Quantum Searchable Encryption for Cloud Data Based on Full-Blind Quantum Computation

WENJIE LIU[1,2], **YINSONG XU**[2], **WEN LIU**[3], **HAIBIN WANG**[1,2], **AND ZHIBIN LEI**[4]

[1]Engineering Research Center of Digital Forensics, Ministry of Education, Nanjing 210044, China
[2]School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China
[3]School of Computer Science and Cybersecurity, Communication University of China, Beijing 100024, China
[4]Hong Kong Applied Science and Technology Research Institute (ASTRI), Hong Kong

Corresponding author: Wenjie Liu (wenjiel@163.com)

ABSTRACT Searchable encryption (SE) is a positive way to protect users sensitive data in cloud computing setting, while preserving search ability on the server side, i.e., it allows the server to search encrypted data without leaking information about the plaintext data. In this paper, a multi-client universal circuit-based full-blind quantum computation (FBQC) model is proposed. In order to meet the requirements of multi-client accessing or computing encrypted cloud data, all clients with limited quantum ability outsource the key generation to a trusted key center and upload their encrypted data to the data center. Considering the feasibility of physical implementation, all quantum gates in the circuit are replaced with the combination of $\pi/8$ rotation operator set $\{R_z(\pi/4), R_y(\pi/4), CR_z(\pi/4), CR_y(\pi/4), CCR_z(\pi/4), CCR_y(\pi/4)\}$. In addition, the data center is only allowed to perform one $\pi/8$ rotation operator each time, but does not know the structure of the circuit (i.e., quantum computation), so it can guarantee the blindness of computation. Then, through combining this multi-client FBQC model and Grover searching algorithm, we continue to propose a quantum searchable encryption scheme for cloud data. It solves the problem of multi-client access mode under searchable encryption in the cloud environment, and has the ability to resist against some quantum attacks. To better demonstrate our scheme, an example of our scheme to search on encrypted 2-qubit state is given in detail. Furthermore, the security of our scheme is analysed from two aspects: external attacks and internal attacks, and the result indicates that it can resist against such kinds of attacks and also guarantee the blindness of data and computation.

INDEX TERMS Quantum searchable encryption, cloud data, full-blind quantum computation, trusted key center, multi-client access, Grover algorithm, $\pi/8$ rotation operator.

I. INTRODUCTION

In recent years, cloud computing has achieved great development in different fields, such as wireless networks [1]–[3], IoT [4]–[8], resource allocation [9]–[11] and so on. As it provides economic and convenient service, more and more clients are planning to upload their data onto the public clouds now. And with the popularity of mobile devices, more and more companies can push the content they want based on the data uploaded by clients, which greatly promotes the

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaochun Cheng.

development of mobile Internet [12]–[15]. However, data stored in the cloud server may suffer from malicious use by cloud service providers since data owners have no longer direct control over data. For instance, data stored in a bank must not be arbitrarily obtained [16]–[18]. Considering data privacy and security, it is a recommended practice for data owners to encrypt data before uploading onto the cloud [19]. Therefore, an efficient search technique for encrypted data is extremely urgent.

A popular way to search over encrypted data is searchable encryption (SE), which is desirable to support the fullest possible search functionality on the server side,

without decrypting the data, and thus, with the smallest possible loss of data confidentiality. The first searchable encryption was proposed by Song *et al.* [20]. This scheme uses stream ciphers and pseudo-random functions to implement ciphertext retrieval, but it also has a series of problems, such as low search efficiency and data privacy. Therefore, Goh [21] built a index structure based on the Bloom filter to achieve fast retrieval of ciphertext data. However, the Bloom filter itself has a certain error rate, and the result returned by the cloud server to the data user may not be accurate. Besides, Curtmola *et al.* [22] and Boneh *et al.* [23] use the idea of "keyword-file" to construct a symmetric searchable encryption scheme and a public key search able encryption scheme, respectively. Both schemes have significant improvements in safety and efficiency. Nowadays, many researchers have tried to use kNN algorithm [24], [25], user interest model [26], blockchain technology [27], [28], multi-keyword ranked search [29] and so on, to improve the search efficiency and data privacy.

However, with the development of quantum computation, the powerful computing power of quantum computers poses an increasingly strong threat to public key systems [30] and symmetric key systems [31], [32]. Besides, quantum computation are also applied in other fields, such as quantum key agreement (QKA) [33], [34], quantum steganography (QS) [35], [36], quantum machine learning [37], [38], and so on. Especially, to protect the privacy of client's data, many researchers have proposed a novel quantum computation model: blind quantum computation (BQC), where the client with limited quantum resources can perform quantum computation by delegating the computation to an untrusted quantum server, and the privacy of the client can still be guaranteed. BQC can be generally divided into two categories: one is the measurement-based blind quantum computation (MBQC), and the other is the circuit-based blind quantum computation (CBQC). In MBQC, measurement is the main driving force of computation, which follows the principle of "entangle-measure-correct", and a certain number of quantum qubits are entangled to form a standard graph state [39]–[41].

Different from MBQC, CBQC is based on the quantum circuit, which is composed of many kinds of quantum gates [42]–[50]. Among them, Fisher *et al.* [44] and Broadbent [45] firstly proposed a representative CBQC model: delegating quantum computation (DQC). In their schemes, an untrusted server can perform arbitrary quantum computations on encrypted quantum bits (qubits) without learning any information about the inputs, where the quantum computations are implemented by a universal set of quantum gates $(X, Z, H, S, T, CNOT)$. And then the client can easily decrypt the results of the computation with the decryption key. Then, Tan and Zhou [43] give 3 circuits of other quantum gates (CZ, $SWAP$, and $Toffoli$) for blind quantum computation. However, in their schemes, the server knows the content of delegating computation. To further protect computation privacy, a few universal circuit-based "full-blind" quantum computation

(FBQC) schemes are proposed [46], [47], i.e., the server also does not know the content of delegated computation. These two schemes use two different strategies to achieve full blindness. Zhang *et al.*'s scheme decomposes all quantum gates into several basic rotation operators, and inserts trap qubits and trap gates to achieve full blindness, where the trap gate is composed of basic rotation operators and does not affect the computation results. In Liu *et al.*'s scheme, the client uses the strategy of oblivious mechanism to make the computation blind, where the desirable delegated quantum operation, one of $\{H, P, CNOT, T\}$, is replaced by a fixed sequence (H, P, CZ, $CNOT$, T). However, all these mentioned CBQC schemes are only a single-client model, i.e., clients can only delegate the server to compute their own data, which are not convenient for different clients to compute others' data.

In order to implement multi-client universal circuit-based FBQC for searchable encryption, i.e., different clients can store or search their data in the quantum cloud server, we propose a quantum searchable encryption scheme for cloud data based on full-blind quantum computation (QSE-FBQC). Clients with limited quantum ability firstly use X and Z gates to encrypt their data with the encryption keys generated by the key center, and then upload the encrypted data to the data center. The data center performs search computation on the encrypted data if other clients need, where the search computation are implemented by a universal set of quantum gates $(X, Z, H, S, T, CNOT, CZ, Toffoli)$. But, the data center only performs one $\pi/8$ rotation operator from $\pi/8$ rotation operator set $\{R_z(\pi/4), R_y(\pi/4), CR_z(\pi/4), CR_y(\pi/4), CCR_z(\pi/4), CCR_y(\pi/4)\}$ on qubits sent by the key center each time, and sends these qubits back to the key center. Repeating this process multiple times can complete any quantum gate in the circuit of search computation. This kind of strategy can make the data center unable to know the positions and the orders of quantum gates in the circuit, which guarantees the blindness of computation. When the search computation finishes, the key center generate corresponding decryption key. Finally, the clients who need the search result from the data center, also use X and Z gates to decrypt the encrypted search result with the decryption key.

The rest of the paper is organized as follows. Sect. II provides some preliminary knowledge about quantum computation and circuit-based blind quantum computation. Then, a quantum searchable encryption scheme for cloud data based on full-blind quantum computation is proposed in Sect. III. Moreover, we give a concrete example that use Grover algorithm to search on encrypted 2-qubit state in Sect. IV. And the security of our scheme is analysed in Sect. V. Sect. VI is devoted to compare our scheme with some existing SE schemes and BQC schemes. Finally, Sect. VII gives discussion and conclusion of this paper.

