Universal quantum circuit evaluation on encrypted data using probabilistic quantum homomorphic encryption scheme

Jing-Wen Zhang(张静文), Xiu-Bo Chen(陈秀波), Gang Xu(徐刚), and Yi-Xian Yang(杨义先)
Citation: Chin. Phys. B, 2021, 30 (**7**): 070309. DOI: 10.1088/1674-1056/ac003b
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Efficient self-testing system for quantum computations based on permutations

Shuquan Ma(马树泉), Changhua Zhu(朱畅华), Min Nie(聂敏), and Dongxiao Quan(权东晓)
Chin. Phys. B, 2021, 30 (**4**): 040305. DOI: 10.1088/1674-1056/abe29a

New semi-quantum key agreement protocol based on high-dimensional single-particle states

Huan-Huan Li(李欢欢), Li-Hua Gong(龚黎华), and Nan-Run Zhou(周南润)
Chin. Phys. B, 2020, 29 (**11**): 110304. DOI: 10.1088/1674-1056/abaedd

Hybrid linear amplifier-involved detection for continuous variable quantum key distribution with thermal states

Yu-Qian He(贺宇千), Yun Mao(毛云), Hai Zhong(钟海), Duang Huang(黄端), Ying Guo(郭迎)
Chin. Phys. B, 2020, 29 (**5**): 050309. DOI: 10.1088/1674-1056/ab8216

Reference-frame-independent quantum key distribution with an untrusted source

Jia-Ji Li(李家骥), Yang Wang(汪洋), Hong-Wei Li(李宏伟), Wan-Su Bao(鲍皖苏)
Chin. Phys. B, 2020, 29 (**3**): 030303. DOI: 10.1088/1674-1056/ab695d

Joint remote preparation of an arbitrary five-qubit Brown state via non-maximally entangled channels

Chang Li-Wei, Zheng Shi-Hui, Gu Li-Ze, Xiao Da, Yang Yi-Xian
Chin. Phys. B, 2014, 23 (**9**): 090307. DOI: 10.1088/1674-1056/23/9/090307

SPECIAL TOPIC — Quantum computation and quantum simulation

Universal quantum circuit evaluation on encrypted data using probabilistic quantum homomorphic encryption scheme*

Jing-Wen Zhang(张静文)[1], Xiu-Bo Chen(陈秀波)[1], Gang Xu(徐刚)[2,†], and Yi-Xian Yang(杨义先)[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

(Received 25 March 2021; revised manuscript received 30 April 2021; accepted manuscript online 12 May 2021)

Homomorphic encryption has giant advantages in the protection of privacy information. In this paper, we present a new kind of probabilistic quantum homomorphic encryption scheme for the universal quantum circuit evaluation. Firstly, the pre-shared non-maximally entangled states are utilized as auxiliary resources, which lower the requirements of the quantum channel, to correct the errors in non-Clifford gate evaluation. By using the set synthesized by Clifford gates and T gates, it is feasible to perform the arbitrary quantum computation on the encrypted data. Secondly, our scheme is different from the previous scheme described by the quantum homomorphic encryption algorithm. From the perspective of application, a two-party probabilistic quantum homomorphic encryption scheme is proposed. It is clear what the computation and operation that the client and the server need to perform respectively, as well as the permission to access the data. Finally, the security of probabilistic quantum homomorphic encryption scheme is analyzed in detail. It demonstrates that the scheme has favorable security in three aspects, including privacy data, evaluated data and encryption and decryption keys.

Keywords: quantum homomorphic encryption, universal quantum circuit, non-maximally entangled state, security

PACS: 05.30.–d, 03.67.Dd, 03.65.–w **DOI:** 10.1088/1674-1056/ac003b

1. Introduction

With the rapid development of the network, it makes information transmission fast and provides a large quantity of information on the Internet. Therefore, the privacy protection of sensitive information is particularly important. When some clients who do not have the computational power cannot calculate their own confidential information, the information needs to be encrypted and sent to a server with rich resources and powerful functions to operate. Homomorphic encryption provides an effective way to process and calculate encrypted data without revealing the contents of the privacy information. Reviewing the classical homomorphic encryption (HE), the idea was first presented by Rivest *et al.*[1] in 1978. It was widely studied and applied, and can only achieve the additively HE schemes. Until a breakthrough was made in 2009, Gentry[2] found and conducted an in-depth study of the fully homomorphic encryption (FHE) scheme based on non-standard computational assumptions, thereby giving the multiplicatively HE scheme. Subsequently, many optimization and improvement schemes for FHE have been proposed.[3–7] With the development of classical homomorphic encryption, many achievements have been made and a large amount of related researches have also been sparked, such as delegating computation,[8–11] functional encryption,[12,13] and obfuscation.[14]

At the same time, this research has drawn attention in the field of quantum information. Quantum homomorphic encryption is that the client delegates quantum computation on the encrypted data to the server, that is, the server performs quantum computation on the ciphertext, and the result is consistent with a valid ciphertext after performing this computation on the original plaintext. In other words, the server implements quantum computation without decrypting, and the client decrypts the computation results to obtain the quantum computation on the original data. In 2012, Rohde *et al.*[15] described a limited quantum homomorphic encryption scheme with the boson scattering model and quantum walks to complete the restricted quantum computation. The concept of quantum homomorphic encryption (QHE) and quantum fully homomorphic encryption (QFHE) was proposed by Liang[16] in 2013. In Liang's scheme, the symmetric QHE scheme was constructed. Then, inspired by the tripartite blind quantum computation,[17] Liang proposed a QHE scheme through the use of universal quantum circuit.[18] It permits universal quantum computation on encrypted quantum state without decryption. Nevertheless, in 2014, Yu *et al.*[19] found that there is a limitation on the QHE scheme with information-theoretically-secure, that is, deterministic QHE with perfect information theoretic se-

*Project supported by the Fundamental Research Funds for the Central Universities (Grant No. 2019XDA02) and the Scientific Research Foundation of North China University of Technology.

†Corresponding author. E-mail: gangxu_bupt@163.com

curity will certainly lead to exponential overhead. This had led to more in-depth discussions among researchers on QFHE schemes that enable to complete universal quantum computation. In the same year, an effective method was proposed by Fisher *et al.*[20] By using single photons and linear optics, it is experimentally proved that arbitrary quantum computation can be adequately implemented through a set of quantum gates with few extra resources. Based on the modification of the above work, Broadbent and Jeffery (BJ15) completed the limited number of non-Clifford gates evaluation by presenting two instructive and secure QHE schemes.[21] The formal definitions of QHE and QFHE were given, and the definition of quantum indistinguishability under chosen plaintext attack was also given. In 2016, Dulek *et al.*[22] extended the non-Clifford gate circuit in BJ15 to arbitrary polynomial-sized quantum circuits. A novel compact QFHE scheme was given that could effectively correct the errors in the T-gate evaluation of encrypted quantum data. Based on the research results of Dulek *et al.*,[22] Alagic *et al.*[23] constructed a QFHE scheme with verification to generate a classical computation log, so that the user can verify the homomorphic quantum computation on the ciphertext. It put forward a new direction for future research, that is, more QFHE schemes with certain properties could be found.

