Blind quantum computation for QFT on multi-qubit states

Xiaoqian Zhang[1], Jian Weng[1],[*] Weiqi Luo[1], and Xiaoqing Tan[2]
[1] *Department of Computer Science, Jinan University, Guangzhou 510632, P.R. China. and*
[2] *Department of Mathematics, Jinan University, Guangzhou, P.R. China*
(Dated: January 15, 2018)

After quantum computers come out, governments and rich companies will have the abilities to buy these useful quantum computers, meanwhile they are familiar with these technologies proficiently. If a client wants to perform quantum computing but she does not have quantum computers with relevant quantum technologies. She can seek help from the server and pay his salary, but she does not want to leak anything to the server. Blind quantum computing (BQC) give a good method for the client to realized her quantum computing. In this article, we propose a new BQC protocol of quantum fourier transform (QFT) performed on multi-qubit states with a trusted, a client and a server, where the trusted center can generate resource states, the client can delegate her quantum computing to a server who can perform universal quantum computing without knowing anything about the client's inputs, algorithms and outputs. We first give the BQC protocols of three-qubit QFT with the equivalently quantum circuits, Greenberg-Horne-Zeilinger(GHZ) entangled states and W entangled states as examples. Further, we extend them to multi-qubit QFT on multi-qubit with the equivalently quantum circuits. At last, we give the analyses and proofs of the blindness and correctness.

PACS numbers: 03.67.Hk, 03.65.Ud.

I. INTRODUCTION

In recent years, various blind quantum computation (BQC) protocols are proposed [1–21]. In the future, when large scale of quantum computers come out, their prices are very expensive such that few people can afford a computer. When they want to perform quantum computing in some cases, they need to delegate their quantum computing to some rich companies owned quantum computers. This is the reason that blind quantum quantum computing becomes a hot topic in academia. BQC allows a client who has few quantum abilities can delegate her quantum computation to servers who have full advanced quantum computers in which her quantum inputs, outputs and algorithms keep unknown to the server. Broadbent et al. [1] in 2009 first proposed an universal BQC protocol with brickwork states, where every single qubit is randomly chosen from a finite set in which every qubit is randomly rotated the multiple of $\frac{\pi}{4}$. Further, Barz et al. [3] made an experiment to demonstrate blind quantum computing by using brickwork state. Since it is perfect BQC protocol based on measurement with the brickwork state, many proposed multi-server BQC protocols were simplified into single-server BQC protocol to construct the brickwork state and realize BQC in [4–6, 8]. Quantum circuits play a key role in constructing BQC protocols, blind quantum computing based on circuits models were widely studied in [9–12, 22]. Since in blind quantum computing, it is always inevitable to transmit qubits from a client to servers or from servers to a client, it is a difficult task to remove quantum channel noises. These noises have already reduce transmission efficiency, so many scholars started to solve this problem and propose anti-noise BQC protocols [6, 23, 24] recently.

In above description, we only review some basic BQC protocols, but it is an open question how to verify the correctness quantum inputs and quantum computing. It will be solved in these verifiable BQC protocols [13–20, 25–28], where the client has the ability to realize the verifiability. Some important problems in BQC protocols have already been conquered by above references. Naturally, we will consider the application of BQC to reflect their values. So many application of BQC protocols are proposed to complete various important tasks in [29–36]. In [35], Huang *et al.* implemented an experimental BQC protocol to factorize the integer 15 in which two quantum servers can classically interact with each other and share three Bell states while the client is classical. With the development of BQC, many outstanding achievements have been presented to the world, a people, Fitzsimons, analyzed and summarized these protocols. In [37], Fitzsimons reviewed some important BQC protocols and analyzed these protocols by security, state preparation, semi-classical client, measurement, multiple servers, computing on encrypted data and homomorphic, physical implementations. This gives us a clear understanding of the development and knows that there exist problems in blind quantum computing.

Since blind quantum computing can be used to realize an algorithm securely, we consider the QFT and propose the corresponding BQC protocols. The quantum fourier transform (QFT) is performed on multi-qubit states introduced in [38]. Our BQC protocols are single client-server BQC protocols, in which a trusted center needs to prepare the initial states and the server only needs to perform rotation operators since the QFT can be replaced by rotation operators. First, we present the BQC protocols of three-qubit QFT performed on Greenberg-

[*] cryptjweng@gmail.com

Horne-Zeilinger(GHZ) entangled states and W entangled states, where the two classes entangled states have already been prepared in experiment [39, 40]. For GHZ states, we detailed analyze and present these BQC protocols of QFT performed on qubits 123 of GHZ states $\{|GHZ^{\pm}_{000}\rangle, |GHZ^{\pm}_{001}\rangle, |GHZ^{\pm}_{010}\rangle, |GHZ^{\pm}_{100}\rangle\}$. We similarly analyze these BQC protocols of QFT performed on multi-qubit states. At last, we prove the blindness and correctness for multi-QFT blind quantum computing protocols.