II. PRELIMINARIES
A. QUANTUM COMPUTATION
In quantum compution, the quantum bit (called qubit) [51] is the basic unit of quantum information and has two possible

states $|0\rangle$ and $|1\rangle$, which is often referred to as quantum superposition state,

$$|\varphi\rangle = \alpha |0\rangle + \beta |1\rangle, \tag{1}$$

where α, β are complex numbers, and $|\alpha|^2 + |\beta|^2 = 1$. $|0\rangle$ and $|1\rangle$ can be represented by vectors,

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{2}$$

Then, $|\varphi\rangle$ can be expressed in vector form $|\varphi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$.

With the information carrier (qubit), we also need some quantum gates to implement the information processing. For single-qubit gates, we have *Pauli-X*, *Pauli-Z*, *H* (*Hadamard*), *S* and *T* gates, which can be described as 2×2 unitary matrices as below,

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$
$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}. \tag{3}$$

Especially, Ref. [51] also points out that for arbitrary unitary operator U performed on single-qubit, there exist θ, α, β and γ, s.t.

$$U = e^{i\theta} R_z(\alpha) R_y(\beta) R_z(\gamma)$$
$$= \begin{pmatrix} e^{i(\theta - \frac{\alpha}{2} - \frac{\gamma}{2})}\cos\frac{\beta}{2} & -e^{i(\theta - \frac{\alpha}{2} + \frac{\gamma}{2})}\sin\frac{\beta}{2} \\ e^{i(\theta + \frac{\alpha}{2} - \frac{\gamma}{2})}\sin\frac{\beta}{2} & e^{i(\theta + \frac{\alpha}{2} + \frac{\gamma}{2})}\cos\frac{\beta}{2} \end{pmatrix} \tag{4}$$

For double-qubit gates, the commonly used multi-qubit gates are *CNOT* and *CZ* gates. The matrix representations and quantum circuits of *CNOT* and *CZ* are shown in Fig. 1 and Fig. 2, respectively.
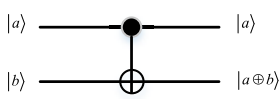

FIGURE 1. Matrix representation and quantum circuit of *CNOT* gate.
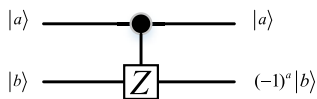
FIGURE 2. Matrix representation and quantum circuit of *CZ* gate.

Finally, for triple-qubit gates, *Toffoli* gate is another frequently used multi-qubit gate, which is illustrated in Fig. 3. With these single-qubit gates and multi-qubit gates, we can implement arbitrary quantum computation.
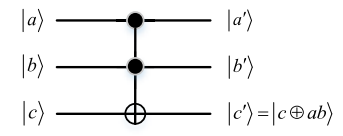

FIGURE 3. Truth table and quantum circuit of *Toffoli* gate.

B. CIRCUIT-BASED BLIND QUANTUM COMPUTATION

Fisher *et al.* [44] and Broadbent [45] proposed a specific blind quantum computation scheme based on quantum circuit. It (see Fig. 4 a) starts with a client who has quantum information that needs to be sent to a remote server for processing. The client first encrypts one input qubit $|\psi\rangle$ and sends it to a quantum server, who performs a computation U on the encrypted qubit. The server returns the state which the client decrypts to get $U|\psi\rangle$.
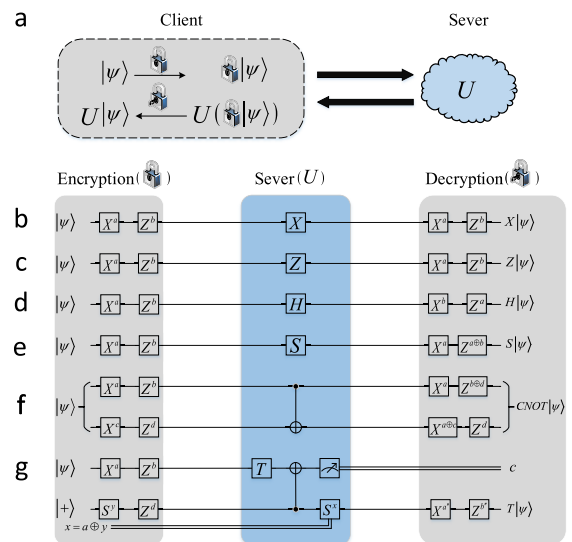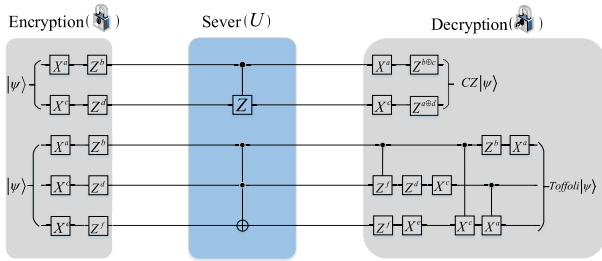

FIGURE 4. The process of blind quantum computation for each quantum gate in Fisher's and Broadbent's schemes.

In the scheme, to encrypt a qubit $|\psi\rangle$, a client applies a combination of Pauli X and Z operations to get a encrypted qubit $X^a Z^b |\psi\rangle$, where $a, b \in \{0, 1\}$ (as well as $c, d \in \{0, 1\}$ for the *CNOT* gate in Fig. 4f). Then, the server perform quantum computing U, which is composed of unitary operations from the Clifford group $\{X, Z, H, S, CNOT\}$ and one additional non-Clifford gate, T gate. As shown in Fig. 4 b-f, when $U \in \{X, Z, H, S, CNOT\}$, clifford gates do not require any additional resources, and decryption is straightforward. However, when $U = T$ (see Fig. 4 g), the server requires the client to send an auxiliary qubit $Z^d P^y |+\rangle$, where $y, d \in \{0, 1\}$. to control a *CNOT* gate with the encrypted qubit. The server measures the encrypted qubit and outcome $c \in \{0, 1\}$ is returned to the client, which is used in decryption. The client sends a single classical bit, $x = a \oplus y$, to control a

S gate on the auxiliary qubit, which is returned to the client as $X^{a''}Z^{b''}R|\psi\rangle$, where $a'' = a \oplus c$ and $b'' = a(c \oplus y \oplus 1) \oplus b \oplus d \oplus y$.

In Ref. [43], Tan *et al.* give the circuit of *CZ* and *Toffoli* gates for blind quantum computation, which is illustrated in Fig. 5.

FIGURE 5. The process of blind quantum computation for *CZ* and *Toffoli* gate.

III. QUANTUM SEARCHABLE ENCRYPTION FOR CLOUD DATA BASED ON UNIVERSAL FULL-BLIND QUANTUM COMPUTATION

A. MULTI-CLIENT UNIVERSAL CIRCUIT-BASED FULL-BLIND QUANTUM COMPUTATION MODEL

As mentioned above, these circuit-based BQC schemes (including circuit-based FBQC schemes) are only a single-client model as shown in Fig. 6 (a), i.e., clients only delegate server to compute over their own encrypted data in this model,

FIGURE 6. Single-client model (a) and multi-client model (b) of circuit-based BQC schemes.

which are not convenient to data sharing. Besides, clients need to interact with server and compute decryption key frequently, which consume a large amount of computing and communication resources. To solve these two problems and keep full-blind, we propose a multi-client universal circuit-based full-blind quantum computation model (see Fig. 7 (b)), where clients ($Alice_1$, $Alice_2$, $\cdots$, $Alice_n$) outsource key generation to a trusted key center (*Charlie*) and let key center interact with the server (i.e., data center *Bob*). *Charlie* and *Bob* compose the quantum cloud servers.

Suppose a client $Alice_1$ as the data owner uploads her encrypted data $|\psi\rangle$ to *Bob*, and another client $Alice_2$ delegates *Bob* to perform quantum computation on $|\psi\rangle$ to get the computation result. The basic process of our scheme is given as below.

Step 1: $Alice_1$ sends a number n (the number of qubits in $|\psi\rangle$) to *Charlie*.

Step 2: *Charlie* sends back a string of $2n$ random binary bits back to $Alice_1$ by BB84 protocol [52]. The $2n$ bits of the binary string act as $ek = (x_i, z_i)$, where $x_i, z_i \in \{0, 1\}$ and $i \in \{1, 2, \cdots, n\}$.

Step 3: $Alice_1$ encrypts her data $|\psi\rangle$ with ek and sends encrypted state $E_{ek}|\psi\rangle = \otimes_{i=1}^{n} X_i^{x_i} Z_i^{z_i} |\psi\rangle$ to *Bob*.

Step 4: $Alice_2$ asks for *Charlie* to delegate *Bob* to perform quantum computation over $E_{ek}|\psi\rangle$, and *Charlie* gets $E_{ek}|\psi\rangle$ from *Bob*.