In 2016, Tan *et al.*[24] presented a private-key QHE scheme by using the thoughts of group theory. The scheme supported a broad range of quantum computation tasks and limited the information that attackers can access to ensure information theoretic security. After exhaustive research, Ouyang and Tan *et al.*[25] designed a QHE from quantum codes that allows for the evaluation of a finite number of non-Clifford gates included in the quantum circuits and has entropy security which is independent of the adversary's computational power. Moreover, this scheme demonstrated that the model of entropy security is stronger than the security model in BJ15. In 2018, Mahadev[26] constructed the first leveled FHE scheme with classical keys for quantum circuits using quantum capable scheme. It makes blind delegate quantum computations possible to the trusted quantum server, while a malicious server cannot get any information from this process. In addition to the above schemes, there are many results related to QHE schemes.[27–31]

The evaluation of the non-Clifford gates will be subject to errors, leading to the failure of the expected computation results in the QHE scheme. As a result, it is an essential and difficult problem to correct the errors of non-Clifford gate evaluation. The schemes in Refs. [21–25] are all leveled QHE schemes, in which the BJ15 framework utilizes the maximum entangled state to process the correction required for the evaluation of the non-Clifford gates until the decryption phase. In other words, the problem of implementing the QHE scheme via the maximum entangled channel has been studied. As a quantum auxiliary resource, different classes of states are considered to be able to complete the correction of non-Clifford gate evaluation errors in the QHE scheme. Since in the realistic environment, a quantum system is open and usually interacts with the surrounding environment, causing the maximal entangled quantum channel tends to degenerate into the non-maximally entangled quantum channel. Also, it may happen that the source does not produce perfect maximally entangled states rather non-maximally entangled pairs. It has become clear that the non-maximally entangled state is not only relatively well prepared, but also shows evident advantages to implement quantum communication protocols in a specific physical system. For example, three-qubit non-maximally entangled state are used as a resource to attain optimal controlled quantum teleportation fidelity, which essentially lowers the requirements of quantum channels.[32] And, for an amplitude damping channel, it was shown that optimal entanglement negativity is obtained only by a non-maximally entangled state.[33] Hence, it is important to investigate the QHE scheme by utilizing the non-maximally entangled state. The pre-shared non-maximally entangled states are used as auxiliary resources to correctly and safely complete the two-party QHE scheme, while lowering the requirements of the quantum channel. This work is of great importance to the experimental realization of the QHE scheme under inevitable noisy effects.

In this paper, we initially introduce non-maximally entangled states as auxiliary resources to correct the erroneous P-gate occurring in the non-Clifford gate evaluation. The arbitrary quantum computation can be performed on the encrypted data and the privacy of data is maintained. Then, unlike other schemes explicated from the perspective of algorithm, we give the process of two-party probabilistic quantum homomorphic encryption scheme from the viewpoint of application. Finally, this scheme has a good performance in terms of security.

The structure of this paper is organized as follows. In Section 2, some preliminary knowledge including quantum computation, quantum one-time pad and quantum homomorphic encryption are introduced. We present our QHE scheme in Section 3. The main idea and the specific process of the scheme are introduced in detail. In Section 4, the security of the scheme is analyzed and discussed. Our work and prospects for future research are summarized in Section 5.

2. Preliminaries

In this section, we provide a detailed introduction to the preliminaries, which helps us to have better understandings of our work. At the same time, the basic definition and related properties of QHE are given. Through these preliminaries, it will be smoother to describe our scheme.

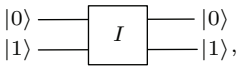
2.1. Quantum computation

A quantum composite system consists of two or more different physical systems. In many cases of quantum mechanics, it is necessary to work with multiparticle states. The quantum state in the composite system can be expressed as the tensor product form of the quantum states in two subsystems, such as $|\varphi_A\rangle|\varphi_B\rangle$. If there are two single qubits that cannot be written as tensor product form, *i.e.*, $|\varphi\rangle \neq |a\rangle|b\rangle$, then $|\varphi\rangle$ is known as entangled state. Quantum entanglement is a property of composite systems which has a significant role in quantum computation.[34] It is also one of the main properties used in this paper. Quantum entanglement can be generated under control in different quantum systems, which reflects nonclassical strong correlation and non-locality in two or more quantum systems. In the processing of quantum information, entangled quantum states are often used as quantum channels. The family of two-qubit entangled states is referred to as Bell states in bipartite system, which can be transformed into each other through local operations and classical communication (LOCC). They are also called EPR states, and the forms are as follows:

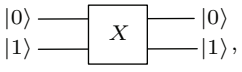
$$\left|\Phi^{\pm}\right\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \quad \left|\Psi^{\pm}\right\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}.$$

Another fundamental assumption of quantum mechanics suggests that the evolution of a closed quantum system can be characterized by the unitary operator. Common unitary single-qubit operators include Pauli operators and Hadamard gate, where the Pauli operators are denoted by $\sigma_0, \sigma_x, \sigma_y$, and σ_z.[35] Their forms and circuit diagram representations are given in the following expressions:

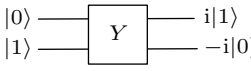
$$\sigma_0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$



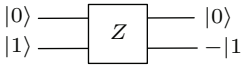
$$\sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$



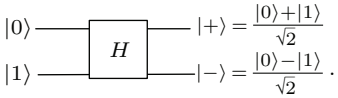
$$\sigma_y = Y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix},$$



$$\sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

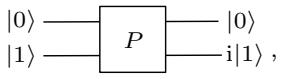


$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

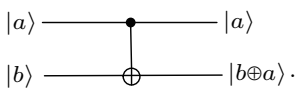


In addition to the quantum logic gates described above, phase shift gate and controlled-NOT gate are also common,

$$P = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{i} \end{pmatrix},$$

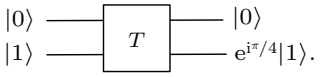


$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

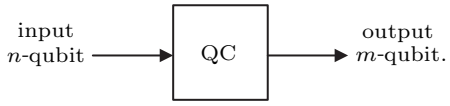


The entire Clifford group circuit can be generated from these gates, but non-Clifford gate, such as T-gate, needs to be added to simulate universal quantum circuit,

$$T = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\pi/4} \end{pmatrix},$$



In a classic computer, the circuit consists of logic gates and wires, where the logic gates are responsible for the processing of the information and the wires are used for the transmission of the information. Quantum circuits consist of quantum gates operated on qubits. Each wire in a quantum circuit may not correspond to a physical connection, but to a physical particle transformation in a period of time or a physical particle moving from one location to another in space. A quantum circuit (QC) with n-qubit input and m-qubit output, from left to right represents the transfer process of quantum states in time or space.



