Computers, Materials & Continua
DOI: 10.32604/cmc.2022.029125
Article

Tech Science Press

A Secure Multiparty Quantum Homomorphic Encryption Scheme

Jing-Wen Zhang[1], Xiu-Bo Chen[1,*], Gang Xu[2,3], Heng-Ji Li[4], Ya-Lan Wang[5], Li-Hua Miao[6] and Yi-Xian Yang[1]

[1]Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China
[2]School of Information Science and Technology, North China University of Technology, Beijing, 100144, China
[3]Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Sichuan, 610025, China
[4]Quantum Technology Lab & Applied Mechanics Group, University of Milan, Milan, 20133, Italy
[5]Department of Computer Science, Faculty of Engineering and Physical Sciences, University of Surrey, Guildford, Surrey, GU2 7XH, United Kingdom
[6]Huawei Technologies Co. Ltd, Shenzhen, 518129, China
*Corresponding Author: Xiu-Bo Chen. Email: flyover100@163.com
Received: 25 February 2022; Accepted: 22 April 2022

Abstract: The significant advantage of the quantum homomorphic encryption scheme is to ensure the perfect security of quantum private data. In this paper, a novel secure multiparty quantum homomorphic encryption scheme is proposed, which can complete arbitrary quantum computation on the private data of multiple clients without decryption by an almost dishonest server. Firstly, each client obtains a secure encryption key through the measurement device independent quantum key distribution protocol and encrypts the private data by using the encryption operator and key. Secondly, with the help of the almost dishonest server, the non-maximally entangled states are preshared between the client and the server to correct errors in the homomorphic evaluation of T gates, so as to realize universal quantum circuit evaluation on encrypted data. Thirdly, from the perspective of the application scenario of secure multi-party computation, this work is based on the probabilistic quantum homomorphic encryption scheme, allowing multiple parties to delegate the server to perform the secure homomorphic evaluation. The operation and the permission to access the data performed by the client and the server are clearly pointed out. Finally, a concrete security analysis shows that the proposed multiparty quantum homomorphic encryption scheme can securely resist outside and inside attacks.

Keywords: Quantum homomorphic encryption; secure multiparty computation; almost dishonest server; security

1 Introduction

Classical homomorphic encryption (HE) is focused on the related notion of homomorphism in the field of abstract algebra. Its central idea is to take advantage of homomorphism as a preserving

function to ensure the security of private data. Under this premise, the operations on the ciphertext are outsourced to a server with powerful computing capabilities. The idea of homomorphic encryption first emerged in 1978 when the professional term was called privacy homomorphism that was proposed by Rivest et al. [1] at that time. Since then, an open question in the international cryptographic circle is how to construct a fully homomorphic encryption scheme capable of arbitrary function transformation of the ciphertext. Until 2009, The first fully homomorphic encryption (FHE) algorithm came into view which was presented by Gentry [2]. It inspired the rapid development of the FHE scheme in the following decades. According to the FHE schemes based on difficult problems, it is mainly divided into the problem of approximate greatest common divisor over the integers [3–5] and learning with errors problem based on lattices [6–8].

The development and progress of quantum computers provide access to accelerate the calculation based on the properties of quantum mechanics. The application of quantum computation in quantum communication network [9,10] and quantum blockchain [11–13] will be practical and feasible in the future, and in the meantime, the concept of quantum homomorphic encryption (QHE) has also been proposed. Similar to the homomorphic characteristics used in classical HE, QHE also completes homomorphic quantum computations without decryption by the server. The ciphertext after the homomorphic quantum computation is the same as a valid ciphertext after performing the same quantum computation on the original plaintext. The difference is that all the above processes are completed in the background of quantum data and quantum computation. In the beginning, a large amount of research work [14–16] addressed the task of secure implementation of delegated quantum computation on the encrypted data, but the interaction requirements of the above schemes lead to the workload of the client is proportional to the size of the homomorphic evaluation circuit. The non-interactive schemes have been given in [17,18], but neither of them is suitable for universal quantum computation. The QHE scheme described in [17] realized a restricted class of quantum computation on the encoded input quantum state through the boson-sampling model under the premise of satisfying some information-theoretic security. Reference [18] used the group theoretical insights to make the scheme support quantum computing tasks including and extending beyond the boson-sampling model with improved security. In 2014, Yu et al. [19] proved that achieving a certain balance between security and compactness in a quantum fully homomorphic encryption (QFHE) scheme would be the optimal trivial scheme. In other words, if a QFHE scheme with information-theoretic security is to meet the non-interactivity and realize universal quantum computation, it will inevitably lead to exponential storage overhead. This allows more research to dive into the study of whether a QFHE scheme can be achieved under the condition of relaxing some properties and requirements. In 2015, Broadbent et al. [20] weakened the security level to computational security and gave the definitions of QHE and QFHE. They proposed two QHE schemes, which were suitable for the homomorphic evaluation of the quantum circuit containing a finite number of T gates. Subsequently, Dulek et al. [21] improved the quantum circuit to the size of any polynomial level and presented a QFHE scheme under the computational security by using auxiliary quantum gadgets. In 2018, Ouyang et al. [22] used quantum codes to encode plaintext and evaluation circuits in parallel under the entropy security model to realize universal quantum computation. In the same year, Mahadev [23] utilized the classical leveled FHE scheme to encapsulate the key and constructed a quantum leveled FHE under the assumption of cyclic security.

At the same time, the functionality and application scenarios of the QHE scheme have also been extensively studied. In 2017, Alagic et al. [24] proposed a verifiable leveled QHE scheme by using classical computing logs, proving that homomorphic evaluation results of the QHE scheme can be verified in a non-interactive way. In 2019, Chen et al. [25] combined the characteristics of the

QHE algorithm with the quantum secret sharing scheme to achieve a flexible and variable number of honest evaluators to perform homomorphic evaluation operations in sequence. Later, Liang [26] corrected errors occurring in the homomorphic quantum computation of T gates based on the quantum technology of gate teleportation and proposed a QHE scheme that allows quantum circuits with arbitrary polynomial size. Reference [27,28] completed the Grover retrieval scheme on secret superposition state based on QHE in 2020. Besides, there are some experimental studies [29–31] on QHE schemes.