Step 5: If *Charlie* wants *Bob* to perform G_i (or $G_{i,l}$, or $G_{i,l,k}$) gate on $|\psi\rangle_i$ (or $|\psi\rangle_{i,l}$, or $|\psi\rangle_{i,l,k}$), *Charlie* needs to insert two trap qubits (or one trap qubits, or no trap qubits) into $|\psi\rangle_i$ (or $|\psi\rangle_{i,l}$, or $|\psi\rangle_{i,l,k}$) randomly (see Fig. 7, 8 and 9), where $G \in \{X, Z, H, S, T, CNOT, CZ, Toffoli\}$, i, l and k represents the ith, lth and kth qubit in $|\psi\rangle$ respectively.

Step 6: *Charlie* sends 3 prepared qubits to *Bob* and instructs *Bob* to perform rotation operator U_i (or $U_{i,l}$, or $U_{i,l,k}$) on these 3 qubits, where $U \in \{R_z(\pi/4), R_y(\pi/4), CR_z(\pi/4), CR_y(\pi/4), CCR_z(\pi/4), CCR_y(\pi/4)\}$, where $R_z(\mu_1\pi/4) = R_z(\pi/4)^{\mu_1}$ and $R_y(\mu_2\pi/4) = R_y(\pi/4)^{\mu_2}$, i, l and k represents the ith, lth and kth qubit in these 3 qubits, respectively.

Step 7: *Bob* performs rotation operator U on 3 qubits, and sends back to *Charlie*.

*Step 8:* *Charlie* performs X and Z operations on 3 qubits as needed.

Step 9: Repeat Step 6 to 8 until *Charlie* gets $(\otimes_{i=1}^{n} X_i^{x'_i} Z_i^{z'_i}) \otimes G|\psi\rangle$ and generates decryption key $dk = (x'_i, z'_i)$, where G gate can be composed of a plurality of U gates (as shown in Eq. 5) and $x'_i, z'_i \in \{0, 1\}$. When U is used as a trap gate, it can be executed in any order.

$$X = e^{\frac{i\pi}{2}} R_y(\pi) R_z(\pi), Z = e^{\frac{i\pi}{2}} R_z(\pi) R_y(0),$$
$$H = e^{\frac{i\pi}{2}} R_y(\frac{\pi}{2}) R_z(\pi), S = e^{\frac{i\pi}{4}} R_z(\frac{\pi}{2}) R_y(0),$$
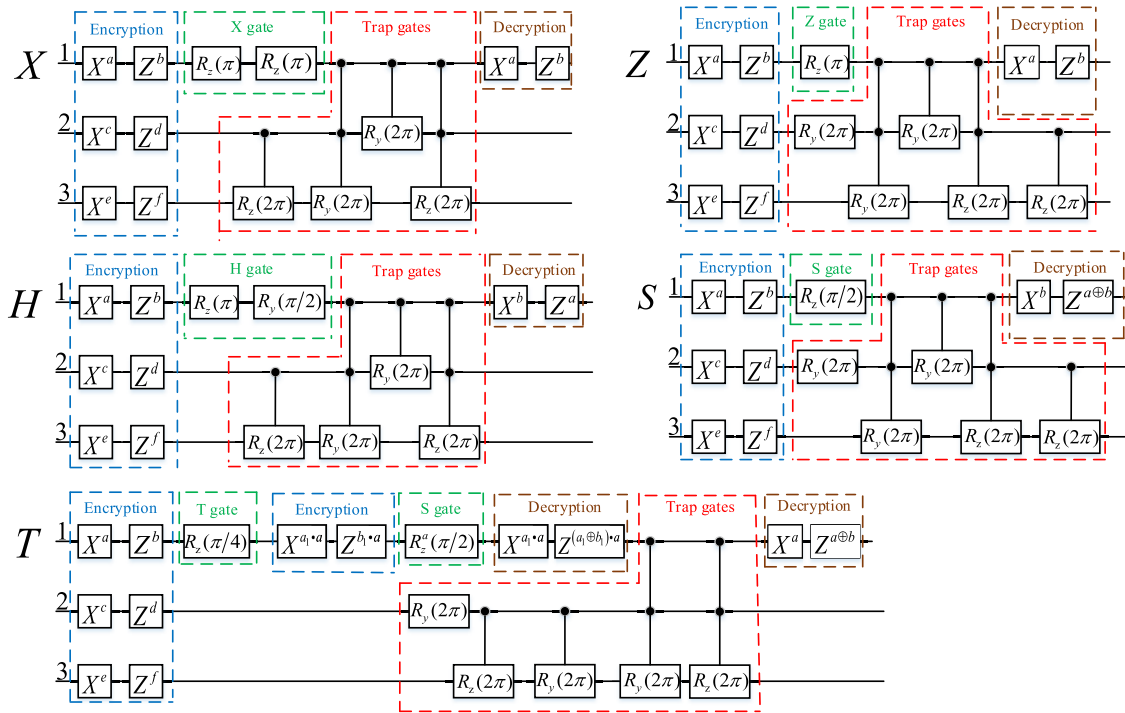$$T = e^{\frac{i\pi}{8}} R_z(\frac{\pi}{4}) R_y(0),$$
$$CZ_{12} = [C - (e^{\frac{i\pi}{2}} R_z(\pi) R_y(0))]_{12},$$
$$CNOT_{12} = [C - (e^{\frac{i\pi}{4}} R_z(\frac{\pi}{2}) R_y(0))]_{12},$$
$$Toffoli_{12,3} = [CC - X]_{12,3}, \quad (5)$$
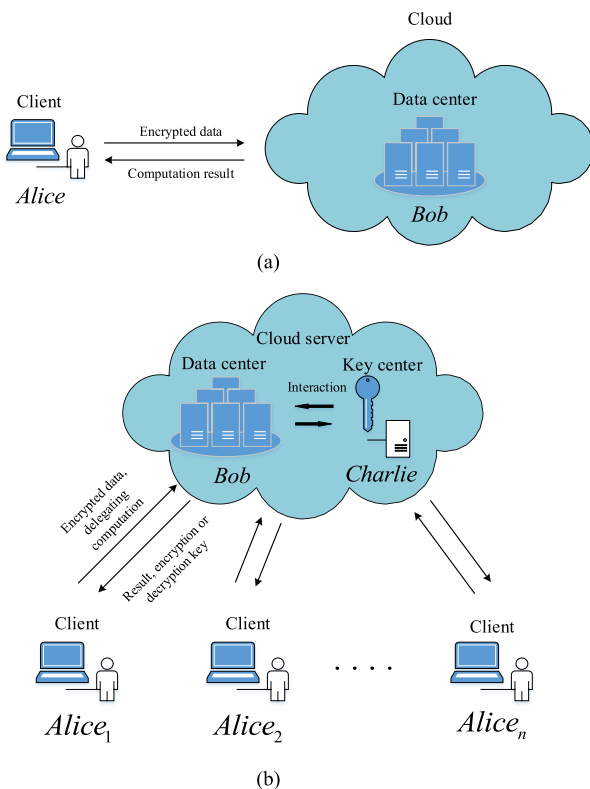
FIGURE 7. Our model for single-qubit gates *X, Z, H, S* and *T* (*a, b, c, d, e, f* ∈ {0, 1}), where the sign 1 belongs to $|\psi\rangle$ and the signs 2 and 3 belong to trap qubits, respectively. And the blue, green, red and brown dotted line indicates the encryption operations, the actual operations, the trap operations and the decryption operations, respectively.

where $R_y(0) = R_z(0) = I$, $-R_y(2\pi) = -R_y(\frac{\pi}{4}) = I$, $R_y(\pi) = R_y(\frac{\pi}{4})^4$, $R_y(\frac{\pi}{2}) = R_y(\frac{\pi}{4})^2$, $R_z(\frac{\pi}{2}) = R_z(\frac{\pi}{4})^2$, $R_z(\pi) = R_z(\frac{\pi}{4})^4$, $(C - R_y(\theta))_{12} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ 0 & 0 & \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}$ and

$(C - R_z(\theta))_{12} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{-\frac{i\theta}{2}} & 0 \\ 0 & 0 & 0 & e^{\frac{i\theta}{2}} \end{pmatrix}$. In our scheme, the global phase factors ($e^{\frac{i\theta}{2}}$) are ignored.

