Computer Modeling in Engineering & Sciences
DOI:10.32604/cmes.2020.010445
Article

Quantum Risk Assessment Model Based on Two Three-Qubit GHZ States

Tao Zheng, Yan Chang and Shibin Zhang*

School of Cyber Security, Chengdu University of Information Technology, Chengdu, 610225, China
*Corresponding Author: Shibin Zhang. Email: cuitzsb@cuit.edu.cn
Received: 05 March 2020; Accepted: 18 May 2020

Abstract: With the acceleration of the construction of quantum communication networks, scholars have proposed different quantum communication protocols for different application scenarios. However, few scholars pay attention to the risk assessment process before communication. In this paper, we propose a novel quantum risk assessment model based on quantum teleportation technology with two three-qubit GHZ states. Only by using Bell states measurements (BSMs) and two-qubit projective measurements (PJMs), the communicators can recovery any arbitrary two-qubit state. This protocol can transmit two-dimension risk assessment factors with better security performance. On the one hand, more sufficient evaluation factors allow the two communicating parties to more objectively evaluate the risk level of communication with the other party, and on the other hand, it also improves the qubit efficiency of the protocol. Moreover, we introduce the third party in this scheme can be semi-trusted, which must be full-trusted in our previous work. This change can reduce the dependence of the communication parties on the third-party organization and improve the privacy of communication. The security analysis shows that this scheme can resist internal and external attacks, and the quantum circuit diagrams also prove that our protocol is physically easier to implement.

Keywords: Quantum risk assessment model; quantum communication; two three-qubit GHZ states; quantum network

1 Introduction

Since Bennett and Brassard put forward the first QKD protocol in 1984 [1], according to different application scenarios, scholars have proposed a large number of quantum information schemes, such as quantum teleportation (QT) [2–5], quantum private query (QPQ) [6–10] and quantum signature (QS) [11–24].

With the rapid development of quantum entangled state preparation and quantum measurement technology, quantum communication network (QCN) is moving towards the stage of practical construction [25]. In the past two decades, scholars have studied QCN from different perspectives and promoted the rapid development of QCN. We briefly introduce the development of QCN according to the development of time: In 1997, Townsend first researched the quantum cryptography on multiuser optical fiber network system [26], which stimulated the enthusiasm of scholars to study QCN. To build the practical quantum key distribution (QKD) system at QCN, Brassard pioneeringly proposed multi-user

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

QKD by using wave-length division multiplexing network [27]. Goodmans et al. [28] also introduced a system perspective on quantum cryptography communication (QCC) based on QKD for QCN system. In 2004, scholars developed the real QCC network with the assistance of multiple sources [29]. In the same year, Brassard et al. proposed the entanglement and wavelength division multiplexing for QCC networks [30]. With the deepening of research, scholars began to study the multi-user QKD (*m-QKD*) system. In 2005, Kumavor et al. [31] introduced a four *m-QKD* schemes at QCC network. Then Zhu et al. [32] introduced a scheme for local QCC networks, and they analyzed the performance of their scheme. In the next year, Deng et al. [33] proposed a scheme for economical quantum secure direct communication network with single photons. In 2008, the researchers from European introduced a more practical QCC network with m-QKD system [34]. Then Hong et al. [35] introduced a scheme which named "*N*-quantum channels are sufficient for m-QKD protocol between *N*-users". In the next year, scholars [36] set up and tested the QKD system in Tokyo QKD network. In 2011, Razavi [37] introduced a protocol of multiple-access quantum-classical networks. Then, the researchers from china [38–40] have proposed many meaningful schemes of QCC network. In recent years, scholars have begun to study quantum network coding scheme [41,42] and practical QKD system [43,44], which accelerated the realization of QCN.

From the introduction above, we can find that most of the quantum communication protocols are based on QKD system which are proved to be unconditional secure, and researchers have pre-supposed that the communicating parties are honest and reliable, or set some prerequisites so that the protocol is not disturbed by the honesty of the communication participants. However, as classic communication network, we must perform a risk assessment of the communication participants to evaluate their reliability and honesty in a quantum communication network. We have studied quantum trust model based on node evaluation [24]. In our previous work, we used quantum teleportation to transmit single qubit as the trust value of node. However, with the deepening of our research, we find that the risk assessment factor value of a node in quantum communication network should be multi-dimensional, and we should find an efficient method to evaluate the risk assessment of the communication participants.

Recently, Li et al. [2] introduced a practical quantum teleportation scheme with two three-qubit GHZ states. The arbitrary two-qubits $|\psi\rangle_{AB} = (\alpha|00\rangle+\beta|10\rangle+\gamma|01\rangle+\eta|11\rangle)_{AB}$ can be teleportation only by using Bell states measurements (BSMs) and two-qubit projective measurements (PJMs) with their protocol.

Inspired by Li et al., we are thinking whether we can transmit more quantum risk assessment factors by using more efficient quantum teleportation technology. We find that the arbitrary two-qubits $|\psi\rangle_{AB} = (\alpha|00\rangle+\beta|10\rangle+\gamma|01\rangle+\eta|11\rangle)_{AB}$ can be applied to carry two-dimension risk assessment factors.

In this paper, we introduce a quantum risk assessment model based on two three-qubit GHZ states. The features of our protocol are reflected in the following aspects:

1. Only by using Bell states measurements (BSMs) and two-qubit projective measurements (PJMs), the communicators can recovery any arbitrary two-qubits state. Our protocol can transmit two-dimension risk assessment factors with better particle utilization efficiency and lower quantum operation complexity.
2. The third trust party (TTP) must be honest in our previous work [24], in this scheme, however, the third party can be semi-trusted because it cannot obtain any useful information when it performs the illegal operation.

The organization of this paper is demonstrated as follows. In Section 2, we review the basic theory of quantum risk assessment, and quantum teleportation with two three-qubit GHZ states. Then we express our proposed scheme in Section 3, and the security analysis is discussed in Section 4. Finally, our conclusion of this scheme is drawn in Section 5.

