Quantum Ciphertext Dimension Reduction Scheme for Homomorphic Encrypted Data

CHANGQING GONG, Shenyang Aerospace University, China
ZHAOYANG DONG, Shenyang Aerospace University, China
ABDULLAH GANI, University of Malaya, Malaysia
HAN QI, Shenyang Aerospace University, China

At present, in the face of the huge and complex data in cloud computing, the parallel computing ability of quantum computing is particularly important. Quantum principal component analysis algorithm is used as a method of quantum state tomography. We perform feature extraction on the eigenvalue matrix of the density matrix after feature decomposition to achieve dimensionality reduction, proposed quantum principal component extraction algorithm (QPCE). Compared with the classic algorithm, this algorithm achieves an exponential speedup under certain conditions. The specific realization of the quantum circuit is given. And considering the limited computing power of the client, we propose a quantum homomorphic ciphertext dimension reduction scheme (QHEDR), the client can encrypt the quantum data and upload it to the cloud for computing. And through the quantum homomorphic encryption scheme to ensure security. After the calculation is completed, the client updates the key locally and decrypts the ciphertext result. We have implemented a quantum ciphertext dimensionality reduction scheme implemented in the quantum cloud, which does not require interaction and ensures safety. In addition, we have carried out experimental verification on the QPCE algorithm on IBM's real computing platform, and given a simple example of executing hybrid quantum circuits in the cloud to verify the correctness of our scheme. Experimental results show that the algorithm can perform ciphertext dimension reduction safely and effectively.

1 INTRODUCTION

In the information era, everyone produces a huge amount of data to be transmitted every day. In order to reduce the footprint of local memory, most users will use the cloud to save this data. In the era of cloud computing, people can operate on data in the cloud. Therefore, how to compress and extract feature data on the premise of ensuring data security in the cloud is particularly important. To ensure the safe and efficient operation of data in the cloud environment has also become the focus of many researchers. For example: Gentry proposed a breakthrough full-homomorphic encryption

Authors' addresses: Changqing Gong, Shenyang Aerospace University, China, gongchangqing@sau.edu.cn; Zhaoyang Dong, Shenyang Aerospace University, China, arcobelano@icloud.com; Abdullah Gani, University of Malaya, Malaysia, abdullah@um.edu.my; Han Qi, Shenyang Aerospace University, China, qihan@sau.edu.cn.

111

scheme (FHE)[13] has been widely studied, so that data processing rights and data ownership can be separated to prevent their own data disclosure, while making use of the computing power of cloud services. With the development of quantum computer, quantum computing will become a practical technology in the future, and quantum computing services can be provided to customers through the cloud. In order to ensure the security of quantum computing, there are mainly two kinds of quantum encryption schemes: blind quantum computing(BQC) [5, 8, 11, 12, 30, 31, 39, 42] and quantum homomorphic encryption (QHE)[35]. However, the existence of non-interactive blind quantum computing (BQC) remains to be proved.

In 2012 an important scheme is proposed by Rohde [35], which allows encrypted data to carry out quantum random walk. Liang Min completely defined the structure of QHE in [22]: key generation algorithm, encryption algorithm, evaluation algorithm and decryption algorithm. Among them, the evaluation algorithm is for the operation of encrypted data in the cloud, and the key generation algorithm proposes a quantum fully homomorphic encryption (QFHE) scheme with perfect security based on quantum one-time pad,. However, the evaluation algorithm of this scheme depends too much on the key, and the server needs to receive the key transmitted by the client in order to work. Therefore, for delegated calculation, these schemes are not applicable. Tan et al proposed a QHE scheme suitable for group theory tools [41], which can perform large-scale quantum computing on encrypted data. However, this scheme does not guarantee security. Because it only encrypts qubits (for encrypted data size). When n approaches infinity, the ratio of hidden data to total data is close to 0 ($1/\log n \to 0$).

In 2014, Fisher et al.[10] believe that computing power on encrypted data is a powerful tool to protect privacy. It is proved that an untrusted server can implement a set of general quantum gates on encrypted qubits without knowing any information about the input, while the client only needs to know the decryption key. The calculation results can be easily decrypted. Min Liang proposed a quantum homomorphic encryption scheme based on general quantum circuit (UQC) in [23]. In this scheme, the decryption key is different from the encryption key, and the encryption key is public. Therefore, the evaluation algorithm has nothing to do with the encryption key, so it is suitable for entrusted quantum computing between the two parties. In 2015, liang [29] constructed a quantum version of fully homomorphic encryption and constructed two schemes. The first is the symmetric QFHE scheme, through some auxiliary qubits provided by the client, the key is a kind of quantum error correction code-CSS code. The asymmetric QFHE scheme is realized through periodic interaction between the client and the server. In 2020, a homomorphic ciphertext retrieval scheme in quantum environment is proposed [16], and there is no need for interaction. The proposal of this scheme provides a new framework and idea for security and private protection in quantum computing.

At present, quantum machine learning is a relatively new field of development in recent years. Driven by the increasing computer ability and the progress of algorithms, machine learning technology has become a powerful tool for discovering patterns in data [33, 36, 37, 43]. The atypical patterns generated by quantum systems are considered to be inefficient in classical systems, so it is reasonable to assume that quantum computers may perform better than classical computers in machine learning tasks. The field of quantum machine learning explores how to design and implement quantum software to make machine learning faster than classical computers. Recent work has produced quantum algorithms that can be used as building blocks of machine learning programs, but the hardware and software challenges are still great. The core of machine learning algorithm and optimization algorithm is matrix calculation [2, 15, 32]. The core of these algorithms is to find the eigenvalue of a matrix or the inversion of a matrix. In quantum machine learning, these steps are accelerated by using some accelerated methods of quantum information and quantum computing [4, 7, 14, 17, 21, 26, 27, 38]. For example, the Shor algorithm for solving large exponential

decomposition problems [38] and the Grover algorithm for disordered database search [17]. Then in 2009, Harrow, Hassidim and Lloyd proposed the HHL algorithm [27], which solves the problem of solving equations in all fields of engineering and science, and calculates on the quantum computer with as the time scale. Compared with the classical solution method, it has exponential acceleration. Many scholars have carried out real experiments on quantum computers in different ways to simply verify the algorithm and give quantum circuits [6, 34]. After the advent of HHL algorithm, the field of quantum machine learning has also ushered in a rich development. By using HHL as the model, a series of quantum machine learning algorithms are born.

Principal component analysis is a classical and widely used dimensionality reduction algorithm, which depends on the eigendecomposition of the covariance matrix. Therefore, quantum acceleration can be used in this field. The quantum phase estimation subroutine PhaseEstim deals with eigenvectors and eigenvalues. In 2013, Lloyd, Mohseni, Patrick proposed quantum principal component analysis (QPCA) [28] to prove that the density matrix of multiple copies of the system can be used to construct a unitary matrix, which can be used in data analysis, process tomography and state discrimination by using phase estimation. and the QPCA algorithm is much faster than any known classical algorithm. But different from the classical principal component analysis algorithm, the quantum algorithm cannot achieve the dimensionality reduction function of the density matrix.

