A Hybrid and Universal Blind Quantum Computation

Xiaoqian Zhang,1 Weiqi Luo,1,∗ Jian Weng,1 Yaxi Yang,1 Minrong Chen,2 and Xiaoqing Tan1

1College of Information Science and Technology, Jinan University, Guangzhou 510632, China
2School of Computer, South China Normal University, Guangzhou 510631, China

(Dated: September 18, 2018)

In blind quantum computation, a client delegates her quantum computation to a server with universal quantum computers who learns nothing about the client’s private information. In measurement-based BQC model, the privacy of client’s inputs, algorithms and outputs can be guaranteed. However, it still remains a challenge to generate a large-scale entangled state in experiment. In circuit-based BQC model, single-qubit gates can be realized precisely, but the entangled gates are probabilistically successful. This remains a challenge to determinately realize entangled gates in some systems. To solve the two problems in BQC, we propose the first universal BQC protocol based on a hybrid model, i.e. measurements and circuits, where the client Alice is responsible for single-qubit states and the server Bob performs the universal quantum computing. We analyse and prove the blindness, correctness, universality and verifiability.

PACS numbers: 03.67.Lx, 03.67.Dd, 03.65.Ud.

I. INTRODUCTION

Recently, blind quantum computation (BQC) becomes a hot topic in quantum information processing since it can be applied to realize clients’ private quantum computing. In BQC, measurement-based model and circuits-based model have been studied for many years [1–13]. A. Broadbent et al. [1] in 2009 firstly implemented an universal BQC protocol by measuring a $m \times n$ dimensional blind brickwork state, which is called BFK protocol. In BFK protocol, the client can prepare single-qubit states $|\pm \rangle = (|0 \rangle + e^{i\theta}|1 \rangle)/\sqrt{2}$, $\theta = 0, \frac{\pi}{2}, \frac{\pi}{4}, \ldots, \frac{\pi}{2}$. Based on BFK protocol, multi-server BQC protocols were proposed in [3–5]. A BQC protocol for single-qubit gates $X$, $Y$, $T$, $Z$ has been realized by measuring blind topological states, where the error threshold has been explicitly calculated [6]. An universal BQC protocol based on Affleck-Kennedy-Lieb-Tasaki (AKLT) states has been implemented, where the universal gates set includes blind $Z$ rotation, blind $X$ rotation and controlled-$Z$ followed by blind $Z$-rotations [7]. In experiment, S. Barz et al. realized a demonstration for the privacy of quantum inputs, computations, and outputs [2]. Furthermore, the verifiability problems and other interesting BQC protocols have been proposed [14–32].

The computational speed of quantum computers is much faster than that of classical computers due to the advantage of quantum parallel computing. For quantum computers, it is important to prepare entangled states since they can be applied to quantum computing [33], quantum simulation [34] and so on. However, the key problem is to generate large-scale entangled states [1, 35] in space-separated and individual-controllable quantum systems such as the brickwork state [1], AKLT state [7]. In experiments, there are some great progresses in preparing multi-qubit entangled states. The number of qubits in an entangled state [36] reaches to 20 in trapped-ion system, while the number is 10 both in superconducting [37] and photonic system [38]. It is difficult to describe a large entangled state since the dimension of Hilbert space is exponentially increasing. In circuit-based BQC model, the successful realization of the entangled gates is probabilistic such as the successful probability in optical system is $\frac{1}{10}$ in [39], $\frac{1}{7}$ in [40], $\frac{1}{4}$ in [41], $\frac{1}{3}$ in [42] and $\frac{1}{23}$ in [43].

In this paper, we first propose a hybrid and universal BQC protocol (HUBQC), i.e. measurements and circuits. We make full use of advantages of two models: entangled cluster states for realizing entangled gates are determinately successful in measurement-based and the single-qubit gates can also be realized without too many qubits in circuit-based. These can avoid perfectly the two problems proposed in Abstract. A client Alice generates initial states and a server Bob is responsible for performing operations and measurements. The entangled gates can be realized by measuring graph states and single-qubit gates can be operated on the suitable qubits by Bob orderly. We not only give the proofs of correctness and blindness but also verifiability, where the verifiability implies to verify Bob’s honesty and the correctness of measurement outcomes. These factors are often considered in BQC protocols. The proof of the verifiability refers to [14]. Finally, we apply HUBQC protocol to realize blind protocol about quantum Fourier transform (BQFT) [44–46]. The encrypted method in measurement process is from the BFK protocol in [1].

The rest of this paper is organized as follows. We present the basic knowledge in Section II. The definition and structure of the graph state $\text{Cluster}$ are presented in Section III. The universal blind quantum computation protocol is in Section IV. We show the analyses and proofs of blindness and correctness as well as a application of our protocol in Section V. At last, our discussions and conclusions are given in Section VI.