2 Basic Theory

2.1 Fuzzy Comprehensive Theory of Quantum Risk Assessment

There are mainly two relationship of trust in the research of trust in QCN [24]: 1) Objective trust. Objective trust refers to the state of trust based on objective facts and not interfered by subjective emotions. 2) Subjective trust. Subjective trust refers to the state of trust based on experience and personal emotion. In the real classic network, when a new node wants to join the network, we usually use subjective trust to make a preliminary evaluation, and determine the specific trust value of a node through objective trust, because objective trust is based on the fuzzy and uncertain real evidence to make a credit evaluation. For a more vivid description of fuzzy comprehensive evaluation theory, we set up a QCN with n user nodes $(u_1, u_2, \ldots, u_n)$ and a trust third party (TTP) and the communication diagram is shown in Fig. 1. The establishment rules of QCN are as follows: each node must register with the TTP before joining the network, and the submitted registration information contains various risk assessment factors. The TTP conducts fuzzy comprehensive risk assessment for all nodes according to the following steps.

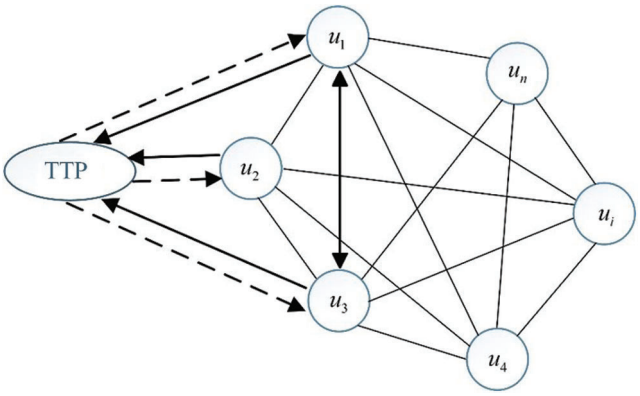

Figure 1: The Communication diagram of node u_1 and node u_3, and the solid line refers the classical channel, the dotted line refers the quantum channel

Step 1 TTP determine the factor set. The determination of factor set refers to the set of all factors that evaluate the object to be evaluated (in this case, the user node u_i), and it is the various elements that can affect the evaluation of the object to be evaluated. Factor set refers to the set of factors that can evaluate behavior credibility. Here, it is assumed that the factor set of the evaluation node is $E = \{e_1, e_2, \ldots, e_n\}$, where n is the number of factors. When the node u_i submits the registration information, TTP will sort out and classify the information to form a set of different factors for risk assessment.

Step 2 TTP determine the comment set. Comment set refers to the different evaluation levels of a single factor, which is a set of various comment levels for a certain factor. For example, to classify scores, you can define a comment set {excellent, good, medium, poor} according to scores, which is a comment set. Here, set the comment set as $C = \{c_1, c_2, \ldots, c_m\}$, where m represents the total number of comments, which can also be called comment level.

Step 3 TTP determine the weight vector of evaluation factors. Because the proportion of each factor of the evaluated research object is not the same, TTP needs to introduce the weight vector of evaluation factors. We set the $W = \{w_1, w_2, \ldots, w_t | 0 \leq w_i \leq 1\}$ as the weight vector of evaluation factors, $\sum_{i=0}^{t} w_i = 1$ and t is the number of factors set. It is worth to note that the determination of the weight value depends on the subjective evaluation result of TTP. The commonly used methods to determine the weight value include expert experience method, expert investigation method, eigenvalue method and weighted average method.

Step 4 The establishment of fuzzy evaluation matrix. Single factor fuzzy evaluation is to determine the membership degree of evaluation object to evaluation set C by evaluating single factor, which is called single factor fuzzy evaluation. The matrix that combines the membership of all single factor fuzzy evaluation to the comment set is called the fuzzy evaluation matrix. Here we set a single fuzzy evaluation vector as $R_{jk} = \{r_{j1}, r_{j2}, \ldots, r_{jk}\}$, then the fuzzy evaluation matrix can be defined as follow:

$$R = \begin{bmatrix} R_1 \\ R_2 \\ R_3 \\ \vdots \\ R_t \end{bmatrix} = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ r_{t1} & r_{t2} & \cdots & r_{tm} \end{bmatrix} \tag{1}$$

Step 5 Vector synthesis of comprehensive evaluation results. TTP selects the appropriate fuzzy synthesis operator for the corresponding synthesis operation, and finally obtains the fuzzy comprehensive evaluation result vector of all the evaluated objects. In this protocol, we define the fuzzy comprehensive evaluation result as:

$$X = W \bullet R = [\omega_1, \omega_2, \cdots, \omega_n] \bullet \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nm} \end{bmatrix} = [x_1, x_2, \cdots, x_m] \tag{2}$$

Step 6 TTP uses weighted average method to obtain fuzzy comprehensive evaluation results. The principle of weighted average is to sum the result vectors of fuzzy comprehensive evaluation by weighting, and calculate the average value. The expression of weighted average principle can be expressed as:

$$f(x) = \frac{\sum_{i=1}^{m} w(e_i) x_i^k}{\sum_{i=1}^{m} x_i^k} \tag{3}$$

where k is the undetermined coefficient, and the value of it is $k = 1$ or $k = 2$.