At present, the existing schemes [20,21,24,26,27] apply the maximally entangled state to remove the P error, that is, an arbitrary quantum calculation can be achieved through the maximally entangled channel. However, the quantum system is generally open in the real physical environment. When coupled with the realistic environment, the maximally entangled state is affected by the ambient noise, resulting in the problem of degenerating into a non-maximally entangled state. Therefore, our scheme uses non-maximally entangled states as quantum resources to assist solve the error problem in the evaluation of T gate. While ensuring the correct execution of the scheme, it reduces the requirements for quantum channels in the previous QHE scheme. In order to improve the universality of the QHE scheme, we will study the QHE scheme with multiple clients and extend its application scenarios to secure multi-party computation. In this paper, we propose a novel secure multi-party QHE scheme by introducing pre-shared non-maximally entangled states that are relatively well prepared between the client and the server as an auxiliary resource. The error correction of the T gate evaluation is completed and the universal quantum circuit evaluation on the quantum ciphertext can be achieved. It is possible for multiple clients to send computation requests to an almost dishonest server in parallel, and guarantee the perfect security of private data.

2 Preliminaries

2.1 Quantum Computation

We will give the symbols and concepts that are essential for the construction of the scheme. For a more detailed introduction to quantum computation, refer to Nielsen et al. [32].

Our work will employ the universal quantum circuit model, denoted as QC, consisting of Clifford gates and non-Clifford gates, where Clifford gates include Pauli gates X and Z, as well as H gate, P gate and $CNOT$ gate, and T gate is chosen as a representative of the non-Clifford gate for computation. Coupled with the computational basis measurements, it is sufficient to realize universal quantum computation.

The entanglement appearance between quantum states is a property of the quantum composite system described in quantum mechanics. Bell state, as the representative of the two-qubit entangled state, is in the maximally entangled state, also known as the EPR (Einstein-Podolsky-Rosen) pair. It consists of four entangled states as follows,

$$\left|\Phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right), \left|\Psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right). \tag{1}$$

We define $|\Theta\rangle = u\,|00\rangle + v\,|11\rangle$ to be a non-maximally entangled state, where u and v are complex numbers and satisfy the normalization condition $|u|^2 + |v|^2 = 1$. Let I_d denote the identity matrix of dimension d, then the completely mixed state can be expressed as I_d/d.

A density matrix ρ is regarded as the quantum plaintext, by randomly selecting the Pauli key, that is, the classical bit $a, b \in \{0, 1\}$ and applying the Pauli operator X and Z on ρ, any quantum plaintext is mapped to the quantum ciphertext, which is in a completely mixed state, since

$$\forall \rho: \sum_{a,b\in\{0,1\}^n} \frac{1}{2^{2n}} X^a Z^b \rho \left(X^a Z^b\right)^\dagger = \frac{1}{2^n} I_{2^n}. \tag{2}$$

This property is allowed to construct a quantum one-time pad (QOTP) and qubits are encrypted in a quantum cryptography scheme. The Pauli key used only once will be randomly generated. Only with the correct key can the quantum ciphertext be decrypted to obtain valid information. So, even if an attacker intercepts the complete quantum ciphertext, it is meaningless to ensure the security of privacy information.

2.2 Quantum Homomorphic Encryption

Quantum homomorphic encryption refers to that the client encrypts the quantum state and sends it to the server. After the server is delegated to perform quantum evaluation operations on the quantum ciphertext, the calculation result is returned to the client for decryption. And the intended result of the quantum evaluation operations on the original quantum state is finally obtained. The concepts introduced in this section include QHE, correctness, compactness, and QFHE. For a more in-depth understanding of the above definitions, refer to Broadbent et al. [20].

Definition 1 (Quantum homomorphic encryption). We now provide the definition of the QHE scheme in the asymmetric key setting. It consists of the following algorithms: key generation, encryption, evaluation, and decryption.

(i) **Key Generation.** $(pk, sk, \rho_{evk}) \leftarrow \text{QHE.KeyGen}\,(1^\kappa)$, where $\kappa \in N$ is the security parameter. pk is used as a public key for encryption, sk is used as a private key for decryption, and both are classical keys. ρ_{evk} is worked as an evaluation key for evaluating the quantum circuit, which is a quantum state.

(ii) **Encryption.** $\sigma \leftarrow \text{QHE.Enc}_{pk}\,(\rho)$. For the quantum plaintext ρ of the message space, the effective public key pk is employed to map it to the quantum ciphertext σ of the cipher space through the encryption algorithm.

(iii) **Homomorphic Evaluation.** $\sigma' \leftarrow \text{QHE.Eval}^{QC}_{\rho_{evk}}\,(\sigma)$, where QC is a universal quantum circuit that acts on the quantum ciphertext σ. The evaluation function maps σ to a certain output space to generate a new quantum ciphertext σ' and consumes the evaluation key ρ_{evk}.

(iv) **Decryption.** $\rho' \leftarrow \text{QHE.Dec}_{sk}\,(\sigma')$. Using the correct private key sk and decryption algorithm, the quantum state σ' is mapped from the output space to the message space to obtain another quantum plaintext ρ', which is consistent with the homomorphic quantum computation conducted on the original quantum plaintext ρ.

Definition 2 (Correctness). A QHE scheme is correct if for any quantum circuit QC and the quantum plaintext ρ, there is a negligible function η such that

$$\Pr\left[\text{QHE.Des}_{sk}\left(\text{QHE.Eval}^{QC}_{\rho_{evk}}\left(\text{QHE.Enc}_{pk}\,(\rho)\right)\right) \neq \Phi_{QC}\,(\rho)\right] \leq \eta\,(\kappa)\,, \tag{3}$$

where Φ denotes a quantum channel, which represents any physically achievable mapping on the quantum register, namely, the quantum circuit QC is applied to the quantum state.

Definition 3 (Compactness). For any quantum circuit QC and quantum ciphertext σ', a QHE scheme is compact, the complexity of the decryption function is independent of the size of the quantum

circuit QC, that is, there is a polynomial $p(\kappa)$, the computational complexity of applying QHE.Dec_{sk} to decrypt the quantum ciphertext σ' is at most $p(\kappa)$.

Definition 4 (Quantum fully homomorphic encryption). If a QHE scheme is correct and compact for all quantum circuits formed by a set of universal quantum gates, the scheme is a QFHE scheme.

3 Secure Multiparty Quantum Homomorphic Encryption Scheme

In this section, we first introduce the probabilistic QHE scheme that uses the non-maximally entangled state to accomplish T gate evaluation. Based on Zhang et al.'s result [33], the main idea of the scheme is described in Section 3.1 which is helpful for our proposal. Then, in Section 3.2, we propose our secure multiparty quantum homomorphic encryption (MQHE) scheme in detail, combined with the evaluation method of T gate, to realize the universal quantum circuit evaluation for multiple clients.

