SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

March 2017, Vol. 60 032501:1–032501:12
doi: 10.1007/s11432-016-0152-4

Qubit-wise teleportation and its application in public-key secret communication

Chenmiao WU[1,2,3] & Li YANG[1,2*]

[1]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;*
[2]*Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing* 100093*, China;*
[3]*University of Chinese Academy of Sciences, Beijing* 100049*, China*

Received April 25, 2016; accepted August 24, 2016; published online December 9, 2016

Abstract We propose a quantum public-key encryption (QPKE) protocol for an unknown multi-qubit state based on qubit-wise teleportation. The private-key is a computational Boolean function, whereas the public-key is a pair of a random bit string and a quantum state. A private-key corresponds to an exponential number of public-keys. Security analysis showed that the proposed protocol has information-theoretic security from attacks for the private-key and the encryption. A multi-partite quantum secret state sharing protocol is presented based on the proposed multi-qubit-oriented QPKE protocol. Such secret state sharing protocol is information-theoretically secure.

Keywords public-key encryption, quantum information, quantum teleportation, quantum cryptography, quantum secret sharing

Citation Wu C M, Yang L. Qubit-wise teleportation and its application in public-key secret communication. Sci China Inf Sci, 2017, 60(3): 032501, doi: 10.1007/s11432-016-0152-4

1 Introduction

The characteristics of quantum teleportation are that the quantum state does not appear in the channel and that only classical information is transmitted. Quantum teleportation emphasizes the interchangeability of different resources in quantum mechanics. A shared EPR (Einstein-Podolsky-Rosen) pair together with two classical bits of communication is a resource that is at least equal to one qubit of communication. Quantum information has revealed a plethora of methods for interchanging resources built upon quantum teleportation, such as entanglement swapping [1, 2] and quantum remote control [3]. A complete hyperentanglement Bell-state analysis was proposed in [4], which is also applied to the quantum teleportation of a particle in an unknown state in two different degrees of freedom. A quantum teleportation of multiple degrees of freedom was proposed in [5], which uses photon pairs entangled in two degrees of freedom as a quantum channel for teleportation. In [6], a protocol was proposed that can be used for teleporting living cells between two remote organisms. A mathematical formalism of teleportation in

* Corresponding author (email: yangli@iie.ac.cn)

Table 1 The unitary operation that Alice can perform to recover the original state corresponding to Bob's measurement

Bob's measurement	Alice's state	P_i
$\|\Phi^+\rangle_{1,2}$	$\alpha U_k\|0\rangle_3 + \beta U_k\|1\rangle_3$	I
$\|\Phi^-\rangle_{1,2}$	$\alpha U_k\|0\rangle_3 - \beta U_k\|1\rangle_3$	Z
$\|\Psi^+\rangle_{1,2}$	$\alpha U_k\|1\rangle_3 + \beta U_k\|0\rangle_3$	X
$\|\Psi^-\rangle_{1,2}$	$\alpha U_k\|1\rangle_3 - \beta U_k\|0\rangle_3$	ZX

terms of anti-conjugate linearity was developed in [7]. Moreover, the notion of teleportation extends to a multi-qubit state [8–14], which is always realized by using multipartite entanglement. This method, however, increases the complexity greatly with the number of parties involved. Another way to realize it is through controlled teleportation, which is actually a "one-to-one" quantum information transmission with the control of agents in a network. Entanglement generation and distribution were studied and developed in [15–17], which can be used for the experimental realization of teleportation. To resist quantum attacks [18–20] on a public-key encryption protocol, we have come up with two ways to achieve this purpose. One is to study a post-quantum public-key encryption protocol, such as a public-key cryptosystem based on complexity under a quantum environment [21]. The other is to construct a quantum public-key encryption (QPKE) protocol. Currently, QPKE [22–26], quantum secret sharing [27–36], and quantum secure direct communication protocols [37–40] have attracted much attention, and the application of teleportation to these protocols [41] is also in great demand. Gottesman [23] was the first to apply teleportation to QPKE of one-qubit. In his protocol, he achieved the goal of single-qubit teleportation. Since 2003, a series of QPKE protocols for quantum plaintext have been proposed [25, 26, 42, 43]. However, these QPKE schemes [25, 26] have only achieved computational security. Liang et al. [43] proposed a quantum-message-oriented QPKE protocol that claims to achieve information-theoretic security, but its outcome is bounded information-theoretic security. As shown in [42], the protocol proposed in [43] can be attacked via applying a Hadamard transformation to get the private-key. Thus far, there is no QPKE protocol capable of transmitting a multi-qubit unknown state with information theoretic security. In this paper, we apply qubit-wise teleportation to construct a QPKE protocol for transmitting a two-qubit message and then generalize the protocol to send a multi-qubit message. A multipartite quantum secret state sharing protocol is also proposed based on a multi-qubit-oriented QPKE scheme.

2 Preliminaries

2.1 Gottesman's QPKE scheme

Gottesman proposed the first public-key encryption protocol with information theoretic security for a single-qubit plaintext [23].

Key generation

(1) Alice randomly chooses k as a private-key. k is considered as the controlled element in the unitary operation U_k.

(2) She uses U_k to prepare her public-key $|\varphi\rangle = \frac{1}{\sqrt{2}}(I \otimes U_k)(|0\rangle|0\rangle + |1\rangle|1\rangle)$.

(3) She then stores her public-key in the public-key registers.

Encryption

(1) Bob downloads Alice's public-key from the public-key registers.

(2) Bob uses the said key to encrypt a quantum message $|m_1\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1$, where $|\alpha|^2 + |\beta|^2 = 1$. Bob teleports the quantum message through the public-key:

$$|m_1\rangle_1|\varphi\rangle_{2,3} = \frac{1}{\sqrt{2}}(\alpha|0\rangle_1 + \beta|1\rangle_1)(|0\rangle_2 \otimes U_k|0\rangle_3 + |1\rangle_2 \otimes U_k|1\rangle_3). \quad (1)$$

(3) Bob performs a Bell-state measurement on the first and second particles, and then he gets the corresponding Pauli matrix P_i. For instance, if the result of the measurement is $|\Psi^+\rangle$, the corresponding operation is $U_k \circ X$, and the Pauli matrix is X. A concrete situation is shown in Table 1.

(4) Bob then sends Alice the ciphertext $(P_i, U_k P_i|m_1\rangle_1)$ along with the second particle of the public-key, which is particle 3.

Decryption After receiving the ciphertext $(P_i, U_k P_i|m_1\rangle_1)$, Alice decrypts it by performing U_k^{-1} and then P_i^{-1} to get the plaintext $|m_1\rangle$.

2.2 Teleportation of a multi-qubit state

Yang and Guo [44] generalized an earlier scheme of Bennett et al. known as quantum teleportation to a multi-particle case. Teleporting an unknown quantum state of N two-state message particles requires N-EPR pairs and N-time manipulations. The whole system is $|\Psi\rangle = \sum_{i=1}^{2^N} a_i \prod_{k=1}^{N} |u_{ik}\rangle_k \otimes \prod_{k=1}^{N} |\Psi^-\rangle_{k'k''}$, where $\prod_{k=1}^{N} |u_{ik}\rangle_k = |u_{i1}\rangle_1 |u_{i2}\rangle_2 |u_{iN}\rangle_N$, $|\Psi^-\rangle_{k'k''} = \frac{1}{\sqrt{2}}(|1\rangle_{k'}|0\rangle_{k''} - |0\rangle_{k'}|1\rangle_{k''})$ is the Bell basis singlet state of the kth EPR pair $P_k(k', k'')$. The sender sends one EPR particle of the first EPR pair to the receiver. Then the sender performs a joint Bell-state measurement on the remaining EPR particle and the first message particle 1, and sends the classical result of this measurement to the receiver through a classical channel. The receiver is able to apply a corresponding unitary transformation on the EPR particle to reconstruct the message particle. By repeating these manipulations, the scheme enables the unknown quantum state of N two-state particles belonging to the sender to be teleported to Bob.