Step 10: Repeat Step 5 to 9 until *Charlie* gets $E_{dk}|result\rangle = (\otimes_{i=1}^n X_i^{x'_i} Z_i^{z'_i})(\otimes_{j=1}^s G_j)|\psi\rangle = (\otimes_{i=1}^n X_i^{x'_i} Z_i^{z'_i})|result\rangle$ and generates final decryption key $dk = (x'_i, z'_i)$, where s represents the number of G gate in the circuit of quantum computation, $j \in \{1, 2, \cdots, s\}$ and $|result\rangle$ is the computation result which *Alice₂* needs.

Step 11: *Charlie* sends $E_{dk}|result\rangle$ and dk to *Alice₂*, where dk is transformed by BB84.

Step 12: *Alice₂* decrypts the encrypted result $E_{dk}|result\rangle$ with dk, to get $|result\rangle$.

To better understand our multi-client universal FBQC scheme, we give three examples of delegating *Bob* to perform one single-qubit gate (*X* gate in Fig. 7), one double-qubit gate (*CZ* gate in Fig. 8), and one triple-qubit gate (*Toffoli* gate in Fig. 9), respectively. For the sake of simplicity, we mainly explain Step 5 to 9 in these examples.

1) SINGLE-QUBIT GATE - *X* GATE

1. *Charlie* sends 3 encrypted qubits $X_1^a Z_1^b|\psi\rangle_1 \otimes X_2^c Z_2^d|\phi\rangle_2 \otimes X_3^e Z_3^f|\phi\rangle_3$ to *Bob* ($|\phi\rangle_2$ and $|\phi\rangle_3$ are trap qubits, and their positions are arbitrary.).

2. *Bob* performs four rounds (i.e., Step 6 to 8) $R_z(\frac{\pi}{4})_1$ on qubit $X_1^a Z_1^b|\psi\rangle_1$ and returns 3 qubits to himself through *Charlie*.

3. *Bob* performs four rounds $R_y(\frac{\pi}{4})_1$ on $R_z(\pi)_1 X^a Z^b|\psi\rangle_1$ and returns 3 qubits to himself through *Charlie*.

4. To confuse the actual delegating operations, *Bob* also performs eight rounds $(C - R_z(\frac{\pi}{4}))_{23}$, $(CC - R_y(\frac{\pi}{4}))_{12,3}$, $(C - R_y(\frac{\pi}{4}))_{12}$ and $(CC - R_z(\frac{\pi}{4}))_{12,3}$ on 3 qubits. Note, all trap gates are randomly inserted without affecting the original circuits.

5. *Charlie* gets $(X_1^a Z_1^b)X_1|\psi\rangle_1$ from *Bob* and generates decryption key $dk = (a, b)_1$.

2) DOUBLE-QUBIT GATE - *CZ* GATE

1. *Charlie* sends 3 encrypted qubits $(X_1^a Z_1^b \otimes X_2^c Z_2^d)|\psi\rangle_{1,2} \otimes X_3^e Z_3^f|\phi\rangle_3$ to *Bob* ($|\phi\rangle_3$ is a trap qubit.).

2. Bob performs four rounds $(C - R_z(\frac{\pi}{4}))_{12}$ on $(X_1^a Z_1^b \otimes X_2^c Z_2^d)|\psi\rangle_{1,2}$ and returns 3 qubits to himself through *Charlie*.

3. To confuse the actual delegating operations, *Bob* also performs eight rounds $(C - R_z(\frac{\pi}{4}))_{23}$, $(CC - R_y(\frac{\pi}{4}))_{12,3}$, $(C - R_y(\frac{\pi}{4}))_{12}$ and $(CC - R_z(\frac{\pi}{4}))_{12,3}$ on 3 qubits.
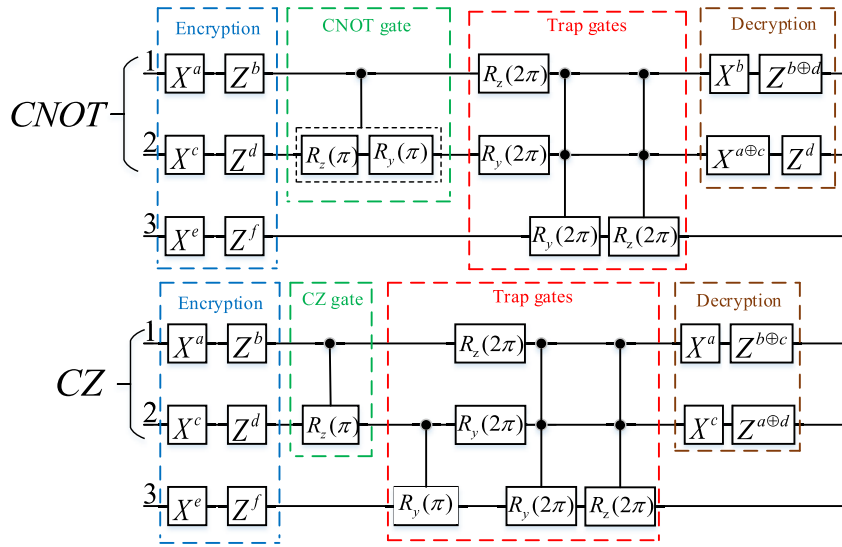
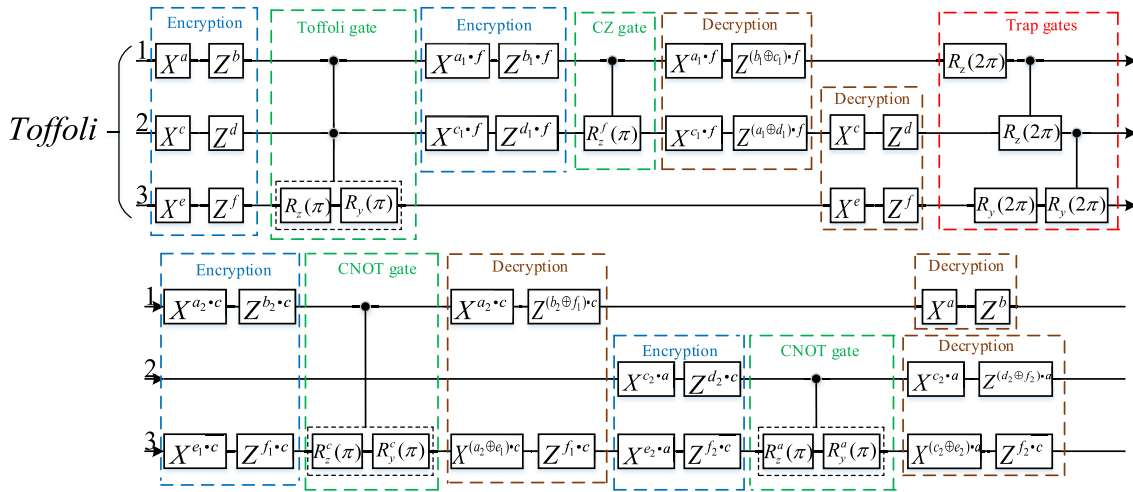**FIGURE 8.** Our model for double-qubit gates *CZ* and *CNOT*.

FIGURE 9. Our model for triple-qubit gate *Toffoli*.

4. *Charlie* gets $(X_1^a Z_1^{b \oplus c} \otimes X_2^c Z_2^{a \oplus d}) CZ_{12} |\psi\rangle_{1,2}$ from *Bob* and generates decryption key $dk = \{(a, b \oplus c)_1, (c, a \oplus d)_2\}$.

3) TRIPLE-QUBIT GATE - *TOFFOLI GATE*

1. *Charlie* sends encryption quantum states $(X_1^a Z_1^b \otimes X_2^c Z_2^d \otimes X_3^e Z_3^f)|\psi\rangle_{1,2,3}$ to *Bob*.

2. *Bob* performs four rounds $(CC - R_z(\frac{\pi}{4}))_{12,3}$ on $(X_1^a Z_1^b \otimes X_2^c Z_2^d \otimes X_3^e Z_3^f)|\psi\rangle_{1,2,3}$ and returns 3 qubits to himself through *Charlie*.

3. *Bob* performs four rounds $(CC - R_y(\frac{\pi}{4}))_{12,3}$ and returns 3 qubits to himself through *Charlie*.

4. When $f = 1$, *Charlie* should encrypt 3 qubits again by performing $(X_1^{a_1 \cdot f} Z_1^{b_1 \cdot f}) \otimes (X_2^{c_1 \cdot f} Z_2^{d_1 \cdot f})$ on first 2 qubits and send them to *Bob*. It is the same for the similar case (when $a = c = 1$). *Bob* performs four rounds $(C - R_z^f(\frac{\pi}{4}))_{12}$ and returns

3 qubits to *Charlie*. *Charlie* needs to decrypt by performing $(X_1^{a_1 \cdot f} Z_1^{(b_1 \oplus c_1) \cdot f}) \otimes (X_2^{c_1 \cdot f} Z_2^{(a_1 \oplus d_1) \cdot f})$ on first 2 qubits.