Step 7 TTP prepares the arbitrary two-qubits quantum states $|\psi\rangle_{AB} = (\alpha|00\rangle + \beta|10\rangle + \gamma|01\rangle + \eta|11\rangle)_{AB}$ to transmit the risk assessment factors of node u_i based on the obtained fuzzy comprehensive evaluation results. In our previous work, we use intuitionistic fuzzy sets theory to describe a node's trust degree when quantum communication occurs. A single quantum qubits $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ to express the node's trust factor in quantum communication network, where $|\alpha|^2$ represents the membership degree of trust factor and $|\beta|^2$ represents the non-membership degree of trust factor, and $|\alpha|^2 + |\beta|^2 = 1$. However, as research progresses, we think that the trustworthiness of a node in a realistic quantum network environment should be determined by a combination of factors, and assessing the risk of a node cannot be based on a single factor alone. Then we tried to use the arbitrary two-qubits quantum states $|\psi\rangle_{AB} = (\alpha|00\rangle + \beta|10\rangle + \gamma|01\rangle + \eta|11\rangle)_{AB}$ to encode more risk evaluation factors, $|\alpha|^2 + |\beta|^2 + |\eta|^2 + |\gamma|^2 = 1$ and we can set that $|\alpha|^2$ to represent the legal operation degree of user node, $|\beta|^2$ represents the honest degree of user node, $|\gamma|^2$ represents the identity credibility degree of user node, and $|\eta|^2$ represents the communication reliability degree of user node.

2.2 Quantum Teleportation of an Arbitrary Two-Qubit State by Using Two Three Qubit GHZ States

A quantum teleportation protocol by using two three-qubit GHZ states and the six-qubit entangled state has been established [2], and Li et al. have described the steps of the protocol in detail. Before giving the detailed steps of our scheme, the basic theory of quantum teleportation protocol by using two three-qubit GHZ states need to be reviewed. Suppose that Alice, Bob and Charlie share two three-qubit GHZ states. Alice possesses qubits pairs (1, 6), Bob possesses qubits pairs (2, 4) and Charlie possesses qubits pairs (3, 5) respectively. The two three-qubit cluster state is described as follows:

$$|\psi\rangle_{123456} = \frac{1}{2}(|000000\rangle + |000111\rangle + |111000\rangle + |111111\rangle)_{123456} \tag{4}$$

Alice holds the arbitrary two-qubits $|\psi\rangle_{AB} = (\alpha|00\rangle + \beta|10\rangle + \gamma|01\rangle + \eta|11\rangle)_{AB}$, which is the qubits to be transmitted. Now the whole system can be written as:

$$\begin{aligned} |\Theta\rangle_{AB123456} \quad &= |\psi\rangle_{AB} \otimes |\psi\rangle_{123456} = (\alpha|00\rangle + \beta|10\rangle + \gamma|01\rangle + \eta|11\rangle)_{AB} \\ &\otimes \tfrac{1}{2}(|000000\rangle + |000111\rangle + |111000\rangle + |111111\rangle)_{123456} \\ &= \tfrac{1}{2}[\alpha|00000000\rangle + \alpha|00000111\rangle + \alpha|00111000\rangle + \alpha|00111111\rangle \\ &+\beta|10000000\rangle + \beta|10000111\rangle + \beta|10111000\rangle + \beta|10111111\rangle \\ &+\gamma|01000000\rangle + \gamma|01000111\rangle + \gamma|01111000\rangle + \gamma|01111111\rangle \\ &+\eta|11000000\rangle + \eta|11000111\rangle + \eta|11111000\rangle + \eta|11111111\rangle]_{AB123456} \end{aligned} \tag{5}$$

Alice performs BSMs on her qubit pairs (A, 1) and (B, 6). In more detail, Alice perform the tensor product operation on $|\psi\rangle_{AB}$ and $S_{16}(|\psi\rangle_{AB} \otimes S_{16})$, then she uses Bell measurement basis $(|00\rangle, |11\rangle, |10\rangle, |01\rangle)$ to obtain the BSMs results. After that, she can get 16 kinds of measurement results with equal probability of 1/16. After Alice's measurement operations, the qubit pairs (2, 3, 4, 5) will also have 16 kinds of collapse results to the corresponding states $|\psi\rangle_{2345}$. Alice informs the measurement results to Bob and Charlie through a classical communication channel. Then Charlie performs a two-qubit projective measurement (PJMs) on the qubit pairs (3, 5), and Charlie sends the measurement outcomes to Bob. After that, Bob performs an appropriate unitary on his qubit pairs (2, 4) and he can reconstruct the state $|\psi\rangle_{AB}$, which means that the qubit $|\psi\rangle_{AB}$ holds by Alice has been transmitted to Bob with quantum teleportation scheme. The detailed quantum teleportation process is shown in Fig. 2.

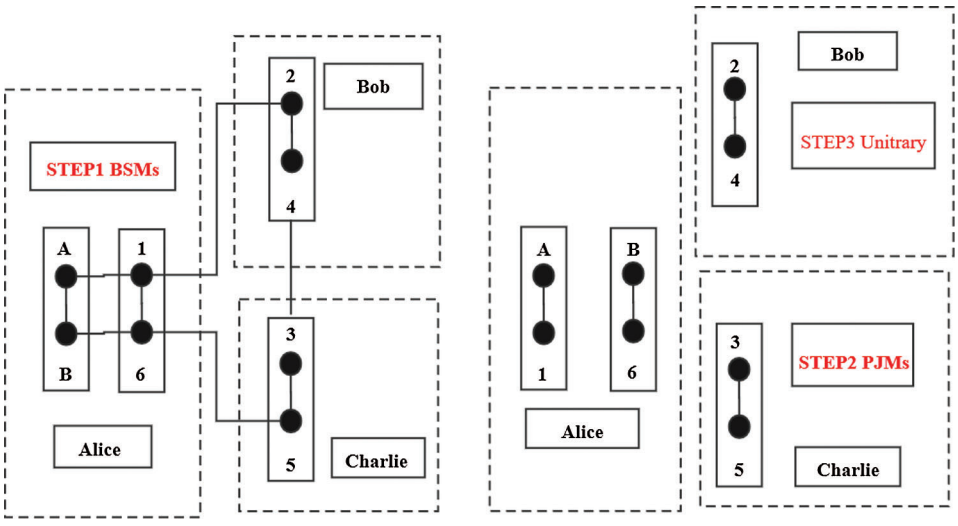

Figure 2: The process of quantum teleportation. Noted that BSMs means the Bell state measurements and PJMs means two qubit projective measurements

It should be noted that this scheme uses two three-qubit GHZ states to construct quantum teleportation channels for information transmitting. Compared with other multi-particle states, GHZ state particles have better particle state stability and are easier to prepare. Moreover, this new quantum teleportation method is much more secure and efficient than our previous protocol.