II. PRELIMINARIES

In [47], it points out that an arbitrary unitary operator $U$ can be decomposed into the combinations of rotation operators.
We first give the rotation operators as follows:

\[
R_x(\alpha) = \begin{pmatrix} \cos \frac{\alpha}{2} & -i \sin \frac{\alpha}{2} \\ -i \sin \frac{\alpha}{2} & \cos \frac{\alpha}{2} \end{pmatrix}, \quad R_y(\beta) = \begin{pmatrix} \cos \frac{\beta}{2} & -\sin \frac{\beta}{2} \\ \sin \frac{\beta}{2} & \cos \frac{\beta}{2} \end{pmatrix}, \\
R_z(\gamma) = \begin{pmatrix} e^{-i\frac{\gamma}{2}} & 0 \\ 0 & e^{i\frac{\gamma}{2}} \end{pmatrix},
\]

(1)

where \( \alpha, \beta, \gamma \in [0, 2\pi] \). Particularly, if the rotation angle is \( \pi \) about \( x \)-axis, \( y \)-axis and \( z \)-axis respectively, we get

\[ R_x(\pi) = iX, \quad R_y(\pi) = XZ, \quad R_z(\pi) = -iZ. \]

If there exist \( \theta, \alpha, \beta \) and \( \gamma \), s.t. an arbitrary unitary operator \( U \) has the decompositions as follows:

\[
U = e^{i\theta}R_x(\alpha)R_y(\beta)R_z(\gamma) = \begin{pmatrix} \cos \frac{\alpha}{2} \cos \frac{\beta}{2} \cos \frac{\gamma}{2} - \sin \frac{\alpha}{2} \sin \frac{\gamma}{2} \\ \sin \frac{\alpha}{2} \cos \frac{\beta}{2} \cos \frac{\gamma}{2} + \cos \frac{\alpha}{2} \sin \frac{\gamma}{2} \\ \sin \frac{\beta}{2} \sin \frac{\gamma}{2} \\ \cos \frac{\beta}{2} \cos \frac{\gamma}{2} \end{pmatrix},
\]

\[
U = e^{i\theta}R_x(\alpha)R_y(\beta)R_z(\gamma) = \begin{pmatrix} \cos \frac{\alpha}{2} \cos \frac{\beta}{2} \cos \frac{\gamma}{2} - \sin \frac{\alpha}{2} \sin \frac{\gamma}{2} \\ \sin \frac{\alpha}{2} \cos \frac{\beta}{2} \cos \frac{\gamma}{2} + \cos \frac{\alpha}{2} \sin \frac{\gamma}{2} \\ \sin \frac{\beta}{2} \sin \frac{\gamma}{2} \\ \cos \frac{\beta}{2} \cos \frac{\gamma}{2} \end{pmatrix},
\]

\[
U = e^{i\theta}R_x(\alpha)R_y(\beta)R_z(\gamma) = \begin{pmatrix} \cos \frac{\alpha}{2} \cos \frac{\beta}{2} \cos \frac{\gamma}{2} - \sin \frac{\alpha}{2} \sin \frac{\gamma}{2} \\ \sin \frac{\alpha}{2} \cos \frac{\beta}{2} \cos \frac{\gamma}{2} + \cos \frac{\alpha}{2} \sin \frac{\gamma}{2} \\ \sin \frac{\beta}{2} \sin \frac{\gamma}{2} \\ \cos \frac{\beta}{2} \cos \frac{\gamma}{2} \end{pmatrix},
\]

(2)

Here, we only show three decomposition forms, the other three decompositions are similar. Next, we give the \( z \)-\( y \)-\( z \) decomposition for gates \( H, S, Z, T, X, Y \) as follows:

\[
H = e^{\frac{i}{2}R_x(\pi)}R_y(\pi), \quad S = e^{\frac{i}{2}R_x(\pi)}R_y(\pi), \quad Z = e^{\frac{i}{2}R_x(\pi)}R_y(\pi), \quad T = e^{\frac{i}{2}R_x(\pi)}R_y(\pi), \quad X = e^{\frac{i}{2}R_x(\pi)}R_y(\pi), \quad iY = e^{\frac{i}{2}R_x(\pi)}R_y(\pi),
\]

For the \( y \)-\( x \)-\( y \) decomposition of rotation operators of above gates, we get

\[
S = e^{\frac{i}{2}R_x(\pi)}R_y(\pi)R_y(\pi), \quad H = e^{\frac{i}{2}R_x(\pi)}R_y(\pi), \quad Z = e^{\frac{i}{2}R_x(\pi)}R_y(\pi), \quad T = e^{\frac{i}{2}R_x(\pi)}R_y(\pi), \quad X = e^{\frac{i}{2}R_x(\pi)}R_y(\pi), \quad iY = e^{\frac{i}{2}R_x(\pi)}R_y(\pi),
\]