Recently, some researchers have begun to pay attention to how to implement quantum algorithms in the quantum cloud. In 2017, Huang et al.[18] realized the homomorphic encryption experiment on the IBM quantum computing platform for the first time. This experiment homomorphically implements the quantum matrix inversion algorithm (HHL) on the IBM quantum computing platform. However, the encryption of this algorithm is not based on any quantum homomorphic encryption scheme. The security cannot be guaranteed, and the client needs to perform additional calculations on the plaintext. In the same year, Sun et al.[40] proposed a symmetric quantum partial homomorphic encryption scheme , in which the evaluation function is independent of the key. Based on this quantum homomorphic encryption scheme, an effective symmetric searchable encryption scheme is given and proved to be secure. However, the search algorithm given in this scheme is linear search, and the efficiency will be very low when the search space is very large.

In summary, in the future, the technology of quantum computers is truly mature, and quantum computers will not be popularized in every household. Therefore, calculations can be performed through a client-server model, and quantum homomorphic encryption will be used to perform dimensionality reduction. The calculated data is encrypted and uploaded to the quantum cloud server. After the data is processed, the server returns the ciphertext result to the client, and the client's local key is updated. There is no need to interact with the server, which can reduce the client's computing pressure.

- In this paper, this paper proposes a quantum principal component extraction algorithm (QPCE) for quantum cloud computing, The construction of the quantum circuit is completed, and a simple example is calculated on the IBMQ computing platform to verify the correctness of the proposed algorithm.
- Based on the scheme [25], a dimensionality reduction scheme based on quantum homomorphic encryption (QHEDR) is proposed for the first time by combining the GT-QHE scheme with our quantum dimensionality reduction algorithm in quantum cloud computing. This scheme does not require interaction to ensure security.
- It is verified that the quantum homomorphic encryption scheme is correct when there is a mixed state of multiple T-gates in the quantum circuit, and that the key update algorithm can satisfy the update of multiple T- gates.

The rest of the paper is organized as follows. We summarized some necessary preliminary knowledge of quantum computing in Sect.2. In the section 3, we propose a quantum principal component extraction algorithm (QPCE) to extract features from the density matrix. Combined with QPCE, we propose a quantum homomorphic ciphertext dimensionality reduction (QHEDR) scheme in quantum cloud computing in Sect.4. In the 5 section, the correctness of the QPCE algorithm and the correctness of the QPCE-based quantum homomorphism dimensionality reduction (QHEDR) scheme are verified through experiments, and the experimental results are obtained. Section 6 analyzes the calculation efficiency of QPCE and the security of QHEDR scheme. Finally, in Section 7 we summarized the work of this article and looked forward to the work to be completed in the future.

2 PRELIMINARIES

2.1 Quantum computation

The change of quantum state can be described in the language of quantum computing. Quantum computing is a new computing model that uses the laws of quantum mechanics to calculate quantum information. In quantum computing, the computational model of quantum circuit is usually composed of wires and basic quantum gates. The classical Clifford quantum bit gate is divided into single quantum bit gate and multi-quantum bit gate. The single quantum bit gate includes: pauli X and Z, Hadamard gate H and phase gate S. The multi-quantum bit gate include: $CNOT$ gate, $SWAP$ gate. For a detailed introduction to quantum computing gate, please refer to [33]. In addition to the Clifford gate, there is only one non-Clifford gate $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$. There is at least one non-Cifford gate in every circuit, so it is very important in quantum computation. The conjugate matrix of T gate is $T^{\dagger} = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{4}} \end{pmatrix}$. In the QHE scheme and quantum principal component extraction algorithm we use, the core is the update of T-gate and the construction of controlled U-gate.

2.2 Quantum Teleportation

First of all, the EPR pair is an entangled quantum state. Four Bell states can be expressed as:

$$|\beta_{ab}\rangle = \left(Z^b X^a \otimes I\right)|\beta_{00}\rangle \tag{1}$$

Which $a, b \in \{0, 1\}$, $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. It can be generated by a Hadamard gate and a CNOT gate. The following in fig.1(a) shows the quantum circuit.

(a) Quantum circuit to create Bell states　　　(b) Quantum circuit for of teleportation a qubit.
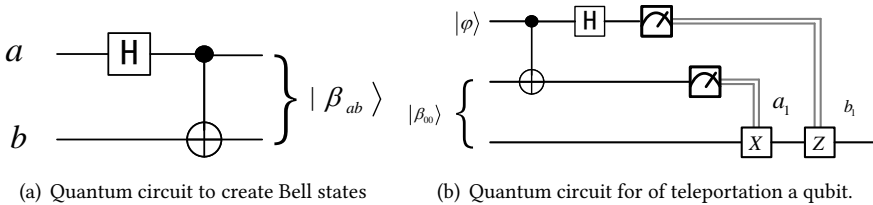
Fig. 1. Two examples of quantum teleportation.

Quantum teleportation is one of the most amazing applications of quantum physics in the field of information theory. Quantum teleportation is a method of moving quantum state without even
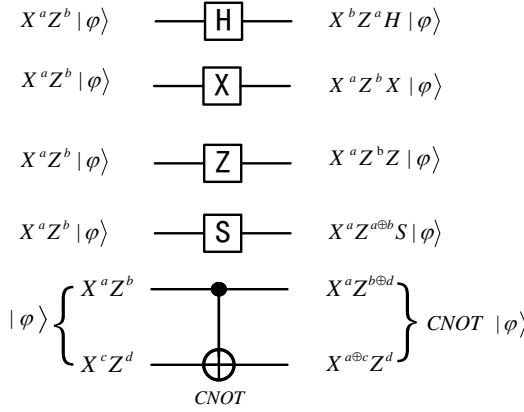
Fig. 2. Key update proces of Clifford gate. Including Pauli $H, X, Z, S, CNOT$ gate key update process.

a quantum communication channel connection between the sender and the receiver. Even when Alice only sends classical information to Bob, it allows quantum information to be transmitted from Alice to Bob. Its quantum circuit is shown in the following figure 1(b):

Through quantum teleportation, the concept of " Rotated Bell basis " is proposed [19]. For any single-bit U-gate, the quantum state that defines " U-rotating Bell basis " can be expressed as

$$|\beta(U)_{ab}\rangle = \left(U^{\dagger} \otimes I\right)|\beta_{ab}\rangle = \left(U^{\dagger} Z^b X^a \otimes I\right)|\beta_{00}\rangle \tag{2}$$

For a single qubit, the quantum state after this operation is as follows:

$$|\varphi\rangle \otimes |\beta_{00}\rangle = \sum_{a,b \in \{0,1\}} \left|\beta(U)_{a,b}\right\rangle \otimes X^a Z^b U |\varphi\rangle \tag{3}$$

According to this definition, 'U-rotate Bell basis'. Liang [24] proposed a quantum homomorphic encryption scheme based on teleportation.

2.3 Key update algorithm

In this scheme, the client and server use Pauli X and Pauli Z gate to implement the encryption and decryption protocol for plaintext and ciphertext.

$$X^a Z^b \rho \rightarrow \varphi \tag{4}$$

Where ρ represents the density matrix of plaintext, φ is the encrypted density matrix a, b represents the encryption key randomly selected from $\{0, 1\}$

In order to ensure the security of the encryption scheme, Boykin and Roychowdhury [3] introduced a secure and feasible quantum one-time pad(QOTP). As long as the keys a and b are randomly generated to make $(a, b) \in \{0, 1\}$, and use it only once. Then the scheme is perfectly safe.Therefore, according to the exchange rules between the Clifford gate and the Pauli matrix, the secret key update rule as shown in the figure 2 is established.

The encrypted quantum state $|\varphi\rangle$ is sent by the client to the server.The server performs quantum computation U on $|\varphi\rangle$, which can be regarded as composed of various quantum gates of $G[1], G[2],...,G[N]$, as shown in figure 3.