4. *Charlie* performs $I_1 \otimes X_2^c Z_2^d \otimes X_3^e Z_3^f$ on 3 qubits and returns them to *Bob*.

5. *Bob* performs four rounds $(C - R_z^c(\frac{\pi}{4}))_{13}$ and $(C - R_y^c(\frac{\pi}{4}))_{13}$, and returns to himself through *Charlie*.

6. *Bob* performs four rounds $(C - R_z^a(\frac{\pi}{4}))_{23}$ and $(C - R_y^a(\frac{\pi}{4}))_{23}$, and returns to himself through *Charlie*.

7. To confuse the actual delegating operations, *Bob* performs eight rounds $R_z(2\pi)_1$, $R_y(2\pi)_3$, $(C - R_z(\frac{\pi}{4}))_{12}$ and $(C - R_y(\frac{\pi}{4}))_{23}$.

8. *Charlie* gets $(X_1^a Z_1^b) \otimes Toffoli_{12,3}|\psi\rangle_{1,2,3}$ from *Bob* and generates decryption key $dk = \{(a, b)_1, (0, 0)_2, (0, 0)_3\}$.

As can be seen from the above, through trap gates, trap qubits and ways of constant interaction, *Bob* cannot
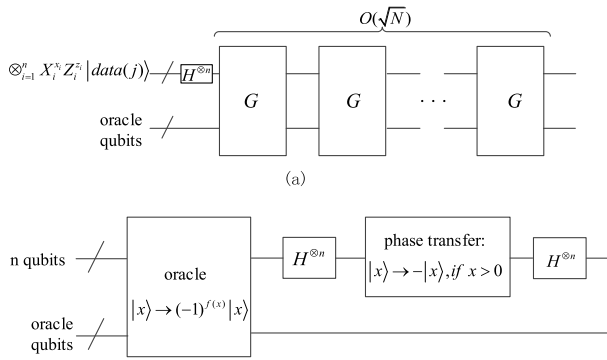
FIGURE 10. Schematic circuit for Grover algorithm. (b) is the schematic circuit for *G* in (a).

distinguish these qubits from *Charlie* every time whether belong to the same original quantum state. Meanwhile, he also cannot distinguish which rotation operators belong to the same original quantum gate.

B. QUANTUM SEARCHABLE ENCRYPTION FOR CLOUD DATA BASED ON FULL-BLIND QUANTUM COMPUTATION

We have established a multi-client universal circuit-based FBQC framework for easy data sharing. To achieve the aim of searchable encryption, we propose a concrete quantum searchable encryption scheme for cloud data based on full-blind quantum computation (QSE-FBQC). For the sake of simplicity, we take four roles (the data owner $Alice_1$, the data searcher $Alice_2$, the data center *Bob* and the key center *Charlie*) as an example to describe our scheme. The specific process of QSE-FBQC scheme is as follows and shown in Fig. 11.
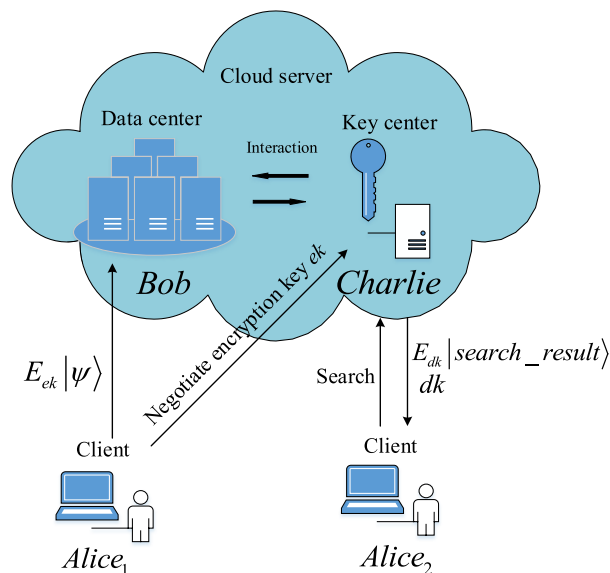

FIGURE 11. The process of our QSE-FBQC scheme.

1. $Alice_1$ sends a number n to *Charlie*, where n is the number of qubits which she wants to encrypt.

2. *Charlie* sends back a string of $2n$ random binary bits back to $Alice_1$ by BB84 [52]. The $2n$ bits of the binary string act as $ek = (x_i, z_i)$, where $x_i, z_i \in \{0, 1\}$ and $i \in \{1, 2, \cdots, n\}$.

3. $Alice_1$ encrypts her plain data $|\psi\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |j, data(j)\rangle$ with ek and sends encrypted state $E_{ek} |\psi\rangle = \frac{1}{\sqrt{M}} (I^{\otimes m} \otimes (\otimes_{i=1}^{n} X_i^{x_i} Z_i^{z_i})) \sum_{j=0}^{M-1} |j, data(j)\rangle$ to *Bob*, where the item index j within $|\psi\rangle$ is not encrypted and composed of m qubits, $M = 2^m$, $data(j)$ is the data and composed of n qubits.

4. $Alice_2$ wants *Bob* to search over $E_{ek} |\psi\rangle$, and *Charlie* interacts with *Bob* according to the quantum circuit of search computing, which is as same as Step 5 to 10. The search computation can be composed of Grover algorithm, which is illustrated in Fig. 10. For a search space of $N = 2^n$ elements and one solution, we only need to apply the search oracle $O(\sqrt{N})$ times to obtain a solution. During the interaction between Bob and Charlie, the sender needs to add decoy qubits to the data and record their location. When the receiver receives the data, the sender announces the states and locations of the decoy qubits (selected from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$), and the receiver confirms whether it is the same as the published state by measuring the state of the decoy qubits. If they are the same, the receiver proceeds to the next step; otherwise, the sender resends the data.

5. When the search computation is completed, *Charlie* sends the search result $E_{dk} |search\_result\rangle$ and decryption key dk to $Alice_2$, where dk is transformed by BB84.

6. $Alice_2$ uses dk to decrypt the state $E_{dk} |search\_result\rangle$, and gets $|search\_result\rangle$.

IV. AN EXAMPLE OF QSE-FBQC SCHEME

Suppose $Alice_1$ has a set 00, 01, 10, 11 and $Alice_2$ wants to find item 01 from this set. It is equivalent to using Grover algorithm to find $|0\rangle |1\rangle$ from $|+\rangle |+\rangle$, and the circuit of search computation is shown in Fig. 12. The example proceeds in seven steps provided below.

1. $Alice_1$ sends a number 2 to *Charlie*.

2. *Charlie* sends a string of 4 random binary bits (act as ek) back to $Alice_1$ by BB84 protocol.

3. $Alice_1$ encrypts her data $|\psi\rangle = |+\rangle_1 |+\rangle_2$ with X and Z gates according to ek.

4. $Alice_2$ wants to get $|0\rangle_1 |1\rangle_2$ from $E_{ek} |\psi\rangle$, and *Charlie* interacts with *Bob* according to the quantum circuit of search computing in Fig. 12. *Charlie* needs to insert an auxiliary qubit $|1\rangle$ into $|\psi\rangle$ firstly. The whole process of search computing is shown in Fig. 13.

5. When the search is completed, *Charlie* sends the search result state $(X_1^{x_1} Z_1^{z_1}) \otimes (X_2^{z_1} Z_2^0) \otimes (X_3^0 Z_3^0) |result\rangle_{1,2,3}$ and $dk = \{(x_1, z_1)_1, (z_1, 0)_2, (0, 0)_3\}$ to $Alice_2$.