The rest of this paper is organized as follows. The background of QFT are introduced in Sect. II. These BQC protocols are presented in III. At last, the conclusions are shown in V.

II. PRILIMENARIES

The the principle of quantum Fourier transform is introduced in Ref.[38]. Here, we only review some useful knowledge in this section for obtaining our BQC protocols. In quantum mechanics system, the quantum Fourier transform can be expressed as an unitary matrix QFT_N and the corresponding quantum circuits is in FIG. 1.

$$\mathrm{QFT}_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \dots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \dots & \omega^{(N-1)(N-1)} \end{pmatrix},$$

where $N = 2^n$ and $\omega = e^{\frac{2\pi i}{2^n}}$. In FIG. 1, the input states are $|j\rangle = |j_1 \dots j_n\rangle$ and the G_k is expressed as

$$G_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}.$$

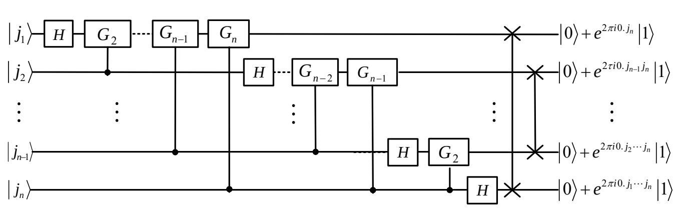

FIG. 1. The quantum circuit for multi-qubit quantum Fourier transform, where Hadamard gate is definited as H : $|j\rangle \mapsto 1/\sqrt{2}(|0\rangle + (-1)^j|1\rangle)$.

Concretely, when $N = 8 = 2^3$ and phase $\omega = e^{\frac{\pi i}{4}}$, the transformation matrix

$$\mathrm{QFT}_8 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \frac{1+i}{\sqrt{2}} & i & \frac{-1+i}{\sqrt{2}} & -1 & -\frac{1+i}{\sqrt{2}} & -i & \frac{1-i}{\sqrt{2}} \\ 1 & i & -1 & -i & 1 & i & -1 & -i \\ 1 & \frac{-1+i}{\sqrt{2}} & -i & \frac{1+i}{\sqrt{2}} & -1 & \frac{1-i}{\sqrt{2}} & i & -\frac{1+i}{\sqrt{2}} \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & \frac{1-i}{\sqrt{2}} & i & \frac{1-i}{\sqrt{2}} & -1 & \frac{1+i}{\sqrt{2}} & -i & \frac{-1+i}{\sqrt{2}} \\ 1 & -i & -1 & i & 1 & i & -1 & i \\ 1 & \frac{-1+i}{\sqrt{2}} & -i & -\frac{1+i}{\sqrt{2}} & -1 & \frac{-1+i}{\sqrt{2}} & i & \frac{1+i}{\sqrt{2}} \end{pmatrix},$$

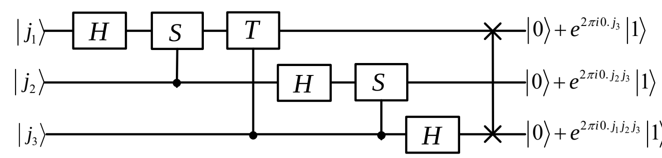

FIG. 2. The circuits of quantum Fourier transform performed on three qubits.