There is a simple demonstration of the teleportation of a multi-qubit state[1)]. Suppose that the multi-qubit state is $|\psi\rangle_{1,\ldots,N} = |0\rangle_1 |x_0\rangle_{2,\ldots,N} + |1\rangle_1 |x_1\rangle_{2,\ldots,N}$. The participants use $|\Phi^+\rangle_{AB}$ as a quantum channel to teleport. The participant Alice teleports the first particle to participant Bob through the quantum channel and then performs a measurement on particles 1 and A. The whole system after the measurement is

$$\begin{aligned}
|\psi\rangle_{1,\ldots,N}|\Phi^+\rangle_{AB} &= (|0\rangle_1|x_0\rangle_{2,\ldots,N} + |1\rangle_1|x_1\rangle_{2,\ldots,N})|\phi^+\rangle_{AB} \\
&= \frac{1}{2}|\Phi^+\rangle_{1A}(|x_0\rangle_{2,\ldots,N}|0\rangle_B + |x_1\rangle_{2,\ldots,N}|1\rangle_B) \\
&\quad + \frac{1}{2}|\Phi^-\rangle_{1A}(|x_0\rangle_{2,\ldots,N}|0\rangle_B - |x_1\rangle_{2,\ldots,N}|1\rangle_B) \\
&\quad + \frac{1}{2}|\Psi^-\rangle_{1A}(|x_0\rangle_{2,\ldots,N}|1\rangle_B - |x_1\rangle_{2,\ldots,N}|0\rangle_B) \\
&\quad + \frac{1}{2}|\Psi^+\rangle_{1A}(|x_0\rangle_{2,\ldots,N}|1\rangle_B + |x_1\rangle_{2,\ldots,N}|0\rangle_B). \qquad (2)
\end{aligned}$$

If the measurement outcome is $|\Psi^-\rangle_{1A}$, the message receiver applies Pauli transformation Z to obtain $|0\rangle_B|x_0\rangle_{2,\ldots,N} + |1\rangle_B|x_1\rangle_{2,\ldots,N} = |\psi\rangle_{B,2,\ldots,N}$. The state $|\psi\rangle_{B,2,\ldots,N} = |0\rangle_2|x'_{B,3,\ldots,N}\rangle + |1\rangle_2|x''_{B,3,\ldots,N}\rangle$.

Alice repeats the above steps to teleport the remaining particles.

We also give a formal proof of the qubit-wise teleportation of a multi-qubit unknown state based on mathematical introduction, which is shown in Appendix A. A multi-qubit unknown state that can be transmitted through qubit-wise teleportation was realized experimentally in [45] and theoretically in [46, 47], which lacks a strict proof.

3 Detailed description of the proposed QPKE protocol

Gottesman's single-qubit-oriented QPKE protocol based on teleportation is information-theoretically secure. However, there is no QPKE protocol capable of transmitting a multi-qubit unknown state. The construction of such protocol is simple, but also deserves some research. Moreover, there are quantum-message-oriented QPKE protocols with computational security, and we hope to construct one with information-theoretic security.

First, we construct a QPKE protocol for transmitting a two-qubit message via qubit-wise teleportation and then extend this protocol to a multi-qubit message.

1) This proof is from Zheng-Wei Zhou.

Table 2 The unitary operation P_{i_1} contained in the ciphertext corresponding to Bob's first measurement

Bob's measurement	Alice's state	P_{i_1}
$\|\Phi^+\rangle_{1,3}$	$\alpha\|0\rangle_2\otimes U_{k_1}\|0\rangle_4+\beta\|1\rangle_2\otimes U_{k_1}\|1\rangle_4+\gamma\|0\rangle_2\otimes U_{k_1}\|1\rangle_4+\delta\|1\rangle_2\otimes U_{k_1}\|0\rangle_4$	I
$\|\Phi^-\rangle_{1,3}$	$\alpha\|0\rangle_2\otimes U_{k_1}\|0\rangle_4-\beta\|1\rangle_2\otimes U_{k_1}\|1\rangle_4-\gamma\|0\rangle_2\otimes U_{k_1}\|1\rangle_4+\delta\|1\rangle_2\otimes U_{k_1}\|0\rangle_4$	Z
$\|\Psi^+\rangle_{1,3}$	$\alpha\|0\rangle_2\otimes U_{k_1}\|1\rangle_4+\beta\|1\rangle_2\otimes U_{k_1}\|0\rangle_4+\gamma\|0\rangle_2\otimes U_{k_1}\|0\rangle_4+\delta\|1\rangle_2\otimes U_{k_1}\|1\rangle_4$	X
$\|\Psi^-\rangle_{1,3}$	$\alpha\|0\rangle_2\otimes U_{k_1}\|1\rangle_4-\beta\|1\rangle_2\otimes U_{k_1}\|0\rangle_4-\gamma\|0\rangle_2\otimes U_{k_1}\|0\rangle_4+\delta\|1\rangle_2\otimes U_{k_1}\|1\rangle_4$	ZX

Table 3 The unitary operation P_{i_2} contained in the ciphertext corresponding to Bob's second measurement

Bob's measurement	Alice's state	P_{i_2}
$\|\Phi^+\rangle_{2,5}$	$\alpha\|0\rangle_1\otimes U_{k_2}\|0\rangle_6+\beta\|1\rangle_1\otimes U_{k_2}\|1\rangle_6+\gamma\|0\rangle_1\otimes U_{k_2}\|1\rangle_6+\delta\|1\rangle_1\otimes U_{k_2}\|0\rangle_6$	I
$\|\Phi^-\rangle_{2,5}$	$\alpha\|0\rangle_1\otimes U_{k_2}\|0\rangle_6-\beta\|1\rangle_1\otimes U_{k_2}\|1\rangle_6-\gamma\|0\rangle_1\otimes U_{k_2}\|1\rangle_6+\delta\|1\rangle_1\otimes U_{k_2}\|0\rangle_6$	Z
$\|\Psi^+\rangle_{2,5}$	$\alpha\|0\rangle_1\otimes U_{k_2}\|1\rangle_6+\beta\|1\rangle_1\otimes U_{k_2}\|0\rangle_6+\gamma\|0\rangle_1\otimes U_{k_2}\|0\rangle_6+\delta\|1\rangle_1\otimes U_{k_2}\|1\rangle_6$	X
$\|\Psi^-\rangle_{2,5}$	$\alpha\|0\rangle_1\otimes U_{k_2}\|1\rangle_6-\beta\|1\rangle_1\otimes U_{k_2}\|0\rangle_6-\gamma\|0\rangle_1\otimes U_{k_2}\|0\rangle_6+\delta\|1\rangle_1\otimes U_{k_2}\|1\rangle_6$	ZX

3.1 QPKE protocol for transmitting a two-qubit unknown state

Key generation

(1) Alice randomly chooses a Boolean function F from the mapping $F:\{0,1\}^m\mapsto\{0,1\}^n$ as a private-key and selects bit string s, $s\in Z_{2^m}$.

(2) She computes k according to the following relationship: $F(s)=k$, $k=(k_1,\ldots,k_n)$. She uses U_k to prepare her public-key $|\varphi_s\rangle=\frac{1}{\sqrt{2}}(I\otimes U_k)(|0\rangle|0\rangle+|1\rangle|1\rangle)$.

(3) She sends the public-key $(s,|\varphi_s\rangle)$ to the public-key registers, which keeps one half of the quantum part of the public-key $|\varphi_s\rangle$, while the other part remains with her.