6. $Alice_2$ uses dk to decrypt the state $(X_1^{x_1} Z_1^{z_1}) \otimes (X_2^{z_1} Z_2^0) \otimes (X_3^0 Z_3^0) |result\rangle_{1,2,3}$, and abandons the auxiliary third qubit to get $|0\rangle_1 |1\rangle_2$ (the global phase factors are ignored).
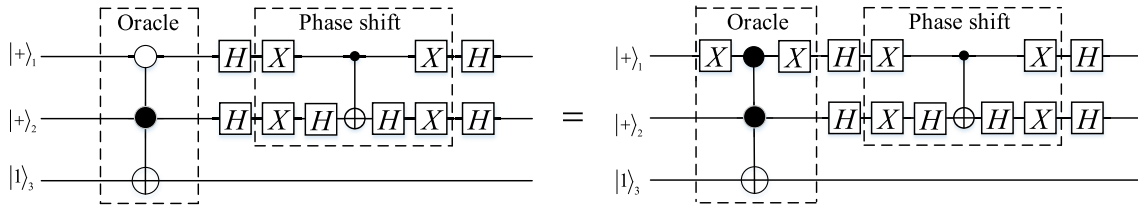
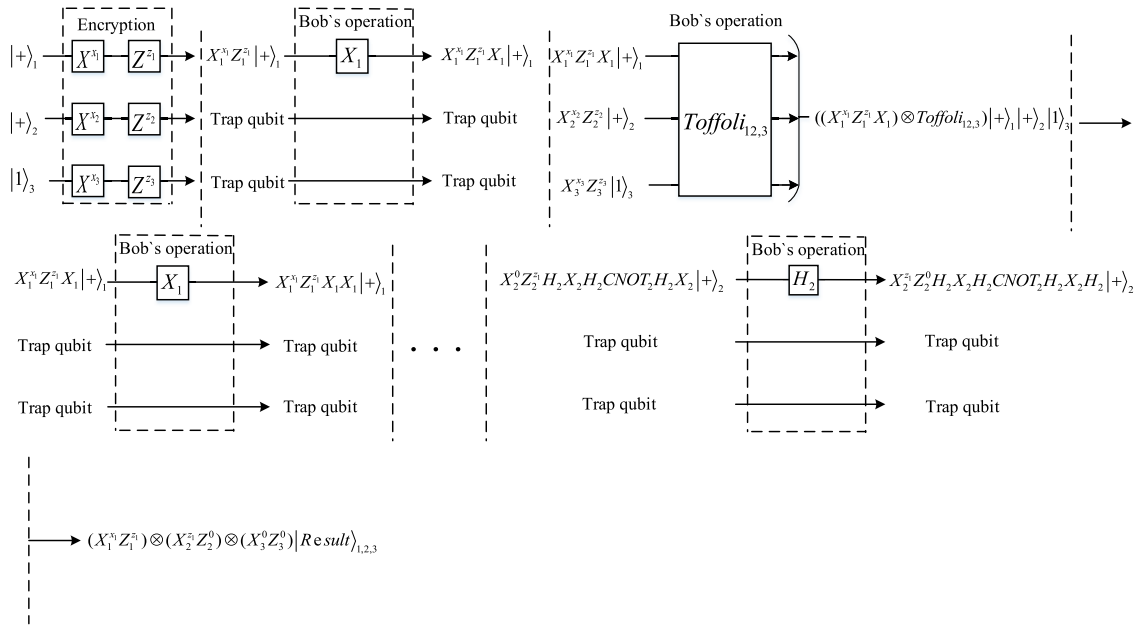**FIGURE 12.** The circuit of Grover algorithm for $|0\rangle_1|1\rangle_2$ from $|+\rangle_1|+\rangle_2$.

FIGURE 13. The whole process of search computing on $|+\rangle_1|+\rangle_2|1\rangle_3$.

V. SECURITY ANALYSIS

In this section, the security of the proposed QSE-FBQC scheme is analyzed as below. We analyze the security from two aspects: external attacks and internal attacks. The former refers to the attacks by the eavesdroppers outside the protocol, while the latter refers to the attacks by the data center in the scheme.

A. EXTERNAL ATTACK

Let Eve be an eavesdropper, who tries to get some information about clients' data. To get the information, he firstly needs to get encryption or decryption key from *Charlie*, because all of the transmitted data are encrypted by the key. First, he can perform the intercept-and-resend attack by intercepting all qubits sent from *Charlie* and resending fake qubits to the client in Step 2 or 11. However, due to the use of BB84 protocol, all qubits are encoded into X or Z basis according to the classical key, Eve cannot distinguish which basis each qubit belongs to and gets nothing form these qubits. And the client can check for the existence of such attack by measuring the received fake qubits. Then, the client can abandon this key and ask *Charlie* to regenerate a new key.

Besides, Eve may also perform the intercept-and-resend attack during the communication between *Bob* and *Charlie*. Due to the existence of tarp qubits and trap gates, Eve cannot distinguish which qubits are not trap qubits, and which required operations are actual operations. But this kind of attack will destroy the results of the delegated computation because of fake qubits sent by Eve. *Charlie* can insert decoy qubits randomly, which consist of X-basis and Z-basis, and record the positions of them. Similar to BB84 protocol, when *Bob* gets all qubits, *Charlie* announce the positions and the state of decoy qubits. *Bob* can check for the existence of such attack with a higher probability by measuring the decoy qubits. For example, if the number of decoy qubits used for eavesdropping checking is m, the success probability of detecting the existence of Eve is $1 - (3/4)^m$, which obviously increases with the increase of m, and which is close to 1 when m is large enough.

B. INTERNAL ATTACK

The internal attack mainly caused by *Bob*, who wants to know the information about the data and the computation. In a sense, to immunize internal attacks is actually to ensure the

blindness of the data and the computation, which is analysed as below.

1) THE BLINDNESS OF DATA

For the blindness of data in our scheme, *Alice* performs encryption operations X and Z on n-qubit state $|\psi\rangle$, and then sends these encrypted qubits $\otimes_{i=1}^{n} X_i^{x_i} Z_i^{z_i} |\psi\rangle$ to *Bob*. Although *Bob* intercepts them, he does not know the value of (x_i, z_i) $(i \in \{1, 2, \cdots, n\})$, he still cannot get anything from the encrypted data.

However, the circuit of T gate and *Toffoli* gate for blind quantum computation is special. Because *Charlie* is not able to perform the S, $CNOT$ and CZ corrections, respectively, which the three operations should be delegated to *Bob*. Once *Bob* obtains the information of corrections, then the encryption keys of encrypted qubits are exposed. So, *Charlie* needs to encrypt qubits again with X and Z operations when the S, $CNOT$ and CZ corrections need to be delegated. Therefore, *Bob* can not distinguish whether these qubits belong to the original quantum state and get nothing from the encrypted qubits.

2) THE BLINDNESS OF COMPUTATION

The computation that the client wants to implement can be seen as a desirable circuit which is made up of the delegated quantum gates, therefore the blindness of computation is equivalent to the blindness of the delegated quantum gates. In order to make the delegated quantum gates blind, these quantum gates (G gate) can be decomposed into the combination of rotation operators (U gate). *Bob* performs partial rotation operators in every round, which can compose the actual G gate or trap gates, so he does not know what is the correct gate. That is, *Charlie* can successfully hide quantum computation process.

Without loss of generality, we give an simple example to explain our model. Suppose *Charlie* wants to delegate quantum gates H, X, CZ and *Toffoli* to *Bob*, while *Bob* cannot know the data and the content of computation in our model. The data have already been all encrypted by *Alice* with gates X and Z. Let all rotation operators have labels according to the order in every quantum circuit from left to right. In quantum circuit of gate H, the performing order of these rotation operators is $h_1, h_2, \cdots, h_m$. In quantum circuit of gate X, the performing order of these rotation operators is $x_1, x_2, \cdots, x_n$. In quantum circuit of gate CZ, the performing order of these rotation operators is $c_1, c_2, \cdots, c_d$. In quantum

circuit of gate *Toffoli*, the performing order of these rotation operators is $t_1, t_2, \cdots, t_w$. Note that, h_i, x_i, c_i and $t_i \in U$. In the model, all gates are started in an arbitrary way, i.e., the process is randomly designed by *Charlie*, such as $t_1, x_1, c_1, h_1, c_2, x_2, \cdots, t_w, x_n, c_d, h_m$. *Bob* cannot distinguish these qubits from *Charlie* every time whether belong to the same original quantum states. Meanwhile, he also cannot distinguish which rotation operators belong to a quantum gate. Therefore, *Bob* cannot know what gates are realized in our model.

VI. PERFORMANCE EVALUATION

In order to evaluate our scheme, we chose two classical searchable encryption (SE) schemes [26], [29] and two blind quantum computation (BQC) schemes [45], [47] as references, and compare our QSE-FBQC scheme with them from the following aspects: time complexity of index construction, time complexity of search, full-blind, multi-client access and eavesdropping detection.

