Controlled remote implementation of operations for many systems

Chengxu Liu

Capital Normal University High School, Beijing, China, 100048

liuchengxu2025@gmail.com

Abstract. Quantum communication plays a key role in the next generation of information transfer and security schemes, by using quantum entanglement and measurements from quantum mechanics. We introduce the mathematical and physical foundations of quantum communication, such as the CNOT gate and Kronecker product. Then we propose two quantum communication protocols, namely dense coding and stealth coding. These protocols offer unique advantages that are theoretically unbreakable. Then we extend the protocols to the quantum communication protocol allowing for third-party supervision to ensure information security. Based on this, a communication protocol involving four parties is designed, enabling them to exchange information while being supervised.

Keywords: quantum entanglement, dense coding, remote implementation of operations

1. Introduction

Quantum entanglement has been used to various quantum protocols such as teleportation and dense coding assisted by classical channels [1,2]. Ref. [3,4] showed the operational principles and mathematical foundations of several existing quantum communication protocols. Besides, quantum protocols can also be used for classical computers [5]. Current existing classical encryption methods are no longer entirely secure, as methods for rapidly breaking classical encryption have been proposed [6]. After addressing issues such as decoherence and noise [7,8], the unique advantages of quantum encryption are gradually becoming apparent [9,10]. Subsequently, researchers investigated practical steps for quantum information transmission protocols, aiming to reduce costs and enhance efficiency [11]. Next, the quantum cost of dense coding and teleportation protocols has been evaluated in terms of CNOT gates [12]. Authors in [13] showed that the quantum remote control may be applied to realize the teleportation unitary gates. Further, the similar technique has been used to teleport angles with a secure way [14]. Further, multipartite scenarios have been considered for a deterministic single-qubit. That is, recent advancements in the field of remote implementation of partially unknown quantum operations on multiple qubits have led to significant breakthroughs, rendering practical operations feasible. These developments have substantially propelled the potential applications of quantum communication and networking forward [15]. Besides, operation sharing with five-qubit cluster state has been established [16,17]. These operations and protocols provide a good foundation for realizing more complex protocols of transmitting information securely.

In this paper, we develop the above protocols by constructing a multi-party quantum security protocol in terms of the so-called remote-controlled implementation of operations. In Sec. II, we delve into the CNOT gate, Hadamard Gate, and the Kronecker product. Subsequently, we provide a detailed exposition on the operational mechanisms of current quantum dense coding and quantum stealth coding protocols. In Sec. III, we discuss a quantum Quantum Communication Protocols, which Bob send massage to Charlie and Alice have ability to control the message transmit. Then in Sec. IV, by redesigning the communication protocol, we achieve the controlled communication among Alice, Bob, Charlie, and Daniel. Alice measures her qubit, and then the receiver Charlie and Daniel both measure their qubit. As a result, Bob, Charlie and Daniel share a stator of particles b, C and D. Then Bob can perform a local unitary gate containing a parameter unknown to Alice, Charlie and Daniel. We finally conclude in Sec. V.

2. Preliminaries

In this section, we review the preliminary knowledge for this paper. In Sec. II A, we review the notion of Kronecker product and its basic properties. In Sec. II B, we review the Hadamard gate, controlled NOT gate and Bell states and so on. In Sec. II C we introduce the protocol of quantum super dense coding. In Sec. II D, we introduce the protocol of quantum teleportation.

2.1. Kronecker product

The Kronecker product is a computational method that allows for the multiplication of any two matrices without the constraints on the number of rows and columns. The following matrices are given.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1q} \\ b_{21} & b_{22} & \cdots & b_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ b_{p1} & b_{p2} & \cdots & b_{pq} \end{pmatrix}.$$

Then we define the Kronecker product

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}.$$

We describe the following properties.