For the \( z \)-\( x \)-\( z \) decomposition of rotation operators of above gates, we obtain

\[
H = e^{\frac{i}{2}R_x(\pi)}R_y(\pi)R_y(\pi), \quad S = e^{\frac{i}{2}R_x(\pi)}R_y(\pi), \quad Z = e^{\frac{i}{2}R_x(\pi)}R_y(\pi), \quad T = e^{\frac{i}{2}R_x(\pi)}R_y(\pi), \quad X = e^{\frac{i}{2}R_x(\pi)}R_y(\pi).
\]

III. THE DEFINITION AND STRUCTURE OF THE GRAPH STATE \( |\text{Cluster}\rangle \)

**Definition.**—In FIG. 1, we show the structure of an \( m \times n \) dimensional entangled state \( |\text{Cluster}\rangle \), where these single-qubit states in the state \( |\text{Cluster}\rangle \) are \( |\pm \rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\pi/4}|1\rangle) \) \((v_j = 0, \frac{\pi}{4}, \ldots, \frac{3\pi}{4})\). Suppose \( m \) denotes the horizontal rows and \( n \) denotes the vertical columns. The physical qubits are labelled as index \((a, b)\), where \( a \) represents the \( a \)-th row and \( b \) represents the \( b \)-th column.

1. For odd rows \( a \) and columns \( b \equiv 1 \) (mod 6), apply operations controlled-\( Z \) (CZ) on qubits \((a, b)\) and \((a + 1, b)\), \((a, b + 2)\) and \((a + 1, b + 2)\).

2. For even rows \( a \) and columns \( b \equiv 4 \) (mod 6), apply operations CZ on qubits \((a, b)\) and \((a + 1, b)\), \((a, b + 2)\) and \((a + 1, b + 2)\).

3. For each row \( a \), apply operations CZ on qubits \((a, b)\) and \((a, b + 1)\) where \( 1 \leq a < m, 1 \leq b < n \).

It can be seen from FIG. 1 that every unit state is an eight-qubit cluster state (See FIG. 2(1)) which can be used to realize entangled gates controlled-NOT (CNOT)(See FIG. 2(2)).

IV. A HYBRID AND UNIVERSAL BQC PROTOCOL

**Our HUBQC Protocol.**—The concrete steps of our protocol are as follows (See FIG. 3), where the client Alice has the abilities to prepare the initial states and the server Bob can perform universal quantum computing without exacting Alice’s any private information.

- **Step 1.** Alice prepares all single-qubit states \(|\pm \rangle, |0\rangle, |1\rangle, |\pm \rangle\) and sends them to Bob, where \( v_j \in \{0, \frac{\pi}{4}, \ldots, \frac{3\pi}{4}\} \). These states \(|\pm \rangle\) are used for computing and \(|0\rangle, |1\rangle, |\pm \rangle\) are trap qubits. The reason choosing \(|0\rangle, |1\rangle\) as trap qubits is that \(|0\rangle, |1\rangle\) are not entangled with \(|\pm \rangle\) when CZ gates are performed. While states \(|\pm \rangle\) can be entangled with each other at most three qubits as long as they are in the suitable places. Note that, the connections with the states \(|\pm \rangle\) are \(|0\rangle\) and \(|1\rangle\).

- **Step 2.** Alice asks Bob to perform CZ gates to get a graph state \(|C\rangle\) (See FIG. 4) composed of eight-qubit cluster states.
In FIG. 4, some qubits connected by dotted lines are trap qubits $|0\rangle$, $|1\rangle$, $|\pm_0\rangle$ and the others are computational qubits $|\pm_q\rangle$. These trap qubits can be randomly attached to the $|\text{Cluster}\rangle$ state as long as they keep the structural consistency and do not affect the efficient computing.

Step 3. In Alice’s target algorithms, if single-qubit gates first needs to be performed, Alice asks Bob to perform the above process in FIG. 3. Bob first performs encrypted rotation operations on two black dots in the cluster state, where the encrypted rotation angles are $\xi_j = \nu_j + r_j \pi$ ($\nu_j$ is true rotation angles and $r_j$ is randomly chosen from $\{0, 1\}$ ). The encrypted angle $\xi_j$ and true rotation angles $\nu_j$ belong to the set $\{0, \frac{\pi}{8}, \frac{3\pi}{8}, \frac{5\pi}{8}, \frac{7\pi}{8}\}$. Next, Bob measures every white dot qubit in the cluster state to get the CNOT gate, where the corresponding measurement angles are $\delta_i = \theta_i + \kappa_i + r_i \pi$ which belongs to the set $\{0, \frac{\pi}{8}, \cdots, \frac{7\pi}{8}\}$. $r_i$ is randomly chosen from the set $\in \{0, 1\}$, and $\theta_i = (-1)^i \theta_i + \frac{\pi}{2} r_i \pi$ depends on previous measurement outcomes. The measurement results are zero in the first row and the first column [1].