2.2. Quantum one-time pad

In classical cryptography, the security of encryption and decryption usually depends on the assumption of computational intractability, while in quantum cryptography, the security of quantum cryptography depends on the information theoretic security of quantum mechanical properties. In the context of quantum data, the encryption process of information can be depicted as follows by using the quantum one-time pad (QOTP).

Alice has a set of K operations $\{U_k\}$, in which each element is an unitary matrix of $2^n \times 2^n$ and the occurrence probability of each element is $1/2^{2n}$, acting on the quantum information of n qubits. A new encryption key is generated each time the qubit is encrypted. The encrypted quantum information would become a completely mixed state, so it is meaningless for Eve to get a complete quantum state, which guarantees the security of quantum information. For the input quantum state ρ carrying information, applying a random Pauli operator to the information state will get the cipher state σ, which is the completely mixed state,[36]

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

where (a,b) are the key to the pad. Pauli operators X and Z are chosen uniformly at random to encrypt the quantum information.

2.3. Quantum homomorphic encryption

This subsection introduces some definitions of quantum homomorphic encryption, homomorphism, compactness, quantum fully homomorphic encryption. For a deeper understanding of these definitions, refer to Ref. [21].

Definition 1 (quantum homomorphic encryption) Here we introduce the QHE for asymmetric-key, which includes the following four algorithms:

(i) **Key Generation** $QHE.KeyGen(1^{\kappa}) \rightarrow (pk, sk, \rho_{evk})$, where $\kappa \in N$ is the security parameter, pk is the classical public key for encrypting quantum information, sk is the classical private key for decrypting, ρ_{evk} is the quantum evaluation key for evaluating circuits on the encrypted quantum information.

(ii) **Encryption** $QHE.Enc_{pk}(\rho) \rightarrow \sigma$. For the input quantum plaintext ρ, it is encrypted into the quantum ciphertext σ using the public key pk.

(iii) **Evaluation** $QHE.Eval^{QC}_{\rho_{\text{evk}}}(\sigma) \rightarrow \sigma'$, where QC represents any quantum evaluation circuit that acts on the encrypted ciphertext σ and outputs a ciphertext quantum state σ'. The evaluation key ρ_{evk} is consumed during the process. This ciphertext is identical to the result of the evaluation circuit acting on the plaintext and then encrypting.

(iv) **Decryption** $QHE.Dec_{sk}(\sigma') \rightarrow \rho'$. For the ciphertext σ', it is decrypted with the private key sk to obtain ρ' as the calculation result of the evaluation algorithm acting on the original plaintext ρ.

Definition 2 (homomorphism) For any quantum circuit QC and the input quantum plaintext ρ, a QHE scheme satisfies homomorphism if there exists a negligible function η such that

$$\begin{aligned}&\Pr[QHE.Des_{sk}(QHE.Eval^{QC}_{\rho_{evk}}(QHE.Enc_{pk}(\rho)))\\ &\neq \Phi_{QC}(\rho)] \leq \eta(\kappa),\end{aligned} \tag{2}$$

where Φ_{QC} is the quantum channel that is induced by the quantum circuit QC.

Definition 3 (compactness) A QHE scheme is compact if the complexity of the decryption algorithm does not depend on the size of the evaluation circuit. That is, for any quantum circuit QC and ciphertext σ, $QHE.Dec$ is applied to $QHE.Eval^{QC}(\sigma)$. There exists a polynomial $p(\kappa)$ such that the complexity of this computational process is at most $p(\kappa)$.

Definition 4 (quantum fully homomorphic encryption) If the QHE scheme satisfies both homomorphism and compactness for all quantum circuits on some universal gate sets, it is a quantum full homomorphic encryption scheme.

3. Our scheme

In this section, based on the model of BJ15, we propose a novel probabilistic quantum homomorphic encryption (PQHE) scheme for universal quantum circuit. Before describing our PQHE scheme, the main idea is given by utilizing the non-maximally entangled state to complete the evaluation of non-Clifford gates. It will be helpful to the proposal of our scheme.

3.1. Main idea

Without decrypting the encrypted data, quantum homomorphic encryption gives a feasible way to perform arbitrary computational evaluations. In the construction of QHE scheme, at least one non-Clifford gate should be added to achieve universality for quantum circuits. However, it is always the focus and barrier of the research to deal with the errors in the evaluation of non-Clifford gates. T-gate, *i.e.*, "$8/\pi$" gate, is the first non-Clifford gate to be known. When the homomorphic evaluation of T-gate is performed on the quantum state encrypted by QOTP, the output will contain an unexpected P error,

$$TX^aZ^b|\varphi\rangle = X^aZ^{a\oplus b}P^aT|\varphi\rangle. \tag{3}$$

In order to obtain the quantum state expected by the evaluator, the error must be corrected. The user decrypts the corrected quantum state to acquire the result of performing T-gate calculation on the initial plaintext.

However, the maximum entangled state is considered to be extremely difficult to prepare in a specific physical system. During the preparation of the maximum entangled state, it must be affected by some factors, such as physical equipment, noise and decoherence. Therefore, our scheme extends the BJ15 scheme under the wise usage of the pre-shared non-maximally entangled states as auxiliary resources to probabilistically correct the erroneous P-gate. Although the probability of success in correcting errors is decreased, it is meaningful from the perspective of experimentally implementing the QHE scheme. The universal quantum circuit with a finite number of non-Clifford gates can be applied on the encrypted quantum state in the evaluation stage.

The major idea of our scheme is that when performing the T-gate evaluation, the state $|\Phi\rangle$ is introduced which is the non-maximally entangled state given by

$$|\Phi\rangle = m|00\rangle + n|11\rangle, \tag{4}$$

where m and n are complex numbers and satisfy the normalization condition $|m|^2 + |n|^2 = 1$. Then, the CNOT operation is applied on the non-maximally entangled state with the evaluation circuit. The auxiliary particle is introduced by the part of the circuit's output. After the defined U operation, the measurement is made. When the final measurement result is $|0\rangle$, the P-gate error is successfully corrected. Otherwise, error correction fails. This process is minutely illustrated in Fig. 1.

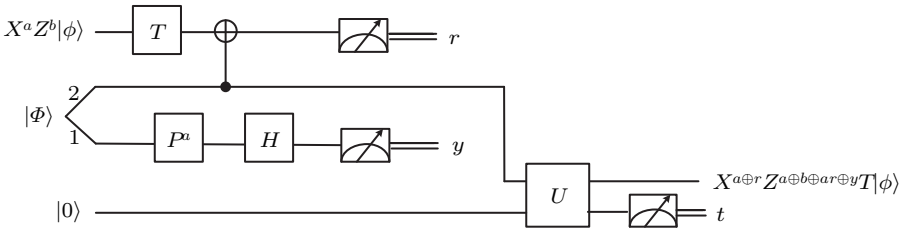


Fig. 1. The homomorphic evaluation of our scheme for T-gate.