(1) If matrix A is an $m \times n$ matrix, and the matrix B is a $p \times q$ matrix, then the Kronecker product of the matrices A and B is defined above, regardless of the size of A and B. In other word, the Kronecker product of A and B, denoted $A \otimes B$, is an $mp \times nq$ matrix, resulting from multiplying every element of A by matrix B. Similarly, the Kronecker product of B and A, denoted $B \otimes A$, is a $pm \times qn$ matrix, resulting from multiplying every element of B by matrix A.

(2) Next, we introduce the distributive property. The Kronecker product has a distributive property over addition, $A \otimes (B + C) = A \otimes B + A \otimes C$.

(3) Third, the mixed product property of Kronecker product is $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$.

(4) Four the transpose property of Kronecker product is $(A \otimes B)^T = A^T \otimes B^T$.

(5) Finally the scalar multiplication property is $c(A \otimes B) = (cA) \otimes B = A \otimes (cB)$.

2.2. Gates and states

We introduce the Hadamard gate as follows.

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

The Hadamard operation can transform the qubit $|0\rangle$ and $|1\rangle$ into their superposition with equal weights. The specific formula is as follows.

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

$$H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}. \tag{3}$$

Next, the CNOT gate is a quantum gate capable of transforming quantum states in the form of $|a, b\rangle$ into $|a, a \oplus b\rangle$ where $a, b = 0,1$. The operating principle of the CNOT gate is to take the first qubit as the control qubit, and perform the opposite transformation on the second qubit based on the state of the control qubit. It is important to note that the CNOT gate cannot operate on individual quantum states, as it automatically considers the first qubit as the decision maker. The CNOT gate has the matrix form as follows.

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{4}$$

There are four forms of Bell states, each of which is a maximally entangled state of two quantum bits. The properties of entanglement are used to transfer information in the following quantum communication. The specific formula of four Bell states are as follows.

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle +|11\rangle), \tag{5}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle -|11\rangle), \tag{6}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle +|10\rangle), \tag{7}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle -|10\rangle). \tag{8}$$
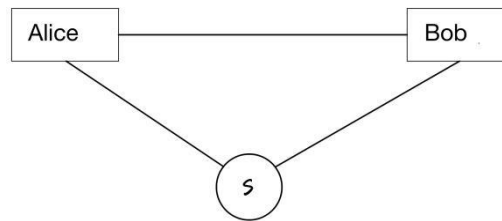
2.3. Quantum Dense Coding

Figure 1. The source S builds an EPR pair and sends the two particles of the pair to Alice and Bob, respectively

The dense coding protocol is presented in Figure 1. The EPR pair has the expression

$$|\phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}. \tag{9}$$

Using the Hadamard gate assisted by the CNOT gate implemented in the product state $|0,0\rangle$, we can prepare the EPR pair as follows.

$$CNOT(H \otimes I)|00\rangle = |\phi^+\rangle. \tag{10}$$

Subsequently, the Hermitian and unitary properties of the Pauli matrices are utilised for information encryption. There are four distinct scenarios, respectively corresponding to the transmission of message states $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. The specific cases are as follows.

First. The message state is $|00\rangle$.

$$I \otimes I |\phi^+\rangle = |\phi^+\rangle. \tag{11}$$

Hence, Alice does nothing from her side. Mathematically, the physical operation is represented by the identity matrix as above.

Second. The message state is $|01\rangle$.

$$\sigma_x \otimes I |\phi^+\rangle = |\phi^+\rangle. \tag{12}$$

The calculation detail is as follows.

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}. \tag{13}$$

Third. The message state is $|10\rangle$.

$$\sigma_z \otimes I |\phi^+\rangle = |\phi^-\rangle. \tag{14}$$

The calculation detail is as follows.

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \end{bmatrix}. \tag{15}$$

Finally. The message state is $|11\rangle$.

$$i\sigma_y \otimes I |\phi^+\rangle = |\psi^-\rangle. \tag{16}$$

The calculation detail is as follows.