This construction also proves that the quantum Fourier transform is unitary, since each gate in the circuit is unitary. For triple-qubit, the circuits of QFT is in FIG. 2 and the relevant results are as follows.

$$\begin{aligned}
|000\rangle &\xrightarrow{\text{QFT}} \frac{1}{2\sqrt{2}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle), \\
|001\rangle &\xrightarrow{\text{QFT}} \frac{1}{2\sqrt{2}}(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle)(|0\rangle + e^{\frac{\pi i}{4}}|1\rangle), \\
|010\rangle &\xrightarrow{\text{QFT}} \frac{1}{2\sqrt{2}}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle), \\
|100\rangle &\xrightarrow{\text{QFT}} \frac{1}{2\sqrt{2}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle - |1\rangle), \\
|101\rangle &\xrightarrow{\text{QFT}} \frac{1}{2\sqrt{2}}(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle)(|0\rangle + e^{\frac{5\pi i}{4}}|1\rangle), \\
|110\rangle &\xrightarrow{\text{QFT}} \frac{1}{2\sqrt{2}}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{3\pi i}{2}}|1\rangle), \\
|011\rangle &\xrightarrow{\text{QFT}} \frac{1}{2\sqrt{2}}(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle)(|0\rangle + e^{\frac{3\pi i}{4}}|1\rangle), \\
|111\rangle &\xrightarrow{\text{QFT}} \frac{1}{2\sqrt{2}}(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{3\pi i}{2}}|1\rangle)(|0\rangle + e^{\frac{7\pi i}{4}}|1\rangle).
\end{aligned} \tag{1}$$

In this paper, we need to know the properties of X and T gates, the relationship between CS, CZ and CT, S, Z and T.

$$\begin{aligned} &\mathrm{X} : |j\rangle \to |j \oplus 1\rangle, \mathrm{T} : |j\rangle \to (e^{\frac{i\pi}{4}})^j |j\rangle, \\ &\mathrm{CZ}_{12} = \mathrm{CS}_{12}^2 = \mathrm{CT}_{12}^4,\ \mathrm{Z} = \mathrm{S}^2 = \mathrm{T}^4. \end{aligned} \tag{2}$$

What's more important is that we use the combination of rotation operators to express a gate, so we must give the decomposition of rotation operators for gates H, T and X.

$$\begin{aligned} &H = e^{\frac{i\pi}{2}} R_y(\frac{\pi}{2}) R_z(\pi), T = e^{\frac{i\pi}{8}} R_z(\frac{\pi}{4}) R_y(0), \\ &X = e^{\frac{i\pi}{2}} R_y(\pi) R_z(\pi). \end{aligned} \tag{3}$$

where $R_y(0) = R_y(2\pi) = R_y(\frac{\pi}{4})^8$, $R_y(\pi) = R_y(\frac{\pi}{4})^4$ and $R_z(\pi) = R_z(\frac{\pi}{4})^4$.

III. BQC PROTOCOLS FOR MULTI-QUBIT QUANTUM FOURIER TRANSFORM

In this section, we will give these BQC protocols in detail. Since all BQC protocols will be performed cross-ways, we first show the procedures for all BQC protocols as follows.

Step 1. A trusted center prepares enough initial states $\{|\mathrm{GHZ}^{\pm}_{000}\rangle, |\mathrm{GHZ}^{\pm}_{001}\rangle, |\mathrm{GHZ}^{\pm}_{010}\rangle, |\mathrm{GHZ}^{\pm}_{100}\rangle\}$ and sends them to Alice.

Step 2. Alice disturbs the order of qubits and sends qubits to Bob.

Step 3. Bob performs rotation operators and returns the operated qubits to Alice. All gates are decomposed into two rotation operators $R_y(\theta)$ and $R_z(\vartheta)$ in Eq.(5). In these BQC protocols, in fact, Bob only performs gates $R_y(\frac{\pi}{4})$, $R_z(\frac{\pi}{4})$, $C-R_y(\frac{\pi}{4})$ and $C-R_z(\frac{\pi}{4})$.

Step 4. They interact with each other multiple rounds by repeating Step 2 and Step 3 to completing the quantum computing.

For three-qubit entangled states, GHZ entangled states and W entangled states are often used to complete communication between remote parties. Therefore, we can clearly get the universal BQC protocols of QFT on three-qubit states by analyzing BQC protocols of QFT on GHZ entangled states and W entangled states. In FIG. 3, the circuits of BQC protocols for three-qubit QFT performed on GHZ states are presented.