As shown in Fig. 1, the quantum state is $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ which will be encrypted by using QOTP, that is, the initial state is encrypted by X^aZ^b, where a and b are random classical bits ($a,b \in \{0,1\}$). The state will be $|\phi_0\rangle = X^aZ^b|\phi\rangle$ and the following four cases are obtained:

$$\{\alpha|0\rangle+\beta|1\rangle, \alpha|0\rangle-\beta|1\rangle, \alpha|1\rangle+\beta|0\rangle, \alpha|1\rangle-\beta|0\rangle\}. \quad (5)$$

When the first T-gate appears in the evaluation circuit, the T-gate will be applied to the ciphertext, $|\phi_1\rangle = TX^aZ^b|\phi\rangle$. And the encrypted state (5) will become

$$\begin{aligned}&\{\alpha|0\rangle + \mathrm{e}^{\mathrm{i}\pi/4}\beta|1\rangle, \alpha|0\rangle - \mathrm{e}^{\mathrm{i}\pi/4}\beta|1\rangle,\\ &\mathrm{e}^{\mathrm{i}\pi/4}\alpha|1\rangle + \beta|0\rangle, \mathrm{e}^{\mathrm{i}\pi/4}\alpha|1\rangle - \beta|0\rangle\}. \end{aligned} \quad (6)$$

In the meantime, the non-maximally entangled state $|\Phi_{12}\rangle = m|00\rangle + n|11\rangle$ is required. Its first particle is used as the control qubit and the quantum state $|\phi_1\rangle$ is used as the target qubit to perform a CNOT operation, *i.e.*, $(I \otimes CNOT)(|\Phi_{12}\rangle \otimes |\phi_1\rangle)$. After applying P^a and H operations on the second particle of the non-maximally entangled state, we will have $(H \otimes I \otimes I)(I \otimes CNOT)(|\Phi_{12}\rangle \otimes |\phi_1\rangle) = (H \otimes CNOT)(|\Phi_{12}\rangle \otimes |\phi_1\rangle)$ when a = 0 and $(HP \otimes I \otimes I)(I \otimes CNOT)(|\Phi_{12}\rangle \otimes |\phi_1\rangle) = (HP \otimes CNOT)(|\Phi_{12}\rangle \otimes |\phi_1\rangle)$ when $a = 1$, namely,

$$\begin{aligned}&(\alpha|0\rangle \pm \mathrm{e}^{\mathrm{i}\pi/4}\beta|1\rangle)(m|00\rangle + n|11\rangle)\\ \xrightarrow{CNOT}\ &m(\alpha|0\rangle \pm \mathrm{e}^{\mathrm{i}\pi/4}\beta|1\rangle)|00\rangle + n(\alpha|1\rangle \pm \mathrm{e}^{\mathrm{i}\pi/4}\beta|0\rangle)|11\rangle\\ \xrightarrow{H}\ &m(\alpha|0\rangle \pm \mathrm{e}^{\mathrm{i}\pi/4}\beta|1\rangle)|0\rangle \cdot \frac{|0\rangle+|1\rangle}{\sqrt{2}}\\ &+n(\alpha|1\rangle \pm \mathrm{e}^{\mathrm{i}\pi/4}\beta|0\rangle)|1\rangle \cdot \frac{|0\rangle-|1\rangle}{\sqrt{2}}, \end{aligned} \quad (7)$$

$$\begin{aligned}&(\mathrm{e}^{\mathrm{i}\pi/4}\alpha|1\rangle \pm \beta|0\rangle)(m|00\rangle + n|11\rangle)\\ \xrightarrow{CNOT}\ &m(\mathrm{e}^{\mathrm{i}\pi/4}\alpha|1\rangle \pm \beta|0\rangle)|00\rangle + n(\mathrm{e}^{\mathrm{i}\pi/4}\alpha|0\rangle \pm \beta|1\rangle)|11\rangle\\ \xrightarrow{HP}\ &m(\mathrm{e}^{\mathrm{i}\pi/4}\alpha|1\rangle \pm \beta|0\rangle)|0\rangle \cdot \frac{|0\rangle+|1\rangle}{\sqrt{2}}\\ &+n(\mathrm{e}^{\mathrm{i}\pi/4}\alpha|0\rangle \pm \beta|1\rangle)|1\rangle \cdot \mathrm{i}\frac{|0\rangle-|1\rangle}{\sqrt{2}}. \end{aligned} \quad (8)$$

Table 1. Measurement results of the target qubit and the second particle of the non-maximally entangled state.

The state to be measured	r	y	The measurement results
$m\left(\alpha\|0\rangle + \mathrm{e}^{\mathrm{i}\pi/4}\beta\|1\rangle\right)\|0\rangle \cdot (\|0\rangle+\|1\rangle)/\sqrt{2}$	0	0	$(1/\sqrt{2})\left(m\alpha\|0\rangle + \mathrm{e}^{\mathrm{i}\pi/4}n\beta\|1\rangle\right)$
$+n\left(\alpha\|1\rangle + \mathrm{e}^{\mathrm{i}\pi/4}\beta\|0\rangle\right)\|1\rangle \cdot (\|0\rangle-\|1\rangle)/\sqrt{2}$	0	1	$(1/\sqrt{2})\left(m\alpha\|0\rangle - \mathrm{e}^{\mathrm{i}\pi/4}n\beta\|1\rangle\right)$
	1	0	$(1/\sqrt{2})\left(\mathrm{e}^{\mathrm{i}\pi/4}m\beta\|0\rangle + n\alpha\|1\rangle\right)$
	1	1	$(1/\sqrt{2})\left(\mathrm{e}^{\mathrm{i}\pi/4}m\beta\|0\rangle - n\alpha\|1\rangle\right)$
$m\left(\alpha\|0\rangle + \mathrm{e}^{\mathrm{i}\pi/4}\beta\|1\rangle\right)\|0\rangle \cdot (\|0\rangle+\|1\rangle)/\sqrt{2}$	0	0	$(1/\sqrt{2})\left(m\alpha\|0\rangle - \mathrm{e}^{\mathrm{i}\pi/4}n\beta\|1\rangle\right)$
$-n\left(\alpha\|1\rangle + \mathrm{e}^{\mathrm{i}\pi/4}\beta\|0\rangle\right)\|1\rangle \cdot (\|0\rangle-\|1\rangle)/\sqrt{2}$	0	1	$(1/\sqrt{2})\left(m\alpha\|0\rangle + \mathrm{e}^{\mathrm{i}\pi/4}n\beta\|1\rangle\right)$
	1	0	$(1/\sqrt{2})\left(-\mathrm{e}^{\mathrm{i}\pi/4}m\beta\|0\rangle + n\alpha\|1\rangle\right)$
	1	1	$(1/\sqrt{2})\left(-\mathrm{e}^{\mathrm{i}\pi/4}m\beta\|0\rangle - n\alpha\|1\rangle\right)$
$m\left(\mathrm{e}^{\mathrm{i}\pi/4}\alpha\|1\rangle + \beta\|0\rangle\right)\|0\rangle \cdot (\|0\rangle+\|1\rangle)/\sqrt{2}$	0	0	$(1/\sqrt{2})\left(m\beta\|0\rangle + \mathrm{i}\,\mathrm{e}^{\mathrm{i}\pi/4}n\alpha\|1\rangle\right)$
$+n\left(\mathrm{e}^{\mathrm{i}\pi/4}\alpha\|0\rangle + \beta\|1\rangle\right)\|1\rangle \cdot \mathrm{i}(\|0\rangle-\|1\rangle)/\sqrt{2}$	0	1	$(1/\sqrt{2})\left(m\beta\|0\rangle - \mathrm{i}\,\mathrm{e}^{\mathrm{i}\pi/4}n\alpha\|1\rangle\right)$
	1	0	$(1/\sqrt{2})\left(\mathrm{e}^{\mathrm{i}\pi/4}m\alpha\|0\rangle + \mathrm{i}\cdot n\beta\|1\rangle\right)$
	1	1	$(1/\sqrt{2})\left(\mathrm{e}^{\mathrm{i}\pi/4}m\alpha\|0\rangle - \mathrm{i}\cdot n\beta\|1\rangle\right)$
$m\left(\mathrm{e}^{\mathrm{i}\pi/4}\alpha\|1\rangle + \beta\|0\rangle\right)\|0\rangle \cdot (\|0\rangle+\|1\rangle)/\sqrt{2}$	0	0	$(1/\sqrt{2})\left(m\beta\|0\rangle - \mathrm{i}\,\mathrm{e}^{\mathrm{i}\pi/4}n\alpha\|1\rangle\right)$
$-n\left(\mathrm{e}^{\mathrm{i}\pi/4}\alpha\|0\rangle + \beta\|1\rangle\right)\|1\rangle \cdot \mathrm{i}(\|0\rangle-\|1\rangle)/\sqrt{2}$	0	1	$(1/\sqrt{2})\left(m\beta\|0\rangle + \mathrm{i}\,\mathrm{e}^{\mathrm{i}\pi/4}n\alpha\|1\rangle\right)$
	1	0	$(1/\sqrt{2})\left(\mathrm{e}^{\mathrm{i}\pi/4}m\alpha\|0\rangle - \mathrm{i}\cdot n\beta\|1\rangle\right)$
	1	1	$(1/\sqrt{2})\left(\mathrm{e}^{\mathrm{i}\pi/4}m\alpha\|0\rangle + \mathrm{i}\cdot n\beta\|1\rangle\right)$