We should note that bit string s varies, so $|\varphi_s\rangle$ is also changed along with s. Thus, a private-key F corresponds to an exponential number of public-keys. Each public-key will only be used once.

Encryption

(1) To transmit a two-qubit message, Bob downloads Alice's public-keys $(s_1,|\varphi_{s_1}\rangle)$ and $(s_2,|\varphi_{s_2}\rangle)$ from the public-key registers.

(2) Bob uses Alice's public-key to encrypt a quantum message $|m_2\rangle_{1,2}=\alpha|00\rangle_{1,2}+\beta|11\rangle_{1,2}+\gamma|01\rangle_{1,2}+\delta|10\rangle_{1,2}$ and sends the first particle to Alice first,

$$|m_2\rangle_{1,2}|\varphi_{s_1}\rangle_{3,4}=\frac{1}{\sqrt{2}}(\alpha|00\rangle_{1,2}+\beta|11\rangle_{1,2}+\gamma|01\rangle_{1,2}+\delta|10\rangle_{1,2})(|0\rangle_3\otimes U_{k_1}|0\rangle_4+|1\rangle_3\otimes U_{k_1}|1\rangle_4). \quad (3)$$

Bob performs a Bell-state measurement on particles 1 and 3, the outcome of which will be one of these four with equal probability $\frac{1}{4}$: $|\Phi^+\rangle_{1,3}$, $|\Phi^-\rangle_{1,3}$, $|\Psi^+\rangle_{1,3}$, and $|\Psi^-\rangle_{1,3}$; Thus, Bob has the corresponding operations P_{i1}: I, Z, X, and ZX according to the result of the measurement. The four cases are shown in Table 2.

(3) Bob sends the second particle by repeating the same procedure above. That is, Bob teleports the second particle in message $|m_2\rangle$ by using the public-key $|\varphi_{s_2}\rangle$,

$$|m_2\rangle_{1,2}|\varphi_{s_2}\rangle_{5,6}=\frac{1}{\sqrt{2}}(\alpha|00\rangle_{1,2}+\beta|11\rangle_{1,2}+\gamma|01\rangle_{1,2}+\delta|10\rangle_{1,2})(|0\rangle_5\otimes U_{k_2}|0\rangle_6+|1\rangle_5\otimes U_{k_2}|1\rangle_6). \quad (4)$$

After the measurement, he obtains the corresponding Pauli matrix, which is shown in Table 3.

Bob gets the corresponding Pauli matrix P_{i2} and sends Alice the ciphertext $(s_1,s_2,P_{i_2},P_{i_1},U_{k_2}P_{i_2}\otimes U_{k_1}P_{i_1}|m_2\rangle_{1,2})$.

Decryption After receiving the ciphertext $(s_1,s_2,P_{i_2},P_{i_1},U_{k_2}P_{i_2}\otimes U_{k_1}P_{i_1}|m_2\rangle_{1,2})$, Alice computes $F(s_1)=k_1$ and $F(s_2)=k_2$. Then she decrypts it by performing the combination of $U_{k_1}^{-1}$, $U_{k_2}^{-1}$ and $P_{i_1}^{-1}$, $P_{i_2}^{-1}$ to get the plaintext $|m_2\rangle$.

3.2 QPKE protocol for transmitting a multi-qubit unknown state

Now, we show the generalization of the QPKE scheme for qubit-wise multi-qubit transmission.

Key generation

(1) Alice randomly chooses a Boolean function F from the mapping $F : \{0,1\}^m \mapsto \{0,1\}^n$ as a private-key and selects bit string s, $s \in Z_{2^m}$.

(2) She prepares the public-key according to the relationship $F(s) = k$ and then sends her public-key $(s, |\varphi_s\rangle)$ to the public-key registers.

Encryption

(1) Bob downloads Alice's public-key $|\varphi_{s_1}\rangle, \ldots, |\varphi_{s_n}\rangle$ from the public-key registers. The whole state for this system is

$$|m_3\rangle_{1,\ldots,n} \otimes |\varphi_{s_1}\rangle_{n+1,n+2} \otimes \cdots \otimes |\varphi_{s_n}\rangle_{3n-1,3n}. \tag{5}$$

(2) If Bob has already performed a qubit-wise transmission of the quantum state of the first $(n-1)$-particle in the n-qubit state, then he gets the operations P_{i_1}, P_{i_2},..., $P_{i_{n-1}}$. Bob teleports the last qubit using Alice's public-key $|\varphi_{s_n}\rangle_{3n-1,3n}$:

$$\begin{aligned}|m_3\rangle_{1,\ldots,n}|\varphi_{s_n}\rangle_{3n-1,3n} &= \sum_{i_1\ldots i_n} \alpha_{i_1\ldots i_n}|i_1\ldots i_n\rangle_{1,\ldots,n}|\varphi_{s_n}\rangle_{3n-1,3n}\\ &= \frac{1}{\sqrt{2}}\Bigg(\sum_{i_1^{'}\ldots i_{n-1}^{'}} \alpha^{'}_{i_1^{'}\ldots i_{n-1}^{'}}|i_1^{'}\ldots i_{n-1}^{'}\rangle_{1,\ldots,n-1}|0\rangle_n\\ &\quad + \sum_{i_1^{''}\ldots i_{n-1}^{''}} \alpha^{''}_{i_1^{''}\ldots i_{n-1}^{''}}|i_1^{''}\ldots i_{n-1}^{''}\rangle_{1,\ldots,n-1}|1\rangle_n\Bigg)\\ &\quad \times(|0\rangle_{3n-1}\otimes U_{k_n}|0\rangle_{3n} + |1\rangle_{3n-1}\otimes U_{k_n}|1\rangle_{3n}).\end{aligned} \tag{6}$$

(3) Bob performs a Bell-state measurement on particles $n, 3n-1$. If the measurement outcomes are $|\Psi^+\rangle_{n,3n-1}$, $|\Psi^-\rangle_{n,3n-1}$, $|\Phi^+\rangle_{n,3n-1}$ and $|\Phi^-\rangle_{n,3n-1}$, the corresponding transformation will be I, Z, X, and ZX, respectively. Bob obtains the Pauli transformation through the measurement and sends Alice the ciphertext:

$$(s_1, \ldots, s_n, P_{i_n}, \ldots, P_{i_1}, U_{k_n}P_{i_n} \otimes \cdots \otimes U_{k_1}P_{i_1}|m_3\rangle_{1,\ldots,n}).$$

Decryption Alice performs a computation based on the equation $F(s) = k$ and obtains $(k_1, \ldots, k_n)$. Then, she uses k_i to apply the unitary operation U_{k_i} and the Pauli transformation P_i to decrypt the ciphertext to obtain the transmitted message.

3.3 Security analysis

The security of the proposed QPKE protocol is analyzed from two aspects: security of the encryption and security of the private-key.

3.3.1 *Security of the encryption*

In the QPKE protocol for a two-qubit message, if the attacker Eve intercepts the transmitted ciphertext, she tries to guess the correct private-key F to decrypt the message. Since the private-key F is an m-input, n-output Boolean function, it can be expressed as follows: $F(s) = (F^{(1)}(s), \ldots, F^{(n)}(s))$.

The minor term expression of every $F^{(j)}(s)$ is $F^{(j)}(s) = (s_1^{a_{j,1,1}}\cdot\ldots\cdot s_n^{a_{j,1,n}})\oplus\cdots\oplus(s_1^{a_{j,p(n),1}}\cdot\ldots\cdot s_n^{a_{j,p(n),n}})$. Each term $s_1^{a_{j,\alpha,1}}\cdot\ldots\cdot s_n^{a_{j,\alpha,n}}$ can be determined by n coin tosses. If we toss the coin $np(n)$ times, $p(n)$ components are determined. Therefore, the Boolean function F will be efficiently generated by $n^2p(n)$ coin tosses. The probability of the attacker Eve guessing the correct private-key F is $\frac{1}{2^{n^2p(n)}}$. Such a probability is negligible. Thus, the attacker cannot decrypt the ciphertext by producing a correct private-key. Similar to the transmission of a two-qubit message, in the multi-qubit-oriented QPKE scheme, the attacker's probability of obtaining the correct private-key is also $\frac{1}{2^{n^2p(n)}}$.

