\psi'\rangle_{abc}$, and $|\psi''\rangle_{abc}$ for the implementation of a nonlocal d-dimensional controlled CP gate. For comparison, $P_s = P'_s = \frac{d-1}{d+1}$ [35] and $P''_s = \frac{d-1}{d}$ [36] are the control power for controlled teleportation with channels $|\psi\rangle_{abc}$, $|\psi'\rangle_{abc}$ and $|\psi''\rangle_{abc}$, respectively. From Fig. 2, one can see that $P'_s < P'$ and $P''_s < P''$. This shows that using the same channel resources, such as



(a)

(b)

(c)

FIG. 2. Control power of three different high-dimensional channels as a function of the dimension parameter d $(2 \leqslant d \leqslant 12)$. (a) $P = 1 - \frac{2}{d+1}$ is the control power for a controlled nonlocal CP gate with the channel $|\psi\rangle_{abc}$ (the red solid line) which is equal to the control power P_s of controlled state teleportation with the channel $|\psi\rangle_{abc}$ (the black dotted line). (b) $P' = 1 - \frac{3+d}{(d+1)^2}$ is the control power for a controlled nonlocal CP gate with the channel $|\psi'\rangle_{abc}$ (the red solid line) which is larger than the control power $P_s' = P_s$ of controlled state teleportation with the channel $|\psi'\rangle_{abc}$ (the black dotted line). (c) $P'' = 1 - \frac{4}{(d+1)^2}$ is the control power for a controlled nonlocal CP gate with the channel $|\psi''\rangle_{abc}$ (the red solid line) and $P_s'' = \frac{d-1}{d}$ is the control power of controlled state teleportation with the channel $|\psi''\rangle_{abc}$ (the black dotted line).

$|\psi'\rangle_{abc}$ and $|\psi''\rangle_{abc}$, the client's control power for supervising nonlocal quantum gate operations between quantum servers is much greater than that of quantum state transfer between quantum servers.

After all calculations are completed, Charlie will get the quantum calculation result returned by the servers. Charlie randomly selects some of them as the control-checking sequence K_c and measures these qudits in the appropriate basis. By comparing the measurement results of these control-checking qubits, Charlie can measure the fidelity and control power in the calculation process. Artur *et al.* [40] concluded that control power could be simulated by classical correlations. However, classical correlations between client and quantum servers cannot be used to guarantee the security of the algorithm information in our scheme.

IV. SECURITY CHECKING

Control power can be used to measure the degree of client's participation in the nonlocal calculation process, but the quantum servers can still steal the client's calculation information to give a correct result. Thus, after confirming that the calculation result is correct by a sample comparison, the client must also check the security of remote computing. In this section, we introduce the safety checking strategies for different potential situations.

Alice and Bob could use the state

$$|\psi\rangle_0^{in} = \frac{1}{d}\sum_{p=0}^{d-1}|p\rangle_{A_0}\sum_{p'=0}^{d-1}|p'\rangle_{B_0}, \tag{28}$$

instead of $|\psi\rangle^{in}$ for performing nonlocal gate operations. After nonlocal controlled CP gating operation $U(n)$ of Eq. (4), the state becomes $\frac{1}{\sqrt{d}}\sum_{p'=0}^{d-1}|p'-n\rangle_{A_0}^x|p'\rangle_{B_0}$. Alice and Bob jointly measure the state in the x basis $\{|p\rangle_{A_0}^x\}$ and in the z basis $\{|p'\rangle_{B_0}\}$, respectively, and compare the measurement results privately to get the value of n. Here, only the local measurement and classical communication (LOCC) are used.