The classical SE schemes generally consists of three main parts: index construction, trapdoor generation and search. Since the process of index construction and trapdoor generation are to encrypt the keyword set W extracted from data or query keywords $\tilde{W}$ through the encryption key SK, the time complexity of each process is similar. Therefore, we only consider the aspect of the time complexity of index construction. Suppose that the number of entries for the data is N. In Cao *et al.*'s and Fu *et al.*'s SE scheme, the major computation in the phase of index construction includes the splitting procedure and two multiplications of a $(cN + u + 1) \times (cN + u + 1)$ matrix and a $(cN + u + 1)$ vector, where c and u are constants, and cN represents the number of keywords in W. So the time complexity is $O(N^2)$. However, it does not need the process of index construction and trapdoor generation, and make search computation over encrypted data directly in Broadbent's BQC scheme, Liu *et al.*'s BQC scheme and our scheme. So the time complexity of index construction is 0. On the other hand, although Fu *et al.*'s SE scheme based on user interest model is more efficient than Cao *et al.*'s scheme when users request more relevant data, the time complexity of search are both $O(N)$. But, these mentioned BQC schemes and our scheme use Grover algorithm to make a quadratic speedup in search, so the time complexity are $O(\sqrt{N})$. For a more intuitive representation, the results of the comparison are shown in Table 1.

As we can see, BQC schemes and our scheme are significantly more efficient than the classical SE schemes in the

TABLE 1. Comparison with classical SE schemes and BQC schemes.

Schemes	Cao *et al.*'s SE scheme [29]	Fu *et al.*'s SE scheme [26]	Broadbent's BQC scheme [45]	Liu *et al.*'s BQC scheme [47]	Our scheme
Time complexity of index construction	$O(N^2)$	$O(N^2)$	0	0	0
Time complexity of search	$O(N)$	$O(N)$	$O(\sqrt{N})$	$O(\sqrt{N})$	$O(\sqrt{N})$
Full-blind quantum computation	No	No	No	Yes	Yes
Multi-client access	Yes	Yes	No	No	Yes
Eavesdropping detection	No	No	No	No	Yes

aspect of search efficiency. However, these BQC schemes do not support multi-client access, which is not convenient for data sharing in cloud environment. And all clients in our scheme outsource the key generation to a trusted key center, which is easy to make each client get search result by the decryption key from the key center. Besides, although Liu *et al.* consider that the desirable delegated quantum operation, one of $\{H, P, CNOT, T\}$, is replaced by a fixed sequence $(H, P, CZ, CNOT, T)$ to make the computation blind, they do not consider detecting eavesdroppers when two parties communicate with each other in their scheme. Our scheme takes the strategy of inserting decoy qubits into transmitted data to check for eavesdropping behavior.

VII. DISCUSSION AND CONCLUSION

In this paper, we firstly propose a multi-client circuit-based full-blind quantum computation model, and then apply this model on the searchable encryption to get a QSE-FBQC scheme. In our scheme, different clients with limited quantum ability can upload their encrypted data to a powerful but untrusted quantum data center and the data center can search on the encrypted data without decryption. Besides, the data center also cannot know what search computation he has implemented by himself, i.e., making the computation blind.

In the field of classical searchable encryption (SE), most schemes are either based on public key (RSA) [23], or based on symmetric key [20], [22]. As we know, RSA has been theoretically broken by Shor algorithm [30] in polynomial time, while some symmetric cryptosystems, such as CBC-MAC, GMAC, GCM, etc., also have been recently broken by using quantum period finding [31], [32]. Therefore, how to use quantum technology to implement SE becomes an interesting work worth studying, which motivates us to study searchable encryption using blind quantum computation. Although some circuit-based BQC schemes [42]–[47] have been continuously proposed in recent years, they only consider the single-client model, which cannot meet the requirements of multi-client accessing or searching data in the cloud environment. Besides, almost all of these schemes focus on guaranteeing the blindness of the data, while ignoring the blindness of the computation. The second motivation of our work is to implement the multi-client access mode as well as guarantee the blindness of computation.

This work designs a multi-client FBQC model, and utilizes it to propose a quantum SE scheme in cloud environment, but it maybe need some improvements or extensions in a practical one. In our scheme, the trusted key center hosts all the keys, so he becomes the cornerstone of the security and would also be the target of attacks (including quantum attacks). How to guarantee his security, i.e., to protect him from various attacks, will become an aspect to be explored. Second, how to prevent illegal user access in the multi-party FBQC model is not considered in this article, maybe quantum identity authentication (QIA) [50] is a feasible one of the candidate solutions.

REFERENCES

[1] F. Wang, J. Xu, X. Wang, and S. Cui, "Joint offloading and computing optimization in wireless powered mobile-edge computing systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1784–1797, Mar. 2018.

[2] X. Xu, Y. Li, T. Huang, Y. Xue, K. Peng, L. Qi, and W. Dou, "An energy-aware computation offloading method for smart edge computing in wireless metropolitan area networks," *J. Netw. Comput. Appl.*, vol. 133, pp. 75–85, May 2019.

[3] X. Li, G. Xu, X. Zheng, K. Liang, E. Panaousis, T. Li, W. Wang, and C. Shen, "Using sparse representation to detect anomalies in complex WSNs," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 6, pp. 1–18, 2019.

[4] K. Ota, M. Dong, J. Gui, and A. Liu, "QUOIN: Incentive mechanisms for crowd sensing networks," *IEEE Netw.*, vol. 32, no. 2, pp. 114–119, Mar./Apr. 2018.

[5] L. Qi, X. Xu, W. Dou, J. Yu, Z. Zhou, and X. Zhang, "Time-aware IoE service recommendation on sparse data," *Mobile Inf. Syst.*, vol. 2016, Nov. 2016, Art. no. 4397061.

[6] X. Xu, Q. Liu, Y. Luo, K. Peng, X. Zhang, S. Meng, and L. Qi, "A computation offloading method over big data for IoT-enabled cloud-edge computing," *Future Gener. Comput. Syst.*, vol. 95, pp. 522–533, Jun. 2019.

[7] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, "Querying in Internet of Things with privacy preserving: Challenges, solutions and opportunities," *IEEE Netw.*, vol. 32, no. 6, pp. 144–151, Nov./Dec. 2018.

[8] G. Xu, Y. Zhang, L. Jiao, E. Panaousis, K. Liang, H. Wang, and X. Li, "DT-CP: A double-TTPs-based contract-signing protocol with lower computational cost," *IEEE Access*, vol. 7, pp. 174740–174749, 2019, doi: 10.1109/ACCESS.2019.2952213.

[9] X. Xu, C. He, Z. Xu, L. Qi, S. Wan, and M. Z. A. Bhuiyan, "Joint optimization of offloading utility and privacy for edge computing enabled IoT," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2019.2944007.

[10] L. Qi, Y. Chen, Y. Yuan, S. Fu, X. Zhang, and X. Xu, "A QoS-aware virtual machine scheduling method for energy conservation in cloud-based cyber-physical systems," *World Wide Web*, to be published, doi: 10.1007/s11280-019-00684-y.

[11] X. Xu, X. Zhang, H. Gao, Y. Xue, L. Qi, and W. Dou, "BeCome: Blockchain-enabled computation offloading for IoT in mobile edge computing," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2019.2936869.

[12] L. Qi, R. Wang, C. Hu, S. Li, Q. He, and X. Xu, "Time-aware distributed service recommendation with privacy-preservation," *Inf. Sci.*, vol. 480, pp. 354–364, Apr. 2018.

[13] G. Xu, W. Wang, L. Jiao, X. Li, K. Liang, X. Zheng, W. Lian, H. Xian, and H. Gao, "SoProtector: Safeguard privacy for native SO files in evolving mobile IoT applications," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2019.2944006.

[14] W. Gong, L. Qi, and Y. Xu, "Privacy-aware multidimensional mobile service quality prediction and recommendation in distributed fog environment," *Wireless Commun. Mobile Comput.*, vol. 2018, Apr. 2018, Art. no. 3075849.

[15] L. Qi, X. Zhang, W. Dou, C. Hu, C. Yang, and J. Chen, "A two-stage locality-sensitive hashing based approach for privacy-preserving mobile service recommendation in cross-platform edge environment," *Future Gener. Comput. Syst.*, vol. 88, pp. 636–643, Nov. 2018.

[16] H. Wang, S. Ma, and H. Dai, "A rhombic dodecahedron topology for human-centric banking big data," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 5, pp. 1095–1105, Oct. 2019.

[17] F. Su, "A survey on big data analytics technologies," in *Proc. Int. Conf. 5G Future Wireless Netw.* Cham, Switzerland: Springer, 2017, pp. 359–370.