When $G \in \{X, Z, H, S, CNOT\}$, the client updates the secret key according to the operation of the server and the secret key update algorithm, and then uses the final updated secret key to decrypt the ciphertext to get $U|\varphi\rangle$. However, when $G \in \left\{T, T^{\dagger}\right\}$ and key $a = 1$,an error occurs,
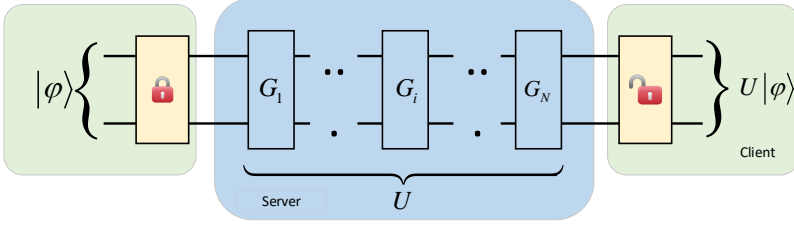
Fig. 3. The composition of Quantum Computing Operation U.

and in order to eliminate this error, the client introduces $|\beta_{00}\rangle_{\text{sc}}$ and measures its 'S^a rotation'.The update process is shown in figure 4:
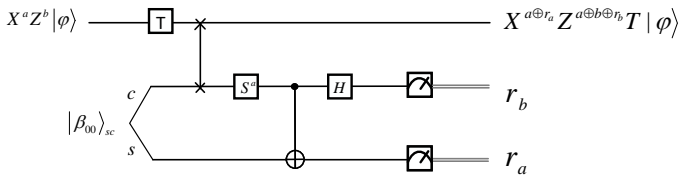

Fig. 4. The process of updating the secret key of the T gate.

The client performs S^a rotation measurement on $|\beta_{00}\rangle_{\text{sc}}$ to get the measurement result r_a, r_b. And update the secret key according to the update formula. This scheme can be used to evaluate the homomorphism of general circuits. the S^a rotation measurement can be postponed until other quantum circuits are completed, and the measurement base $\Phi(S^a)$ only depends on the secret key a.The specific update steps of the T gate of the update algorithm can be found in [3, 24].

3 QUANTUM PRINCIPAL COMPONENT EXTRACTION ALGORITHM

In this secrtion, we will explain the main steps of the quantum principal component extraction algorithm (QPCE) and the effect of its implementation. We give n copies of a density matrix ρ. The quantum phase estimation algorithm can be used to calculate the eigenvalues and Eigenvectors of the matrix. However, the quantum phase estimation algorithm requires the unitary matrix $U = e^{-i\rho t}$ as the input. An operation enables us to apply the construction of unitary gate $e^{-i\rho t}$ of any Hermitian matrix to any density matrix σ.

$$tr_P e^{-iS\Delta t} \rho \otimes \sigma e^{iS\Delta t} = \left(\cos^2 \Delta t\right) \sigma + \left(\sin^2 \Delta t\right) \rho - i\sin^2 \Delta t \left[\rho, \sigma\right]$$
$$= \sigma - i\Delta t \left[\rho, \sigma\right] + O\left(\Delta t^2\right) \tag{5}$$

In short, for the given n copies, the unitary gate $e^{-i\rho t}$ can be obtained by repeating ep.6 n times. This method was proposed by Lloyd et al. in [28].

We input the quantum state of the density matrix $|\varphi_\rho\rangle$, the unitary matrix $e^{i\rho t_0}$ and a threshold constant τ, and output the quantum state.

$$|\varphi_s\rangle = \sum_{k=1}^{s} (\lambda_k - \tau) |e_k\rangle |v_k\rangle \tag{6}$$

Next we will describe the specific details of the algorithm.

3.1 Quantum state preparation

The steps for preparing the quantum state to be input are as follows:

Step1: To standardize and normalize the classical data, where each sample v_k with N-dimensional vector,$k = \{1, ..., M\}$. First of all, we should subtract average value $\bar{v}$ from each training vector, and divide it by the vector norm to normalize it to construct an appropriate quantum state.

$$v_k \rightarrow v_k - \bar{v}, v_k \rightarrow |v_k|^{-1} v_k \tag{7}$$

In addition, the processed v_k can also be standardized to obtain the correlation matrix, but this is not necessary.

Step2: The $i = \{1, ..., N\}$ components of the classical training vector v are encoded into quantum states. i.e. $v \rightarrow |v\rangle = \sum_{i=1}^{n} v_i |i\rangle$, where the quantum state is accurately defined and the probability addition is 1. N-dimensional vectors can be encoded into $n = \log_2 N$ qubits.

Step3: The covariance matrix is represented by the density matrix, and the mixed state is represented by the density matrix $\rho = \frac{1}{M} \sum_{k=1}^{M} |v_k\rangle \langle v_k|$. The tensor product $|v_k\rangle \langle v_k|$ can be expressed as a matrix

$$|v_k\rangle \langle v_k| = \begin{bmatrix} v_1^{(k)} v_2^{(k)} & v_1^{(k)} v_2^{(k)} & \cdots & v_1^{(k)} v_N^{(k)} \\ v_2^{(k)} v_1^{(k)} & v_1^{(k)} v_1^{(k)} & \cdots & v_2^{(k)} v_N^{(k)} \\ \vdots & \vdots & & \vdots \\ v_N^{(k)} v_1^{(k)} & v_N^{(k)} v_2^{(k)} & \cdots & v_N^{(k)} v_N^{(k)} \end{bmatrix} \tag{8}$$

So we get the sum of the tensor product:

$$\frac{1}{M} \sum_{k=1}^{M} |v_k\rangle \langle v_k| = \frac{1}{M} \begin{bmatrix} \sum_k v_1^{(k)} v_2^{(k)} & \sum_k v_1^{(k)} v_2^{(k)} & \cdots & \sum_k v_1^{(k)} v_N^{(k)} \\ \sum_k v_2^{(k)} v_1^{(k)} & \sum_k v_1^{(k)} v_1^{(k)} & \cdots & \sum_k v_2^{(k)} v_N^{(k)} \\ \vdots & \vdots & & \vdots \\ \sum_k v_N^{(k)} v_1^{(k)} & \sum_k v_N^{(k)} v_2^{(k)} & \cdots & \sum_k v_N^{(k)} v_N^{(k)} \end{bmatrix} \tag{9}$$

Therefore, for the reduced-dimensional data, it is equivalent to the covariance matrix, and the classical data is also standardized in the first step of the algorithm, which can be equivalent to the corresponding density matrix of the correlation matrix.

3.2 Implementation steps of Quantum principal component extraction

Secondly, the whole process of dQuantum principal component extraction can be expressed as follows:

$$U_{QPCE} = \left(I^a \otimes U_{PE}^{\dagger} \right) \left(U_R \otimes I^b \right) \left(I^a \otimes U_{PE} \right) \tag{10}$$

Where U_{PE} represents phase estimation and U_R represents controlled rotation. $U_{PE}^{\dagger}$ stands for the inverse operation of U_{PE}. Obviously, the quantum principal component extraction algorithm (QPCE) is similar to the matrix inversion algorithm (HHL algorithm). However, due to the functions of QPCE and HHL are different, U_{PE} and U_R need to be improved.