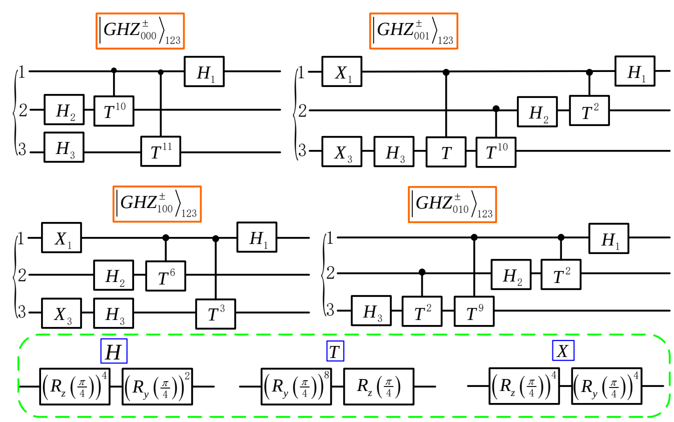

FIG. 3. The equivalent quantum circuits for quantum Fourier transform performed on three qubits of GHZ states. In the green box, three circuits are the composed circuits of rotation operations of gates H, X and T.

BQC protocol 1. For states $|\mathrm{GHZ}^{\pm}_{000}\rangle$, we give the BQC protocol of QFT performed on qubits 123. Alice sends qubit 2 to Bob and Bob performs one round operation H_2 (That is, Bob performs four rounds $R_z(\frac{\pi}{4})$ and two rounds $R_y(\frac{\pi}{4})$). Bob returns the result to Alice and Alice sends 3 to Bob. Bob performs H_3 (That is, Bob performs four rounds $R_z(\frac{\pi}{4})$ and two rounds $R_y(\frac{\pi}{4})$) and returns to Alice. Alice sends 12 to Bob and Bob performs 10 rounds CT_{12} (In every round CT operation, Bob performs eight rounds $C-R_y(\frac{\pi}{4})$ and one round $C-R_z(\frac{\pi}{4})$), where C is controlled) and returns them to Alice. Alice sends 13 to Bob and Bob performs 11 rounds CT_{13} (That is, in every round CT operation, Bob performs eight rounds $C-R_y(\frac{\pi}{4})$ and one round $C-R_z(\frac{\pi}{4})$). Bob returns it to Alice and Alice sends 1 to Bob. Bob performs H_1 (That is, Bob performs four rounds $R_z(\frac{\pi}{4})$ and two rounds $R_y(\frac{\pi}{4})$) and returns it to Alice. Alice obtains $\mathrm{QFT}|\mathrm{GHZ}_{000}\rangle$.

BQC protocol 2. For $|\mathrm{GHZ}^{\pm}_{001}\rangle$, Alice sends qubit 1 to Bob and Bob performs operation X_1 (In fact, Bob performs four rounds $R_z(\frac{\pi}{4})$ and four rounds $R_y(\frac{\pi}{4})$). Bob returns the qubit to Alice and Alice sends qubits 3 to Bob and Bob performs operation X_3 (In fact, Bob performs four rounds $R_z(\frac{\pi}{4})$ and four rounds $R_y(\frac{\pi}{4})$). Bob returns the qubit to Alice and Alice sends qubits 3 to Bob who performs operation H_3 (In fact, Bob performs four rounds $R_z(\frac{\pi}{4})$ and two rounds $R_y(\frac{\pi}{4})$). Bob returns the qubit to Alice and Alice sends qubits 13 to Bob and Bob performs operation CT_{13} (In fact, in every round CT operation, Bob performs eight rounds $C-R_y(\frac{\pi}{4})$ and one round $C-R_z(\frac{\pi}{4})$). Bob returns them to Alice and Alice sends qubits 23 to Bob. Bob perfoRms 10 rounds CT_{23} (In fact, in every round CT operation, Bob performs eight rounds $C-R_y(\frac{\pi}{4})$ and one round $C-R_z(\frac{\pi}{4})4)$ and returns them to Alice. Alice sends 2 to Bob and Bob performs H_2 (In fact, Bob performs four rounds $R_z(\frac{\pi}{4})$ and two rounds $R_y(\frac{\pi}{4})$). Bob returns it to Alice and Alice sends 12 to Bob. Bob performs two rounds CT_{12} (In fact, in every round CT operation, Bob performs eight rounds $C-R_y(\frac{\pi}{4})$ and one round $C-R_z(\frac{\pi}{4})$). Bob returns them to Alice and Alice sends 1 to Bob and Bob performs H_1 (In fact, Bob performs four rounds $R_z(\frac{\pi}{4})$ and two rounds $R_y(\frac{\pi}{4})$). Bob returns it to Alice and Alice obtains $\mathrm{QFT}|\mathrm{GHZ}_{001}\rangle$.