If the attacker tries to guess k_i, the probability of guessing the correct k_i is $\frac{1}{2}$. The whole probability for Eve of acquiring the corresponding operation U_k is $\frac{1}{2^n}$. In the multi-qubit message case, the probability is negligible. Thus, our scheme is secure from an intercept attack.

Next, we consider the case where the attacker Eve intercepts two ciphertexts ρ_1 and ρ_2, where

$$\rho_1 = \sum_F U_{F(s_n)}P_{i_n} \otimes \cdots \otimes U_{F(s_1)}P_{i_1}|m_3\rangle\langle m_3|(U_{F(s_n)}P_{i_n} \otimes \cdots \otimes U_{F(s_1)}P_{i_1})^\dagger$$

and

$$\rho_2 = \sum_{F'} U_{F'(s_n)}P'_{i_n} \otimes \cdots \otimes U_{F'(s_1)}P'_{i_1}|m_3\rangle\langle m_3|(U_{F'(s_n)}P'_{i_n} \otimes \cdots \otimes U_{F'(s_1)}P'_{i_1})^\dagger.$$

We denote that $P_{i_1,\ldots,i_n} = P_{i_1} \otimes \ldots \otimes P_{i_n}$ and $U_{1,\ldots,n} = U_{F(s_n)} \otimes \ldots \otimes U_{F(s_1)}$, so the expression of ρ_1 can be rewritten as follows:

$$\rho_1 = \sum_F U_{1,\ldots,n} \otimes P_{i_1,\ldots,i_n}|m_3\rangle\langle m_3|P_{i_1,\ldots,i_n} \otimes U_{1,\ldots,n}. \tag{7}$$

Since F iterates through all the possible values for a given s, the quantum state ρ_1 is an ultimate state if the unknown state $|m_3\rangle\langle m_3|$ is randomly and independently selected. The situation is similar with ρ_2. We can obtain the trace distance for these two ciphertexts as

$$D(\rho_1, \rho_2) = 0. \tag{8}$$

The definition of information-theoretic quantum ciphertext-indistinguishability for the QPKE protocol is presented in [48]: a QPKE scheme is information-theoretically ciphertext-indistinguishable if every quantum circuit family $\{C_n\}$, every positive polynomial $p(\cdot)$, all sufficiently large n, and any two plaintexts x and y, satisfy

$$\left|\Pr\left[C_n(G(1^n), E_{G(1^n)}(x)) = 1\right] - \Pr\left[C_n(G(1^n), E_{G(1^n)}(y)) = 1\right]\right| < \frac{1}{p(n)}, \tag{9}$$

where G is the key generation algorithm, E is the quantum encryption algorithm, and the ciphertexts $E(x)$ and $E(y)$ are the quantum states. It is also proven that a QPKE scheme is information-theoretically secure if the trace distance between any two ciphertexts is $O(\frac{1}{2^n})$ [48] and Eq. (9) holds. According to the definition, the attacker Eve cannot distinguish any two ciphertexts encrypted by different private-keys because of (8).

Finally, we consider the case where the attacker Eve acquires two different ciphertexts encrypted by different public-keys corresponding to the same private-key. The ciphertexts can be denoted as

$$\sigma_1 = \sum_F U_{F(s_n)}P_{i_n} \otimes \cdots \otimes U_{F(s_1)}P_{i_1}|m_3\rangle\langle m_3|(U_{F(s_n)}P_{i_n} \otimes \cdots \otimes U_{F(s_1)}P_{i_1})^\dagger$$

and

$$\sigma_2 = \sum_F U_{F(s_n)}P_{i_n} \otimes \cdots \otimes U_{F(s_1)}P_{i_1}|m'_3\rangle\langle m'_3|(U_{F(s_n)}P_{i_n} \otimes \cdots \otimes U_{F(s_1)}P_{i_1})^\dagger.$$

On the basis of the above analysis, we can prove that σ_1 and σ_2 are both ultimately mixed states. Therefore, the trace distance between the two different ciphertexts encrypted by the same private-key is zero, i.e., $D(\sigma_1, \sigma_2) = 0$.

Thus, the proposed QPKE protocol is information-theoretically secure from attacks on the encryption.

3.3.2 *Security of the private-key*

According to the proposed scheme, only one copy of each quantum public-key $(s, |\varphi_s\rangle)$ is allowed to be generated from s and F. Thus, any two public-keys are different for a user and a private-key corresponds to an exponential number of public-keys. We should note that each public-key is only used once, so an attack on the ciphertext is equal to an attack on a quantum one-time pad [49–51].

If a malicious message sender downloads a user's public-key and then measures it, the public-key state for him is

$$\rho_1 = \sum_F p_F|\varphi_s\rangle\langle\varphi_s| = \frac{1}{2}\sum_F p_F(|0\rangle\langle 0| \otimes U_{F(s)}|0\rangle\langle 0|U_{F(s)} + |1\rangle\langle 1| \otimes U_{F(s)}|1\rangle\langle 1|U_{F(s)}). \tag{10}$$

For every given s, $F(s)$ iterates through all the possible values. Therefore, the quantum states $\sum_F(U_{F(s)}|0\rangle\langle 0|U_{F(s)})$ and $\sum_F(U_{F(s)}|1\rangle\langle 1|U_{F(s)})$ are ultimately mixed states. Moreover, the number of possible values of F is $2^{n^2p(n)}$, and that of k is 2^n. F iterates through all the possible values of k. Thus, the public-key state for a malicious message sender can be expressed as

$$\rho_1 = \frac{1}{2}\sum_F p_F\left(|0\rangle\langle 0|\otimes\frac{I}{2^n}+|1\rangle\langle 1|\otimes\frac{I}{2^n}\right)=\frac{1}{2}(|0\rangle\langle 0|+|1\rangle\langle 1|)\otimes\frac{I}{2^n}=\frac{I}{2}\otimes\frac{I}{2^n}=\frac{I}{2^{n+1}}. \tag{11}$$

The public-key state is an ultimately mixed state for a malicious message sender who has no idea about the private-key F. By measuring such an ultimately mixed state, the malicious message sender cannot obtain any useful information from the private-key F. The relation between s and F is as follows: $F(s)=k$. If s and k are known, F can be solved. Since a private-key corresponds to an exponential number of public-keys, extracting the value of k by measurement is the same as attacking a one-time pad in classical cryptography. Therefore, extracting the value of k is information-theoretically impossible. Furthermore, if the attacker has a public-key $(s,|\varphi_s\rangle)$, it is impossible for him/her to determine the private-key from the bit string s and the ciphertext. However, the trace distance between two different public-keys is 0, i.e., $D(|\varphi_{s_1}\rangle,|\varphi_{s_2}\rangle)=0$, because the public-key state for someone who is not in possession of the private-key is an ultimately mixed state.

4 Multi-partite secret sharing with n agents

In this section, we introduce a multi-party secret sharing scheme of an unknown quantum state based on qubit-wise teleportation. First, we give a simple example of a two-qubit quantum state with two agents.

Assume that there are two agents, Bob and Charlie. Alice is the secret dealer who wants to distribute an unknown arbitrary two-qubit state between Bob and Charlie. Only when Bob and Charlie cooperate can they recover the unknown quantum state.