3 Protocol

In this section, we describe the process of our quantum trust model in detail. And we assume that STP is the semi-trust third party, node u_i wants to communicate with node v_i, the detail steps of our scheme are as follow.

3.1 Initial Phase

On assumption that the information used to describe the fuzzy comprehensive risk assessment value of u_i is stored in STP previously by means of registering, which is expressed in the form of quantum state as follows (prepared by STP before sending):

$$\begin{aligned} |\psi\rangle_{AB(u_i)} &= \sum_{j=1}^{m} t_j\left(\alpha_j|00\rangle + \beta_j|10\rangle + \gamma_j|01\rangle + \eta_j|11\rangle\right)_{AB} \\ &= \alpha_i|00\rangle + \beta_i|10\rangle + \gamma_i|01\rangle + \eta_i|11\rangle \end{aligned} \tag{6}$$

Here ${\alpha_i}^2 + {\beta_i}^2 + {\gamma_i}^2 + {\eta_i}^2 = 1$ and $i = 1, 2, \ldots, n$. STP prepares the two three-qubit GHZ states, each of which is in the state $|\psi\rangle_{123456} = \frac{1}{2}(|000000\rangle + |000111\rangle + |111000\rangle + |111111\rangle)_{123456}$.

3.2 Distribute the Quantum Key

After registration, STP prepares and shares the quantum key Key_{uT} with node u_i, and the quantum key Key_{vT} with node v_i. This process can be implemented by QKD system. More Specifically, Wang et al. [45] proposed a novel Measurement Device Independent Quantum Key Distribution (MDI-QKD) scheme with two-mode state source. Their protocol is relatively simple to operate and enables the quantum key to be transmitted over long distances with a small number of quantum resources. These features meet the requirements for quantum resources in quantum communication networks, so we choose this protocol to generate the quantum key.

In our scheme, node u_i and node v_i are the two senders who control the light sources separately to generate a two-mode state. In general, the *T*-mode is detected by u_i or v_i, and the *S*-mode is sent to the Semi-Trust Party (which named STP in our protocol). Therefore, our scheme needs an additional signal state and single quantum qubits as light source (when the MDI-QKD system uses the BB84 protocol as original protocol for quantum key generation).

3.3 Distribute the Quantum Qubit Sequence

We denote the ordered N bits of two three-qubit GHZ states by:

$$\begin{Bmatrix} [P_1(1), P_1(2), P_1(3), P_1(4), P_1(5), P_1(6)], [P_2(1), P_2(2), P_2(3), P_2(4), P_2(5), P_2(6)], \ldots, \\ [P_{N-1}(1), P_{N-1}(2), P_{N-1}(3), P_{N-1}(4), P_{N-1}(5), P_{N-1}(6)], [P_N(1), P_N(2), P_N(3), P_N(4), P_N(5), P_N(6)] \end{Bmatrix} \tag{7}$$

where the subscript indicates the order of each state in the sequence and $(1, 2, 3, 4, 5, 6)$ represent the six particles in each state. STP takes one and six particles from each state to compose an ordered particle sequence S_{16}, The remaining particles compose S_{35} and S_{24} according to the same rules.

3.4 Establish Communication Connection

Suppose that node u_i wants to communicate with node v_i, u_i sends a request to STP. When STP receives the request and confirms which is sent from u_i, STP prepares quantum state $|\psi\rangle_{AB} = (\alpha|00\rangle + \beta|10\rangle + \gamma|01\rangle + \eta|11\rangle)_{AB}$ based on the registration information of u_i, and informs v_i that u_i wants to communicate with v_i. STP encrypts S_{35} with key Key_{uT} and sends it to node u_i. Then STP encrypts S_{24} with Key_{vT} and sends it to node v_i.

3.5 Transmit Risk Assessment Factors by Quantum Teleportation

After both two nodes are sure to receive the quantum sequences, the two nodes decrypt the quantum sequence with their secret quantum key. STP performs BSMs on qubit pairs $(A, 1)$ and $(B, 6)$, and the measurement result is M_B and the $(2, 3, 4, 5)$ will collapse to the corresponding entangled states, which is shown in Tab. 1.

Table 1: STP's BSMs results M_B, and the corresponding collapse states $|\psi\rangle_{2345}$

M_B	$\|\psi\rangle_{2345}$
$\|\phi\rangle^{+}_{A1}\|\phi\rangle^{+}_{B6}$	$\|\psi\rangle^{1}_{2345} = \frac{1}{4}(\alpha\|0000\rangle + \beta\|1100\rangle + \gamma\|0011\rangle + \eta\|1111\rangle)$
$\|\phi\rangle^{-}_{A1}\|\phi\rangle^{+}_{B6}$	$\|\psi\rangle^{5}_{2345} = \frac{1}{4}(\alpha\|0000\rangle - \beta\|1100\rangle + \gamma\|0011\rangle - \eta\|1111\rangle)$
$\|\psi\rangle^{+}_{A1}\|\phi\rangle^{+}_{B6}$	$\|\psi\rangle^{9}_{2345} = \frac{1}{4}(\alpha\|1100\rangle + \beta\|0000\rangle + \gamma\|1111\rangle + \eta\|0011\rangle)$
$\|\psi\rangle^{-}_{A1}\|\phi\rangle^{+}_{B6}$	$\|\psi\rangle^{13}_{2345} = \frac{1}{4}(\alpha\|1100\rangle - \beta\|0000\rangle + \gamma\|1111\rangle - \eta\|0011\rangle)$