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ -1 \\ 0 \end{bmatrix}. \tag{17}$$

We also need decode the message by inverse operation. That is,

$$\left(\text{CNOT}(H \otimes I)\right)^{-1} = (H \otimes I)\text{CNOT}. \tag{18}$$

We record this operator as B. By taking the decoding operator, Bob can finally obtain the correct message.

$$B|\psi^+\rangle = |01\rangle B, |\psi^-\rangle = |11\rangle, B|\phi^+\rangle = |00\rangle, B|\phi^-\rangle = |10\rangle. \tag{19}$$

2.4. Quantum teleportation
Quantum invisible transmission of states through quantum entanglement of Bell states allows the transmission of quantum information at both ends solely through the classical channel. The principles and methods are as follows.
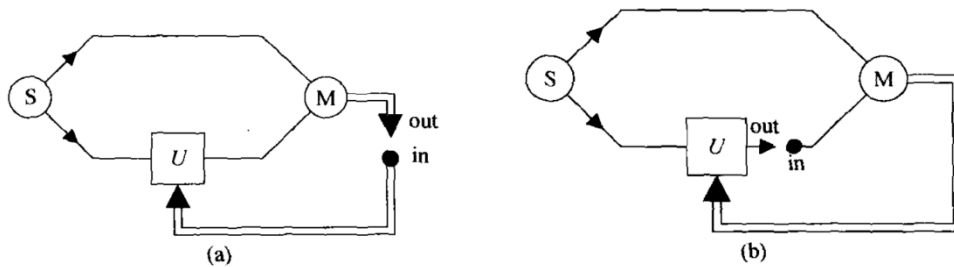

Figure 2. (a) Image content is densely coded (b) for quantum invisible state transfer

Suppose Alice wants to convey to Bob the two-energy-level quantum information that is in a superposition state $\alpha|0\rangle + \beta|1\rangle$. She can use the second method which is shown in Figure 2.

Step 1. We build the EPR pair.

The source S generates an EPR pair namely a Bell state, and sends the first half to Alice and the second half to Bob. Make sure the pair of quanta is in an entangled state $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. To build this EPR pair, S should carry out the physical operation as follows.

$$CNOT(H \otimes I)|00\rangle = |\psi^+\rangle. \tag{20}$$

By sending the EPR pair to Alice and Bob, Alice has two particles, which are respectively half of the EPR pair and the message qubit she wants to transmit to Bob. On the other hand Bob only has one qubit, namely the other half of EPR pair.

The state of the three qubits are given by the tensor product of $|\psi\rangle$ and $|\psi^+\rangle$ as follows.

$$
\begin{aligned}
|\psi\rangle \otimes |\psi^+\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
&= \frac{\alpha}{\sqrt{2}}(|001\rangle + |010\rangle) + \frac{\beta}{\sqrt{2}}(|101\rangle + |110\rangle).
\end{aligned} \tag{21}
$$

Step 2. Joint measurement by Alice.

The reason why Alice needs to do the joint measurement is that if Alice only determines message qubit, this quantum will collapse to $|0\rangle$ or $|1\rangle$. The way out of this problem is to make measurements on the Bell state, i.e., $|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle$.

$$
\begin{cases}
|00\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\phi^-\rangle), \\
|11\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\phi^-\rangle), \\
|01\rangle &= \frac{1}{\sqrt{2}}(|\psi^+\rangle + |\psi^-\rangle), \\
|10\rangle &= \frac{1}{\sqrt{2}}(|\psi^+\rangle - |\psi^-\rangle).
\end{cases} \tag{22}
$$

Then we insert Equation 22 into Equation 21, by transforming the computational basis into the Bell basis.

$$
\begin{aligned}
|\psi\rangle \otimes |\psi^+\rangle &= \frac{\alpha}{2}(|\phi^+\rangle + |\phi^-\rangle)\big|1\rangle + \frac{\alpha}{2}(|\psi^+\rangle + |\psi^-\rangle)\big|0\rangle \\
&\quad + \frac{\beta}{2}(|\psi^+\rangle - |\psi^-\rangle)\big|1\rangle + \frac{\beta}{2}(|\phi^+\rangle - |\phi^-\rangle)\big|0\rangle \\
&= \frac{1}{2}\big|\psi^+\rangle(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}\big|\psi^-\rangle(\alpha|0\rangle - \beta|1\rangle) \\
&\quad + \frac{1}{2}\big|\phi^+\rangle(\alpha|1\rangle + \beta|0\rangle) + \frac{1}{2}\big|\phi^-\rangle(\alpha|1\rangle - \beta|0\rangle).
\end{aligned} \tag{23}
$$