At the beginning, Alice downloads Bob's public-key $(s_B,|\varphi_{s_B}\rangle)$, where $|\varphi_B\rangle=\frac{1}{\sqrt{2}}(I\otimes U_{k_B})(|0\rangle|0\rangle+|1\rangle|1\rangle)$, and also gets Charlie's public-key $(s_C,|\varphi_{s_C}\rangle)$, where $|\varphi_C\rangle=\frac{1}{\sqrt{2}}(I\otimes U_{k_C})(|0\rangle|0\rangle+|1\rangle|1\rangle)$, from the public-key registers. Particles 1 and 2 are in an unknown arbitrary two-qubit state, which can be described as follows:

$$|m_2\rangle_{1,2}=\alpha|00\rangle_{1,2}+\beta|11\rangle_{1,2}+\gamma|01\rangle_{1,2}+\delta|10\rangle_{1,2},$$

where

$$|\alpha|^2+|\beta|^2+|\gamma|^2+|\delta|^2=1.$$

The whole system of the six particles can be written as

$$|m_2\rangle_{1,2}\otimes|\varphi_B\rangle_{3,4}\otimes|\varphi_C\rangle_{5,6}. \tag{12}$$

Alice transfers the quantum state of the two particles to Bob and Charlie consequently through qubit-wise teleportation.

(1) First, Alice uses Bob's public-key to transfer the local quantum state of particle 1. Alice performs a Bell-state measurement on particles 1 and 3 and then tells Bob the measurement outcome,

$$\begin{aligned}|m_2\rangle_{1,2}|\varphi_B\rangle_{3,4}=&\frac{1}{2}|\Phi^+\rangle_{1,3}(\alpha|0\rangle_2\otimes U_{k_B}|0\rangle_4+\beta|1\rangle_2\otimes U_{k_B}|1\rangle_4+\gamma|0\rangle_2\otimes U_{k_B}|1\rangle_4+\delta|1\rangle_2\otimes U_{k_B}|0\rangle_4)\\&+\frac{1}{2}|\Phi^-\rangle_{1,3}(\alpha|0\rangle_2\otimes U_{k_B}|0\rangle_4-\beta|1\rangle_2\otimes U_{k_B}|1\rangle_4-\gamma|0\rangle_2\otimes U_{k_B}|1\rangle_4+\delta|1\rangle_2\otimes U_{k_B}|0\rangle_4)\\&+\frac{1}{2}|\Psi^+\rangle_{1,3}(\alpha|0\rangle_2\otimes U_{k_B}|1\rangle_4+\beta|1\rangle_2\otimes U_{k_B}|0\rangle_4+\gamma|0\rangle_2\otimes U_{k_B}|0\rangle_4+\delta|1\rangle_2\otimes U_{k_B}|1\rangle_4)\\&+\frac{1}{2}|\Psi^-\rangle_{1,3}(\alpha|0\rangle_2\otimes U_{k_B}|1\rangle_4-\beta|1\rangle_2\otimes U_{k_B}|0\rangle_4\end{aligned}$$

$$-\gamma|0\rangle_2 \otimes U_{k_B}|0\rangle_4 + \delta|1\rangle_2 \otimes U_{k_B}|1\rangle_4). \tag{13}$$

(2) Then, Alice teleports the local quantum state of particle 2 to Charlie using the same method. After she performs the Bell-state measurement, the subsystem becomes

$$\begin{aligned}|m_2\rangle_{1,2}|\varphi_C\rangle_{5,6} = {} & \frac{1}{2}|\Phi^+\rangle_{2,5}(\alpha|0\rangle_1 \otimes U_{k_C}|0\rangle_6 + \beta|1\rangle_1 \otimes U_{k_C}|1\rangle_6 + \gamma|0\rangle_1 \otimes U_{k_C}|1\rangle_6 + \delta|1\rangle_1 \otimes U_{k_C}|0\rangle_6)\\ & +\frac{1}{2}|\Phi^-\rangle_{2,5}(\alpha|0\rangle_1 \otimes U_{k_C}|0\rangle_6 - \beta|1\rangle_1 \otimes U_{k_C}|1\rangle_6 - \gamma|0\rangle_1 \otimes U_{k_C}|1\rangle_6 + \delta|1\rangle_1 \otimes U_{k_C}|0\rangle_6)\\ & +\frac{1}{2}|\Psi^+\rangle_{2,5}(\alpha|0\rangle_1 \otimes U_{k_C}|1\rangle_6 e + \beta|1\rangle_1 \otimes U_{k_C}|0\rangle_6 + \gamma|0\rangle_1 \otimes U_{k_C}|0\rangle_6 + \delta|1\rangle_1 \otimes U_{k_C}|1\rangle_6)\\ & +\frac{1}{2}|\Psi^-\rangle_{2,5}(\alpha|0\rangle_1 \otimes U_{k_C}|1\rangle_6 - \beta|1\rangle_1 \otimes U_{k_C}|0\rangle_6\\ & -\gamma|0\rangle_1 \otimes U_{k_C}|0\rangle_6 + \delta|1\rangle_1 \otimes U_{k_C}|1\rangle_6). \end{aligned}\tag{14}$$

(3) If Alice's measurement outcomes are $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, and $|\Psi^-\rangle$, the operations for Bob and Charlie cooperating to reconstruct the unknown quantum state are I, Z, X, and ZX, respectively.

Next, we consider the n-party quantum state sharing scheme with n agents. Suppose that the n-qubit quantum state is $|m_3\rangle = \sum_{i_1\ldots i_n} \alpha_{i_1\ldots i_n}|i_1\ldots i_n\rangle_{1,\ldots,n}$. Suppose that the n agents are $\mathrm{Bob}_1,\ldots,\mathrm{Bob}_n$; the corresponding public-key is $(s_{B_i}, |\varphi_{B_i}\rangle)$. The whole system is $|m_3\rangle_{1,\ldots,n} \otimes |\varphi_{B_1}\rangle \otimes \cdots \otimes |\varphi_{B_n}\rangle$. Only when $\mathrm{Bob}_1,\ldots,\mathrm{Bob}_n$ cooperate together will they be able to reconstruct the unknown multi-qubit message.

For each Bob_i, Alice teleports one particle to him. If Alice performs a Bell-state measurement, the subsystem becomes

$$\begin{aligned}|m_3\rangle_{1,\ldots,n} \otimes |\varphi_{B_i}\rangle_{n+i,n+i+1} = {} & \frac{1}{2}|\Phi^+\rangle_{n,n+i}\Bigg(\sum_{i_1'\ldots i_{n-1}'} \alpha'_{i_1'\ldots i_{n-1}'}|i_1'\ldots i_{n-1}'\rangle_{1,\ldots,n-1}U_{k_n}|0\rangle_{n+i+1}\\ & + \sum_{i_1''\ldots i_{n-1}''} \alpha''_{i_1''\ldots i_{n-1}''}|i_1''\ldots i_{n-1}''\rangle_{1,\ldots,n-1}U_{k_n}|1\rangle_{n+i+1}\Bigg)\\ & +\frac{1}{2}|\Phi^-\rangle_{n,n+i}\Bigg(\sum_{i_1'\ldots i_{n-1}'} \alpha'_{i_1'\ldots i_{n-1}'}|i_1'\ldots i_{n-1}'\rangle_{1,\ldots,n-1}U_{k_n}|0\rangle_{n+i+1}\\ & - \sum_{i_1''\ldots i_{n-1}''} \alpha''_{i_1''\ldots i_{n-1}''}|i_1''\ldots i_{n-1}''\rangle_{1,\ldots,n-1}U_{k_n}|1\rangle_{n+i+1}\Bigg)\\ & +\frac{1}{2}|\Psi^+\rangle_{n,n+i}\Bigg(\sum_{i_1'\ldots i_{n-1}'} \alpha'_{i_1'\ldots i_{n-1}'}|i_1'\ldots i_{n-1}'\rangle_{1,\ldots,n-1}U_{k_n}|1\rangle_{n+i+1}\\ & + \sum_{i_1''\ldots i_{n-1}''} \alpha''_{i_1''\ldots i_{n-1}''}|i_1''\ldots i_{n-1}''\rangle_{1,\ldots,n-1}U_{k_n}|0\rangle_{n+i+1}\Bigg)\\ & +\frac{1}{2}|\Psi^-\rangle_{n,n+i}\Bigg(\sum_{i_1'\ldots i_{n-1}'} \alpha'_{i_1'\ldots i_{n-1}'}|i_1'\ldots i_{n-1}'\rangle_{1,\ldots,n-1}U_{k_n}|1\rangle_{n+i+1}\\ & - \sum_{i_1''\ldots i_{n-1}''} \alpha''_{i_1''\ldots i_{n-1}''}|i_1''\ldots i_{n-1}''\rangle_{1,\ldots,n-1}U_{k_n}|0\rangle_{n+i+1}\Bigg). \end{aligned}\tag{15}$$