To avoid these situations, the client Charlie should introduce security checking. After safely distributing N identical entangled three-qudit states $|\psi\rangle_{a_ib_ic_i}$ $(i = 1, 2, \ldots, N)$, Charlie randomly selects some of them as the security checking sequence K. In the nonlocal controlled CP gating operations, Charlie picks the qudits c_k in the security checking sequence K, and measures the qudit c_k in the z basis $\{|l'+p\rangle\}_{c_k}$. As l' is the measurement result of qudit a, Charlie can get the value of p at the same time. In this step, according to Eq. (5), the state of the qudits A_kB_k becomes $|p\rangle_{A_k}|p\rangle_{B_k}^{x'}$ ignoring the overall phase (here, $|p\rangle_{B_k}^{x'} = \sum_{p'=0}^{d-1} e^{-\frac{2\pi i}{d}p'p}\beta_{p'}|p'\rangle_{B_k}$). After all calculations are completed, Charlie will get the quantum calculation result returned by the servers. Charlie picks the calculation results of security checking sequence K and checks the results according to the state of qudits A_kB_k is $|p\rangle_{A_k}|p\rangle_{B_k}^{x'}$. If Alice and Bob want to steal information from Charlie, they will give back a result according to the state of qudits A_kB_k is $\sum_{p=0}^{d-1} e^{\frac{2\pi i}{d}pn_0}\alpha_p|p\rangle_{A_k}|p\rangle_{B_k}^{x'}$. Therefore, once Charlie performs the security checking on this state, Alice only have a probability of $1/d$ on average to provide the right answer to Charlie. That means the client has a probability of $\chi = \frac{d-1}{d}$ to discover that Alice and Bob have stolen information.

With the channel $|\psi'\rangle_{abc}$, after nonlocal controlled CP gating operation $U(n_1, n_2)$ of Eq. (10), the state $|\psi\rangle_0^{in}$ becomes

$$\begin{aligned}&\frac{1}{\sqrt{d}}\sum_{p=0}^{d-1} e^{\frac{2\pi i}{d}pn_1}|p\rangle_{A_0}|p-n_2\rangle_{B_0}^x\\&\quad = \frac{1}{\sqrt{d}}\sum_{p'=0}^{d-1} e^{\frac{2\pi i}{d}p'n_2}|p'-n_1\rangle_{A_0}^x|p'\rangle_{B_0}.\end{aligned} \tag{29}$$

Alice and Bob can measure the state in the x basis $\{|p\rangle_{A_0}^x\}$ and in the z basis $\{|p'\rangle_{B_0}\}$, respectively, and compare the measurement results privately to get the value of n_1. Since Charlie tells Alice and Bob the corresponding operation $\sigma_{A,z}^{\tilde{k}+n_2}$ and $\sigma_{B,z}^{\tilde{k}+n_1}$, respectively, Alice and Bob can get the value of $n_1 - n_2$, and with n_1, they can obtain the value of n_2. Here, only the LOCC is used. To prevent this, Charlie selects the qudits belonging to the security checking sequence K, and measures the qudit c_k in the z basis. According to Eq. (11), the state of the qudits $A_kB_kc_k$ becomes $\sum_{p=0}^{d-1} e^{-\frac{2\pi i}{d}p(k+p)}\alpha_p|p\rangle_{A_k}\beta_{d-k-p}|d-k-p\rangle_{B_k}|k\rangle_c$. If Alice and Bob want to steal information from Charlie, they will give back a result according to the state of qudits A_kB_k is $\sum_{p,p'=0}^{d-1} e^{\frac{2\pi i}{d}(pn_1+p'n_2-pp')}\alpha_p|p\rangle_A\beta_{p'}|p'\rangle_B$. As p and p' are independent of each other, once Charlie implements the security checking on this state, Alice and Bob only have a probability of $1/d$ on average to provide the right answer to Charlie. That means the client has a probability of $\chi = \frac{d-1}{d}$ to discover that Alice and Bob have stolen information.

In the case of the $|\psi''\rangle_{abc}$ channel, after the gating operation, Alice and Bob can jointly perform a nonlocal inverse operation of U_{CP} on the qubits A_0 and B_0 using entangled resources so that the state $|\psi\rangle_0^{in}$ becomes $|d-n_1\rangle_{A_0}^x|d-n_2\rangle_{B_0}^x$. Then, Alice and Bob measure the state in the x basis, respectively, and by sharing the measurement results privately get the values of n_1 and n_2. Here, the quantum nonlocal cooperation (QNC) and LOCC are required. Charlie picks the qudits belonging to security checking sequence K and measures the qudit c_{k1} in the $(-x)$ basis $\{|\tilde{k}_1\rangle_c^{-x}\}$ ($|k_1\rangle_c = \frac{1}{\sqrt{d}}\sum_{\tilde{k}_1=0}^{d-1} e^{-\frac{2\pi i}{d}k_1\tilde{k}_1}|\tilde{k}_1\rangle_c^{-x}$) and the qudit c_{k2} in the x basis. The state of the qudits $A_kB_kc_kc_{k1}c_{k2}$ becomes $\alpha_p\beta_{p'}|p\rangle_{A_k}|p'\rangle_{B_k}|p\rangle_{c_{k1}}^{-x}|p'\rangle_{c_{k2}}^x$ ignoring the overall phase. If Alice and Bob want to steal information from Charlie, they will give back a result according to the state of qudits A_kB_k is $\sum_{p,p'=0}^{d-1} e^{\frac{2\pi i}{d}(pn_1+p'n_2-pp')}\alpha_p|p\rangle_A\beta_{p'}|p'\rangle_B$. Once Charlie does the security checking on this state, Alice and Bob only have a probability of $1/d^2$ on average to give a right answer to Charlie. Hence the client has a probability of $\chi = \frac{d^2-1}{d^2}$ to discover that Alice and Bob have stolen information.