In this case, if Alice does a Bell Measurement, she has the same chance to obtain every state of $|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle$. By using suitable unitary operation (see the next subsection), Alice can change these four measurement results to some message which can be sent by classical channels.

$$
\begin{aligned}
&\frac{1}{2}\big|01\rangle(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}\big|11\rangle(\alpha|0\rangle - \beta|1\rangle) \\
&+ \frac{1}{2}\big|00\rangle(\alpha|1\rangle + \beta|0\rangle) + \frac{1}{2}\big|10\rangle(\alpha|1\rangle - \beta|0\rangle).
\end{aligned} \tag{24}
$$

Step 3. Unitary operation is carried out by Bob.

Alice sends the result of the Bell measurements to Bob by classical messages. Bob can use this message to determine which of the quantum states is this message corresponds to.

$$
\begin{aligned}
|00\rangle &\rightarrow (\alpha|1\rangle + \beta|0\rangle) \rightarrow \sigma_x, \\
|10\rangle &\rightarrow (\alpha|1\rangle - \beta|0\rangle) \rightarrow i\sigma_y, \\
|01\rangle &\rightarrow (\alpha|0\rangle + \beta|1\rangle) \rightarrow I, \\
|11\rangle &\rightarrow (\alpha|0\rangle - \beta|1\rangle) \rightarrow \sigma_z.
\end{aligned}
\tag{25}
$$

By taking this operation, Bob can obtain the message qubit $\alpha|0\rangle + \beta|1\rangle$. So we have completed the protocol of quantum teleportation.

3. Controlled Remote Implementation of Operations in Three participants

The main goal in this section is to send the unitary operation $U = \otimes_{j=1}^{N} \exp\left[i\alpha_j \sigma_{n_{o_j}}\right]$ to other participants assisted by the controller.

3.1. Basic configuration

Three participants have a configuration in Figure 3. In this case, they share the tripartite graph state
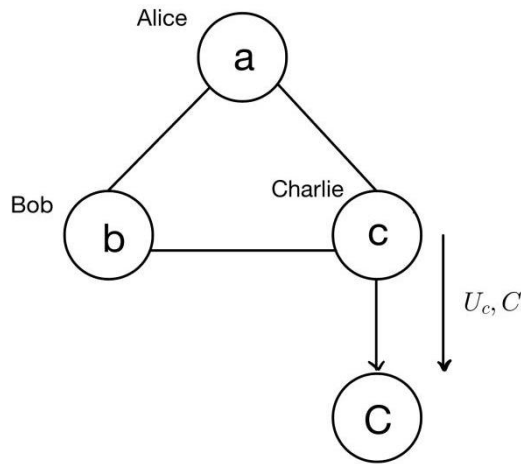

Figure 3. (a) Image content is densely coded (b) for quantum invisible state transfer

$$
\begin{aligned}
|h_3\rangle &= CZ_{(a,b)}CZ_{(a,c)}|+\rangle^{\otimes 3} \\
&= \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle - |101\rangle - |110\rangle + |111\rangle)_{a,b,c}.
\end{aligned}
\tag{26}
$$

3.2. Build quantum pair

To accomplish our goal, we implement the unitary operation $U_C = \exp\left[i\alpha\sigma_{n_c}\right]$ on system belonging to Charlie

$$
U_{c,C} = |0\rangle_c\langle 0| \otimes I_C + |1\rangle_c\langle 1| \otimes \sigma_{n_C}.
\tag{27}
$$