3.1 T gate Evaluation in Quantum Homomorphic Encryption

As a non-Clifford gate, T gate does not have the property of commuting with the Pauli group. When it is applied to the encrypted quantum state, we will get $TX^aZ^b|\phi\rangle = P^aX^aZ^bT|\phi\rangle$. This result contains an unexpected P error and is unable to be corrected by using Pauli corrections. Therefore, the main method we adopt is to pre-share the non-maximally entangled state $|\Theta_{12}\rangle = u|00\rangle + v|11\rangle$ $\left(|u|^2 + |v|^2 = 1\right)$ between the client and the server, where the first particle is owned by the client, and the second particle is owned by the server. After a series of operations, the P error is successfully corrected with a certain probability, and the T gate evaluation in the QHE scheme is realized. Next, we will give the specific process of the main method, which be minutely illustrated in Fig. 1 below.

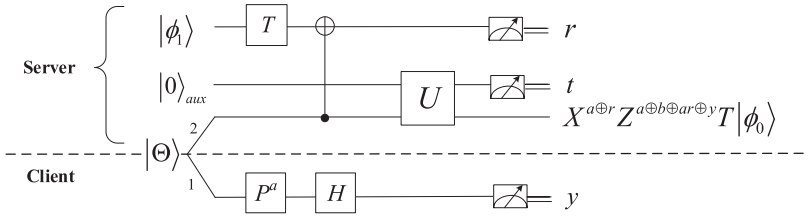

Figure 1: Quantum circuit of T gate evaluation

At first, the client prepares a quantum state $|\phi_0\rangle = \alpha|0\rangle + \beta|1\rangle$. The secure encryption key is $ek = (a, b)$ $(a, b \in \{0, 1\})$. The client encrypts the initial quantum state by using QOTP and we will get $|\phi_1\rangle = X^aZ^b|\phi_0\rangle = X^aZ^b(\alpha|0\rangle + \beta|1\rangle)$ which then be sent to the server. The server performs T gate and outputs $|\phi_2\rangle = T|\phi_1\rangle = TX^aZ^b(\alpha|0\rangle + \beta|1\rangle)$. Meanwhile, the non-maximally entangled state $|\Theta_{12}\rangle$ is introduced. The server performs the $CNOT$ gate with the second particle of $|\Theta_{12}\rangle$ as the control qubit and $|\phi_2\rangle$ as the target qubit. Then we will have $|\Lambda\rangle = (I \otimes CNOT)(|\Theta_{12}\rangle \otimes |\phi_2\rangle)$. The client performs the P^a operation and the Hgate on the first particle of the $|\Theta_{12}\rangle$ in the hand, and the quantum state becomes $|\Omega\rangle = (HP^a \otimes I \otimes I)|\Lambda\rangle = (HP^a \otimes CNOT)(|\Theta_{12}\rangle \otimes |\phi_2\rangle)$. More specifically, if $a = 0$, the quantum states in the circuit are as follows

$$
\begin{aligned}
&(H \otimes CNOT)\left(|\Theta_{12}\rangle \otimes |\phi_2\rangle\right) \\
&= (H \otimes CNOT)\left(u\,|00\rangle + v\,|11\rangle\right) \otimes \left(\alpha\,|0\rangle \pm e^{\frac{i\pi}{4}}\beta\,|1\rangle\right) \\
&= u \cdot H\,|0\rangle\,|0\rangle\left(\alpha\,|0\rangle \pm e^{\frac{i\pi}{4}}\beta\,|1\rangle\right) + v \cdot H\,|1\rangle\,|1\rangle\left(\alpha\,|1\rangle \pm e^{\frac{i\pi}{4}}\beta\,|0\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left[u\left(|0\rangle\,|0\rangle + |1\rangle\,|0\rangle\right)\left(\alpha\,|0\rangle \pm e^{\frac{i\pi}{4}}\beta\,|1\rangle\right) + v\left(|0\rangle\,|1\rangle - |1\rangle\,|1\rangle\right)\left(\alpha\,|1\rangle \pm e^{\frac{i\pi}{4}}\beta\,|0\rangle\right)\right].
\end{aligned} \tag{4}
$$

Similarly, if $a = 1$, the quantum state obtained can be expressed as Eq. (5).

$$
\begin{aligned}
&(HP \otimes CNOT)\left(|\Theta_{12}\rangle \otimes |\phi_2\rangle\right) \\
&= (HP \otimes CNOT)\left(u\,|00\rangle + v\,|11\rangle\right) \otimes \left(e^{\frac{i\pi}{4}}\alpha\,|1\rangle \pm \beta\,|0\rangle\right) \\
&= u \cdot HP\,|0\rangle\,|0\rangle\left(e^{\frac{i\pi}{4}}\alpha\,|1\rangle \pm \beta\,|0\rangle\right) + v \cdot HP\,|1\rangle\,|1\rangle\left(e^{\frac{i\pi}{4}}\alpha\,|0\rangle \pm \beta\,|1\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left[u\left(|0\rangle\,|0\rangle + |1\rangle\,|0\rangle\right)\left(e^{\frac{i\pi}{4}}\alpha\,|1\rangle \pm \beta\,|0\rangle\right) + iv\left(|0\rangle\,|1\rangle - |1\rangle\,|1\rangle\right)\left(e^{\frac{i\pi}{4}}\alpha\,|0\rangle \pm \beta\,|1\rangle\right)\right].
\end{aligned} \tag{5}
$$

Then the first and third particles in the $|\Omega\rangle$ are measured with the basis $\{|0\rangle, |1\rangle\}$, and we denote the corresponding outputs as y and r. The obtained quantum states will be in the following set which all hold up to an irrelevant global phase, namely $\left\{\frac{1}{\sqrt{2}}\left(u\alpha\,|0\rangle \pm e^{\frac{i\pi}{4}}v\beta\,|1\rangle\right), \frac{1}{\sqrt{2}}\left(e^{\frac{i\pi}{4}}u\beta\,|0\rangle \pm v\alpha\,|1\rangle\right)\right\}$. It can be seen that the quantum state of the entire system contains the uncertain values u and v. For the purpose of attaining the correct T gate evaluation results, the server prepares an auxiliary quantum state $|0\rangle_{aux}$ and carries out the defined unitary operator, which is denoted as $U = \begin{pmatrix} I & 0 \\ 0 & U_a \end{pmatrix}$. The unitary matrix $U_a = e^{\frac{-i\pi}{2}} e^{\frac{i\pi \cdot \hat{\mathbf{n}} \cdot \sigma}{2}}$, where $\hat{\mathbf{n}} = \left(\sqrt{1 - u^2/v^2}, 0, u/v\right)$ and $\sigma = \left(\sigma_x, \sigma_y, \sigma_z\right)$, and its calculation process is concretely given in [33]. Here we give the matrix expression form as follows,

$$
U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{u}{v} & \sqrt{1 - \frac{u^2}{v^2}} \\ 0 & 0 & \sqrt{1 - \frac{u^2}{v^2}} & -\frac{u}{v} \end{bmatrix}. \tag{6}
$$