If quantum servers in the network provide the quantum channels for the client, they can replace the original GHZ-type channel with one or two Bell-state channels. The quantum servers can measure the entangled qudits in the same basis as Charlie, and they can achieve the specific information of the algorithm. In this case, the security checking strategy is also applicable for different channels with the same probability to discover the colluding quantum servers. Our proposed quantum security strategy prevents quantum servers in the network from stealing each other's information or jointly stealing the client information through specific methods. Fortunately, our scheme uses three-qudit entanglement which is also a valuable resource to perform some quantum information tasks in a device-independent way. This will lead to trustworthy security protocols for our controlled quantum computation distribution with device-independent security guarantees and device-independent randomness certifications.

V. CONCLUSION AND SUMMARY

Through the above analysis, we can see that the error rate in security checking and control power in control checking are used to describe the impact on the whole nonlocal quantum calculation from two different perspectives when users and quantum servers do not cooperate with each other. For the quantum servers, the control power reflects the degree of distortion in the whole calculation process caused by the user's "inaction" behavior, and it shows the importance of the user's participation. The error rate in security checking indicates the probability that the user can discover the inappropriate behavior of the server. The performance of different channels in security and control power is shown and compared in Table I. Clients can select the channel that best balances their security and control needs, depending on their priorities. If necessary, the client can store the results on the quantum servers, and when he extracts the calculation result from the servers, he performs security and control-checking simultaneously. If the security and control power cannot be guaranteed, the client will discard these calculation results.

TABLE I. The security and control power of channels.

Channel	Function	Eavesdropping ways	χ	Control power
$\|\psi\rangle_{abc}$	$U(n)$	LOCC	$\frac{d-1}{d}$	$\frac{d-1}{d+1}$
$\|\psi'\rangle_{abc}$	$U(n_1, n_2)$	LOCC	$\frac{d-1}{d}$	$1-\frac{d+3}{(d+1)^2}$
$\|\psi''\rangle_{abc}$	$U(n_1, n_2)$	QNC & LOCC	$\frac{d^2-1}{d^2}$	$1-\frac{4}{(d+1)^2}$

A three-dimensional three-particle [42,43] and high-dimensional four-party [44] GHZ state has recently been experimentally created using photons. Experimental demonstrations of local high-dimensional single-photon quantum gates and two-qubit controlled-NOT quantum operation have also been recently published [45,46]. Therefore, the quantum channel and the main elements of our high-dimensional controlled distributed computation scheme have been realized experimentally. We expect that further laboratory implementations of high-dimensional operations will be published in the near future. Our results are thus of relevance both from a theoretical and an applied perspective.

In summary, we have proposed a scheme for clients to remotely control nonlocal gates in a secure manner. To quantify the client's control power, we also defined a measure of the client's control power in analogy to the control power used to assess controlled teleportation. By replacing the bipartite quantum channel with a tripartite entangled quantum state, the client has the power to monitor successful quantum gate performance between two quantum computers even when they collude. Our proposed quantum security strategy prevents quantum servers in the network from stealing each other's information or jointly stealing the client information through specific methods. From the view of control power, the client has two options for performing confidential nonlocal quantum computing. One is to encrypt the calculated state, and the other is to encrypt the algorithm. Assuming that the security is guaranteed, our analysis of control power shows that given the same channel resources, the client's control power over nonlocal quantum gate operations between quantum servers is much greater than that of quantum state transfer between quantum servers. Our framework for nonlocal controlled quantum gate operations in arbitrary dimensions provides a feasible method and new directions of exploration for the future construction of quantum computing networks. Furthermore, it may provide new ideas and methods to develop the resource theory of quantum channels.