By insert Equation 27 to Equation 26 we can get a formula as follows.

$$
\begin{aligned}
S_3' &= \frac{1}{2\sqrt{2}}(|000\rangle_{a,b,c} \otimes I_C + |001\rangle_{a,b,c} \otimes \sigma_{n_C} + |010\rangle_{a,b,c} \otimes I_C + |011\rangle_{a,b,c} \otimes \sigma_{n_C} \\
&\quad + |100\rangle_{a,b,c} \otimes I_C - |101\rangle_{a,b,c} \otimes \sigma_{n_C} - |110\rangle_{a,b,c} \otimes I_C + |111\rangle_{a,b,c} \otimes \sigma_{n_C}) \\
&= \frac{1}{2}|+\rangle_a(|00\rangle_{b,c} \otimes I_C + |11\rangle_{b,c} \otimes \sigma_{n_C}) + \frac{1}{2}|-\rangle_a(|10\rangle_{b,c} \otimes I_C + |01\rangle_{b,c} \otimes \sigma_{n_C}).
\end{aligned}
\tag{28}
$$

3.3. Alice measurements

Alice makes measurements. She has the same opportunity to get result $|+\rangle$, $|-\rangle$. Then Alice informs Bob of the measurement result. If she obtains the result $|-\rangle$, then Bob performs the operation σ_x on qubit b, otherwise Bob need not perform any operation. They can obtain the stator as follows.

$$S_3'' = |00\rangle_{b,c} \otimes I_C + |11\rangle_{b,c} \otimes \sigma_{n_C}. \tag{29}$$

3.4. Charlie measurements

Charlie does measurements, and sends the message to Bob. To predict the result he can get, we need to change Equation 29 to the formula based on $|+\rangle, |-\rangle$.

$$S_3'' = |+\rangle(|0\rangle_b \otimes I_C + |1\rangle_b \otimes \sigma_{n_C}) + |-\rangle(|0\rangle_b \otimes I_C - |1\rangle_b \otimes \sigma_{n_C}). \tag{30}$$

By having this state, when Charlie does the measurements, he also has equal opportunity to obtain the result from $|+\rangle, |-\rangle$. Then, he can send the information of result to Bob. If the result is $|-\rangle$, then Bob implements the operation σ_z on qubit b, otherwise he does nothing. They can obtain the result as follows.

$$S_3 = |0\rangle_b \otimes I_C + |1\rangle_b \otimes \sigma_{n_C}. \tag{31}$$

3.5. Bob measurements and information transmit

Bob implements the operation $e^{i\alpha\sigma_{x_b}}$ on S_3. One can show that, this is equivalent to the effect that Charlie implements the operation $e^{i\alpha\sigma_{n_C}}$ on his qubit C.

$$
\begin{aligned}
|s\rangle &= e^{i\alpha\sigma_{x_b}} S_3 |\Phi_C\rangle \\
&= (|0\rangle_b \otimes I_C + |1\rangle_b \otimes \sigma_{n_C}) e^{i\alpha\sigma_{n_C}} |\Phi_C\rangle.
\end{aligned}
\tag{32}
$$

In this case, Bob does the projective measurement by $|0\rangle$ and $|1\rangle$. Then he gives the result to Charlile. If the result is $|1\rangle$, then Charlie implements the operation $\exp[i\pi\sigma_{n_C}/2]$ on qubit c, otherwise he does nothing. Then he can obtain the operation : $e^{i\alpha\sigma_{n_C}}$.

4. Generalized protocol of more parties

In this section, we generalize the protocol in the last section to the case of more parties. We shall implement a global two-qubit unitary gate on two distant parties controlled by different systems. The message is still known by the sender only.

For simplicity we consider four parties, in which Alice is still the judge, Bob is still the sender, and Charlie and Daniel are the receivers, see Figure 4. Suppose the four parties share the four-qubit Greenberger-Horner-Zeilinger (GHZ) state $|\text{GHZ}\rangle = \dfrac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle) \in H_A \otimes H_B \otimes H_C \otimes H_D$.