Without loss of generality, we take the $\frac{1}{\sqrt{2}}\left(u\alpha\,|0\rangle + e^{\frac{i\pi}{4}}v\beta\,|1\rangle\right)$ as an example to elaborate the operation which is shown in Eq. (7). Other quantum states also have a similar calculation process.

$$
\begin{aligned}
&\frac{1}{\sqrt{2}} U\left(u\,\alpha\,|0\rangle + e^{\frac{i\pi}{4}}v\beta\,|1\rangle\right) \otimes |0\rangle_{aux} \\
&= \frac{1}{\sqrt{2}}\left(u\alpha\,|0\rangle\,|0\rangle_{aux} + e^{\frac{i\pi}{4}}u\beta\,|1\rangle\,|0\rangle_{aux} + e^{\frac{i\pi}{4}}v\sqrt{1 - \frac{u^2}{v^2}} \cdot \beta\,|1\rangle\,|1\rangle_{aux}\right) \\
&= \frac{1}{\sqrt{2}}\left[u\left(\alpha\,|0\rangle + e^{\frac{i\pi}{4}}\beta\,|1\rangle\right) \otimes |0\rangle_{aux} + e^{\frac{i\pi}{4}}v\sqrt{1 - \frac{u^2}{v^2}} \cdot \beta\,|1\rangle \otimes |1\rangle_{aux}\right]
\end{aligned} \tag{7}
$$

At last, the auxiliary particle $|0\rangle_{aux}$ is measured under the basis $\{|0\rangle, |1\rangle\}$. When the measurement result is $|0\rangle$, the T gate evaluation is accomplished and the expected result can be obtained with a probability of $u^2/2$. Otherwise, the P error cannot be corrected this time. Hence, we can see that our method verifies that the non-maximally entangled state can solve the obstacles in the homomorphic

quantum computation of the T gate but at the expense of the probability of successfully correcting the P error. From the perspective of experimental implementation, our scheme can not only be true of the homomorphic evaluation of the universal quantum circuit, but is also more flexible in the choice of quantum resources.

3.2 Multiparty Quantum Homomorphic Encryption Scheme

In this subsection, we propose a secure MQHE scheme, which allows multiple clients to complete the evaluation of the universal quantum circuit on encrypted private data in parallel with the assistance of the almost dishonest server. In particular, the quantum circuit includes Clifford gates and a finite number of non-Clifford gates. The almost dishonest server in our scheme is the one with great computing capability, which will loyally perform quantum computations. It will not cooperate with clients to launch a collusion attack but will take the initiative to steal clients' private data. At the same time, a trusted key center is introduced and responsible for the execution of the key generation algorithm, and updating the encryption key to obtain the decryption key.

Next, we will specifically describe our MQHE scheme. Assume that there are $n\,(n \geq 2)$ clients which are denoted as $P_i\,(i = 1, 2, \cdots, n)$. Firstly, the server uses the measurement device independent quantum key distribution (MDI-QKD) protocol to distribute secure keys to multiple clients and the trusted key center, i.e., Charlie. Each client uses QOTP technology to encrypt their private data and sends it to the server. The expected quantum circuit is determined and sent to Charlie and the server simultaneously. Then, the server successively acts on the received quantum ciphertext according to the order of the quantum gates in the quantum circuit to complete the homomorphic evaluation while keeping the private data in the quantum ciphertext. And the result of the homomorphic evaluation is received by the client. Finally, according to the quantum circuit and the encryption key shared with each client, Charlie updates the encryption key through the key update rules to acquire the decryption key, which is transmitted to the corresponding client for decryption. The client decrypts to obtain the intended outcome of the quantum circuit acted on the quantum plaintext. The above process is depicted in Fig. 2 below.

The complete process of our scheme is illustrated by step as follows.

S1. Key generation. $ek_i = (a_i, b_i) \leftarrow$ MQHE.KeyGen, where $a_i, b_i \in \{0, 1\}$, $i \in \{1, 2, \cdots, n\}$. There are clients P_i and Charlie randomly prepare one of the quantum states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$. Let $|\varphi_{p_{ij}}\rangle$ denotes the j-th quantum state prepared by the i-th client, and $|\varphi_{c_{ij}}\rangle$ denotes the quantum state prepared by Charlie. When P_i and Charlie transmit them to the server, they form j pairs of quantum states $|\varphi_{p_{ij}}\rangle |\varphi_{c_{ij}}\rangle$. The server performs joint Bell state measurement on $|\varphi_{p_{ij}}\rangle |\varphi_{c_{ij}}\rangle$ and returns the measurement results to both parties through a trusted and authenticated classical channel. According to the measurement results $\left\{ |\Phi^{\pm}\rangle_{p_{ij}c_{ij}}, |\Psi^{\pm}\rangle_{p_{ij}c_{ij}} \right\}$, P_i and Charlie retain the quantum state corresponding to the successful measurement and announce the preparation basis used. Only the quantum states with the same preparation basis are reserved. At this time, the key obtained is the sifted key. Finally, P_i and Charlie publishes a part of the sifted key to perform post-processing. If the error rate is lower than the set threshold, it is confirmed that there is no eavesdropper, the quantum channel between the two parties is secure. And in accordance with the agreed encoding rules, $|0\rangle$ and $|+\rangle$ are encoded as the classic bit "0", $|1\rangle$ and $|-\rangle$ are encoded as the classic bit "1". Whereupon, both parties can get the same security key which is of the form $ek_i = (a_i, b_i)$.