The quantum subroutine U_{PE} can be expressed as:

$$\begin{aligned} U_{PE} &= U_{PE} \left(\rho \right) \\ &= \left(F_T^{\dagger} \otimes I^B \right) \left(\sum_{\tau=0}^{T-1} |\tau\rangle \langle \tau|^C \otimes e^{i\rho\tau t_0/T} \right) \left(H^{\otimes t} \otimes I^B \right) \end{aligned} \tag{11}$$

In left-to-right order, H is the precision represented by the Hadamard gate acting on register B and t represents the accuracy represented by phase estimation.

The second part is a part of the controlled U gate, which indicates that the phase estimation operation is performed on the characteristic space of ρ[27], The mathematical form can be expressed as eq.13.

$$\sum_{\tau=0}^{T-1} |\tau\rangle \langle\tau|^C \otimes e^{i\rho\tau t_0/T} \tag{12}$$

$F_T^\dagger$ is the inverse transform of quantum fourier transform [33]. At this time, through the phase estimation algorithm, the current state is changed to:

$$\text{tr} \left(|\varphi_1\rangle \langle\varphi_1|\right) = 1/\text{m}^2 \sum_{k=0}^{m} v_k{}^2 |\lambda_k\rangle \langle\lambda_k| \otimes |e_k\rangle \langle e_k| \tag{13}$$

U_R indicates that the purpose of controlled rotation is to redistribute the proportion

$$|\varphi_1\rangle = 1/m \sum_{k=0}^{m} \lambda_k |e_k\rangle |v_k\rangle \tag{14}$$

of each feature in the quantum state, and the method of dimensionality reduction by threshold is also realized here. It can be expressed as:

$$|0\rangle |z\rangle = \left(\frac{\eta \left(\sqrt{z} - \tau\right)}{\sqrt{z}} |1\rangle + \sqrt{1 - \frac{\eta^2 \left(\sqrt{z} - \tau\right)^2}{z}} |0\rangle \right) |z\rangle \tag{15}$$

where $\sqrt{z} > \tau$. By changing the probabilistic amplitude of each ground state $|e_k\rangle |v_k\rangle$ from λ_k to $(\lambda_k - \tau)_+$, it is realized by a transformation $(\lambda_k - \tau)_+ = \lambda_k \times \frac{\left(\sqrt{\lambda_k^2} - \tau\right)_+}{\sqrt{\lambda_k^2}}$. The specific other implementation steps are similar to the implementation of the QSVT algorithm [1].

Finally, we get the density matrix $|\varphi_s\rangle$ in eq.6 after dimensionality reduction. At this time, we can decoherent the system through inverse quantum phase estimation, and what is obtained after decoherence is the reduced-dimensional density matrix.

4 A DIMENSIONALITY REDUCTION SCHEME BASE ON QHE IN QUANTUM CLOUD COMPUTING

In this part, we will propose the details of our dimensionality reduction scheme based on QHE (QHEDR) . We use the quantum principal component extraction (QPCE) proposed in the Sect.3 to realize the dimensionality reduction function in the ciphertext environment in quantum cloud computing. In our scheme, we assume that Alice is the client and bob is the server. If Alice's computing power is limited, Bob is required to do a matrix dimensionality reduction in the cloud. And you need to make sure that Bob doesn't know the specific solution. Quantum principal component analysis algorithm and quantum homomorphic encryption algorithm can ensure the speed and security. Therefore, we combine quantum principal component extraction algorithm with quantum homomorphic encryption to produce a new quantum dimensionality reduction scheme for ciphertext data. Alice overlays and encrypts plaintext and sends the ciphertext to Bob. Then Bob carries out the dimensionality reduction operation of principal component extraction on the ciphertext in the cloud. And the measurement results are returned to Alice. Alice updates the key according to the process of quantum principal component analysis and decrypts the measurement results. That is, the final result of dimensionality reduction can be obtained.
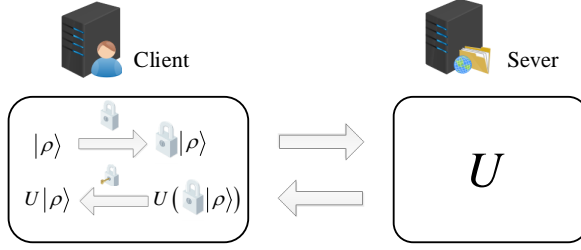
Fig. 5. The specific solution of Quantum homomorphic encryption Scheme. The interaction process does not need to upload the key.

Quantum circuit C can be composed of six parts: **preparation state, secret key generation, encryption, evaluation function, measurement and decryption**. The general process of the scheme is shown in the figure 5:

Next, we will introduce the detailed scheme:

1. State preparation: Alice standardizes a set of N-dimensional data v_k to obtain training vectors, in which $k \in \{1, ..., N\}$. The density matrix P is formed and quantized. And the M group Bell state $\{|\beta_{00}\rangle_{c_i, s_i}, i = 1, ..., M\}$ is generated as an auxiliary quantum state to be saved by the client and the server respectively.

2. Generate secret key: Alice randomly generates a pair of 2n bits of initial key $ek = (a_0, b_0) \in \{0, 1\}^n$

3. Encryption: $Enc(ek, \rho)$. For n-bit density matrix clients that need to encrypt, use the secret key to perform one secret operation at a time. $\varphi \rightarrow Enc(ek, \rho) = X^{a_0} Z^{b_0} \rho Z^{b_0} X^{a_0}$ And send the ciphertext result φ to Bob.

4. Evaluation function: $Eval\left(C, \{s_i, c_i\}_{i=1}^{M}, \varphi\right)$. The server needs to undertake two tasks here.

4.1. Quantum principal component extraction: With the help of the auxiliary qubit s_i, the server performs the operation of the quantum circuit C of the Quantum principal component extraction. The QPCE performs N-step gate operation on the encryption matrix φ as $G[1], G[2], ..., G[N]$. And when it is executed to the $j - th$ Gate ($j \in \{1 \leq j \leq N - 1\}$). According to the difference of quantum gate G, there are two cases:

- When $G[j] \notin \{T, T^\dagger\}$, the server directly executes the quantum gate $G[j]$.
- when $G[j] \in \{T, T^\dagger\}$, where $j = j_i (1 \leq i \leq M)$. The server will first execute the quantum gate $G[j]$ on the ω_i qubit, and then the server will perform the swap exchange operation SWAP (qubit ω_i, qubit s_i).

4.2. Calculate the generation of key update functions $\{h_i\}_{i=1}^{M}$ and f according to key update rules.

- According to key-updating rules in Fig.2, the server generates the polynomial of the secret key a_{j_i-1}

$$a_{j_i-1}(\omega_i) = \begin{cases} h_i(a_0, b_0), & i = 1; \\ h_i(a_0, b_0, r_a(1), r_b(1), ..., r_a(i-1), r_b(i-1)), & i = 2, ..., M \end{cases} \quad (16)$$

- The update function in which the server calculates the final secret key (a_{final}, b_{final}) can be expressed as:

$$f(a_{final}, b_{final}) = f(a_0, b_0, r_a(1), r_b(1), ..., r_a(M), r_b(M)) \quad (17)$$
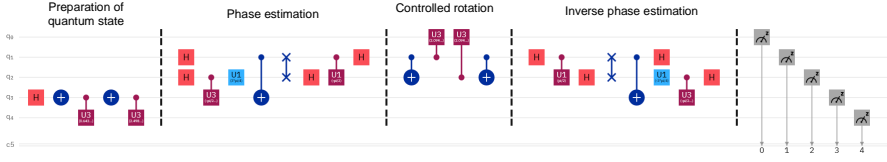
Fig. 6. Quantum circuit of quantum principal component extraction. The quantum circuit includes four parts, Quantum state preparation, Phase estimation U_{PE}, Controlled rotation U_R and Inverse phase estimation $U_{PE}^{\dagger}$.