If the measurement outcomes are $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, and $|\Psi^-\rangle$, the corresponding transformation U_i will be I, Z, X, and ZX, respectively. Alice obtains the Pauli transformation through the measurement and sends Bob_i the measurement result U_i. Bob_1,...,Bob_n use the corresponding operation U_i to reconstruct the message sent by Alice.

If Alice directly distributes the quantum state to n agents, a substitution attack and a man-in-the-middle attack will be effective. The application, however, of the proposed QPKE scheme to a secret sharing protocol can resist these attacks.

5 Discussion and conclusion

Compared with the existing methods for realizing quantum teleportation, qubit-wise teleportation neither introduces an auxiliary particle nor uses multipartite entanglement. The owner of a multi-qubit unknown state transfers the local quantum state to the receiver via qubit-wise teleportation, and the interchangeability of resources is realized between them. Moreover, it only requires the receiver to implement a local unitary operation to reconstruct the multi-qubit unknown state. The proposed QPKE protocol based on qubit-wise teleportation employs a Boolean function to enhance its security, but the disadvantage of this is that, if part of the information in the ciphertext is lost, the communication between the two legal users will fail, and another session will need to be set up. Moreover, our proposed QPKE protocol has some characteristics. First, we use a Boolean function F as a private-key and apply a one-way function to produce the controlled element in the public-key. Second, the public-key varies with different choices of bit strings. A private-key in our scheme corresponds to an exponential number of public-keys, which differs greatly from classical public-key encryption. Third, this proposed QPKE protocol achieves information-theoretic security. Furthermore, we apply qubit-wise teleportation to construct a multi-partite quantum secret state sharing protocol. However, the verification of this secret state sharing protocol needs to be developed.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61173157, 61672517).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Zukowski M, Zeilinger A, Horne M A, et al. "Event-ready-detectors"Bell experiment via entanglement swapping. Phys Rev Lett, 1993, 71: 4287–4290
2 Pan J W, Bouwmeester D, Weinfurter H, et al. Experimental entanglement swapping: entangling photons that never interacted. Phys Rev Lett, 1998, 80: 3891–3894
3 Huelga S F, Vaccaro J A, Chefles A, et al. Quantum remote control: teleportation of unitary operations. Phys Rev A, 2001, 63: 042303
4 Sheng Y B, Deng F G, Long G L. Complete hyperentangled-Bell-state analysis for quantum communication. Phys Rev A, 2010, 82: 032318
5 Wang X L, Cai X D, Su Z E, et al. Quantum teleportation of multiple degrees of freedom of a single photon. Nature, 2015, 518: 516–519
6 Li T C, Yin Z Q. Quantum superpositon, entanglement, and state teleportation of a microorganism on an electromechanical oscillator. Sci Bull, 2016, 61: 163–171
7 Uhlmann A. Anti-(conjugate) linearity. Sci China-Phys Mech Astron, 2016, 59: 630301
8 Yan F L, Yang L G. Ecomomical teleprotation of multiparticle quantum state. Nuovo Cimento Soc Ital Fis B, 2003, 118: 79–82
9 Zheng Y Z, Gu Y J, Wu G C, et al. Teleportation of a multiqubit state by an entangled qubit channel. Chinese Phys, 2003, 12: 1070–1075
10 Pan J W, Daniell M, Gasparoni S, et al. Experimental demonstration of four-photon entanglement and high-fidelity teleportation. Phys Rev Lett, 2001, 86: 4435
11 Zhang Z J, Man Z X. Many-agent controlled teleportation of multi-qubit quantum information. Phys Lett A, 2005, 341: 55–59
12 Zhang Z J, Liu Y M, Man Z X. Many-agent controlled teleportation of multi-qubit quantum information via quantum entanglement swapping. Commun Theory Phys, 2005, 44: 847
13 Yang C P, Chu S I, Han S. Efficient many-party controlled teleportation of multiqubit quantum information via entanglement. Phys A, 2004, 70: 022329
14 Jie Y. Multi-agent controlled teleportation of multi-qubit quantum information via two-step protocol. Chinese Phys, 2005, 14: 2149–2152
15 Wu Y L, Li S J, Ge W, et al. Generation of polarization-entangled photon pairs in a cold atomic ensemble. Sci Bull, 2016, 61: 302–306
16 Cao D Y, Liu B H, Wang Z, et al. Multiuser-to-multiuser entanglement distribution based on 1550 nm polarization-entangled photons. Sci Bull, 2015, 60: 1128–1132
17 René H, Markus G, Stenfan N, et al. A novel integrated quantum circuit for high-order W-state generation and its highly precise characterization. Sci Bull, 2015, 60: 96–100
18 Li F, Bao W, Fu X. A quantum algorithm for the dihedral hidden subgroup problem based on lattice basis reduction