Otherwise, Alice asks Bob to perform the below process in FIG. 3. Bob first measures the white dots qubits and then performs rotation operators in black dots qubits.

Note that for gates CNOT, if the cluster states don’t contain final quantum outputs in FIG. 4, the correction operations $R_z(-\frac{\pi}{2})$ can be naturally absorbed by performing the projective measurements $|\pm_0, -\frac{\pi}{2}\rangle$ since $|\pm_0, -\frac{\pi}{2}\rangle$ is the same as $R_z(-\frac{\pi}{2})|\pm_0\rangle = \frac{1}{\sqrt{2}}(e^{i\frac{\pi}{4}}|0\rangle \pm e^{i\frac{\pi}{4}}|1\rangle) = \frac{1}{\sqrt{2}}|0\rangle \pm e^{i\frac{\pi}{4}}|1\rangle$ except for a global phase factor.

The above two processes can also be performed in trap qubits, therefore, Bob can not distinguish which are useful CNOT gates and trap gates CNOT in FIG. 4 to strengthened the blindness and security of our protocol.

Step 4. In the final quantum outputs, Alice asks Bob to perform the correct operations $H$ and $R_z(-\frac{\pi}{4})$. After Bob returns all quantum outputs, Alice first measures the trap qubits to verify Bob’s honesty, where the number of trap qubits is optimal without affecting the computational efficiency.

In the protocol, Bob maybe implement Pauli attacks to change the original graph states. If Bob performs Pauli attacks X on $|0\rangle$, $|1\rangle$ or Z on $|\pm_0\rangle$ or XZ on $|0\rangle$, $|1\rangle$, $|\pm_q\rangle$, Alice will get violative results and she aborts the protocol. Note that, Alice know all measurement results on traps with related basis. If Bob passes the test, Alice will discard all traps and accept the results.

V. PROOFS AND APPLICATIONS

We first prove the correctness and blindness of our HUBQC protocol.

Correctness. All quantum outputs are correct when Bob performs the protocol honestly.

Proof: 1) In measurement-based process, the correctness of gate CNOT is showed in FIG. 3[48].

Since $H = e^{i\frac{\pi}{4}}R_x(\frac{\pi}{4})R_z(\frac{\pi}{4})R_y(\frac{\pi}{4})$ holds, we get $R_x(-\frac{\pi}{4})H = e^{i\frac{\pi}{4}}R_x(\frac{\pi}{4})R_z(\frac{\pi}{4})$ in the below lines. After that, we obtain the circuit (1). And we get the circuit (2) via the relationship $HR_y(\alpha)H = R_y(\alpha)$. After correcting H and $R_y(\frac{\pi}{4})$, we receive the gate CNOT via the relationship $(R_y(\frac{\pi}{4})\otimes R_z(\frac{\pi}{4}))CZ(\otimes R_y(\frac{\pi}{4}))CZ = CNOT$.

In the circuit process, the correctness can also be ensured since we have

\[
R_x(v_j + r\pi) = \begin{cases} R_x(v_j), & r = 0 \\
                        iX R_x(v_j), & r = 1 \end{cases},
\]

\[
R_z(v_j + r\pi) = \begin{cases} R_z(v_j), & r = 0 \\
                        X Z R_z(v_j), & r = 1 \end{cases},
\]

\[
R_Z(v_j + r\pi) = \begin{cases} R_Z(v_j), & r = 0 \\
                        -iZ R_z(v_j), & r = 1 \end{cases},
\]

where X, Z are commuted with other operations so they are easily removed. □

Blindness (quantum inputs). Suppose the quantum inputs are single-qubit states $|\pm_0\rangle$, $|0\rangle$, $|1\rangle$. Bob can not get anything from these qubits since the density matrices are maximally mixed from his point of view.
is the same as the BFK protocol. The blindness of quantum algorithms and outputs:

\[ \Xi_j \]

\[ \text{tr} (\rho) = 0 \]

Bob get nothing from the initial states.

\[ p(\Xi_j = (\xi_j)^{m_{i_1}}_{r_j=1}, \Lambda = j, \Sigma_j = (\varepsilon_j)^{m_{i_1}}_{r_j=1}) \]

This implies that the conditional probability distribution of rotation angles known by Bob is equal to its priori probability distribution. So our HUBQC protocol satisfies the condition a).