After the above operation is completed, the measurement will be made in the basis $\{|0\rangle,|1\rangle\}$. The measurement results of the target qubit and the second particle of the non-maximally entangled state will be two classical bits that recorded as r and y respectively. In Table 1, the values of the measurement results are displayed substantially which all hold up to an irrelevant global phase.

Through the above series of operations, the coefficient of the state will contain the uncertain values m and n. In order to attain the desired result of T-gate acting on the encrypted state, it will be required to introduce an auxiliary particle $|0\rangle$ and perform the defined unitary operation that denoted as U, where

$$U = \begin{pmatrix} I & 0 \\ 0 & U_a \end{pmatrix}. \tag{9}$$

U gate corresponds to a target qubit rotation characterized by $U_a = \mathrm{e}^{-\mathrm{i}\pi/2}\mathrm{e}^{\mathrm{i}\pi/2\cdot\hat{\boldsymbol{n}}\cdot\boldsymbol{\sigma}}$,[37] which is a rotation operator in a $\pi/2$ angle around the unitary vector $\hat{\boldsymbol{n}}$, specifically $\hat{\boldsymbol{n}} = (\sqrt{1-m^2/n^2}, 0, m/n)$ and $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. Next, we give the calculation process of U_a operator as follows:

$$\begin{aligned} U_a &= \mathrm{e}^{-\mathrm{i}\pi/2}\mathrm{e}^{\mathrm{i}\pi/2\cdot\hat{\boldsymbol{n}}\cdot\boldsymbol{\sigma}} \\ &= \left[\cos\left(-\frac{\pi}{2}\right) + \mathrm{i}\sin\left(-\frac{\pi}{2}\right)\right] \\ &\quad \times \left[\cos\left(-\frac{\pi}{2}\right)\cdot I - \mathrm{i}\sin\left(-\frac{\pi}{2}\right)\right. \\ &\quad \left.\times\left(\sqrt{1-\frac{m^2}{n^2}}\cdot\sigma_x + \frac{m}{n}\cdot\sigma_z\right)\right] \\ &= -\mathrm{i}\cdot\mathrm{i}\left[\begin{pmatrix} 0 & \sqrt{1-m^2/n^2} \\ \sqrt{1-m^2/n^2} & 0 \end{pmatrix}\right. \\ &\quad \left.+\begin{pmatrix} m/n & 0 \\ 0 & -m/n \end{pmatrix}\right] \\ &= \begin{pmatrix} m/n & \sqrt{1-m^2/n^2} \\ \sqrt{1-m^2/n^2} & -m/n \end{pmatrix}. \end{aligned} \tag{10}$$

Without loss of generality, the measurement result $m\alpha|0\rangle + \mathrm{e}^{\mathrm{i}\pi/4}n\beta|1\rangle$ is taken as an example, the operation of U gate after introducing $|0\rangle$ is exhibited in detail,

$$\begin{aligned} &\frac{1}{\sqrt{2}}U(m\alpha|0\rangle|0\rangle + \mathrm{e}^{\mathrm{i}\pi/4}n\beta|1\rangle|0\rangle) \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & m/n & \sqrt{1-m^2/n^2} \\ 0 & 0 & \sqrt{1-m^2/n^2} & -m/n \end{pmatrix}\begin{pmatrix} m\alpha \\ 0 \\ \mathrm{e}^{\mathrm{i}\pi/4}n\beta \\ 0 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix} m\alpha \\ 0 \\ \mathrm{e}^{\mathrm{i}\pi/4}m\beta \\ \mathrm{e}^{\mathrm{i}\pi/4}n\beta\cdot\sqrt{1-m^2/n^2} \end{pmatrix} \\ &= \frac{1}{\sqrt{2}}\left[m(\alpha|0\rangle + \mathrm{e}^{\mathrm{i}\pi/4}\beta|1\rangle)|0\rangle\right. \\ &\quad \left.+\mathrm{e}^{\mathrm{i}\pi/4}n\beta\cdot\sqrt{1-\frac{m^2}{n^2}}|1\rangle|1\rangle\right]. \end{aligned} \tag{11}$$

The final state Eq. (11) is measured. If the measurement result is $|0\rangle$, the P-gate error is successfully corrected. The desired result of the first T-gate acting on the encrypted state is obtained, which is $TX^aZ^b|\phi\rangle = \alpha|0\rangle + \mathrm{e}^{\mathrm{i}\pi/4}\beta|1\rangle$ $(a=0, b=0)$ in the example. This result is also consistent with

$$\begin{aligned} &X^{a\oplus r}Z^{a\oplus b\oplus ar\oplus y}T|\phi\rangle = X^0Z^0T|\phi\rangle = \alpha|0\rangle + \mathrm{e}^{\mathrm{i}\pi/4}\beta|1\rangle \\ &(a=0, b=0, r=0, y=0). \end{aligned} \tag{12}$$

It can be seen that the correct result is obtained with the probability $\frac{1}{2}m^2$ by measuring the auxiliary particle under the basis $\{|0\rangle,|1\rangle\}$. If the measurement result is $|1\rangle$, the correction of the P-gate error fails. It means that our PQHE scheme can realize the homomorphic calculation of the T gate with the probability $\frac{1}{2}m^2$ when the quantum channel shared between the user and the evaluator is non-maximally entangled.