After the two sub-steps in step 4, the server has obtained the results of the dimensionality reduction calculation φ', auxiliary qubits s_i, together with update-key formula $\{h_i\}_{i=1}^{M}$ and f. It is worth noting that the server only passes the final key calculation formula and ciphertext result to the client, and the server itself does not use any keys.

5. Measure The client needs to alternately calculate $\{h_i\}_{i=1}^{M}$ and measure $\{s_i, c_i\}_{i=1}^{M}$ to ensure the reliability of one secret at a time. First, the client uses the initial secret key $ek = (a_0, b_0)$ and the measurement result $r_a(1), r_b(1)$. The specific implementation method is reviewed in Sect.2.3

The first secret key bit a is calculated according to the formula $\{h_i\}_{i=1}^{M}$, and then the measurement basis $\Phi(S^a)$ is obtained. The client then measures the following qubits $\{s_i, c_i\}_{i=2}^{M}$ to get all the measurement results $\{r_a(i), r_b(i)\}_{i=1}^{M}$.

6. Decryption $Dec\left(ek, \{r_a(i), r_b(i)\}_{i=1}^{M}, f, \varphi'\right)$. According to the initial secret key $ek = (a_0, b_0)$ and all the measurement results $\{r_a(i), r_b(i)\}_{i=1}^{M}$, the final secret key $dk = \left(a_{final}, b_{final}\right)$ is calculated by the formula f in eq.17. And finally, through the decryption operation.

$$Dec(dk, \varphi') = X^{a_{final}} Z^{b_{final}} \varphi' \rightarrow \rho' \tag{18}$$

Finally get the result we expect ρ'.

5 EXPERIMENT

This section will use the IBMQ Experience to briefly describe the feasibility of this scheme. The verification will be carried out from two aspects. first, we will verify the correctness of our quantum principal component extraction algorithm on IBM Quantum experience. Due to the existence of multiple T-gates gates in QPCE, it is necessary to verify whether the QHE is correct when the quantum circuit is a hybrid quantum circuit of multiple T-gates. In addition, the IBM quantum computing platform cannot provide enough quantum registers at this stage, so we verify the dimensionality reduction scheme in cloud computing through a multi-T-gate hybrid quantum circuit simulation.

5.1 Experimental implementation of Quantum principal component extraction based on IBMQ Experience

According to our description in Sect.3, the quantum principal component extraction algorithm is mainly divided into four parts, Preparation of quantum state $\left|\varphi_\rho\right\rangle$, Phase estimation U_{PE}, Controlled rotation U_R, Inverse phase estimation $U_{\mathrm{PE}}^{\dagger}$. The quantum circuit is shown in the figure 6.

The interior of the dotted line corresponds to four parts respectively. In this experiment, it is assumed that the input density matrix $\rho = \frac{1}{2}\begin{bmatrix} 3 & 1 \\ 1 & 3 \end{bmatrix}$, the threshold $\tau = 0.8$.

Preparation of quantum state $\left|\varphi_\rho\right\rangle$ **:** In the quantum circuit, we enter the normalized vector form form $\left|\varphi_\rho\right\rangle$ of ρ, It is normalized to get $\left|\varphi_\rho\right\rangle = [0.670, 0.223, 0.223, 0.670]^T$. The quantum state
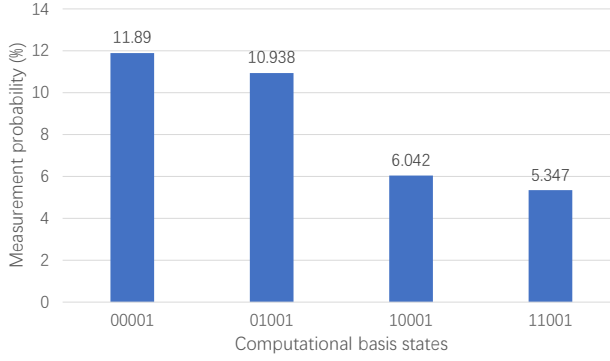
Fig. 7. The results of the verification experiment of QPCE

is prepared by the method described in [20]. After calculation, the parameter of $U_3 (\theta, 0, 0)$ is $\theta_1 = 0.643$, $\theta_2 = 2.498$.

Phase estimation U_{PE} : This part is the same as the function implemented by HHL algorithm. The quantum circuit is designed according to [1, 6, 34]. It is necessary to realize $c - e^{ei\rho t/4}$ and $c - e^{ei\rho t/2}$ in the quantum circuit and simplify it. If $t = 2\pi$ is set, it can be proved that $c - e^{-ei\rho t/2} = CNOT$. At this time, $e^{ei\rho\pi/4} = e^{\frac{\pi}{4}i(3I+\sigma_x)} = R_I \left(-\frac{3\pi}{2}\right) \cdot R_x \left(-\frac{\pi}{2}\right)$ According to the formula in [33].

$$R_x (\theta) \equiv e^{-i\theta X/2} = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y \quad (19)$$

$e^{ei\rho\pi/4}$ can be converted to

$$R_x \left(-\frac{\pi}{2}\right) = \cos\left(-\frac{\pi}{4}\right)I - i\sin\left(-\frac{\pi}{4}\right)\sigma_X = \begin{bmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2}i \\ \frac{\sqrt{2}}{2}i & \frac{\sqrt{2}}{2} \end{bmatrix} = U_3 \left(-\frac{\pi}{2}, -\frac{\pi}{2}, \frac{\pi}{2}\right) \quad (20)$$

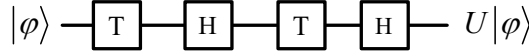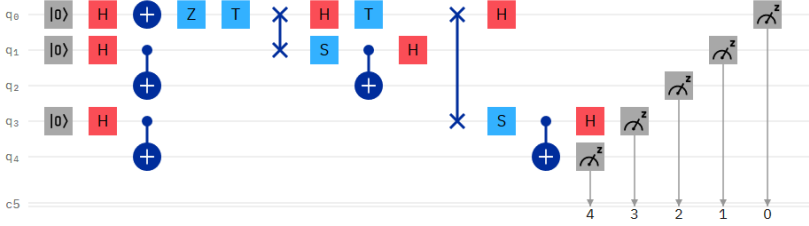$$c - R_1 \left(-\frac{3}{2}\pi\right) = U_1 \left(\frac{3}{4}\pi\right) \quad (21)$$

$e^{ei\rho\pi/4}$ can be converted to $U_3 \left(-\frac{\pi}{2}, -\frac{\pi}{2}, \frac{\pi}{2}\right) \cdot U_1 \left(\frac{3}{4}\pi\right)$. The rest is the detailed steps of quantum Fourier transform [33].

Controlled rotation U_R : Because of the density matrix $\rho = \frac{1}{2}\begin{bmatrix} 3 & 1 \\ 1 & 3 \end{bmatrix}$, the eigenvalues are

$\lambda_1 = 1$, $\lambda_2 = 2$. In addition, in order to simplify the circuit. we order $\tau = 0.8$, so that $\frac{\lambda_1}{\lambda_2} = \frac{1}{2} = |01\rangle$: $|10\rangle$ can be converted to $\frac{1-\tau/\lambda_1}{1-\tau/\lambda_2} = \frac{3}{1} = |01\rangle : |11\rangle$. $|10\rangle \rightarrow |11\rangle$ can be converted into a $CNOT$ operation on a quantum circuit. Next, the parameters for the controlled rotation of $R_y(\alpha)$ are set to $\alpha = 2.094$. The method of calculation can be obtained from the optimization formula in[9].