Similarly, we can get the conditional probability as follows:

\[ p(R_j = (r_j)^{m_{i_1}}_{j=1} | \Lambda = j, \Sigma_j = (\varepsilon_j)^{m_{i_1}}_{r_j=1}) \]

\[ p(R_j = (r_j)^{m_{i_1}}_{j=1} | \Lambda = j, \Sigma_j = (\varepsilon_j)^{m_{i_1}}_{r_j=1}) \]

\[ p(R_j = (r_j)^{m_{i_1}}_{j=1} | \Lambda = j, \Sigma_j = (\varepsilon_j)^{m_{i_1}}_{r_j=1}) \]

The result shows that the value \( (r_j)^{m_{i_1}}_{j=1} \) is independent of \( \Xi_j = (\xi_j)^{m_{i_1}}_{r_j=1} \), so our HUBQC protocol satisfies the condition b).

Verifiability (Bob’s honesty and the correctness of quantum computing). The verifiability is that the client Alice can obtain the correct results if the server Bob is honest. That is, if all measurements on traps show the correct results, the probability that a logical state of Alice’s computation is changed is exponentially small. Otherwise Bob gets nothing of Alice’s secret information.

In our protocol, Alice adds some trap qubits around the state (Cluster). Bob knows neither the number of trap qubits nor their positions. When Bob returns these results, Alice makes a comparison between true results and Bob’s results on the trap qubits. If the error rate is acceptable, Alice accepts these results on computational qubits. Moreover, Alice can measure the quantum outputs traps, and then successfully verifies the Bob’s honesty and correctness of quantum computing.

Bob replaces the true \( |C\rangle \) state with any states \( \rho \). This equal to that Bob performs Pauli attacks I, X, Z, XX. The proof is as follows, which refers to [14].

Now we should show that the probability that Alice is fooled by Bob is exponentially small. Hence our protocol is verifiable. Since Bob might be dishonest, he will deviate from the correct steps. His general attack is a creation of a different state \( \rho \) instead of \( \sigma_q |C_p\rangle \). If he is honest, \( \rho = \sigma_q |C_p\rangle \). If he is honest, \( \rho \) can be any state. The case can be statuted to Pauli attacks by a completely positive-trace-preserving (CPTP) map, and the detail can refer to [14].

Proof: For single-qubit states \(|\pm\rangle\) and \(|0\rangle\, |1\rangle\), where \( \theta \in \{0, \frac{\pi}{4}, \ldots, \frac{3\pi}{4}\} \), we have

\[
\begin{aligned}
\sum_{j=1}^4 [\pm\theta] \pm\theta |\pm\rangle \pm\theta |\pm\rangle |0\rangle |1\rangle |1\rangle
\end{aligned}
\]

\[
\begin{aligned}
\sum_{j=1}^4 [\pm\theta] \pm\theta |\pm\rangle \pm\theta |\pm\rangle |0\rangle |1\rangle |1\rangle = \frac{1}{2} J. 
\end{aligned}
\]

Blindness (graph states). The graph state \(|G\rangle\) is completely blind including the dimension since it contains trap qubits.

Proof: Suppose the dimension of the graph state \(|G\rangle\) is \(m \times n\) known by Bob. However, the true dimension of state \( |G\rangle \) is smaller than \( m \times n \). All unit cluster states are all eight-qubit cluster states, so nothing about the structure of state \(|G\rangle\) is leaked. And the number and the positions of CNOT gates are secret for Bob. Moreover, all measurement angles are encrypted by one-time-pad. Therefore, Bob can not know anything about Alice’ quantum computing.

Blindness (algorithms and outputs). Here, two cases need to be considered: measurement-based process and circuit-based process. Bayes’ theorem can be used to prove the blindness of quantum algorithms and outputs: a) the conditional probability distribution of computational angles known by Bob is equal to its priori probability distribution, when Bob knows some classical information and measurement outcomes of any positive-operator valued measures (POVMs) at any time; b) all quantum outputs are one-time-padded to Bob.

Proof: In measurement-based process, the encrypted form is the same as the BFK protocol [1], the blindness proofs of algorithms and outputs can refer to [6, 7]. In circuit process, the encryption form is \( \xi_j = v_j + r\pi \), we give the blindness proofs of algorithms and outputs as follows.

We firstly analyse the effect of Bob’s rotation angles information \( \Xi_j = (\xi_j)^{m_{i_1}}_{r_j=1} \) on Alice’s privacy [6, 7]. Suppose \( V_j = \{v_j\}^{m_{i_1}}_{r_j=1}, R_j = \{r_j\}^{m_{i_1}}_{j=1} \), where \( R_j \in \{0, 1\} \) is a random variable chosen by Alice and \( \{\Xi_j, V_j\} \in \mathcal{S} = \{\pm\theta \, |k = 0, 1, 2, 4, 5, 6\} \).

\[ \Lambda \in \{1, \cdots, m\} \] is a random variable related with an operation. The conditional probability distribution of \( \Xi_j \) given by \( \Lambda = j \) and \( V_j \) shows Bob’s knowledge which is about Alice’ rotation angles information. Based on Bayes’ theorem, we get

\[
p(\Xi_j = (\xi_j)^{m_{i_1}}_{r_j=1} | \Lambda = j, V_j = (v_j)^{m_{i_1}}_{r_j=1}) 
\]

The simplification process of CNOT gate.