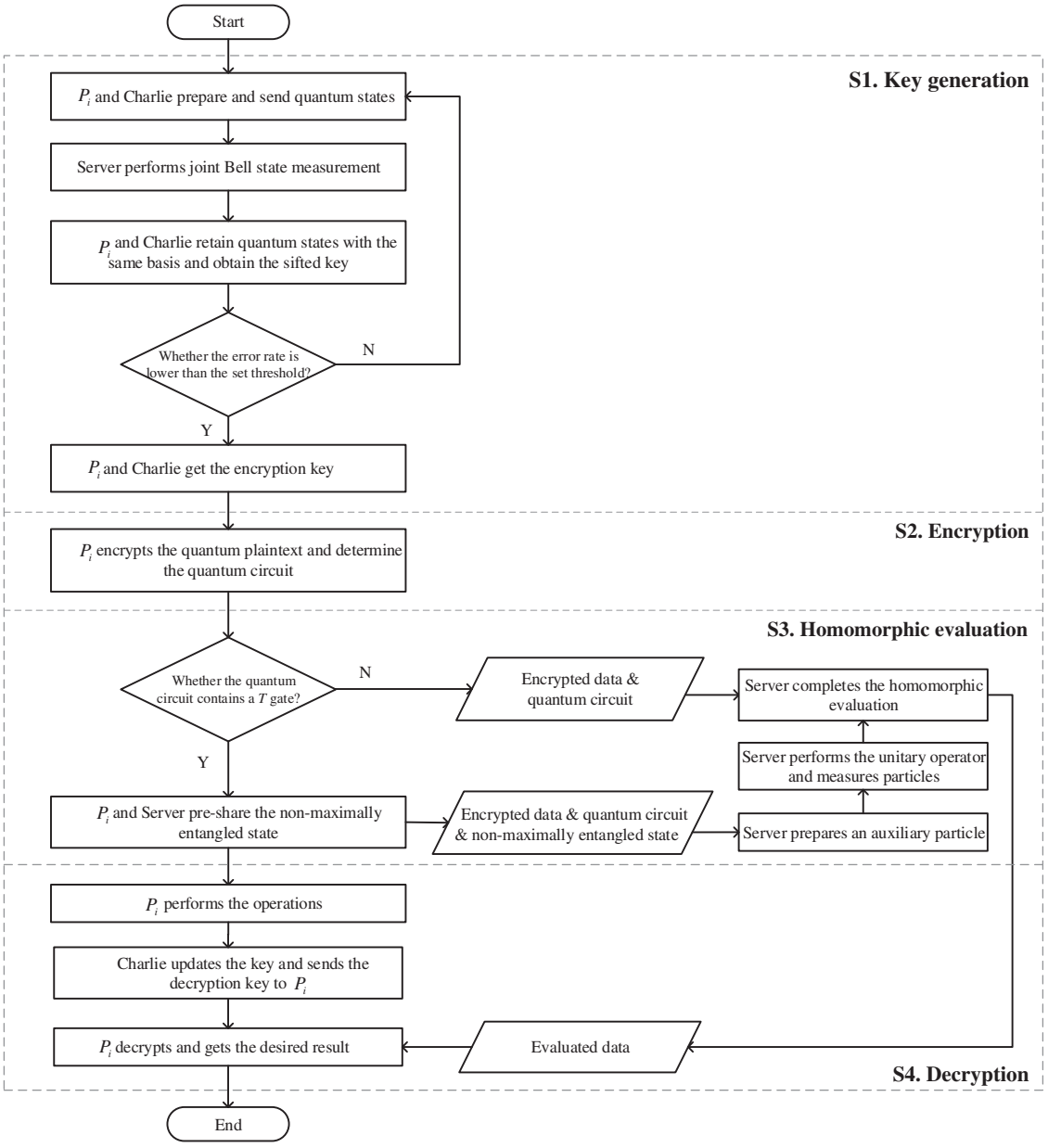

Figure 2: Flow chart of the MQHE scheme

S2. Encryption. $|\phi_{i_1}\rangle = X^{a_i} Z^{b_i} |\phi_{i_0}\rangle \leftarrow \text{MQHE.Enc}_{ek_i}(|\phi_{i_0}\rangle)$. P_i has the quantum plaintext to be encrypted as $|\phi_{i_0}\rangle = \alpha_i |0\rangle + \beta_i |1\rangle$ and use ek_i in S1 as the encryption key of QOTP to execute the encryption algorithm. In the meantime, P_i determines the quantum circuit QC_i containing m quantum gates G_d $(d = 1, 2, \ldots, m)$ to be performed on the quantum ciphertext, which is composed of $\{X, Z, H, P, CNOT, T\}$. After that, P_i transmits the quantum ciphertext $|\phi_{i_1}\rangle$ and QC_i to the server, and only sends QC_i to Charlie. When QC_i contains a T gate, the client should share the non-maximally entangled state, namely $|\Theta_{i_{12}}\rangle = u_i |00\rangle + v_i |11\rangle$ $(|u_i|^2 + |v_i|^2 = 1)$, with the server in advance.

S3. Homomorphic evaluation. $QC_i\left(X^{a_i}Z^{b_i}\left|\phi_{i_0}\right\rangle\right) \leftarrow \text{MQHE.Eval}^{QC_i}\left(\left|\phi_{i_1}\right\rangle\right)$. The form of the quantum ciphertext received by the server is as $\left(X^{a_1}Z^{b_1}\otimes X^{a_2}Z^{b_2}\otimes\cdots\otimes X^{a_n}Z^{b_n}\right)\left|\phi_{1_0}\right\rangle\left|\phi_{2_0}\right\rangle\cdots\left|\phi_{n_0}\right\rangle$. A server will faithfully perform operations on the corresponding quantum ciphertext according to the order of the quantum gates in QC_i. When the quantum gate $G_d \in \{X,Z,H,P,CNOT\}$, it is directly applied to the encrypted qubits, and Charlie can update the encryption key in a direct way. When $G_d = T$, the server adopts the main method introduced in Section 3.1 to remove the P error and complete T gate evaluation, including the application of a $CNOT$ gate, the introduction of an auxiliary particle $|0\rangle_{aux}$, the implementation of the defined unitary operator and the measurement. The client's operation on the non-maximally entangled particle in his hands will be delayed until the decryption stage. After the homomorphic evaluation, the server returns the evaluated data to the corresponding client P_i.