ACKNOWLEDGMENTS

This work is supported in part by the Ministry of Science and Technology (MOST) of China under Grant

2016YFA0301304, in part by the National Natural Science Foundation of China under Grant No. 62071064, in part of the Fundamental Research Funds for the Central Universities of China under Grant No. 2019XD-A02, and in part by the Fund of State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, China, and the Natural Sciences and Engineering Council of Canada.

[1] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello, Distributed quantum computation over noisy channels, Phys. Rev. A **59**, 4249 (1999).

[2] A. Serafini, S. Mancini, and S. Bose, Distributed Quantum Computation via Optical Fibers, Phys. Rev. Lett. **96**, 010503 (2006).

[3] W. K. Wootters, Entanglement of Formation of An Arbitrary State Of Two Qubits, Phys. Rev. Lett. **80**, 2245 (1998).

[4] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed-state entanglement and quantum error correction, Phys. Rev. A **54**, 3824 (1996).

[5] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[6] L. Vaidman, Teleportation of quantum states, Phys. Rev. A **49**, 1473 (1994).

[7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[8] C. H. Bennett and S. J. Wiesner, Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States, Phys. Rev. Lett. **69**, 2881 (1992).

[9] C. Wang, F.-G. Deng, Y.-S. Li, X.-S. Liu, and G. L. Long, Quantum secure direct communication with high-dimension quantum superdense coding, Phys. Rev. A **71**, 044305 (2005).

[10] J. Eisert, K. Jacobs, P. Papadopoulos, and M. B. Plenio, Optimal local implementation of nonlocal quantum gates, Phys. Rev. A **62**, 052317 (2000).

[11] Z. Yi-Zhuang, G. Yong-Jian, C. Li-Bing, and G. Guang-Can, Implementation of nonlocal quantum swap operation on two entangled pairs, Chin. Phys. (Beijing, China) **11**, 529 (2002).

[12] X.-F. Zhou, Y.-S. Zhang, and G.-C. Guo, Nonlocal gate of quantum network via cavity quantum electrodynamics, Phys. Rev. A **71**, 064302 (2005).

[13] Y.-S. Zhang, M.-Y. Ye, and G.-C. Guo, Conditions for optimal construction of two-qubit nonlocal gates, Phys. Rev. A **71**, 062331 (2005).

[14] L. Yu, R. B. Griffiths, and S. M. Cohen, Efficient implementation of bipartite nonlocal unitary gates using prior entanglement and classical communication, Phys. Rev. A **81**, 062315 (2010).

[15] Z. J. Deng, X. L. Zhang, H. Wei, K. L. Gao, and M. Feng, Implementation of a nonlocal n-qubit conditional phase gate by single-photon interference, Phys. Rev. A **76**, 044305 (2007).

[16] B. Groisman and B. Reznik, Implementing nonlocal gates with nonmaximally entangled states, Phys. Rev. A **71**, 032322 (2005).

[17] S. Yokoyama, R. Ukai, J.-i. Yoshikawa, P. Marek, R. Filip, and A. Furusawa, Nonlocal quantum gate on quantum continuous variables with minimal resources, Phys. Rev. A **90**, 012311 (2014).

[18] L. Chen and Y.-X. Chen, Probabilistic implementation of a nonlocal operation using a nonmaximally entangled state, Phys. Rev. A **71**, 054302 (2005).

[19] Y.-F. Huang, X.-F. Ren, Y.-S. Zhang, L.-M. Duan, and G.-C. Guo, Experimental Teleportation of a Quantum Controlled-Not Gate, Phys. Rev. Lett. **93**, 240501 (2004).

[20] H.-L. Huang, Q. Zhao, X. Ma, C. Liu, Z.-E. Su, X.-L. Wang, L. Li, N.-L. Liu, B. C. Sanders, C.-Y. Lu, and J.-W. Pan, Experimental Blind Quantum Computing for a Classical Client, Phys. Rev. Lett. **119**, 050503 (2017).

[21] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li *et al.*, Ground-to-satellite quantum teleportation, Nature (London) **549**, 70 (2017).

[22] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, Satellite-Relayed Intercontinental Quantum Network, Phys. Rev. Lett. **120**, 030501 (2018).

[23] M. Hillery, V. Bužek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999).

[24] A. Karlsson and M. Bourennane, Quantum teleportation using three-particle entanglement, Phys. Rev. A **58**, 4394 (1998).

[25] A. Broadbent, J. Fitzsimons, and E. Kashefi, Universal blind quantum computation, in *IEEE 50th Annual Symposium on Foundations of Computer Science (FOCS 2009)* (IEEE Computer Society, Los Alamitos, 2009).