As described in the section, it is clear that our QHE scheme is probabilistic for universal quantum circuit containing a limited number of T-gates. Compared with BJ15, it is shown that the non-maximally entangled state can also be chosen to perfectly solve the problem of the T-gate evaluation in our scheme with the probability $\frac{1}{2}m^2$, which provides an idea that may simplify the implementation of the experiment. The cost of this scheme is to decrease the probability of success. In the practical physical system, the environment or other factors will affect the preparation of quantum states, leading to a great difficulty in the preparation of maximum entangled states. It is also difficult to maintain the maximally entanglement. On the other hand, non-maximally entangled states are comparatively easier to prepare. In brief, it follows that extension of the BJ15 scheme with the non-maximally entangled state not only allows for the universal quantum circuit evaluation, but is also more accessible to experiment.

3.2. Our PQHE scheme

In this section, we will specifically present our PQHE scheme. From the perspective of application, there is a clear division of the computations between the client and the server, as well as the determined access rights to the keys and data. Our scheme is a novel two-party PQHE scheme which allows for arbitrary quantum computation within a large class of quantum circuits. Here, the quantum circuit contains Clifford group gates and a finite number of non-Clifford group gates (*i.e.*, T-gates). In this scheme, firstly, the client randomly generates an encryption key that will be only used once through the key generation algorithm. The private data is encrypted by using QOTP to guarantee the information theoretic security. The encrypted data and the predetermined evaluation circuit are transmitted to the server. Secondly, the server evaluates

the received encrypted data according to the sequence of gate operations in the evaluation circuit without decryption. And the evaluated data is returned to the client. Finally, the client generates the decryption key by utilizing the key update rules according to the order of the evaluation circuit and the private key it holds. The evaluated data will be decrypted to get the expected result of the evaluation operation on the original private data. Figure 2 depicts it explicitly.

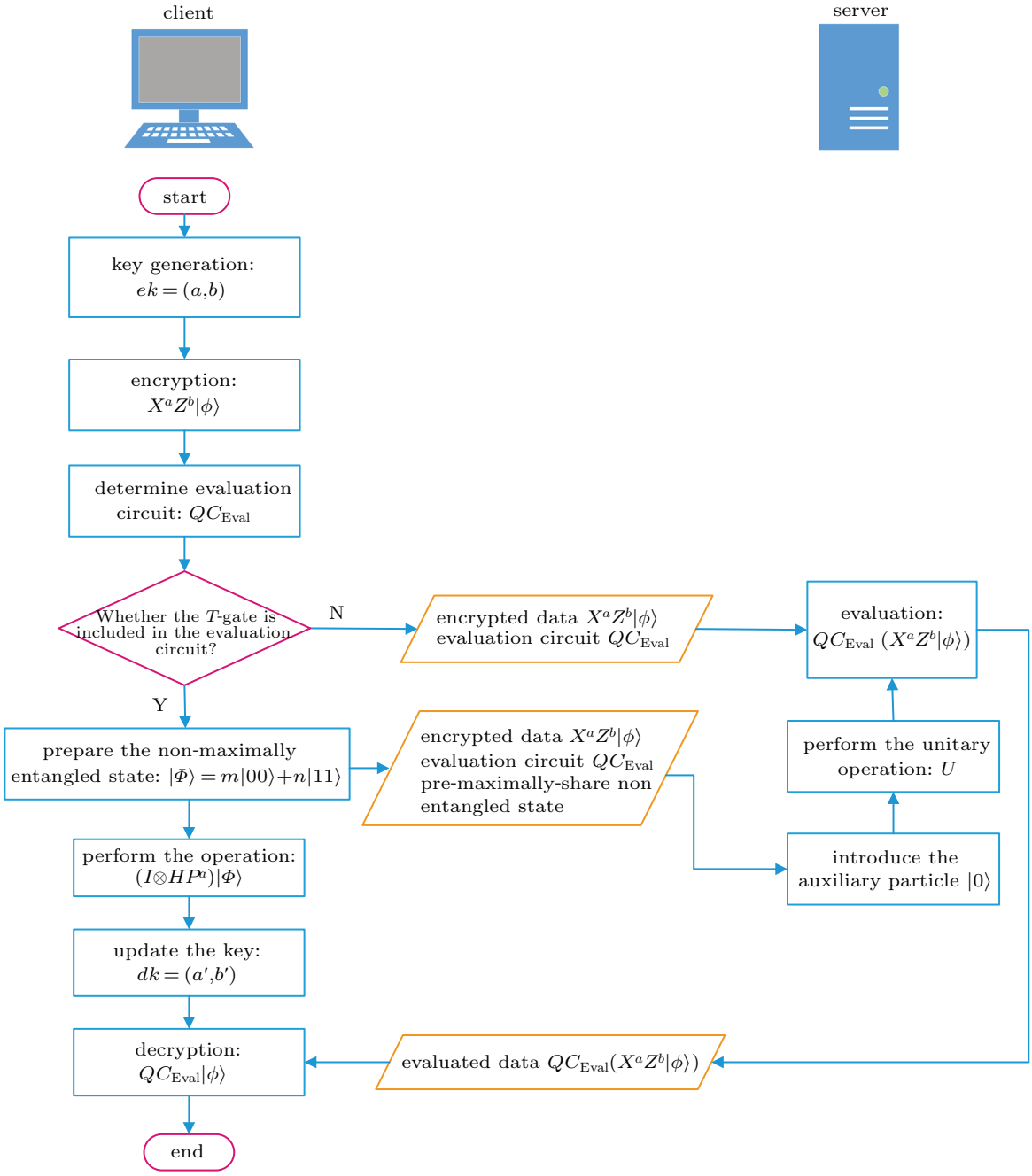


Fig. 2. Evaluation of our PQHE scheme for T-gate.

The following process will describe our two-party PQHE scheme by step.

Step 1 $PQHE.KeyGen \rightarrow ek=(a,b)$, where $a,b \in \{0,1\}$. The quantum state to be encrypted is $|\phi\rangle=\alpha|0\rangle+\beta|1\rangle$. The client performs a key generation algorithm to generate a random encryption key ek that is only used once. The quantum circuit QC_{Eval} intended to be performed on the data will be confirmed corresponding to the sequence of gate operations from the set $\Gamma=\{X,Z,H,P,CNOT\}$ and the T-gates. It will be used to implement universal quantum circuit evaluation on encrypted data.