[18] H. Wang, S. Ma, H. N. Dai, M. Imran, and T. Wang, "Blockchain-based data privacy management with nudge theory in open banking," *Future Gener. Comput. Syst.*, to be published, doi: 10.1016/j.future.2019.09.010.

[19] C. Bösch, P. Hartel, W. Jonker, and A. Peter, "A survey of provably secure searchable encryption," *ACM Comput. Surv.*, vol. 47, no. 2, pp. 1801–1851, 2014.

[20] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. IEEE Symp. Secur. Privacy. S&P*, Berkeley, CA, USA, 2000, pp. 44–55.

[21] E.-J. Goh, "Secure indexes," *IACR Cryptol. ePrint Arch.*, 2003, p. 216, 2003.

[22] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, 2006, pp. 79–88.

[23] D. Boneh, D. C. Giovanni, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Proc. Adv. Cryptology-EUROCRYPT*, Interlaken, Switzerland, 2004, pp. 506–522.

[24] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.

[25] G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, "Enabling efficient and geometric range query with access control over encrypted spatial data," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 4, pp. 870–885, Apr. 2019.

[26] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 9, pp. 2546–2559, Sep. 2016.

[27] L. X. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Gener. Comput. Syst.*, vol. 95, pp. 420–429, Jun. 2019.

[28] H. Wang, C. Guo, and S. Cheng, "LoC—A new financial loan management system based on smart contracts," *Future Gener. Comput. Syst.*, vol. 100, pp. 648–655, 2019.

[29] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 1, pp. 222–233, Jan. 2014.

[30] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, 1997.

[31] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, "Breaking symmetric cryptosystems using quantum period finding," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 9815. Berlin, Germany: Springer, 2016, pp. 207–237.

[32] X. Dong, Z. Li, and X. Wang, "Quantum cryptanalysis on some generalized Feistel schemes," *Sci. China Inf. Sci.*, vol. 62, no. 2, p. 22501, 2019.

[33] W. Huang, Q. Su, B. Liu, Y. H. He, F. Fan, and B. J. Xu, "Efficient multiparty quantum key agreement with collective detection," *Sci. Rep.*, vol. 7, no. 1, p. 15264, 2017.

[34] W.-J. Liu, Y. Xu, C.-N. Yang, P.-P. Gao, and W.-B. Yu, "An efficient and secure arbitrary N-party quantum key agreement protocol using bell states," *Int. J. Theor. Phys.*, vol. 57, no. 1, pp. 195–207, 2018.

[35] F. Wu, X. Zhang, W. Yao, Z. Zheng, L. Xiang, and W. Li, "An advanced quantum-resistant signature scheme for cloud based on eisenstein ring," *Comput., Mater. Continua*, vol. 56, no. 1, pp. 19–34, 2018.

[36] Z. Qu, T. Zhu, J. Wang, and X. Wang, "A novel quantum stegonagraphy based on brown states," *Comput., Mater. Continua*, vol. 56, no. 1, pp. 47–59, 2018.

[37] W.-J. Liu, P.-P. Gao, W.-B. Yu, Z.-G. Qu, and C.-N. Yang, "Quantum relief algorithm," *Quantum Inf. Process.*, vol. 17, no. 10, p. 280, 2018.

[38] W. Liu, P. Gao, Y. Wang, W. Yu, and M. Zhang, "A unitary weights based one-iteration quantum perceptron algorithm for non-ideal training sets," *IEEE Access*, vol. 7, no. 4, pp. 36854–36865, 2019.

[39] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation," in *Proc. 50th Annu. IEEE Symp. Found. Comput. Sci.*, Atlanta, GA, USA, Oct. 2009, pp. 517–526.

[40] X. Kong, Q. Li, C. Wu, F. Yu, J. He, and Z. Sun, "Multiple-server flexible blind quantum computation in networks," *Int. J. Theor. Phys.*, vol. 55, no. 6, pp. 3001–3007, 2016.

[41] E. Kashefi and A. Pappa, "Multiparty delegated quantum computing," *Cryptography*, vol. 1, no. 2, p. 12, 2017.

[42] P. Arrighi and L. Salvail, "Blind quantum computation," *Int. J. Quantum Inf.*, vol. 4, no. 5, pp. 883–898, 2006.

[43] X. Tan and X. Zhou, "Universal half-blind quantum computation," *Ann. Telecommun.*, vol. 72, no. 9, pp. 589–595, 2017.

[44] K. A. G. Fisher, A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. J. Resch, "Quantum computing on encrypted data," *Nature Commun.*, vol. 5, 2014, Art. no. 3074.

[45] A. Broadbent, "Delegating private quantum computations," *Can. J. Phys.*, vol. 93, no. 9, pp. 941–946, 2015.

[46] X. Zhang, J. Weng, X. Li, W. Luo, X. Tan, and T. Song, "Single-server blind quantum computation with quantum circuit model," *Quantum Inf. Process.*, vol. 17, no. 6, p. 134, 2018.

[47] W. Liu, Z. Chen, J. Liu, Z. Su, and L. Chi, "Full-blind delegating private quantum computation," *Comput., Mater. Continua*, vol. 56, no. 2, pp. 211–223, 2018.

[48] Y. B. Sheng and L. Zhou, "Blind quantum computation with a noise channel," *Phys. Rev. A, Gen. Phys.*, vol. 98, no. 5, p. 052343, 2018.

[49] J. F. Fitzsimons and E. Kashefi, "Unconditionally verifiable blind quantum computation," *Phys. Rev. A, Gen. Phys.*, vol. 96, no. 1, p. 012303, 2017.

[50] Q. Li, Z. Li, W. H. Chan, S. Zhang, and C. Liu, "Blind quantum computation with identity authentication," *Phys. Lett. A*, vol. 382, no. 14, pp. 938–941, 2018.

[51] M. A. Nielsen, and I. Chuang, *Quantum Computation and Quantum Information*. New York, NY, USA: Cambridge Univ. Press, 2002, pp. 20–30.

[52] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. Int. Conf. Comput., Syst. Signal Process.* Bengaluru, India: Springer, 1984, pp. 175–179.

WENJIE LIU was born in 1979. He received the bachelor's degree from Huazhong Agricultural University (HZAU), China, in 2001, the master's degree from Wuhan University (WHU), China, in 2004, and the Ph.D. degree from Southeast University (SEU), China, in 2011. He was a Visiting Professor with the Centre for Quantum Computing and Intelligent Systems, University of Technology Sydney. He is currently an Associate Professor of computer science with the Engineering Research Center of Digital Forensics, Ministry of Education, and the Nanjing University of Information Science and Technology, China. In recent five years, he has published almost 30 SCI-indexed articles. His research interests include quantum machine learning, quantum secure multi-party computation, and quantum cryptography communication. He was a recipient of the China NSF Grant, the Jiangsu NSF Grant, and the Six talent peaks project in Jiangsu Province.

YINSONG XU was born in 1996. He received the bachelor's degree from the Nanjing University of Information Science and Technology, China, in 2018, where he is currently pursuing the master's degree with the School of Computer and Software. His research interests include quantum secure multi-party computation and quantum cryptography communication.

WEN LIU was born in 1982. She received the Ph.D. degree in information security from the Beijing University of Posts and Telecommunications, China, in 2009. She is currently a Professor with the School of Computer Science and Cybersecurity, Communication University of China. In recent years, she has published over ten SCI-indexed articles. Her general research interests include the realm of privacy preserving, quantum secure multi-party computation, and quantum cryptography. She was a recipient of the China NSF Grant, Beijing Higher School Young Talents Project.

HAIBIN WANG was born in 1980. He received the bachelor's degree from the Nanjing University of Information and Science Technology (NUIST), China, in 2001, the master's degree in system analysis and integration from the University of Information and Science Technology, Nanjing, China, in 2004, and the Ph.D. degree from the Nanjing University of Information and Science Technology, Nanjing, in 2011. He currently works at the Engineering Research Center of Digital Forensics, Ministry of Education, and the Nanjing University of Information Science and Technology, China. His research interests include quantum machine learning and quantum secure multi-party computation.

ZHIBIN LEI received the bachelor's degree in mathematics from Beijing University, in 1989, and the Ph.D. degree in electrical engineering from Brown University, in 1997. He has worked at Bell Labs, Lucent Technologies, Panasonic Research, Chinese University of Hong Kong, and The Hong Kong University of Science and Technology. He is currently with the Hong Kong Applied Science and Technology Research Institute (ASTRI). He has more than 120 publications in journals, conferences, and patent applications. His research has led to technology startups and received several international recognitions.

● ● ●