To realize this state, we need carry out three CNOT gates on parties AB, AC and AD, respectively, see Figure 5. Like the protocol in the last section, Charlie and Daniel respectively perform the controlled unitary gate as follows.

$$U_{cC} = |0\rangle\langle 0| \otimes I_2 + |1\rangle\langle 1| \otimes \sigma_{n_1}, \tag{33}$$

$$V_{dD} = |0\rangle\langle 0| \otimes I_2 + |1\rangle\langle 1| \otimes \sigma_{n_2}, \tag{34}$$

where C and D are two parties belonging to Charlie and Daniel, respectively. Hence, they can prepare the following stator

$$S_1 = \frac{1}{\sqrt{2}} |0000\rangle \otimes I_2 \otimes I_2 + \frac{1}{\sqrt{2}} |1111\rangle \otimes \sigma_{n_1} \otimes \sigma_{n_2}. \tag{35}$$

Next, Alice measures her qubit using the basis $\{|\pm\rangle = \dfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\}$ of the Pauli gate σ_x. Then Alice need notify Bob of the measurement result. If the result is $|+\rangle$ then Bob does nothing, otherwise Bob performs the Pauli gate σ_z. One can see that Bob, Charlie and Daniel are in the following stator of particle b, c, d, C and D.

$$S_2 = \frac{1}{\sqrt{2}}|000\rangle \otimes I_2 \otimes I_2 + \frac{1}{\sqrt{2}}|111\rangle \otimes \sigma_{n_1} \otimes \sigma_{n_2}. \tag{36}$$

Third, Charlie and Daniel measure respectively particle b and c using the basis $\{|\pm\rangle\}$. Then they need notify Bob of the measurement result. If the results are both $+$ or $-$, then Bob does nothing. Otherwise, Bob performs the gate σ_z. One can see that Bob, Charlie and Daniel are in the following stator of particle b, C and D.

$$S_3 = \frac{1}{\sqrt{2}}|0\rangle \otimes I_2 \otimes I_2 + \frac{1}{\sqrt{2}}|1\rangle \otimes \sigma_{n_1} \otimes \sigma_{n_2}. \tag{37}$$

Fourth, Bob implements the local Pauli gate σ_{x_b}, and one can show that $\sigma_{x_b}S_3 = (\sigma_{n1} \otimes \sigma_{n2})S_3$. Hence we have

$$\sum_{k=0}^{+\infty} \frac{\alpha\sigma_{x_b}^k}{k!}S_3 = \sum_{k=0}^{+\infty} \frac{(\alpha\sigma_{n1} \otimes \sigma_{n2})^k}{k!}S_3. \tag{38}$$

Equivalently we have

$$e^{i\alpha\sigma_{x_b}}S_3 = e^{i\alpha(\sigma_{n1}\otimes\sigma_{n2})}S_3 = S_3 e^{i\alpha(\sigma_{n1}\otimes\sigma_{n2})}. \tag{39}$$

Finally, Bob measures his qubit using the basis $|0\rangle, |1\rangle$. Then Bob need notify Charlie and Daniel of the measurement result. If the result is $|0\rangle$ then they do nothing, otherwise they perform the local unitary operation $\sigma_{n1} \otimes \sigma_{n2}$. As a result, Bob and Charlie have implemented the global unitary gate $e^{i\alpha(\sigma_{n1}\otimes\sigma_{n2})}$ on their particles C and D.
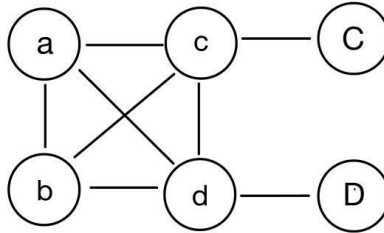