STP informs node u_i to perform a two-qubit projective measurements (PJMs) on $(3, 5)$, and the measurement result is M_P. Node u_i encrypts M_P with Key_{uT} and sends it to STP with classic communication channel, then STP decrypts and obtains M_P. STP encrypts the M_B and M_P with Key_{vT}, and sends the result to node v_i with classic communication channel. After decryption, based on the information of M_B and M_P, node v_i can recovery the quantum state $|\psi\rangle_{AB}$ which represents comprehensive trust factor of node u_i by using appropriate unitary operation, and the detailed operation is shown in Tab. 2, and U (2, 4) means node $v_i$performs Unitary operation on qubits pairs (2, 4). STP sends the detail information about $|\psi\rangle_{AB}$ to node v_i, node v_i calculates the risk assessment factors value of u_i based on the quantum state $|\psi\rangle_{AB}$ he reconstructed and compares the two quantum states. According to the above comparison, he can judge whether node u_i is credible or not.

Table 2: The collapse relationship of node u and v's operation

Node u's result	Node v's collapse state	U (2, 4)
$\|+\rangle_3\|+\rangle_5 = \frac{1}{2}(\|00\rangle + \|01\rangle + \|10\rangle + \|11\rangle)_{35}$	$\|\psi\rangle^{1}_{24} = \frac{1}{16}(\alpha\|00\rangle + \beta\|10\rangle + \gamma\|01\rangle + \eta\|11\rangle)$	$I \otimes I$
$\|+\rangle_3\|-\rangle_5 = \frac{1}{2}(\|00\rangle - \|01\rangle + \|10\rangle - \|11\rangle)_{35}$	$\|\psi\rangle^{2}_{24} = \frac{1}{16}(\alpha\|00\rangle + \beta\|10\rangle - \gamma\|01\rangle - \eta\|11\rangle)$	$I \otimes \sigma_Z$
$\|-\rangle_3\|+\rangle_5 = \frac{1}{2}(\|00\rangle + \|01\rangle - \|10\rangle - \|11\rangle)_{35}$	$\|\psi\rangle^{3}_{24} = \frac{1}{16}(\alpha\|00\rangle - \beta\|10\rangle + \gamma\|01\rangle - \eta\|11\rangle)$	$\sigma_Z \otimes I$
$\|-\rangle_3\|-\rangle_5 = \frac{1}{2}(\|00\rangle - \|01\rangle - \|10\rangle + \|11\rangle)_{35}$	$\|\psi\rangle^{4}_{24} = \frac{1}{16}(\alpha\|00\rangle - \beta\|10\rangle - \gamma\|01\rangle + \eta\|11\rangle)$	$\sigma_Z \otimes \sigma_Z$

4 Security Analysis

Before starting security analysis, we discuss that third party can be semi-honest: The risk assessment factors information is stored in STP, so STP must be reliable to some extent. But we can use obfuscation function or quantum random numbers to encrypt trust information, and use quantum one-time pad (OTP) to update the node's trust information. The two quantum keys and the three qubit pairs are prepared by

STP, which means STP may insert some decoy qubits to eavesdrop the communication information. In our proposed scheme, if STP performs the illegal operation, the entanglement relationship between STP and two nodes will be disrupted, and both two nodes can find this illegal behavior by qubit measurement. Therefore, we can introduce a semi-trust third party to reduce the dependence of a third-party center.

4.1 The Internal Attack

Suppose node u_i wants to cheat node v_i, then node u_i must cooperate with Eve to intercept the original qubits sent by STP. After that, node u_i will send v_i the entanglement qubits that are prepared beforehand. In this case, u_i will find it tough to get the appropriate quantum information when he needs to reconstruct the original qubits. In another case, if node v_i wants to cheat node u_i, with the help of STP, both two nodes can obtain the risk assessment factors value, which means that neither node can cheat the other with internal attack.

4.2 The External Attack

If the external attacker Eve wants to forge the trust factor state $|\psi\rangle_{AB}$, Eve must know the information about key Key_{uT} and Key_{vT}. The QKD and QOTP guarantee the unconditional security of the two keys and the communication channels. Even if Eve obtains the two keys, the forge is impossible without STP's BSMs outcomes and the qubit pairs S_{24} hold by node v_i. We can quantify the Eve and node v_i's (u_i's) mutual information of the key Key_{vT} (Key_{uT}) by Shannon entropy theory. Suppose the probability for Eve is detected by v_i (u_i) is P_d, and the mutual information can be defined as:

$$H(B:E) = -P_d \log_2 P_d - (1-P_d)\log_2(1-P_d) \tag{8}$$

The relationship between the amount of mutual information Eve obtains and the probability that he is detected is shown in Fig. 3. It shows that if Eve want to obtain the full information ($H(B:E)=1$), the probability of the eavesdropping detection is $P_d = 50\%$, When the length of the two keys (n) is large enough, Eve's eavesdropping behavior must be detected.