FIG. 5. (Color online) The simplification process of CNOT gate.
Suppose the qubits number of state $|C\rangle$ is $2N$, where the number of traps and computational qubits is $N$ respectively. Here, we denote that the number $N$ is optimal for traps. Then, the probability that all $X$ operators of $\sigma_x$ do not change any trap is $(\frac{2^{N-a}}{(2N)!})^N < (\frac{1}{\sqrt{2}})^a < (\frac{1}{\sqrt{2}})^{\alpha/2}$. We can obtain the same result for $\max(a, b, c) = b$. For $\max(a, b, c) = c$, we have $(\frac{2^{N-a}}{(2N)!})^N < (\frac{1}{\sqrt{2}})^a < (\frac{1}{\sqrt{2}})^{\alpha/2}$. It implies that the probability that Alice is fooled by Bob is exponentially small.

Blind quantum Fourier transform.—With the help of our HUBQC protocol, we study the quantum Fourier transform (QFT) and show the corresponding blind protocol since multi-qubit QFT are the combinations of some single-qubit gates and entangled gates orderly.

We first explain how to realize blind two-qubit QFT. In FIG. 6, all gates can be decomposed into rotation operations and CNOT gates. In [47], the decomposition principle of every controlled unitary operator $U$ has been given. For the unitary operator $U$, there are unitary operators A, B, C such that $ABC = I$ and $U = e^{i\alpha}AXBXC$, where $\alpha$ is a global phase factor. Suppose $A = R_x(\beta)R_y(\frac{\pi}{2})$, $B = R_x(-\frac{\pi}{2})R_y(\frac{\alpha-(\delta+\beta)}{2})$, $C = R_z(\frac{\delta-\beta}{2})$, $U = S$, we have $S = e^{i\alpha}R_y(\beta)R_z(\gamma)R_x(\delta) = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$. Set $\alpha = \frac{\theta}{2}, \beta = \frac{\theta}{2}$ and $\gamma = \delta = 0$, so we get the FIG. 6 (3) about the decomposition of controlled-S entangled gate.

We also give the multi-qubit QFT referred to [47] and the corresponding blind protocol also can be realized via a similar way, where gate controlled-$G_n$ can also be decomposed into a combination of rotation operations and CNOT gates. Let $U = G_n$, we have $U = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix}$. We set $\alpha = \frac{\theta}{2}, \gamma = 0$ and $\beta + \delta = \frac{\theta}{2}$.

VI. DISCUSSIONS AND CONCLUSIONS

In this section, we will discuss the measurement-based UBQC, circuit-based UBQC and our protocols.  
1) In measurement-based UBQC model, every gate needs ten-qubit cluster states. So it brings a challenge to generate multi-qubits entangled states in experiment. In our protocol, we can divide the UBQC protocol into two processes: measurement-based process and circuit-based process. We don’t need a large-scale entangled states since only entangled gates need to be realized by using cluster states.  
2) In circuit-based UBQC model, entangled gates in some systems are probabilistically successful, while the cluster states can be to determinately realize entangled gates.

3) In both processes of our HUBQC protocol, the encrypted forms are similar. In measurement-based process, $\theta' + \kappa_i$ represents an actual measurement angle and $r_j$ is randomly chosen from $[0, 1]$ in $\delta_i = \theta' + \kappa_i + r_j \pi$. However, in circuit-based process, $r_j$ is also randomly chosen from $[0, 1]$ such that $\xi_j$ can be mapped to a uniform distribution set. In both processes, quantum outputs are all encrypted.

In summary, we propose an universal blind quantum computation protocol based on measurements and circuits which only needs two participants: a client Alice and a server Bob. Alice prepares the initial states and sends to Bob who creates the entangled state. According to the computations, Alice asks Bob to perform single-qubit rotation operators or entangled gates. Since the graph state $|\text{Cluster}\rangle$ is surrounded by many traps, and the structure of traps is the same as that of computational qubits, the state $|\text{C}\rangle$ is blind from Bob’s perspective. In both measurement-based process and the circuit process, we encrypt the measurement angles and the rotation angles by one-time-pad. The correctness, blindness and verifiability have already been proved and the universality is obvious since the universal gates set is $H, T, \text{CNOT}$ in our protocol.