The inverse phase estimation $U_{\text{PE}}^{\dagger}$ is the inverse operation of all previous operations. The measurement results of the quantum circuit are shown in the figure 7.

The experimental results are completed by IBM quantum computing platform, and the number of experiments is 8192. As we can see the result is

$$\rho_e = [sqrt (0.1189), sqrt (0.10938), sqrt (0.06042), sqrt (0.05347)]^T$$
$$= [0.3448, 0.2534, 0.2312, 0.3307]^T$$

$$|\varphi\rangle - \boxed{T} - \boxed{H} - \boxed{T} - \boxed{H} - U|\varphi\rangle$$

Fig. 8. An example of a single-qubit quantum circuit C

Fig. 9. Verification the key update algorithm with multiple T-gates on IBMQ

According to the example, the result of the theory is $\rho_t = [0.6325, 0.3162, 0.3162, 0.6325]^T$. Calculate the normalized value of $\rho_e^\wedge = [0.5863, 0.4308, 0.3932, 0.5623]^T$. The success of the calculation results can be verified by the fidelity, that is, $\left\|\langle \rho_e^\wedge | \rho_t \rangle\right\|^2 = 0.9870$. In summary, our algorithm can be verified by experiments.

5.2 Verify the correctness of the key update algorithm with multiple T-gates in the circuit

The verification circuit is designed according to the key update algorithm of T-gate and the rotated Bell basis. We design a example of quantum circuit C with two T-gates in the figure 8, Where the operation of qubits $U = HTHT$. Experiments are carried out on the IBMQ cloud platform. The design quantum circuit is shown in Fig.9.

According to the QHE scheme, Client's initial secret key is $\{a_0, b_0\}$,The final decryption key is $\{a_f, b_f\}$ is calculated from the initial key and the measurement.In step 5.42,The server needs to calculate $M + 1 = 3$ key-update functions according to the key update rule.In this quantum circuit, the key- update function as follows.

$$h_1(a_0, b_0) = a_0 \tag{22}$$

$$h_2(a_0, b_0, r_a(1), r_b(1)) = a_0 \oplus b_0 \oplus r_b(1) \tag{23}$$

The final Key-updating function is

$$\{a_f, b_f\} = f(a_0, b_0, r_a(1), r_b(1), r_a(2), r_b(2)) \tag{24}$$

where $a_f = b_0 \oplus r_a(1) \oplus r_b(1) \oplus r_b(2)$, $b_f = a_0 \oplus b_0 \oplus r_b(1) \oplus r_a(2)$.

In the decryption process of the quantum circuit, the client needs to carry out two steps of operation.

- When the key update function $h_1=1$, the client executes the measurement basis on the first T-gates $\Phi(S^{a_0})$, and measure it to get a pair of qubits $(r_a(1), r_b(1))$.
- When the key update function $h_2=1$, the client executes the measurement basis on the first T-gates $\Phi\left(S^{a_f = b_0 \oplus r_a(1) \oplus r_b(1) \oplus r_b(2)}\right)$ and measure it to get a pair of qubits $(r_a(2), r_b(2))$.

Finally, according to the $r_a(1), r_b(1), r_a(2), r_b(2)$ measured by the client above and the key-update function f calculated by the server, the client gets the final key $\{a_f, b_f\}$ and decrypts the result to get the final result.
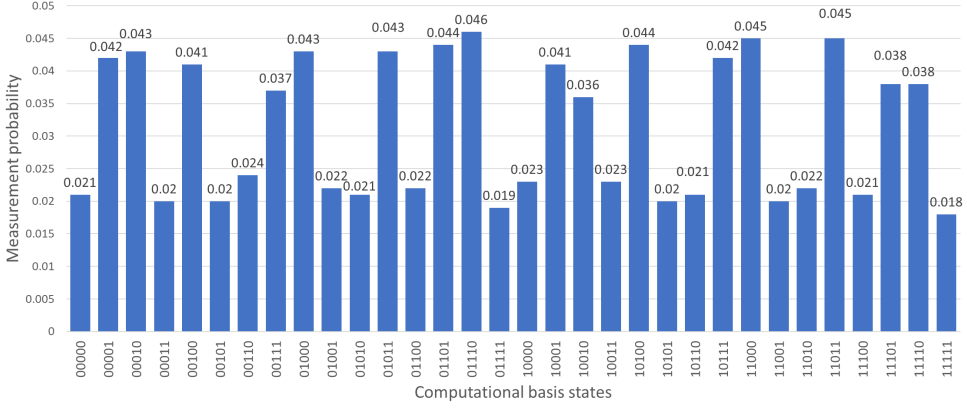
Fig. 10. The measurement result of verifying the quantum homomorphic encryption scheme is based on IBMQ

Table 1. Updated keys and measurement result

$r_a(2)$	$r_b(2)$	$r_a(1)$	$r_b(1)$	$b_0 \oplus r_a(1) \oplus r_b(1) \oplus r_b(2)$	$a_0 \oplus b_0 \oplus r_b(1) \oplus r_a(2)$	measurement result of q_0
0	0	0	0	1	0	1
0	0	0	1	0	1	0
0	1	0	1	1	1	1
0	1	1	1	0	1	0

This experiment is carried out by using IBMQ computing platform located in melbourne (ibmq_16_melbourne). In order to ensure the accuracy of the experiment, the highest number of runs is 8192. The plaintext q_0 in the circuit is set to $|0\rangle$. Set encryption initial key $EK = \{a_0, b_0\} = \{1, 1\}$. $\{q1, q2\}, \{q3, q4\}$ is two sets of auxiliary Bell state. According to the definition of rotated Bell basis, we perform S^a rotation measurement on $\{q1, q2\}, \{q3, q4\}$. The measurement results are $r_a(2), r_b(2), r_a(1), r_b(1), q_0$ from left to right. The running results of the experiment are as follows in figure 10.

Obviously, the result we want will be displayed with high probability. Four results of $\{00001, 00010, 01011, 01110\}$ are randomly selected as examples in the measurement results, and the key-update process is shown in Table 1.

First, we execute the quantum circuit shown in Fig. 8 in plaintext, and the result of q_0 is 0. We use the updated key to decrypt the ciphertext, according to the decryption formula.

$$X^{a_f} Z^{b_f} \varphi' \to \rho' \tag{25}$$

We use the decrypted final key $\{a_f, b_f\}$ to decrypt the result of q_0 measurement. We can get a phenomenon. If $a_f = b_0 \oplus r_a(1) \oplus r_b(1) \oplus r_b(2) = 1$, the measurement result of q_0 is always 1. On the other hand, If $a_f = 0$, the measurement result of q_0 is always 0. In this way, we can always decrypt it and get $q_0 = 0$. In summary, our scheme can be proved to be correct.

Compared with the verification test of a single t-gates verified in[16], we can conclude that when there are more T-gates in the circuit, as long as we strictly follow the quantum key-update algorithm, we can get the correct decryption key.