S4. Decryption. $QC_i\left|\phi_{i_0}\right\rangle \leftarrow \text{MQHE.Dec}_{dk_i}\left(QC_i\left(X^{a_i}Z^{b_i}\left|\phi_{i_0}\right\rangle\right)\right)$. In the final phase, Charlie updates the encryption key to acquire the decryption key, i.e., $dk_i = \left(a_i^{'}, b_i^{'}\right)$, and sends it to P_i through the classical authenticated channel. Next, we show how the key is updated according to the key update rules.

(a) If $G_d = X$ or $G_d = Z$, $ek_i = (a_i, b_i) \overset{\text{update}}{\rightarrow} dk_i = (a_i, b_i)$.
(b) If $G_d = H$, $ek_i = (a_i, b_i) \overset{\text{update}}{\rightarrow} dk_i = (b_i, a_i)$.
(c) If $G_d = P$, $ek_i = (a_i, b_i) \overset{\text{update}}{\rightarrow} dk_i = (a_i, a_i \oplus b_i)$.
(d) If $G_d = CNOT$, because $CNOT$ is a two-qubit gate, both the control qubit and the target qubit need the encryption keys, namely $ek_i = (a_i, b_i, c_i, d_i)$, and the decryption key is $dk_i = \left(a_i^{'}, b_i^{'}, c_i^{'}, d_i^{'}\right)$. The corresponding key transformation is $ek_i = (a_i, b_i, c_i, d_i) \overset{\text{update}}{\rightarrow} dk_i = (a_i, b_i \oplus d_i, a_i \oplus c_i, d_i)$.
(e) If $G_d = T$, the client operates on the first particle in the non-maximally entangled state, that is, $(HP^{a_i}\otimes I)\left|\Theta_{12}\right\rangle$, where a_i is the value of the X-encryption key obtained by the client in S1, and then measures this particle. In this case, the rule for updating the encryption key requires two measurement results after the evaluation of the T gate, namely y_i and r_i, then there is $ek_i = (a_i, b_i) \overset{\text{update}}{\rightarrow} dk_i = (a_i \oplus r_i, a_i \oplus b_i \oplus a_i r_i \oplus y_i)$.

In the end, P_i uses the decryption key to decrypt the evaluated data, and acquire the homomorphic evaluation of the quantum circuit acting on the quantum plaintext $\left|\phi_{i_0}\right\rangle$.

Through the description of the above scheme, we propose a novel MQHE scheme, which enables any number of clients to request homomorphic quantum computations from the almost dishonest but computationally capable server in parallel. The server implements homomorphic evaluation of the universal quantum circuit including a limited number of T gate while ensuring the perfect security of private data. In short, our scheme completes the secure homomorphic evaluation of multi-party quantum private data in a non-interactive way and guarantees key security through the trusted key center. From the perspective of simplifying the experimental implementation, we choose the pre-shared non-maximally entangled state to solve the difficult problems and guarantee the correctness of the proposed scheme.

4 Security Analysis

This section will discuss the security of our MQHE scheme in different aspects, mainly from the outside attack and inside attack. An outside attack means that an external eavesdropper attempts to

grab the private data. An inside attack means that an attack initiated by the client, server, and key center.

4.1 Outside Attack

On the one hand, this scheme uses the MDI-QKD protocol to ensure the security of the key for possible security loopholes when the server performs measurement during the key distribution process. On the other hand, the QOTP technology is utilized to encrypt private data, thereby minimizing the risk of data leakage to guarantee the security of private data. According to the four stages of the QHE scheme, we specifically analyze and prove that our scheme can resist outside attacks.

Initially, the security of the key generation stage is analyzed. In our scheme, the distribution of quantum keys adopts the MDI-QKD protocol. It can resist the attack of the external eavesdropper Eve that has been rigorously proved in [34]. The device independence means that the security of the protocol does not depend on the actual measurement device, which is consistent with the security assumption that the server is almost dishonest in the proposed scheme. When the server sends the results of Bell state measurement to P_i and Charlie, there is an active interception behavior by Eve. Suppose $|\Phi^+\rangle_{p_{ij}c_{ij}} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is intercepted, and since $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$, Eve can only judge that P_i and Charlie have randomly prepared the same quantum state this time, and cannot effectively distinguish whether the quantum state is prepared in Z basis $\{|0\rangle, |1\rangle\}$ or X basis $\left\{|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\right\}$. In addition, when performing post-processing on the sifted key, P_i and Charlie analyze whether there is an eavesdropper according to the error rate. The final key is secure and random, making Eve unable to accurately infer the genuine value of the key. Therefore, the key generation stage can resist outside attacks.

Then, in the encryption stage, each client has only access to their original private data and uses the secure key as the Pauli key to encrypt the private data in combination with the QOTP method. It is an asymmetric encryption method that uses random keys makes the encrypted quantum ciphertext in a totally mixed state. The effective information cannot be obtained by Eve without the correct key so that the security of private data is guaranteed in the transmission process. Now, we prove the aforesaid conclusion.

Proof. Define ρ to be a quantum plaintext and σ to be the quantum ciphertext. The encryption operator of QOTP is denoted with $X^{\alpha_i}Z^{\beta_i}$, where $X^{\alpha_i} = \otimes_{k=1}^{n}\sigma_x{}^{\alpha_i(k)}$ $(\alpha_i(k) \in \{0,1\})$ and $Z^{\beta_i} = \otimes_{k=1}^{n}\sigma_z{}^{\beta_i(k)}$ $(\beta_i(k) \in \{0,1\})$. As well as X^{α_i} means whether to apply σ_x according to the classical bit at the k-th position in the n cbits string α_i, namely the value of $\alpha_i(k)$. The same goes for Z^{β_i}. The Eq. (8) is obtained below.

$$\begin{aligned}\sigma &= \sum_i \left(X^{a_i}Z^{b_i}\right)|\phi_{i_0}\rangle\langle\phi_{i_0}|\left(Z^{b_i}X^{a_i}\right)\\ &= \frac{1}{2^{2n}}\sum_{\alpha_i,\beta_i\in\{0,1\}^n}\left(\otimes_{t=1}^{n}\sigma_x{}^{\alpha_i(k)}\sigma_z{}^{\beta_i(k)}\right)\rho\left(\otimes_{t=1}^{n}\sigma_z{}^{\beta_i(k)}\sigma_x{}^{\alpha_i(k)}\right)\end{aligned}$$

$$= \frac{1}{2^{2n}} \sum_{\alpha_i,\beta_i \in \{0,1\}^n} X^{\alpha_i} Z^{\beta_i} \rho Z^{\beta_i} X^{\alpha_i}$$

$$= \frac{I_{2^n}}{2^n} \tag{8}$$

It can be seen that the quantum plaintext is mapped to the same output density matrix $I_{2^n}/2^n$. If Eve intercepts the quantum ciphertext, he is ignorant of any information about the quantum input state without knowing the key. It is impossible for Eve to distinguish the plaintext state owned by each client P_i, so as to ensure the security of private information in the encryption stage. Similarly, in the homomorphic evaluation stage, after the server applies $G_d \in \{X, Z, H, P, CNOT, T\}$ to the quantum ciphertext according to the MQHE scheme, the evaluated quantum state is still a completely mixed state. If the results of the homomorphic evaluation cannot be decrypted, it is unaware for Eve to get the specific content of the universal quantum circuit operating on the original quantum plaintext. So, the homomorphic evaluation can also be immune to outside attacks.