ACKNOWLEDGMENTS

This work was supported by National Key R&D Plan of China (Grant No. 2017YFB0802203), National Natural Science Foundation of China (Grant Nos. U1736203, 61877029, 61872153, 61732021, 61472165, 61373158, 61672014 and 61502200), Guangdong Provincial Engineering Technology Research Center on Network Security Detection and Defense (Grant No. 2014B090904067), Guangdong Provincial Special Funds for Applied Technology Research and Development and Transformation of Important Scientific and Technological Achieve (Grant No. 2016B010124009), National Science Foundation of Guangdong Province (Grant No. 2016A030313090), the Zhuhai Top Discipline–Information Security, Guangzhou Key Laboratory of Data Security and Privacy Preserving, Guangdong Key Laboratory of Data Security and Privacy Preserving, National Joint Engineering Research Center of Network Security Detection and Protection Technology, National Cryptography Development Fund MMJ2018010109, and the Fundamental Research Funds for the Central Universities.
[1] A. Broadbent, J. Fitzsimons, E. Kashefi, Universal blind quantum computation, In Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (2009) 517–526.
[2] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, P. Walther, Demonstration of blind quantum computing, Science 335 (2012) 303–308.
[3] T. Morimae, K. Fujii, Secure entanglement distillation for double-server blind quantum computation, Phys. Rev. Lett. 111 (2013) 020502.
[4] L. Qin, C. W. Hong, W. Chunhui, W. Zhonghua, Triple-server blind quantum computing using entanglement swapping, Phys. Rev. A 89 (2014) 040302.
[5] Y.-B. Sheng, L. Zhou, Deterministic entanglement distillation for secure double-server blind quantum computation, Sci. Rep. 5 (2015) 7815.
[6] T. Morimae, K. Fujii, Blind topological measurement-based quantum computation, Nat. Commun. 3 (2012) 1036.
[7] T. Morimae, V. Dunjko, E. Kashefi, Ground state blind quantum computation on aklt states, Quantum Inf. Comput. 15 (2015) 200–234.
[8] J. F. Fitzsimons, Private quantum computation: an introduction to blind quantum computing and related protocols, npj Quant. Inf. 3 (2017) 1–11.
[9] A. M. Childs, Secure assisted quantum computation, Quantum Inf. Comput. 5 (2005) 456–466.
[10] K. Fisher, A. Broadbent, L. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, K. Resch, Quantum computing on encrypted data, Nat. Commun. 5 (2014) 3074.
[11] A. Broadbent, Delegating private quantum computations, Can. J. Phys. 93 (2015) 941–946.
[12] T. Sueki, T. Koshiha, T. Morimae, Ancilla-driven universal blind quantum computation, Phys. Rev. A 87 (2013) 060301.
[13] J. F. Fitzsimons, Private quantum computation: an introduction to blind quantum computing and related protocols, npj Quantum Information 3 (2017) 1–11.
[14] T. Morimae, Verification for measurement-only blind quantum computing, Phys. Rev. A 89 (2014) 060302.
[15] M. Hayashi, T. Morimae, Verifiable measurement-only blind quantum computing with stabilizer testing, Phys. Rev. Lett. 115 (2015) 220502.
[16] A. Gheorghiu, E. Kashefi, P. Walther, Robustness and device independence of verifiable blind quantum computing, New J. Phys. 17 (2015) 083040.
[17] J. F. Fitzsimons, E. Kashefi, Unconditionally verifiable blind quantum computation, Phys. Rev. A 96 (2017) 012303.
[18] M. Hajdusek, C. A. Pérez-Delgado, J. Fitzsimons, Device-independent verifiable blind quantum computation, arXiv:1502.02563v2.
[19] K. Fuji, M. Hayashi, Verifiable fault tolerance in measurement-based quantum computation, Phys. Rev. A 96 (2017) 030301.
[20] T. Morimae, Measurement-only verifiable blind quantum computing with quantum input verification, Phys. Rev. A 94 (2016) 042301.
[21] A. Broadbent, How to verify a quantum computation, Theory of computing 14 (2018) 1–37.
[22] T. Morimae, Blind quantum computing can always be made verifiable, arXiv:1803.06624v1.
[23] A. Mantri, C. A. Pérez-Delgado, J. F. Fitzsimons, Optimal blind quantum computation, Phys. Rev. Lett. 111 (2013) 230502.