6   PERFORMANCE ANALYSIS

The quantum principal component extraction algorithm implemented in this paper completely retains the main framework of HHL-like algorithm. The completeness and correctness of the algorithm are realized by quantum subroutines: quantum phase estimation, controlled rotation and inverse quantum phase estimation. While ensuring the correctness of quantum principal component extraction, it is also necessary to ensure the correctness, security and quasi-compactness of the encryption process.

1.This scheme has been proved to be correct[24]. The scheme points out that if the logic gates in the quantum circuit in the evaluation function in the encryption process are all composed of

$$S = \{X, Z, H, S, P, CNOT, T, T^\dagger\} \tag{26}$$

Then the GT scheme is a fully homomorphic encryption scheme. In this scheme, the algorithm not only has these quantum logic gates, but also has revolving gates R_y. But in [33] the formula (4.4)

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Y \tag{27}$$

where θ is the parameter. It can be seen that it is simply derived from the unit matrix I and the pauli Y matrix. Therefore, it also meets the correctness requirements of the GT scheme[25]. For arbitrary n-qubit quantum circuits C and n-qubit qubit data ρ. There is a decryption process $Dec\left(ek, \{r_a(i), r_b(i)\}_{i=1}^M, f, Eval\left(C, \{s_i\}_{i=1}^M, \varphi'\right)\right)$, where C is composed of General quantum gate $G[1], G[2],..., G[N]$ and $M = \{j | G[j_i] \in \{T, T^\dagger\}\}$.

In this scheme, we use the rotary measurement operation $\Phi\left(S^{a_{j_i-1}(\omega_i)}\right)$ to eliminate the errors introduced by the T gate in the encryption process, so that it can correctly evaluate the homomorphism, and represents the currently encrypted quantum T gate $G[j_i]$,.

The rotary measuring operation $\Phi\left(S^{a_{j_i-1}(\omega_i)}\right)$ contains two operations completed in $Eval$ and Dec: SWAP——the exchange operation and the measurement operation. The measurement of Dec mainly depends on whether an intermediate qubit is correct or not. If it is correct, it can be executed normally.

According to the fourth step in the scheme, we can know that because the order of the quantum gates is fixed, we can postpone the measurement of $\Phi\left(S^{a_{j_i-1}(\omega_i)}\right)$ and have no effect on the final result. Therefore, it is assumed that the operational measurements of both parts of $\Phi\left(S^{a_{j_i-1}(\omega_i)}\right)$ are carried out accurately in $Eval$ and accurate results are obtained $\{r_a(1), r_b(1)\}, ..., \{r_a(M), r_b(M)\}$.

In this way, in the process of $Eval$, when we implement our quantum principal component extraction for plaintext, we encrypt it in turn according to the quantum gate order we designed in advance. And ensure that every time the quantum gate is executed, the quantum secret key update algorithm is strictly implemented, and the intermediate secret key-updating function $\{h_i\}_{i=1}^M$ and the final key-updating function f are obtained. Finally, in the Dec, the intermediate key $(a_i, b_i)_M$ and the final key $\left(a_{final}, b_{final}\right)$ calculated in $Eval$ are correct. After the decryption step:

$$Dec(dk, \varphi') = Z^{a_{final}} X^{b_{final}} \varphi' X^{b_{final}} Z^{a_{final}} \tag{28}$$

The final decryption gets the correct result ρ'

2.This scheme is perfectly safe. In the encryption process, the encryption scheme can perfectly hide our initial key $ek = (a_0, b_0)$ and plaintext ρ. As long as you ensure that keys and randomly select a set of keys consisting of 0,1. And the client uses the combination of quantum gate pauli X

and pauli Z to act on plaintext ρ $\left(\rho \rightarrow \varphi = X^a Z^b \rho\right)$. For the input plaintext quantum state ρ and the output ciphertext quantum state ρ' is the maximum mixed state.

$$\frac{1}{2^{2n}} \sum_{a,b \in \{0,1\}^n} X^a Z^b \rho \left(X^a Z^b\right)^\dagger = \frac{I_{2^n}}{2^n} \tag{29}$$

Where $\frac{I_{2^n}}{2^n}$ is the maximum mixed state. According to this formula, Boykin and Roychowdhury have also been proved in quantum one-time pad(QOTP) [3]. And there is no interaction between the client and server during the evaluation process. its benefits from the quantum one-time pad(QOTP) encryption transformation we use also. Makes it impossible for the server to know any information about the key and plaintext throughout the execution of the scheme. In the process of performing decryption, the client only carries out some classical calculations and multiple quantum measurements, and does not interact with the client, and the measurement itself is a part of the decryption. Therefore, this scheme is perfectly safe.

3.The scheme itself is quasi-compact. Since every key update formula can be regarded as a binary number composed of XOR gates, according to our update rule, we can see:

$$\begin{cases} h_i : \{0,1\}^{2n+2(i-1)} \rightarrow \{0,1\}, i = 1, ..., M; \\ f : \{0,1\}^{2n+2M} \rightarrow \{0,1\}^{2n}. \end{cases} \tag{30}$$

The maximum computational complexity of the decryption process can be obtained as follows:

$$\sum_{i=1}^{M} \log_2 (2n + 2(i-1)) + 2n\log_2 (2n + 2M) = O\left((M + n) \log_2 (M + n)\right) \tag{31}$$

Where the computational complexity of h_i is $\log_2 2n + 2(i-1)$. The measurement operation in the decryption process requires M measurements and n-bit decryption, and the quantum complexity of the operation is $M + 2n$. Therefore, the decryption process has the quasi-compactness of $M \log M$ to the quantum circuit.

7 CONCLUSION AND FUTURE WORK

In this paper, a new quantum principal component extraction (QPCE) is proposed. Compared with the classical algorithm, this algorithm has an exponential improvement. Combined with the quantum homomorphic encryption scheme, a quantum homomorphic ciphertext dimension reduction scheme (QHEDR) is proposed for the first time. When the amount of data is large, plaintext can be calculated on the cloud (server) by once encryption, and there is no need for key-interaction. The client only requires M measurements and QOTP key update of n-bit quantum to get the calculated results. The scheme ensures security, correctness and quasi-compactness.

In addition, an example is given to verify the circuit of the quantum principal component extraction algorithm on the IBMQ computing platform. However, the complexity of the circuit T-gate of QPCE is high, so the decryption process of this scheme is more complex. And when there is a T-gate, two auxiliary quantum circuits are needed. The quantum circuits supported by the IBMQ computing cloud platform are insufficient. Therefore, we verify the correctness of the hybrid quantum circuit to replace the correctness of the complete QPCE under the ciphertext. The experimental results show that when there are T-gates in the quantum circuit and there are enough auxiliary quantum circuit, it is feasible to implement QHEDR scheme.

The proposal of the quantum computing scheme provides a solution and idea for the privacy problem in the cloud. In the future, we will implement this scheme on a real quantum circuit to reduce the complexity of T-gate and optimize the encryption scheme, so as to reduce the workload of the client and server.

ACKNOWLEDGMENTS

REFERENCES

[1] Duan Bojia, Yuan Jiabin, Liu Ying, and Li Dan. 2018. Efficient quantum circuit for singular-value thresholding. *Physical Review A* 98, 1 (2018), 012308−.

[2] Stephen Boyd, Stephen P Boyd, and Lieven Vandenberghe. 2004. Convex optimization. (2004).

[3] P. Oscar Boykin and Vwani Roychowdhury. 2003. Optimal Encryption of Quantum Bits. *Physical Review A* 67, 4 (2003), 645−648.