Figure 4. Alice, Bob, Charlie and Daniel respectively possess the particles a,b,c and d. As the judge, Alice measures her qubit, and then the receiver Charlie and Daniel both measure their qubit. As a result, Bob, Charlie and Daniel share a stator of particle b, C and D. Then Bob can perform a local unitary gate containing a parameter unknown to Alice, Charlie and Daniel. It turns out that C and D are performed by a collective unitary gate containing the parameter. So the protocol can transmit classical messages confidentially by quantum means.
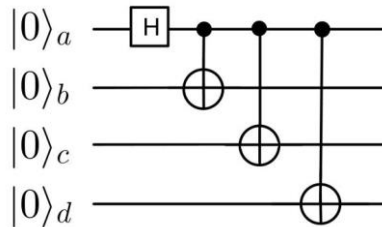

Figure 5. The preparation of four-qubit GHZ state using one Hadamard gate and three CNOT gates.

5. Conclusions

We have shown the protocol of controlled remote implementation of operations in both two and three participants. They show the quantum security guaranteed by the basic rules of quantum mechanics by

using entanglement and measurement. An open problem unsolved in this paper is to extend the results to controlled remote implementation of operations of many parties. Whether entanglement in this protocol could be decreased is also an interesting issue for the next step.

Acknowledgments

References

[1]   Bennett, Brassard, Crepeau, Jozsa, Peres, and Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. Physical review letters, 70(13):1895–1899, 1993.

[2]   Bennett and Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. Physical review letters, 69(20):2881–2884, 1992.

[3]   Nicolas Gisin, Gr´egoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. Reviews of Modern Physics, 74:145–195, 2002.

[4]   Christopher Portmann and Renato Renner. Security in quantum cryptography. Reviews of Modern Physics, 94:025008, 2022.

[5]   Deutsch D. and Jozsa R. Rapid solution of problems by quantum computation. Proceedings of the Royal Society A: Mathematical, 439(1907):553–558, 1992.

[6]   Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. Siam Journal on Computing, 1997.

[7]   Yuri Alexeev, Dave Bacon, Kenneth R. Brown, Robert Calderbank, Lincoln D. Carr, Frederic T. Chong, Brian DeMarco, Dirk Englund, Edward Farhi, Bill Fefferman, Alexey V. Gorshkov, Andrew Houck, Jungsang Kim, Shelby Kimmel, Michael Lange, Seth Lloyd, Mikhail D. Lukin, Dmitri Maslov, Peter Maunz, Christopher Monroe, John Preskill, Martin Roetteler, Martin J. Savage, and Jeff Thompson. Quantum computer systems for scientific discovery. PRX Quantum, 2:017001, 2021.

[8]   J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello. Distributed quantum computation over noisy channels. Physical Review A, 59:4249–4254, 1999.

[9]   Alessio Serafini, Stefano Mancini, and Sougato Bose. Distributed quantum computation via optical fibers. Physical Review Letters, 96:010503, 2006.

[10]   Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. Nature, 390(6660):575–579, 1997.

[11]   Iulia Georgescu. 25 years of experimental quantum teleportation. Nature Reviews Physics, 2022.

[12]   Xinyu Qiu and Lin Chen. Quantum cost of dense coding and teleportation. Physical Review A, 105:062451, 2022.

[13]   S. F. Huelga, J. A. Vaccaro, A. Chefles, and M. B. Plenio. Quantum remote control: Teleportation of unitary operations. Physical Review A, 63(4), 2001.

[14]   S. F. Huelga, M. B. Plenio, and J. A. Vaccaro. Remote control of restricted sets of operations: Teleportation of angles. Physical Review A, 65(4), 2002.

[15]   An Min Wang. Combined and controlled remote implementations of partially unknown quantum operations of multiqubits using greenberger-horne-zeilinger states. Physical Review A, 75(6), 2007.

[16]   M. A. Nielsen and I. L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, Cambridge, 2000.

[17]   Shengfang Wang, Yimin Liu, Jianlan Chen, Xiansong Liu, and Zhanjun Zhang. Deterministic single-qubit operation sharing with five-qubit cluster state. Quantum Information Processing, 12(7):2497–2507, 2013.