[26] V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, Efficient Universal Blind Quantum Computation, Phys. Rev. Lett. **111**, 230501 (2013).

[27] A. Mantri, C. A. Pérez-Delgado, and J. F. Fitzsimons, Optimal Blind Quantum Computation, Phys. Rev. Lett. **111**, 230502 (2013).

[28] T. Morimae, Continuous-Variable Blind Quantum Computation, Phys. Rev. Lett. **109**, 230502 (2012).

[29] T. Morimae and K. Fujii, Secure Entanglement Distillation For Double-Server Blind Quantum Computation, Phys. Rev. Lett. **111**, 020502 (2013).

[30] E. K. A. Pappa, Multiparty delegated quantum computing, Cryptography **1**, 12 (2017).

[31] Y. Dulek, A. B. Grilo, S. Jeffery, C. Majenz, and C. Schaffner, Secure multi-party quantum computation with a dishonest majority, *Advances in Cryptology - EUROCRYPT 2020*, edited by A. Canteaut and Y. Ishai, Lecture Notes in Computer Science, Vol. 12107 (Springer, Cham, 2020), pp. 729–758.

[32] B. W. Reichardt, F. Unger, and U. Vazirani, Control power in perfect controlled teleportation via partially entangled channels, Nature (London) **496**, 456 (2013).

[33] Q. Li, W. H. Chan, C. Wu, and Z. Wen, Triple-server blind quantum computation using entanglement swapping, Phys. Rev. A **89**, 040302(R) (2014).

[34] X.-H. Li and S. Ghose, Control power in perfect controlled teleportation via partially entangled channels, Phys. Rev. A **90**, 052305 (2014).

[35] X.-H. Li and S. Ghose, Analysis of *n*-qubit perfect controlled teleportation schemes from the controller's point of view, Phys. Rev. A **91**, 012320 (2015).

[36] T. J. Wang, G. Q. Yang, and C. Wang, Control power of high-dimensional controlled teleportation, Phys. Rev. A **101**, 012323 (2020).

[37] K. Jeong, J. Kim, and S. Lee, Minimal control power of the controlled teleportation, Phys. Rev. A **93**, 032328 (2016).

[38] A. Barasiński and J. c. v. Svozilík, Controlled teleportation of qubit states: Relation between teleportation faithfulness, controller's authority, and tripartite entanglement, Phys. Rev. A **99**, 012306 (2019).

[39] A. Barasiński, I. I. Arkhipov, and J. Svozilík, Localizable entanglement as a necessary resource of controlled quantum teleportation, Sci. Rep. **8**, 15209 (2018).

[40] A. Barasiński, A. Černoch, and K. Lemr, Demonstration of Controlled Quantum Teleportation for Discrete Variables on Linear Optical Devices, Phys. Rev. Lett. **122**, 170501 (2019).

[41] G. K. Brennen, D. P. O'Leary, and S. S. Bullock, Criteria for exact qudit universality, Phys. Rev. A **71**, 052318 (2005).

[42] L. L. Lu, L. J. Xia, Z. Y. Chen, L. Z. Chen, T. H. Yu, T. Tao, W. Ma, Y. Pan, X. Cai, Y. Lu, S. Zhu, and X.-S. Ma, Three-dimensional entanglement on a silicon chip, npj Quantum Inf. **6**, 30 (2020).

[43] M. Erhard, M. Malik, M. Krenn, and A. Zeilinger, Experimental Greenberger–Horne–Zeilinger entanglement beyond qubits, Nat. Photonics **12**, 759 (2018).

[44] P. Imany, J. A. Jaramillo-Villegas, M. S. Alshaykh, J. M. Lukens, O. D. Odele, A. J. Moore, D. E. Leaird, M. Qi, and A. M. Weiner, High-dimensional optical quantum logic in large operational spaces, npj Quantum Inf. **5**, 59 (2019).

[45] A. Babazadeh, M. Erhard, F. Wang, M. Malik, R. Nouroozi, M. Krenn, and A. Zeilinger, High-Dimensional Single-Photon Quantum Gates: Concepts and Experiments, Phys. Rev. Lett. **119**, 180510 (2017).

[46] F. Brandt, M. Hiekkamäki, F. Bouchard, M. Huber, and R. Fickler, High-dimensional quantum gates using full-field spatial modes of photons, Optica **7**, 98 (2020).