Finally, in the decryption stage, the trusted key center renews the decryption key according to the secure encryption key obtained in S1, the quantum gate used in the quantum circuit in S2, and the key update rule given in S4. The decryption key is sent to P_i through the trusted and authenticated classical channel. As time goes by, the key is irregular, so the adversary cannot get valid content about the decryption key. To conclude, the encryption and decryption keys have good performance in terms of security.

Through the discussion in this section, our MQHE scheme can securely against outside attacks, thereby protecting any information about private data and keys from being leaked.

4.2 Inside Attack

Clients, servers, and trusted key centers are the main participants in the scheme. If an inside attack is launched, it may pose a serious security threat to the cryptographic scheme. Without loss of generality, suppose there exists a dishonest client P_e $(1 \leq e \leq n)$ that wants to steal private data from $n-1$ honest clients and intercepts the quantum state sent by one of them during transmission, but P_e cannot possess the key of the honest client. In our scheme setting, with the assistance of the server, each client acquires a secure key by exploiting the MDI-QKD protocol to encrypt private data. The process of executing the encryption algorithm does not involve the help of other parties. Hence, in addition to using their own keys and operations to process private data, the clients have neither interaction with other clients, nor the authority to access other clients' data or keys.

As an almost dishonest third-party server, there is data exchange with the client, and it can faithfully complete the homomorphic evaluation of the universal quantum circuit without colluding with the malicious client. Unfortunately, the server will evade eavesdropping detection and try to grab the private data. In our scheme, both the encrypted data and the evaluated data are in a completely mixed state and have information-theoretic security. If the server eavesdrops on the quantum channel in the transmission, it will be treated as an outside attacker and unable to extract meaningful information by the means of the outside attack. In QOTP, all keys are randomized and used only once. The security of the key distribution is guaranteed by the MDI-QKD protocol. The replication and retransmission of the quantum state by a malicious server will introduce errors with a certain probability and may be monitored in the post-processing step of the key. In other words, the server cannot infer the value of the key.

The trusted key center, Charlie, introduced in our scheme, is responsible for cooperating with each client to realize the secure distribution of the encryption key, and updating the correct decryption key depending on the quantum circuit and key update rules. Charlie will honestly abide by the requirements of the MQHE scheme, and will not disclose the encryption and decryption keys to anyone other than P_i. Not only the process of the key renewing but also the details of the quantum circuit are kept confidential and will not disclose. At the same time, Charlie will not be affected by any attacker who attempts to illegally get the P_i' private data or the quantum circuit. It further guarantees that the private data and keys are secure. Therefore, our scheme has the ability to resist the participant' attack and third-party' attack.

In summary, it is demonstrated that the proposed MQHE scheme is good at security in terms of private data and keys, and has outstanding performance in resisting outside and inside attacks.

5 Conclusions

This paper presents a secure MQHE scheme. On the one hand, the non-maximally entangled state is used to tackle the computational issues of T gate evaluation that relaxes the technical requirements for implementation of the universal quantum circuit evaluation. On the other hand, drawing on the idea of secure multi-party quantum computation, we expand the application scenario of the QHE scheme and propose a workable scheme that multiple clients request a homomorphic evaluation from the third-party server in parallel, reflecting the significant advantages of QHE in protecting private data. In addition, the trusted key center is employed to ensure the security of key distribution and the encryption and decryption keys, so that the scheme performs well in terms of correctness and security. What's more, we hope that the constructed scheme can inspire the application of the QHE scheme in secure multi-party computation scenarios, making it possible to transmit large-scale quantum information safely and efficiently.

Funding Statement: This work was supported by the Open Fund of Advanced Cryptography and System Security Key Laboratory of Sichuan Province (Grant No. SKLACSS-202101), NSFC (Grant Nos. 62176273, 61962009), the Foundation of Guizhou Provincial Key Laboratory of Public Big Data (No. 2019BDKFJJ010, 2019BDKFJJ014), the Fundamental Re-search Funds for Beijing Municipal Commission of Education, Beijing Urban Governance Re-search Base of North China University of Technology, the Natural Science Foundation of Inner Mongolia (2021MS06006), Baotou Kundulun District Science and technology plan project (YF2020013), and Inner Mongolia discipline inspection and supervision big data laboratory open project fund (IMDBD2020020).

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

References

[1] R. L. Rivest, L. Adleman and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of Secure Computation*, vol. 4, no. 11, pp. 169–180, 1978.

[2] C. Gentry, "A fully homomorphic encryption scheme, Ph.D. thesis, Stanford University, American," 2009.

[3] M. Van Dijk, C. Gentry, S. S.Halevi and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," in *Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques*, Berlin, Heidelberg, Springer, pp. 24–43, 2010.

[4] J. S. Coron, A. Mandal, D. Naccache and M. Tibouchi, "Fully homomorphic encryption over the integers with shorter public keys," in *Annual Cryptology Conf.*, Berlin, Heidelberg, Springer, pp. 487–504, 2011.