[24] V. Giovannetti, L. Maccone, T. Morimae, T. G. Rudolph, Efficient universal blind quantum computation, Phys. Rev. Lett. 111 (2013) 230501.
[25] V. Dunjko, E. Kashefi, A. Leverrier, Blind quantum computing with weak coherent pulses, Phys. Rev. Lett. 108 (2012) 200502.
[26] Z. Sun, J. Yu, P. Wang, L. Xu, Symmetrically private information retrieval based on blind quantum computing, Phys. Rev. A 91 (2015) 052303.
[27] C. Greganti, M. C. Roehsner, S. Barz, T. Morimae, P. Walther, Demonstration of measurement-only blind quantum computing, New J. Phys. 18 (2016) 013020.
[28] C. A. Pérez-Delgado, J. F. Fitzsimons, Iterated gate teleportation and blind quantum computation, Phys. Rev. Lett. 114 (2015) 220502.
[29] H. L. Huang, W. S. Bao, T. Li, F. G. Li, X. Q. Fu, S. Zhang, H. L. Zhang, X. Wang, Universal blind quantum computation for hybrid system, Quantum Inf. Process. 16 (2017) 199.
[30] S. Aaronson, A. Cojocarui, A. Gheorghiu, E. Kashefi, On the implausibility of classical client blind quantum computing, arXiv:1704.08482v1.
[31] H. L. Huang, Q. Zhao, X. F. Ma, C. Liu, Z. E. Su, X. L. Wang, L. Li, N. L. Liu, B. C. Sanders, C. Y. Lu, J. W. Pan, Experimental blind quantum computing for a classical client, Phys. Rev. Lett. 119 (2017) 050503.
[32] K. Marshall, C. S. Jacobsen, C. Schäfermeier, T. Gehring, C. Weedbrook, U. L. Andersen, Continuous-variable quantum computing on encrypted data, Nat. Comm. 7 (2016) 13795.
[33] R. Raussendorf, H. J. Briegel, A one-way quantum computer, Phys. Rev. Lett. 86 (2001) 5188–5191.
[34] S. Lloyd, Universal quantum simulators, Science 273 (1996) 1073.
[35] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, Quantum entanglement, Rev. Mod. Phys. 81 (2009) 865.
[36] N. Fiuris, O. Marty, C. Maier, C. Hempel, M. Holzäpfel, P. Jurcevic, M. B. Plenio, M. Huber, C. Roos, R. Blatt, B. Lanyon, Observation of entangled states of a fully controlled 20-qubit system, Phys. Rev. X 8 (2018) 021012.
[37] C. Song, K. Xu, W. Liu, C. Yang, S. Zheng, H. Deng, X. Xie, K. Huang, Q. Guo, L. Zhang, P. Zhang, D. Xu, D. Zheng, X. Zhu, H. Wang, Y. A. Chen, C. Y. Lu, S. Han, J. W. Pan, 10-qubit entanglement and parallel logic operations with a superconducting circuit, Phys. Rev. Lett. 119 (2017) 180511.
[38] X.-L. Wang, X.-K. Chen, W. Li, H.-L. Huang, C. Liu, C. Chen, Y.-H. Luo, Z.-E. Su, D. Wu, Z.-D. Li, H. Lu, Y. Hu, X. Jiang, C.-Z. Peng, L. Li, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, J.-W. Pan, Experimental ten-photon entanglement, Phys. Rev. Lett. 117 (2016) 210502.
[39] M. Koashi, T. Yamamoto, N. Imoto, Probabilistic manipulation of entangled photons, Phys. Rev. A 63 (2001) 030301.
[40] T. C. Ralph, N. K. Langford, T. B. Bell, A. G. White, Linear optical controlled-not gate in the coincidence basis, Phys. Rev. A 65 (2002) 062324.
[41] T. B. Pittman, B. C. Jacobs, J. D. Franson, Probabilistic quantum logic operations using polarizing beam splitters, Phys. Rev. A 64 (2001) 062311.
[42] H. F. Hofmann, S. Takeuchi, Quantum phase gate for photonic qubits using only beam splitters and postselection, Phys. Rev. A 66 (2002) 024308.
[43] J. L. O’Brien, G. J. Pryde, A. G. White, T. C. Ralph, D. Branning, Demonstration of an all-optical quantum controlled-not gate, Nature 426 (2003) 264–267.
[44] F. Marquezino, R. Portugal, F. Sasse, Obtaining the quantum
fourier transform from the classical fft with qr decomposition, Journal of Computational and Applied Mathematics 235 (2010) 74–81.

[45] Y. S. Nam, R. Blümel, Robustness of the quantum fourier transform with respect to static gate defects, Phys. Rev. A 89 (2014) 042337.

[46] L. Ruiz-PerezEmail, J. C. Garcia-Escartin, Quantum arithmetic with the quantum fourier transform, Quant. Inf. Process. 16 (2017) 152.

[47] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.

[48] X. Zhang, J. Weng, X. Tan, T. Song, W. Luo, Measurement-based universal blind quantum computation with minor resources, arxiv:1801.03090[quant-ph](2018).