Step 2 By using the key ek, the encrypted private data takes the form of

$$PQHE.Enc_{ek}(|\phi\rangle) \rightarrow X^aZ^b|\phi\rangle,(a,b\in\{0,1\}). \quad (13)$$

Assume that the evaluation circuit QC_{Eval} contains N quan-

tum gates G_i $(i = 1,\ldots,N)$. When $G_i \in \Gamma$, the client will transmit the encrypted data $X^aZ^b|\phi\rangle$ and evaluation circuit QC_{Eval} to the server through the channel. When a T-gate is included in the evaluation circuit, in addition to the above-mentioned data and circuit, the client needs to pre-share a non-maximally entangled state with the server and its form is $|\Phi\rangle = m|00\rangle + n|11\rangle (|m|^2 + |n|^2 = 1)$.

Step 3 The server with computational power performs the corresponding operations on the encrypted data $X^aZ^b|\phi\rangle$ in the order of the evaluation circuit QC_{Eval}, and it cannot know the specific content of the data. When the evaluation circuit consists of quantum gates G_i $(i = 1,\ldots,N)$, the evaluated data is of the form

$$\text{PQHE.Eval}^{QC_{\text{val}}}\left(X^aZ^b|\phi\rangle\right) \to QC_{\text{Eval}}\left(X^aZ^b|\phi\rangle\right). \quad (14)$$

With regard to QC_{Eval} containing the T-gate, the operations plotted in the previous section are performed by the server, including the CNOT operations, the defined U operations and measurements. The operation on the non-maximally entangled state $|\Phi\rangle = m|00\rangle + n|11\rangle$ will be delayed to the decryption phase and carried out by the client. At last, the evaluated data is returned to the client.

Step 4 In the final stage, the encryption key ek will be updated as the decryption key by the client, where the decryption key is denoted as $dk = (a', b')$. When the quantum gates $G_i \in \Gamma$ $(\Gamma = \{X, Z, H, P, CNOT\})$ acting on the encrypted data, the key update rules are listed as follows:

a) When $G_i = X$ or Z,

$$ek = (a,b) \xrightarrow{\text{update}} dk = (a', b') = (a,b).$$

b) When $G_i = H$,

$$ek = (a,b) \xrightarrow{\text{update}} dk = (a', b') = (b,a).$$

c) When $G_i = P$,

$$ek = (a,b) \xrightarrow{\text{update}} dk = (a', b') = (a, a \oplus b).$$

d) When $G_i = CNOT$, since $CNOT$ is a two-qubit gate, both the control qubit and the target qubit require keys, that is $ek = (a,b,c,d)$ and $dk = (a', b', c', d')$. Meanwhile, the encrypted state should be $(X^aZ^b \otimes X^cZ^d)|\phi\rangle$. The corresponding key update rule is

$$ek = (a,b,c,d) \xrightarrow{\text{update}} dk = (a', b', c', d') = (a, b \oplus d, a \oplus c, d).$$

e) When the T-gate acts on the encrypted data, the operations are first performed on it by the client, those are $(I \otimes HP^a)|\Phi\rangle$. And the measurement is made on the operated non-maximally entangled state to get the classical bit y. Then, the client needs to use the two measurements in the evaluation process of T-gate when updating the key, namely classical bit r and y. The key transformation is $ek = (a,b) \xrightarrow{\text{update}} dk = (a', b') = (a \oplus r, a \oplus b \oplus ar \oplus y)$.

In the end, the evaluated data is decrypted using the decryption key to obtain the quantum circuit QC_{Eval} that performed on the original private data. It is a series of operations and computations that determined by the client in Step 1 in order to get the operated plaintext in private, since

$$PQHE.Dec_{dk}\left(QC_{\text{Eval}}\left(X^aZ^b|\phi\rangle\right)\right) \to QC_{\text{Eval}}|\phi\rangle\left(X^aZ^b|\phi\rangle\right). \quad (15)$$

As introduced in the above scheme, we have made the novel two-party PQHE scheme come true. In the process of evaluating the T-gates, it can be seen from the expression (3) that when $a = 0$, there is no error that needs to be corrected. In the case where $a = 1$, the evaluator has to correct the error. However, as we will see, the evaluator does not have access to the value of a as the X-encryption key. The solution provided in our scheme is that the client and the server share the non-maximally entangled state in advance. The conditional P correction needs to be delayed until decryption. The price we have to pay is that the value of the measurement result required to update the key can only be measured as part of the decryption algorithm. The proposal of the above scheme can not only correct the errors in the evaluation of the T-gates, but also ensure the correctness of the QHE scheme. At the same time, the security of the key can be guaranteed, which will not be obtained by the evaluator. Next, we will conduct a detailed security analysis of the proposed PQHE scheme.

4. Security analysis

In this section, we now analyze the security of our PQHE scheme in two ways, namely data and key.

Initially, for the original privacy data, only the client has access to them. Before transmitting this quantum information to the server, the client will use the QOTP technology to encrypt the privacy data $|\phi\rangle$. The QOTP is an asymmetric quantum encryption method, which generates a pair of random key $ek = (a,b)(a,b \in \{0,1\})$ that is used only once. Therefore, the encrypted information becomes a totally mixed state, namely $(1/2^n)I$. The expression (1) proves it clear. Even if an attacker may intercept the encrypted information and receive the complete quantum state $X^aZ^b|\phi\rangle$ during the transmission, the specific information still cannot be obtained. He has no idea about the value of the key, and the randomness of the key makes it irregular. The key is changed every time the information is encrypted. It will minimize the risk of information leakage, so the perfect security of privacy data is ensured.

Then, in the evaluation stage, the quantum circuit QC_{Eval} is used by the server to perform universal quantum computation. The result is still a ciphertext $QC_{\text{Eval}}\left(X^aZ^b|\phi\rangle\right)$. If the evaluated data is intercepted by an attacker in the process of transmission, he does not have the ability to decrypt it. No one except the client can decrypt evaluated data to derive the valid information, because the decryption key $dk = (a',b')\,(a',b' \in \{0,1\})$ is only held by the client in secret. From the attacker's point of view, even if he can get the complete evaluated data, it is still meaningless if the data cannot be decrypted. In other words, the security of evaluated data is ensured. And it is a fairly good way to make further efforts to prevent the leakage of the original private data.

Finally, the encryption key ek is a pair of classical bits (a,b) randomly generated by the client to carry out the key generation algorithm. Each pair of keys will be used only once in the encryption stage, making it impossible for the server to deduce the content of the key by studying regular pattern over time. At the same time, the decryption key dk is renewed from the secure encryption key by the key update rules. It is only consumed by the client. The key update rules are securely owned and applied by the client itself. The encryption keys and decryption keys will not be transmitted over the channel, so the server or other attackers will not be able to get any information about the keys. To conclude, it is obvious that the encryption and decryption keys have a perfect security.

In summary, through the above analysis, our PQHE scheme has good security performance on privacy data, evaluated data, encryption keys and decryption keys.