[4] Gilles Brassard, Peter Hoyer, Michele Mosca, and Alain Tapp. 2000. Quantum Amplitude Amplification and Estimation. *AMS Contemporary Mathematics Series* 305 (06 2000). https://doi.org/10.1090/conm/305/05215

[5] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. 2008. Universal blind quantum computation. (2008).

[6] X. D. Cai, C. Weedbrook, Z. E. Su, M. C. Chen, Mile Gu, M. J. Zhu, Li Li, Nai Le Liu, Chao Yang Lu, and Jian Wei Pan. 2013. Experimental Quantum Computing to Solve Systems of Linear Equations. *Physical Review Letters* (2013).

[7] Chao-Yang, Pang, Ri-Gui, Zhou, Cong-Bao, Ding, Ben-Qiong, and Hu. 2013. Quantum search algorithm for set operation. *Quantum Information Processing* (2013).

[8] Andrew M Childs. 2005. Secure assisted quantum computation. *Quantum Information & Computation* 5, 6 (2005), 456−466.

[9] Iris Cong and Luming Duan. 2016. Quantum discriminant analysis for dimensionality reduction and classification. *New Journal of Physics* 18, 7 (jul 2016), 073011. https://doi.org/10.1088/1367-2630/18/7/073011

[10] K. A. G. Fisher, A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. J. Resch. 2014. Quantum computing on encrypted data. *Nature Communications* 5, 2 (2014), 3074.

[11] Fitzsimons and F. Joseph. 2017. Private quantum computation: an introduction to blind quantum computing and related protocols. *Npj Quantum Information* 3, 1 (2017), 23.

[12] Joseph F. Fitzsimons and Elham Kashefi. 2017. Unconditionally verifiable blind quantum computation. *Phys.rev.a* 96, 1 (2017), 012303.

[13] Craig Gentry. 2009. *A fully homomorphic encryption scheme.* Stanford University.

[14] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. 2008. Quantum Random Access Memory. *Physical Review Letters* (2008).

[15] G. H. Golub and C. F. Van Loan. 1989. *Johns hopkins series in the mathematical sciences.* Johns Hopkins University Press.

[16] Du J. Dong Z. et al Gong, C. 2020. Grover algorithm-based quantum homomorphic encryption ciphertext retrieval scheme in quantum cloud computing. *Quantum Information Processing* 19, 3 (2020), 1−17.

[17] L. K. Grover. 1997. A fast quantum mechanical algorithm for database search. *Phys. Rev. Lett* 79 (1997).

[18] He Liang Huang, You Wei Zhao, Tan Li, Feng Guang Li, Yu Tao Du, Xiang Qun Fu, Shuo Zhang, Xiang Wang, and Wan Su Bao. 2017. Homomorphic encryption experiments on IBM's cloud quantum computing platform. *Frontiers of Physics* 12, 1 (2017), 120305.

[19] R. Jozsa. 2005. An introduction to measurement based quantum computation. *arXiv: Quantum Physics* (2005).

[20] Iordanis Kerenidis and Anupam Prakash. 2016. Quantum recommendation systems. *arXiv preprint arXiv:1603.08675* (2016).

[21] Dan Li, Michael Mc Gettrick, Fei Gao, Jie Xu, and Qiao Yan Wen. 2016. Generic quantum walks with memory on regular graphs. *Physical Review A* 93, 4 (2016), 042323.

[22] Liang and Min. 2013. Symmetric quantum fully homomorphic encryption with perfect security. *Quantum Information Processing* 12, 12 (2013), 3675−3687.

[23] Liang and Min. 2015. Quantum fully homomorphic encryption scheme based on universal quantum circuit. *Quantum Information Processing* 14, 8 (2015), 1−11.

[24] Min Liang. 2019. Teleportation-based quantum homomorphic encryption scheme with quasi-compactness and perfect security. *Quantum Information Processing* 19, 1, Article 28 (Dec. 2019), 28 pages. https://doi.org/10.1007/s11128-019-2529-6 arXiv:quant-ph/1812.07107

[25] Min Liang. 2020. Teleportation-based quantum homomorphic encryption scheme with quasi-compactness and perfect security. *Quantum Information Processing* 19, 1 (2020), 28.

[26] Ying Liu, Jiabin Yuan, Bojia Duan, and Dan Li. 2017. Quantum walks on regular uniform hypergraphs. (2017).

[27] Seth Lloyd and Avinatan Hassidim. 2010. Quantum Algorithm for Linear Systems of Equations. *APS* (03 2010).

[28] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. 2014. Quantum principal component analysis. *Nature Physics* 10, 9 (2014), 108−113 vol. 1.

[29] Liang Min and Yang Li. 2015. Quantum fully homomorphic encryption scheme based on quantum faulttolerant construction. (2015). arXiv:1503.04061v1

[30] Tomoyuki Morimae. 2012. Continuous-variable blind quantum computation. *Physical Review Letters* 109, 23 (2012), 230502.

[31] Tomoyuki Morimae and Keisuke Fujii. 2012. Blind topological measurement-based quantum computation. *Nature Communications* 3, 3 (2012), 1036.

[32] Kevin Murphy. 2012. *Machine Learning: A Probabilistic Perspective*. Vol. 58.

[33] Michael A Nielsen and Isaac L Chuang. 2011. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press.

[34] Jian Pan, Yudong Cao, Xiwei Yao, Zhaokai Li, Chenyong Ju, Xinhua Peng, Sabre Kais, and Jiangfeng Du. 2013. Experimental realization of quantum algorithm for solving linear systems of equations. (2013).

[35] Peter P. Rohde, Joseph F. Fitzsimons, and Alexei Gilchrist. 2012. Quantum walks with encrypted data. *Physical Review Letters* 109, 15 (2012), 150501.

[36] Maria Schuld, Ilya Sinayskiy, and Francesco Petruccione. 2015. An introduction to quantum machine learning. *Contemporary Physics* 56, 2 (2015), 172–185.

[37] Gael Sentis, John Calsamiglia, Ramon Munoz Tapia, and E. Bagan. 2012. Quantum learning without quantum memory. *Scientific reports* 2 (10 2012), 708. https://doi.org/10.1038/srep00708

[38] Peter W. Shor. 1996. Fault-tolerant quantum computation. *Foundations of Computer Science Annual Symposium on* (1996).

[39] Takahiro Sueki, Takeshi Koshiba, and Tomoyuki Morimae. 2013. Ancilla-Driven Universal Blind Quantum Computation. *Physical Review A* 87, 6 (2013), 4077–4082.

[40] Xiaoqiang Sun, Ting Wang, Zhiwei Sun, Ping Wang, Jianping Yu, and Weixin Xie. 2017. An efficient quantum somewhat homomorphic symmetric searchable encryption. *International Journal of Theoretical Physics* 56, 4 (2017), 1335–1345.

[41] Si Hui Tan, Joshua A Kettlewell, Yingkai Ouyang, Lin Chen, and Joseph F Fitzsimons. 2014. A quantum approach to fully homomorphic encryption. *eprint arxiv* (2014).

[42] Vittorio, Giovannetti, Lorenzo, Maccone, Tomoyuki, Morimae, Terry, G., and Rudolph. 2013. Efficient Universal Blind Quantum Computation. *Physical Review Letters* (2013).

[43] Wittek and Peter. 2014. Quantum Machine Learning: What Quantum Computing Means to Data Mining. (2014), 125–138.