algorithm. Chinese Sci Bull, 2014, 59: 2552–2557
19 Grover L K. Quantum mechanics helps in searching for a needle in haystack. Phys Rev Lett, 1997, 79: 325–328
20 Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Comput, 1997, 26: 1484–1509
21 Wu W Q, Zhang H G, Wang H Z, et al. A public key cryptosystem based on data complexity under quantum environment. Sci China Inf Sci, 2015, 58: 110102
22 Okamoto T, Tanaka K, Uchiyama S. Quantum public-key cryptosystems. In: Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology. London: Springer-Verlag, 2000. 147–165
23 Gottesman D. Quantum public key cryptography with information-theoretic security. In: Proceedings of Workshop on Classical and Quantum Information Security, California, 2005. 15–18
24 Kawachi A, Koshiba T, Nishimura H, et al. Computational indistinguishability between quantum states and its cryptographic application. In: Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2005. 268–284
25 Yang L. Quantum public-key cryptosystem based on classical NP-complete problem. arXiv:quant-ph/0310076, 2003
26 Fujita H. Quantum McEliece public-key cryptosystem. Quantum Inf Comput, 2012, 12: 181–202
27 Deng F G, Li X H, Li C Y, et al. Multiparty quantum secret splitting and quantum state sharing. Phys Lett A, 2006, 354: 190–195
28 Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829
29 Karlsson A, Koashi M, Imoto N. Quantum entanglement for secret sharing and secret splitting. Phys Rev A, 1999, 59: 162
30 Deng F G, Long G L, Zhou H Y. An efficient quantum secret sharing scheme with Einstein-Podolsky-Rosen pairs. Phys Lett A, 2005, 340: 43–50
31 Xiao L, Long G L, Deng F G, et al. Efficient multiparty quantum-secret-sharing schemes. Phys Rev A, 2004, 69: 052307
32 Karimipour V, Bahraminasab A, Bagherinezhad S. Entanglement swapping of generalized cat states and secret sharing. Phys Rev A, 2002, 65: 042320
33 Cleve R, Gottesman D, Lo H K. How to share a quantum secret. Phys Rev Lett, 1999, 83: 648
34 Lance A M, Symul T, Bowen W P, et al. Tripartite quantum state sharing. Phys Rev Lett, 2004, 92: 177903
35 Yang Y G, Wen Q Y. Threshold quantum secret sharing between multi-party and multi-party. Sci China Ser G-Phys Mech Astron, 2008, 51: 1308–1315
36 Yang Y G, Wen Q Y. Circular threshold quantum secret sharing. Chinese Phys B, 2008, 17: 419
37 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002, 65: 032302
38 Boström K, Felbinger T. Deterministic secure direct communication using entanglement. Phys Rev Lett, 2002, 89: 187902
39 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 52319
40 Hoffmann H, Bostroem K, Felbinger T. Comment on Secure direct communication with a quantum one-time pad. Phys Rev A, 2005, 72: 16301
41 Yan F L, Zhang X Q. A scheme for secure direct communication using EPR pairs and teleportation. Eur Phys J B, 2004, 41: 75–78
42 Yang L, Yang B Y, Xiang C. Quantum public-key encryption schemes based on conjugate coding. arXiv:1112.0421
43 Liang M, Yang L. Public-key encryption and authentication of quantum information. Sci China Ser G-Phys Mech Astron, 2012, 55: 1618–1629
44 Yang C P, Guo G C. Multiparticle generalization of teleportation. Chinese Phys Lett, 2000, 17: 162
45 Ikram M, Zhu S Y, Zubairy M S. Quantum teleportation of an entangled state. Phys Rev A, 2000, 62: 022307
46 Lee J, Min H, Oh S D. Multipartite entanglement for entanglement teleportation. Phys Rev A, 2002, 66: 052318
47 Rigolin G. Quantum teleportation of an arbitrary two-qubit state and its relation to multipartite entanglement. Phys Rev A, 2005, 71: 032303
48 Yang L, Xiang C, Li B. Qubit-string-based bit commitment protocols with physical security. arXiv:1011.5099
49 Boykin P O, Roychowdhury V. Optimal encryption of quantum bits. Phys Rev A, 2003, 67: 042317
50 Boykin P O. Information security and quantum mechanics: security of quantum protocols. Dissertation for Ph.D. Degree. Los Angeles: University of California, 2002
51 Ambainis A, Mosca M, Tapp A, et al. Private quantum channels. In: Proceedings of IEEE 54th Symposium on Foundations of Computer Science. Washington: IEEE Computer Society, 2000. 547

Appendix A

In this section, we give a direct demonstration of the proposed method based on mathematical induction.

Proof. First, we consider the case of two-qubit teleportation.

Suppose that an unknown arbitrary two-qubit state can be described as follows:

$$|\psi_0\rangle_{1,2} = \alpha|00\rangle_{1,2} + \beta|11\rangle_{1,2} + \gamma|01\rangle_{1,2} + \delta|10\rangle_{1,2}, \tag{A1}$$

where $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$.

We also assume that both the EPR pairs are originally prepared in one of the four Bell states $|\Phi^+\rangle$. The EPR pairs are preshared by Alice and Bob. That is, $|\Phi^+\rangle_{3,4}\otimes|\Phi^+\rangle_{5,6}$; particles 3 and 5 are retained by Bob and particles 4 and 6 are sent to Alice.

At the beginning, the message sender Bob sends the local quantum state of particle 2 in $|\psi_0\rangle_{1,2}$ to Alice through teleportation:

$$\begin{aligned}|\psi_0\rangle_{1,2}\otimes|\Phi^+\rangle_{3,4} &= \frac{1}{\sqrt{2}}(\alpha|00\rangle_{1,2}+\beta|11\rangle_{1,2}+\gamma|01\rangle_{1,2}+\delta|10\rangle_{1,2})(|0\rangle_3|0\rangle_4+|1\rangle_3|1\rangle_4)\\ &= \frac{1}{\sqrt{2}}(\alpha|0\rangle_1|00\rangle_{2,3}|0\rangle_4+\alpha|0\rangle_1|01\rangle_{2,3}|1\rangle_4+\beta|1\rangle_1|10\rangle_{2,3}|0\rangle_4\\ &\quad+\beta|1\rangle_1|11\rangle_{2,3}|1\rangle_4+\gamma|0\rangle_1|10\rangle_{2,3}|0\rangle_4+\gamma|0\rangle_1|11\rangle_{2,3}|1\rangle_4\\ &\quad+\delta|1\rangle_1|00\rangle_{2,3}|0\rangle_4+\delta|1\rangle_1|01\rangle_{2,3}|1\rangle_4).\end{aligned}\tag{A2}$$

If Bob performs a Bell-state measurement on particles 2 and 3, the measurement outcomes will be one of these four states: $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, and $|\Psi^-\rangle$, which will occur with equal probability $\frac{1}{4}$. Consequently, the subsystem becomes

$$\begin{aligned}|\psi_0\rangle_{1,2}\otimes|\Phi^+\rangle_{3,4} &= \frac{1}{2}|\Phi^+\rangle_{2,3}(\alpha|00\rangle_{1,4}+\beta|11\rangle_{1,4}+\gamma|01\rangle_{1,4}+\delta|10\rangle_{1,4})\\ &\quad+\frac{1}{2}|\Phi^-\rangle_{2,3}(\alpha|00\rangle_{1,4}-\beta|11\rangle_{1,4}-\gamma|01\rangle_{1,4}+\delta|10\rangle_{1,4})\\ &\quad+\frac{1}{2}|\Psi^+\rangle_{2,3}(\alpha|01\rangle_{1,4}+\beta|10\rangle_{1,4}+\gamma|00\rangle_{1,4}+\delta|11\rangle_{1,4})\\ &\quad+\frac{1}{2}|\Psi^-\rangle_{2,3}(\alpha|01\rangle_{1,4}-\beta|10\rangle_{1,4}-\gamma|00\rangle_{1,4}+\delta|11\rangle_{1,4}).\end{aligned}\tag{A3}$$

Then, Bob sends the results of the measurement to Alice. If the results of Bob's measurement are $|\Phi^+\rangle_{2,3}$, $|\Phi^-\rangle_{2,3}$, $|\Psi^+\rangle_{2,3}$, and $|\Psi^-\rangle_{2,3}$, the corresponding operation U_1 that Alice can perform on particle 4 to reconstruct the quantum state of particle 2 is one of these four possibilities: I, Z, X, and ZX, respectively. To be specific, in the case where Bob's measurement outcome yields $|\Phi^+\rangle_{2,3}$, Alice does not need to do anything. If the measurement outcome is $|\Phi^-\rangle_{2,3}$, then Alice can fix up her state by applying the Z gate. If the measurement outcome is $|\Psi^+\rangle_{2,3}$, Alice performs transformation X to reconstruct the state. If $|\Psi^-\rangle_{2,3}$, Alice uses first an X and then a Z gate to recover the state.