5. Conclusions

Quantum homomorphic encryption has affirmative advantages in protecting the privacy data, which can perform arbitrary quantum computation during the evaluation. And in the processing of encrypted quantum state, the privacy data is kept secret for the server. The focal point of computation is to correct errors in the evaluation of non-Clifford gate. When applied to a real communication scenario, under the influence of the noise in the outside environment, the maximum entangled state encountered obstacles in the preparation process. Hence, a novel two-party PQHE scheme is proposed. Our scheme shows that the non-maximally entangled state can be used as auxiliary resource to assist in the evaluation of universal quantum circuit. It ensures the security of private data and effectively implements the PQHE scheme. In a broader context, our work opens up a new possible way for the realization of QHE. Compared with the previous scheme, the technical requirements were relaxed in the preparation of quantum entangled states in our scheme. It lowers the requirements for quantum channel, so that our PQHE scheme is more likely to be implemented under the existing experimental conditions.

Firstly, the non-maximally entangled state was introduced when evaluating T-gates to complete the correction of the P errors in the evaluation stage. From an experimental viewpoint, we chose non-maximally entangled state to alleviate the stress on the quantum resources required in the scheme. And it indicated that the evaluation of the non-Clifford gates could be effectively implemented. Secondly, we constructed the specific two-party PQHE scheme described step by step through the explicit illustration. The homomorphic computation of universal quantum circuit on encrypted information was applied. The computations and operations were clarified that both the client and the server need to perform, and the access rights to the keys and data were determined respectively in the PQHE scheme. Finally, the scheme guaranteed the security of privacy data, evaluated data, encryption keys and decryption keys. In conclusion, our PQHE scheme attracts wide attention and may be an achievable QHE scheme, which is of practical importance for the realization of more sophisticated secure quantum computation and multiparty quantum communication.

We hope that the proposed scheme provides inspiration in speeding up the practical proceeding of QHE scheme and establishing the theoretical basis of information security in the context of quantum communication. Our results make contribution to the application of the theory of QHE in secure quantum computation, but the problem that remains open is the construction of the QFHE scheme. Therefore, it is one of our following researches to study how to combine the QHE scheme with other quantum and classical cryptography protocols to construct a QFHE scheme that has a more efficient performance.

References

[1] Rivest R L, Adleman L and Dertouzos M L 1978 *Found. Secure Comput.* **4** 169

[2] Gentry C 2009 *A fully homomorphic encryption scheme*, Ph.D. thesis (Stanford University)

[3] Van Dijk M, Gentry C, Halevi S and Vaikuntanathan V 2010 *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, May 30–June 3, 2010, Springer, Berlin, p. 24

[4] Brakerski Z and Vaikuntanathan V 2014 *SIAM J. Comput.* **43** 831

[5] Stehlé D and Steinfeld R 2010 *International Conference on the Theory and Application of Cryptology and Information Security*, December 5–9, 2010, Springer, Berlin, p. 377

[6] Brakerski Z and Vaikuntanathan V 2011 *Annual cryptology conference*, August 14–18, 2011, Springer, Berlin, p. 505

[7] Vaikuntanathan V 2011 *IEEE 52nd Annual Symposium on Foundations of Computer Science*, October 22–25, 2011, Palm Springs, CA, p. 5

[8] Xu G, Xiao K, Li Z P, Niu X X and Ryan M 2019 *Comput. Mater. Continua* **58** 809

[9] Broadbent A, Fitzsimons J and Kashefi E 2009 *50th Annual IEEE Symposium on Foundations of Computer Science*, October 25–27, 2009, Los Alamitos, CA, p. 517

[10] Fitzsimons J F 2017 *npj Quantum Inf.* **3** 23

[11] Goldwasser S, Kalai Y T and Rothblum G N2015 *J. Am. Comput. Mach.* **62** 27

[12] Boneh D, Sahai A and Waters B 2011 *Theory of Cryptography Conference*, March 28-30, 2011, Springer, Berlin, p. 253

[13] Okamoto T and Takashima K 2010 *Annual cryptology conference*, August 15–19, 2010, Springer, Berlin, p. 191

[14] Garg S, Gentry C, Halevi S, Raykova M, Sahai A and Waters B 2016 *SIAM J. Comput.* **45** 882
[15] Rohde P P, Fitzsimons J F and Gilchrist A 2012 *Phys. Rev. Lett.* **109** 150501
[16] Liang M 2013 *Quantum Inf. Process.* **12** 3675
[17] Liang M 2013 arXiv: 1311.6304 [quant-ph]
[18] Liang M 2015 *Quantum Inf. Process.* **14** 2749
[19] Yu L, Pérez-Delgado C A and Fitzsimons J F 2014 *Phys. Rev. A* **90** 050303
[20] Fisher K A G, Broadbent A, Shalm L K, Yan Z, Lavoie J, Prevedel R, Jennewein T and Resch K J 2014 *Nat. Commun.* **5** 3074
[21] Broadbent A and Jeffery S *Annual Cryptology Conference*, August 16–20, 2015, Springer, Berlin, p. 609
[22] Dulek Y, Schaffner C and Speelman F 2016 *Annual International Cryptology Conference*, August 14–18, 2016, Springer, Berlin, p. 3
[23] Alagic G, Dulek Y, Schaffner C and Speelman F 2017 *International Conference on the Theory and Application of Cryptology and Information Security*, December 3–7, 2017, Springer, Cham, p. 438
[24] Tan S H, Kettlewell J A, Ouyang Y, Chen L and Fitzsimons J F 2016 *Sci. Rep.* **6** 33467
[25] Ouyang Y, Tan S H and Fitzsimons J F 2018 *Phys. Rev. A* **98** 042334
[26] Mahadev U 2018 *IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, 2018, IEEE, New York, p. 332
[27] Tan S H, Ouyang Y and Rohde P P 2018 *Phys. Rev. A* **97** 042308
[28] Marshall K, Jacobsen C S, Schäfermeier C, Gehring T, Weedbrook C and Andersen U L 2016 *Nat. Commun.* **7** 13795
[29] Zeuner J, Pitsios I, Tan S H, Sharma A N, Fitzsimons J F, Osellame R and Walther P 2021 *npj Quantum Inf.* **7** 1
[30] Tham W K, Ferretti H, Bonsma-Fisher K, Brodutch A, Sanders B C, Steinberg A M and Jeffery S 2020 *Phys. Rev. X* **97** 011038
[31] Chen X B, Sun Y R, Xu G and Yang Y X 2019 *Inf. Sci.* **501** 172
[32] Xu G, Shan R T, Chen X B, Dong M X and Chen Y L 2021 *Comput. Mater. Continua* **69** 339
[33] Pal R and Bandyopadhyay S 2018 *Phys. Rev. A* **97** 032322
[34] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 *Rev. Mod. Phys.* **81** 865
[35] Nielsen M A and Chuang I 2002 *Am. J. Phys.* **70** 558
[36] Boykin P O and Roychowdhury V 2003 *Phys. Rev. A* **67** 042317
[37] Roa L and Groiseau C 2015 *Phys. Rev. A* **91** 012344