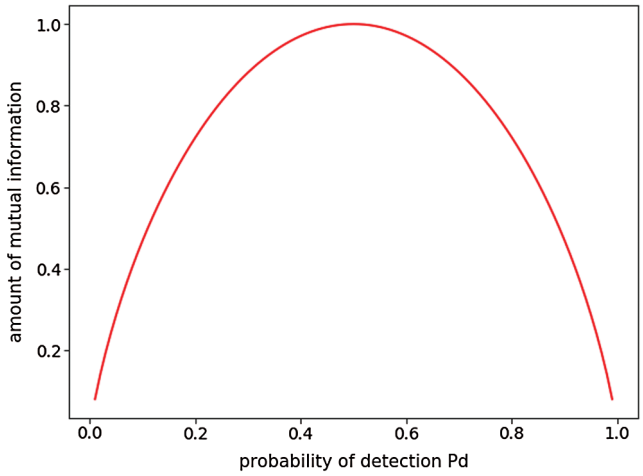

Figure 3: Relationship between the amount of mutual information eve obtains and his detected probability

4.3 Analysis of the Two Pre-Shared Keys

Due to the unconditional security of quantum key distribution, only STP and node u_i know the secret key Key_{uT}. According to the analysis of the protocol flow, Key_{uT} is used to encrypt the quantum sequence S_{35}. After that, node v_i or external attackers are unable to obtain any information related to Key_{uT}. The analysis of

key Key_{vT} is the same as that of Key_{uT}. When a failure occurs in the eavesdropping check or when the secret keys are used for a long period of time does, the new secret keys have to be shared again.

4.4 The Qubit Efficiency

Quantum protocol's qubit efficiency can be calculated with equation $\eta = \frac{c}{q+b}$. Parameter c represents the number of secret bits, q is the total number of transmitted qubits, and b is the total number of classical bits. In our protocol, we assume that the length of $|\psi\rangle_{AB}$ is n, and the length of measurement results (M_B and M_P) is $14n$: The length of M_P is $2n$ which is equals to the length of qubit sequence S_{35}. The length of M_B is $4n$ which is equals to the length of qubit sequence S_{16} and $|\psi\rangle_{AB}$. Analysis of the protocol process reveals that the measurement result M_B will be transmitted two times. Based on the above analysis, we can obtain that $c = 2n$, $q = 2 \times 2n + 4n = 8n$ and $b = 4n + 2n = 6n$. In our previous scheme [24], the trust factor values are encoded in a single qubit $|\varphi\rangle_a$, and TTP performs a Bell states measurement on $|\varphi\rangle_a$ with Bell states $\left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and measurement results are transmitted via a classical channel, then node u will perform unitary operation corresponding to TTP's announce classical information 01, 10, 11, and 00. Therefore, we can obtain that $c = n$, $q = 2n + 3n = 5n$ and $b = 3n$. Tab. 3 shows the comparison of this scheme's qubit efficiency with our previous work.

Table 3: The comparison of qubit efficiency

Protocol	c	q	b	$\eta(\%)$
Our previous scheme	n	$5n$	$3n$	12.5
This protocol	$2n$	$8n$	$6n$	14.3

4.5 The Implementation of Quantum Circuit

Based on the above analysis, our scheme needs to perform the Bell states measurements (BSMs) operation, two-qubit projective measurements (PJMs) and unitary operation. The quantum qubit prepared in this protocol are two three-qubit GHZ states $|\psi\rangle_{123} = \frac{1}{2}(|000\rangle + |111\rangle)_{123}$ and $|\psi\rangle_{456} = \frac{1}{2}(|000\rangle + |111\rangle)_{456}$. Moreover, an arbitrary two-qubits states $|\psi\rangle_{AB} = (\alpha|00\rangle + \beta|10\rangle + \gamma|01\rangle + \eta|11\rangle)_{AB}$ is also needed in this protocol.

The quantum circuit implementation diagram of our scheme is shown in Fig. 4. In the Fig. 4, "H" stands for Hadamard-gate operation, which turns a single photon into an entangled state and its transformation process of the Hadamard-gate operation can be represented by Eq. (9).

$$\sigma_H(|0\rangle, |1\rangle) \rightarrow \left(|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) \tag{9}$$

"+" represents the range of entangled qubits under the Hadamard-gate operation. And "$BSMs(m, n)$" implies performing Bell States Measurement on qubits pairs (m, n). "$PJMs(m)$" means to perform two qubits Projective Measurement on qubit m and "$U(m, n)$" implies performing Unitary operation on qubits pairs (m, n).

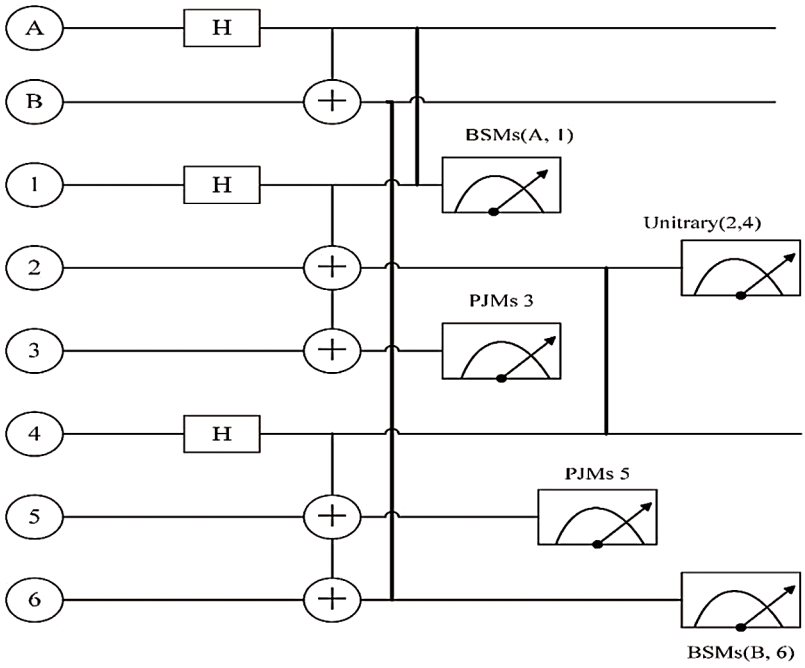

Figure 4: The quantum circuit of this scheme

5 Conclusion

In this paper, we introduce a quantum risk assessment model based on two three-qubit GHZ states. By using a new way of quantum teleportation, our scheme can carry more risk assessment factors, which is more in line with the characteristics of classic networks. The security analysis show that our scheme has a better performance in communication security and qubit efficiency. The quantum circuit diagram also shows that the implementation of our scheme is easier to implement physically. As a future work, we shall research ways to eliminate the influence of various noises, and how to use the advantages of quantum blockchain [46] to reduce dependence on third parties.