To transmit the local quantum state of the first particle in this unknown quantum state, Bob repeats the above steps and the subsystem becomes

$$\begin{aligned}|\psi_0\rangle_{1,2}\otimes|\Phi^+\rangle_{5,6} &= \frac{1}{2}|\Phi^+\rangle_{1,5}(\alpha|00\rangle_{2,6}+\beta|11\rangle_{2,6}+\gamma|01\rangle_{2,6}+\delta|10\rangle_{2,6})\\ &\quad+\frac{1}{2}|\Phi^-\rangle_{1,5}(\alpha|00\rangle_{2,6}-\beta|11\rangle_{2,6}-\gamma|01\rangle_{2,6}+\delta|10\rangle_{2,6})\\ &\quad+\frac{1}{2}|\Psi^+\rangle_{1,5}(\alpha|01\rangle_{2,6}+\beta|10\rangle_{2,6}+\gamma|00\rangle_{2,6}+\delta|11\rangle_{2,6})\\ &\quad+\frac{1}{2}|\Psi^-\rangle_{1,5}(\alpha|01\rangle_{2,6}-\beta|10\rangle_{2,6}-\gamma|00\rangle_{2,6}+\delta|11\rangle_{2,6}).\end{aligned}\tag{A4}$$

Once Alice has learned the measurement outcome sent by Bob, she can fix up her state, recovering $|\psi_0\rangle$ by applying the appropriate quantum gate. The operation U_2 that Alice can perform to reconstruct the quantum state of particle 1 also has four possibilities: I, Z, X, and ZX, respectively. From the overall perspective, the operation to reconstruct the unknown two-qubit state is $U_1\otimes U_2$

Then, we suppose that the $(n-1)$-qubit state $|\psi_1\rangle=\sum_{i_1,\ldots,i_{n-1}}\alpha_{i_1,\ldots,i_{n-1}}|i_1,\ldots,i_{n-1}\rangle$ has already been transmitted successfully by using the same method for sending the two-qubit state. Moreover, the operations to reconstruct the $(n-1)$ particles are $U_1\otimes\cdots\otimes U_{n-1}$. Now, we prove that the quantum state of an n-qubit state will be sent by N-EPR pairs $|\Phi^+\rangle$. The arbitrary n-qubit unknown state can be expressed as $|\psi_2\rangle=\sum_{i_1\ldots i_n}\alpha_{i_1\ldots i_n}|i_1\ldots i_n\rangle_{1,\ldots,n}=|\psi_{21}\rangle|0\rangle+|\psi_{22}\rangle|1\rangle$, where $|\psi_{21}\rangle$ and $|\psi_{22}\rangle$ are independent of each other. Therefore, another expression of $|\psi_2\rangle$ is

$$\begin{aligned}|\psi_2\rangle &= |\psi_{21}\rangle_{1,\ldots,n-1}|0\rangle_n+|\psi_{22}\rangle_{1,\ldots,n-1}|1\rangle_n\\ &= \sum_{i_1^{'}\ldots i_{n-1}^{'}}\alpha^{'}_{i_1^{'}\ldots i_{n-1}^{'}}|i_1^{'}\ldots i_{n-1}^{'}\rangle_{1,\ldots,n-1}|0\rangle_n+\sum_{i_1^{''}\ldots i_{n-1}^{''}}\alpha^{''}_{i_1^{''}\ldots i_{n-1}^{''}}|i_1^{''}\ldots i_{n-1}^{''}\rangle_{1,\ldots,n-1}|1\rangle_n.\end{aligned}\tag{A5}$$

Alice and Bob preshare an EPR pair $|\Phi^+\rangle_{n+1,n+2},\ldots,|\Phi^+\rangle_{3n-1,3n}$. On the basis of the assumption that an $(n-1)$-qubit state is transmitted by using the same method for sending a two-qubit message, Bob sends the nth qubit through teleportation as follows:

$$\begin{aligned}&\sum_{i_1\ldots i_n}\alpha_{i_1\ldots i_n}|i_1\ldots i_n\rangle_{1,\ldots,n}|\Phi^+\rangle_{3n-1,3n}\\ &=\Big(\sum_{i_1^{'}\ldots i_{n-1}^{'}}\alpha^{'}_{i_1^{'}\ldots i_{n-1}^{'}}|i_1^{'}\ldots i_{n-1}^{'}\rangle_{1,\ldots,n-1}|0\rangle_n+\sum_{i_1^{''}\ldots i_{n-1}^{''}}\alpha^{''}_{i_1^{''}\ldots i_{n-1}^{''}}|i_1^{''}\ldots i_{n-1}^{''}\rangle_{1,\ldots,n-1}|1\rangle_n\Big)\\ &\quad\times\frac{1}{\sqrt{2}}(|0\rangle_{3n-1}|0\rangle_{3n}+|1\rangle_{3n-1}|1\rangle_{3n}).\end{aligned}\tag{A6}$$

If Bob performs a Bell-state measurement on particle n and particle $3n-1$, the subsystem becomes

$$\begin{aligned}
&\sum_{i_1\ldots i_n}\alpha_{i_1\ldots i_n}|i_1\ldots i_n\rangle_{1,\ldots,n}|\Phi^+\rangle_{3n-1,3n}\\
&=\frac{1}{2}|\Phi^+\rangle_{n,3n-1}\Bigg(\sum_{i_1^{'}\ldots i_{n-1}^{'}}\alpha^{'}_{i_1^{'}\ldots i_{n-1}^{'}}|i_1^{'}\ldots i_{n-1}^{'}\rangle_{1,\ldots,n-1}|0\rangle_{3n}+\sum_{i_1^{''}\ldots i_{n-1}^{''}}\alpha^{''}_{i_1^{''}\ldots i_{n-1}^{''}}|i_1^{''}\ldots i_{n-1}^{''}\rangle_{1,\ldots,n-1}|1\rangle_{3n}\Bigg)\\
&+\frac{1}{2}|\Phi^-\rangle_{n,3n-1}\Bigg(\sum_{i_1^{'}\ldots i_{n-1}^{'}}\alpha^{'}_{i_1^{'}\ldots i_{n-1}^{'}}|i_1^{'}\ldots i_{n-1}^{'}\rangle_{1,\ldots,n-1}|0\rangle_{3n}-\sum_{i_1^{''}\ldots i_{n-1}^{''}}\alpha^{''}_{i_1^{''}\ldots i_{n-1}^{''}}|i_1^{''}\ldots i_{n-1}^{''}\rangle_{1,\ldots,n-1}|1\rangle_{3n}\Bigg)\\
&+\frac{1}{2}|\Psi^+\rangle_{n,3n-1}\Bigg(\sum_{i_1^{'}\ldots i_{n-1}^{'}}\alpha^{'}_{i_1^{'}\ldots i_{n-1}^{'}}|i_1^{'}\ldots i_{n-1}^{'}\rangle_{1,\ldots,n-1}|1\rangle_{3n}+\sum_{i_1^{''}\ldots i_{n-1}^{''}}\alpha^{''}_{i_1^{''}\ldots i_{n-1}^{''}}|i_1^{''}\ldots i_{n-1}^{''}\rangle_{1,\ldots,n-1}|0\rangle_{3n}\Bigg)\\
&+\frac{1}{2}|\Psi^-\rangle_{n,3n-1}\Bigg(\sum_{i_1^{'}\ldots i_{n-1}^{'}}\alpha^{'}_{i_1^{'}\ldots i_{n-1}^{'}}|i_1^{'}\ldots i_{n-1}^{'}\rangle_{1,\ldots,n-1}|1\rangle_{3n}-\sum_{i_1^{''}\ldots i_{n-1}^{''}}\alpha^{''}_{i_1^{''}\ldots i_{n-1}^{''}}|i_1^{''}\ldots i_{n-1}^{''}\rangle_{1,\ldots,n-1}|0\rangle_{3n}\Bigg). \quad \text{(A7)}
\end{aligned}$$

Bob's measurement outcome should be one of these four possibilities: $|\Phi^+\rangle_{n,3n-1}$, $|\Phi^-\rangle_{n,3n-1}$, $|\Psi^+\rangle_{n,3n-1}$ and $|\Psi^-\rangle_{n,3n-1}$. The probability of each result is $\frac{1}{4}$. Alice can get the corresponding operation U_n in one of these four quantum gates: I, Z, X, and ZX, respectively. Finally, she takes uses $U_1\otimes\cdots\otimes U_n$ to reconstruct the global unknown state.