[5] J. S. Coron, T. Lepoint and M. Tibouchi, "Scale-invariant fully homomorphic encryption over the integers," in *Int. Workshop on Public Key Cryptography*, Berlin, Heidelberg, Springer, pp. 311–328, 2014.
[6] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," *SIAM Journal on Computing*, vol. 43, no. 2, pp. 831–871, 2014.
[7] Z. Brakerski, C. Gentry and V. Vaikuntanathan, "(Leveled) fully homomorphic encryption without bootstrapping," *ACM Transactions on Computation Theory (TOCT)*, vol. 6, no. 3, pp. 1–36, 2014.
[8] Z. Brakerski, "Fully homomorphic encryption without modulus switching from classical GapSVP," in *Annual Cryptology Conf.*, Berlin, Heidelberg, Springer, pp. 868–886, 2012.
[9] G. Xu, K. Xiao, Z. P. Li, X. X. Niu and M. Ryan, "Controlled secure direct communication protocol via the three-qubit partially entangled set of states," *Computers, Materials & Continua*, vol. 58, no. 3, pp. 809–827, 2019.
[10] S. Y. Chen, G. Xu, X. B. Chen, H. Ahmad and Y. L. Chen, "Measurement-based quantum repeater network coding," *Intelligent Automation & Soft Computing*, vol. 30, no. 1, pp. 273–284, 2021.
[11] H. L. Chen, G. Xu, Y. L. Chen, X. B. Chen, Y. X. Yang *et al.,* "Cipherchain: A secure and efficient ciphertext blockchain via mPECK," *Journal of Quantum Computing*, vol. 2, no. 1, pp. 57–83, 2020.
[12] J. S. Zhang, G. Xu, X. B. Chen, H. Ahmad, X. Liu *et al.,* "Towards privacy-preserving cloud storage: a blockchain approach," *Computers, Materials & Continua*, vol. 69, no. 3, pp. 2903–2916, 2021.
[13] G. Xu, Y. Cao, S. Xu, K. Xiao, X. Liu *et al.,* "A novel post-quantum blind signature for log system in blockchain," *Computer Systems Science and Engineering*, vol. 41, no. 3, pp. 945–958, 2022.
[14] M. Liang, "Symmetric quantum fully homomorphic encryption with perfect security," *Quantum Information Processing*, vol. 12, no. 12, pp. 3675–3687, 2013.
[15] M. Liang, "Quantum fully homomorphic encryption scheme based on universal quantum circuit," *Quantum Information Processing*, vol. 14, no. 8, pp. 2749–2759, 2015.
[16] K. A. G. Fisher, A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie *et al.,* "Quantum computing on encrypted data," *Nature Communications*, vol. 5, no. 1, pp. 1–7, 2014.
[17] P. P. Rohde, J. F. Fitzsimons and A. Gilchrist, "Quantum walks with encrypted data," *Physical Review Letters*, vol. 109, no. 15, pp. 150501, 2012.
[18] S. H. Tan, J. A. Kettlewell, Y. Ouyang, L. Chen and J. F. Fitzsimons, "A quantum approach to homomorphic encryption," *Scientific Reports*, vol. 6, no. 1, pp. 33467, 2016.
[19] L. Yu, C. A. Pérez-Delgado and J. F. Fitzsimons, "Limitations on information-theoretically-secure quantum homomorphic encryption," *Physical Review A*, vol. 90, no. 5, pp. 50303, 2014.
[20] A. Broadbent and S. Jeffery, "Quantum homomorphic encryption for circuits of low T-gate complexity," in *Annual Cryptology Conf.*, Berlin, Heidelberg, Springer, pp. 609–629, 2015.
[21] Y. Dulek, C. Schaffner and F. Speelman, "Quantum homomorphic encryption for polynomial-sized circuits," in *Annual Int. Cryptology Conf.*, Berlin, Heidelberg, Springer, pp. 3–32, 2016.
[22] Y. Ouyang, S. H. Tan and J. F. Fitzsimons, "Quantum homomorphic encryption from quantum codes," *Physical Review A*, vol. 98, no. 4, pp. 42334, 2018.
[23] U. Mahadev, "Classical homomorphic encryption for quantum circuits," in *2018 IEEE 59th Annual Symp. on Foundations of Computer Science (FOCS)*, Paris, France, IEEE, pp. 3332–3338, 2018.
[24] G. Alagic, Y. Dulek, C. Schaffner and F. Speelman, "Quantum fully homomorphic encryption with verification," in *Int. Conf. on the Theory and Application of Cryptology and Information Security*, Hong Kong, China, Springer, pp. 438–467, 2017.
[25] X. B. Chen, Y. R. Sun, G. Xu and Y. X. Yang, "Quantum homomorphic encryption scheme with flexible number of evaluator based on (k, n)-threshold quantum state sharing," *Information Sciences*, vol. 501, no. 1, pp. 172–181, 2019.
[26] M. Liang, "Teleportation-based quantum homomorphic encryption scheme with quasi-compactness and perfect security," *Quantum Information Processing*, vol. 19, no. 1, pp. 1–32, 2020.
[27] C. Gong, J. Du, Z. Dong, Z. Guo, A. Gani *et al.,* "Grover algorithm-based quantum homomorphic encryption ciphertext retrieval scheme in quantum cloud computing," *Quantum Information Processing*, vol. 19, no. 3, pp. 1–17, 2020.

[28] Q. Zhou, S. Lu, Y. Cui, L. Li and J. Sun, "Quantum search on encrypted data based on quantum homomorphic encryption," *Scientific Reports*, vol. 10, no. 1, pp. 1–11, 2020.
[29] K. Marshall, C. S. Jacobsen, C. Schäfermeier, T. Gehring, C. Weedbrook *et al.,* "Continuous-variable quantum computing on encrypted data," *Nature Communications*, vol. 7, no. 1, pp. 1–7, 2016.
[30] W. K. Tham, H. Ferretti, K. Bonsma-Fisher, A. Brodutch, B. C. Sanders *et al.,* "Experimental demonstration of quantum fully homomorphic encryption with application in a two-party secure protocol," *Physical Review X*, vol. 10, no. 1, pp. 11038, 2020.
[31] J. Zeuner, I. Pitsios, S. H. Tan, A. N. Sharma, J. F. Fitzsimons *et al.,* "Fitzsimons et al., "Experimental quantum homomorphic encryption," *npj Quantum Information*, vol. 7, no. 1, pp. 1–6, 2021.
[32] M. A. Nielsen and I. Chuang, "Quantum computation and quantum information," *American Journal of Physics*, vol. 70, no. 5, pp. 558–559, 2002.
[33] J. W. Zhang, X. B. Chen, G. Xu and Y. X. Yang, "Universal quantum circuit evaluation on encrypted data using probabilistic quantum homomorphic encryption scheme," *Chinese Physics B*, vol. 30, no. 7, pp. 70309, 2021.
[34] D. Gottesman, H. K. Lo, N. Lutkenhaus and J. Preskill, "Security of quantum key distribution with imperfect devices," in *Int. Symp. on Information Theory*, Chicago, IL, USA, pp. 136, 2004.