Funding Statement: This work is supported by the National Natural Science Foundation of China (No. 61572086, No. 61402058), the Key Research and Development Project of Sichuan Province (No. 20ZDYF2324, No. 2019ZYD027, No. 2018TJPT0012), the Innovation Team of Quantum Security Communication of Sichuan Province (No. 17TD0009), the Academic and Technical Leaders Training Funding Support Projects of Sichuan Province (No. 2016120080102643), the Application Foundation Project of Sichuan Province (No. 2017JY0168), the Science and Technology Support Project of Sichuan Province (No. 2018GZ0204, No. 2016FZ0112).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Bennett, C. H., Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science, 560(1),* 7–11. DOI 10.1016/j.tcs.2014.05.025.
2. Li, D. F., Wang, R. J., Baagyere, E. (2019). Quantum teleportation of an arbitrary two-qubit state by using two three-qubit GHZ states and the six-qubit entangled state. *Quantum Information Processing, 18(5),* 147. DOI 10.1007/s11128-019-2252-3.

3. Childs, A. M., Gosset, D., Webb, Z. (2013). Universal computation by multiparticle quantum walk. *Science, 339 (6121),* 791–794. DOI 10.1126/science.1229957.
4. Chang, Y., Zhang, S. B., Yan, L. L., Han, G. H., Song, H. Q. et al. (2019). A quantum authorization management protocol based on EPR-pairs. *Computers, Materials & Continua, 59(3),* 1005–1014. DOI 10.32604/cmc.2019.06297.
5. Wang, Y., Shang, Y., Xue, P. (2017). Generalized teleportation by quantum walks. *Quantum Information Processing, 16(9),* 221. DOI 10.1007/s11128-017-1675-y.
6. Jakobi, M., Simon, C., Gisin, N., Branciard, C. (2011). Practical private database queries based on a quantum-key-distribution protocol. *Physical Review A, 83(2),* 022301. DOI 10.1103/PhysRevA.83.022301.
7. Gao, F., Liu, B., Wen, Q. Y. (2012). Flexible quantum private queries based on quantum key distribution. *Optical Express, 20(16),* 17411–17420. DOI 10.1364/OE.20.017411.
8. Yang, Y. G., Sun, S. J., Xu, P., Tian, J. (2014). Flexible protocol for quantum private query based on B92 protocol. *Quantum Information Processing, 13(3),* 805–813. DOI 10.1007/s11128-013-0692-8.
9. Yang, Y. G., Zhang, M. O., Yang, R. (2015). Private database queries using one quantum state. *Quantum Information Processing, 14(3),* 1017–1024. DOI 10.1007/s11128-014-0902-z.
10. Yan, L. L., Chang, Y., Zhang, S. B., Wang, Q. R., Sheng, Z. W. et al. (2019). Measure-resend semi-quantum private comparison scheme using GHZ class states. *Computers, Materials & Continua, 61(2),* 877–887. DOI 10.32604/cmc.2019.06222.
11. Gottesman, D., Chuang, I. (2001). Quantum digital signatures. *arXiv preprint arXiv:* quant-ph/0105032.
12. Zeng, G., Keitel, C. H. (2002). Arbitrated quantum-signature scheme. *Physical Review A, 65(4),* 042312. DOI 10.1103/PhysRevA.65.042312.
13. Lee, H., Hong, C., Kim, H., Lim, J., Yang, H. (2004). Arbitrated quantum signature scheme with message recovery. *Physics Letters A, 321(5–6),* 295–300. DOI 10.1016/j.physleta.2003.12.036.
14. Curty, M., Lütkenhaus, N. (2008). Comment on arbitrated quantum-signature scheme. *Physical Review A, 77(4),* 046301. DOI 10.1103/PhysRevA.77.046301.
15. Zeng, G. (2008). Reply to comment on arbitrated quantum-signature scheme. *Physical Review A, 78(1),* 016301. DOI 10.1103/PhysRevA.78.016301.
16. Li, Q., Chan, W. H., Long, D. Y. (2009). Arbitrated quantum signature scheme using Bell states. *Physical Review A, 79(5),* 054307. DOI 10.1103/PhysRevA.79.054307.
17. Zou, X., Qiu, D. (2010). Security analysis and improvements of arbitrated quantum signature schemes. *Physical Review A, 82(4),* 042325. DOI 10.1103/PhysRevA.82.042325.
18. Gao, F., Qin, S. J., Guo, F. Z., Wen, Q. Y. (2011). Cryptanalysis of the arbitrated quantum signature protocols. *Physical Review A, 84(2),* 022344. DOI 10.1103/PhysRevA.84.022344.
19. Choi, J. W., Chang, K. Y., Hong, D. (2011). Security problem on arbitrated quantum signature schemes. *Physical Review A, 84(6),* 062330. DOI 10.1103/PhysRevA.84.062330.
20. Yang, Y. G., Zhou, Z., Teng, Y. W., Wen, Q. Y. (2011). Arbitrated quantum signature with an untrusted arbitrator. *European Physical Journal D, 61(3),* 773–778. DOI 10.1140/epjd/e2010-10157-4.
21. Zhang, K. J., Zhang, W. W., Li, D. (2013). Improving the security of arbitrated quantum signature against the forgery attack. *Quantum Information Processing, 12(8),* 2655–2669. DOI 10.1007/s11128-013-0554-4.
22. Li, F. G., Shi, J. H. (2015). An arbitrated quantum signature protocol based on the chained CNOT operations encryption. *Quantum Information. Processing, 14(6),* 2171–2181. DOI 10.1007/s11128-015-0981-5.
23. Yang, Y. G., Lei, H., Liu, Z. C., Zhou, Y. H., Shi, W. M. (2016). Arbitrated quantum signature scheme based on cluster states. *Quantum Information Processing, 15(6),* 2487–2497. DOI 10.1007/s11128-016-1293-0.
24. Zhang, S. B., Xie, Z. H., Yin, Y. F., Chang, Y., Sheng, Z. W. et al. (2017). Study on quantum trust model based on node trust evaluation. *Chinese Journal of Electronics, 26(3),* 608–613. DOI 10.1049/cje.2016.11.007.
25. Zhang, S. B., Chang, Y., Yan, L. L., Sheng, Z. W., Yang, F. et al. (2019). Quantum communication networks and trust management: A survey. *Computers, Materials & Continua, 61(3),* 1145–1174. DOI 10.32604/cmc.2019.05668.

26. Townsend, P. (1997). Quantum cryptography on multiuser optical fiber network. *Nature, 385(6611),* 47–49. DOI 10.1038/385047a0.
27. Brassard, G., Bussieres, F., Godbout, N., Lacroix, S. (2003). Multi-user quantum key distribution using wavelength division multiplexing. *Proceedings of Society of Photo-Optical Instrumentation Engineers, 5260(6),* 149–153.
28. Goodmans, M., Toliver, P., Runser, R. J., Chapuran, T. (2003). Quantum cryptography for optical networks: A system perspective. *Proceedings of the IEEE Lasers and Electro-Optics Society, Arizona*, 1040–1041.
29. Elliott, C., Colvin, A., Pearson, D., Pikalo, O., Schlafer, J. et al. (2005). Current status of the DARPA quantum network. *Proceedings of Society of Photo-Optical Instrumentation Engineers 2005, 5815,* 138–149.
30. Brassard, G., Bussieres, F., Godbout, N., Lacroix, S. (2004). Entanglement and wavelength division multiplexing for quantum cryptography networks. *Proceedings of American Institute of Physics Conference 2004, 734,* 323–326.
31. Kumavor, P., Cherian, L., Donkor, E., Wang, B. C., Yelin, S. F. (2004). Comparison of four multi-user quantum key distribution schemes over passive optical networks. *Journal of Lightwave Technology, 23(1),* 268–276.
32. Zhu, C. H., Pei, C. X., Ma, H. X., Yu, X. F. (2006). A scheme for quantum local area networks and performance analysis. *Journal of Xidian University, 33(6),* 839–843.
33. Deng, F. G., Li, X. H., Li, C. Y., Zhou, P., Zhou, H. Y. (2007). Economical quantum secure direct communication network with single photons. *Chinese Physics, 16(12),* 3553–3559. DOI 10.1088/1009-1963/16/12/001.
34. Peev, M., Poppe, A., Maurhart, O. (2009). The SECOQC quantum key distribution network in Vienna. *New Journal of Physics, 11(7),* 075001(1–4). DOI 10.1088/1367-2630/11/7/075001.
35. Hong, C. H., Heo, J. O., Khym, G. L., Lim, J., Hong, S. K. (2010). N quantum channels are sufficient for multi-user quantum key distribution protocol between users. *Optics Communications, 283(10),* 2644–2646. DOI 10.1016/j.optcom.2010.02.037.
36. Sasaki, M., Fujiwara, M., Ishizuka, H., Klaus, W., Wakui, K. et al. (2011). Field test of quantum key distribution in the Tokyo QKD network. *Optics Express, 19(11),* 10387–10409. DOI 10.1364/OE.19.010387.
37. Razavi, M. (2011). Multiple-access quantum-classical networks. *The 10th Proceedings of International Conference on Quantum Communication, Measurement and Computing, America. Institute of Physics Conference*, *1363,* 39–42.
38. Yu, X. T., Xu, J., Zhang, Z. C. (2012). Routing protocol for wireless ad hoc quantum communication network based on quantum teleportation. *Acta Physica Sinica, 61(22),* 514–518.
39. Gong, L. H., Liu, Y., Zhou, N. R. (2013). Novel quantum virtual private network scheme for PON via quantum secure direct communication. *International Journal of Theoretical Physics, 52(9),* 3260–3268. DOI 10.1007/s10773-013-1622-3.
40. Liu, Y., Cao, Y., Curty, M., Liao, S. K., Wang, J. et al. (2014). Experimental unconditionally secure bit commitment. *Physical Review Letters, 112(1),* 208–220.
41. Li, J., Chen, X. B., Xu, G., Yang, Y. X., Li, Z. P. (2015). Perfect quantum network coding independent of classical network solutions. *IEEE Communications Letters, 19(2),* 115–118. DOI 10.1109/LCOMM.2014.2379253.
42. Li, J., Chen, X., Sun, X., Li, Z. P., Yang, Y. X. (2016). Quantum network coding for multi-unicast problem based on 2D and 3D cluster states. *Science China Information Sciences, 59(4),* 042301. DOI 10.1007/s11432-016-5539-3.
43. Mehic, M., Maurhart, O., Rass, S., Voznak, M. (2017). Implementation of quantum key distribution network simulation module in the network simulator NS-3. *Quantum Information Processing, 16(10),* 253. DOI 10.1007/s11128-017-1702-z.
44. Yuan, Z. L., Plews, A., Takahashi, R., Doi, K. (2018): 10-mb/s quantum key distribution. *Journal of Lightwave Technology, 36(16),* 3427–3433.
45. Wang, L., Zhou, Y. Y., Zhou, X. J., Chen, X., Zhang, Z. (2018). New scheme for measurement-device-independent quantum key distribution. *Quantum Information Processing, 17(9),* 231. DOI 10.1007/s11128-018-1991-x.
46. Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. (2018). Quantum-secured blockchain. *Quantum Science Technology, 3(035004),* 1–8. DOI 10.1088/2058-9565/aabc6b.