BQC protocol 3. For $|\mathrm{GHZ}^{\pm}_{010}\rangle$, Alice sends qubit 3 to Bob who performs operation H_3 (In fact, Bob performs four rounds $R_z(\frac{\pi}{4})$ and two rounds $R_y(\frac{\pi}{4})$). Bob returns the qubit to Alice and Alice sends qubits 23 to Bob who performs two rounds CT_{23} (In fact, in every round CT operation, Bob performs eight rounds $C-R_y(\frac{\pi}{4})$ and one round $C-R_z(\frac{\pi}{4})$). Bob returns the qubit to Alice and Alice sends qubits 13 to Bob who performs nine rounds CT_{13} (In fact, in every round CT operation, Bob performs eight rounds $C-R_y(\frac{\pi}{4})$ and one round $C-R_z(\frac{\pi}{4})$). Alice sends qubit 2 to Bob who performs operation H_2 (In fact, Bob performs four rounds $R_z(\frac{\pi}{4})$ and two rounds $R_y(\frac{\pi}{4})$). Bob returns the qubit to Alice and Alice sends qubits 12 to Bob who performs two rounds CT_{12} (In fact, in every round CT operation, Bob performs eight rounds $C-R_y(\frac{\pi}{4})$ and one round $C-R_z(\frac{\pi}{4})$). Bob returns them to Alice and Alice sends qubits 1 to Bob. Bob performs two rounds H_1 (In fact, Bob performs four rounds $R_z(\frac{\pi}{4})$ and two rounds $R_y(\frac{\pi}{4})$) and returns them to Alice. Alice obtains $\mathrm{QFT}|\mathrm{GHZ}_{010}\rangle$.

BQC protocol 4. For $|\mathrm{GHZ}_{100}\rangle$, Alice sends qubit 1 to Bob who performs operation X_1 (In fact, Bob performs four rounds $R_z(\frac{\pi}{4})$ and four rounds $R_y(\frac{\pi}{4})$). Bob returns the qubit to Alice and Alice sends qubits 3 to Bob who performs operation X_3 (In fact, Bob performs four rounds $R_z(\frac{\pi}{4})$ and four rounds $R_y(\frac{\pi}{4})$). Bob returns the qubit to Alice and Alice sends qubits 2 to Bob who performs operation H_2 (In fact, Bob performs four rounds $R_z(\frac{\pi}{4})$ and two rounds $R_y(\frac{\pi}{4})$). Bob returns the qubits to Alice and Alice sends qubits 3 to Bob who performs operation H_3 (In fact, Bob performs four rounds $R_z(\frac{\pi}{4})$ and two rounds $R_y(\frac{\pi}{4})$). Bob returns them to Alice and Alice sends qubits 12 to Bob. Bob performs five rounds CT_{12} (In fact, in every round CT operation, Bob performs eight rounds $C-R_y(\frac{\pi}{4})$ and one round $C-R_z(\frac{\pi}{4})4$) and returns them to Alice. Alice sends 13 to Bob and Bob performs three rounds CT_{13} (In fact, in every round CT operation, Bob performs eight rounds $C-R_y(\frac{\pi}{4})$ and one round $C-R_z(\frac{\pi}{4})$). Bob returns them to Alice and Alice sends qubit 1 to Bob and Bob performs H_1(In fact, Bob performs four rounds $R_z(\frac{\pi}{4})$ and two rounds $R_y(\frac{\pi}{4})$). Bob returns them to Alice. Alice obtains $\mathrm{QFT}|\mathrm{GHZ}_{100}\rangle$.

For the other three-qubit states $|W\rangle = \frac{1}{\sqrt{3}}(|010\rangle + |100\rangle + |001\rangle)$, the equation

$$\begin{aligned}|W\rangle &\xrightarrow{\mathrm{QFT}} \frac{1}{2\sqrt{6}}[(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)(|0\rangle+e^{\frac{\pi i}{2}}|1\rangle)\\ &+(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)+(|0\rangle-|1\rangle)\\ &(|0\rangle+e^{\frac{\pi i}{2}}|1\rangle)(|0\rangle+e^{\frac{\pi i}{4}}|1\rangle)].\end{aligned}$$

is equivalent to

$$\begin{aligned}|W\rangle &\xrightarrow{H_3} \frac{1}{\sqrt{6}}[|01\rangle(|0\rangle+|1\rangle)+|00\rangle(|0\rangle-|1\rangle)+|10\rangle(|0\rangle+|1\rangle)]\\
&\xrightarrow{CT_{23}^2} \frac{1}{\sqrt{6}}[|01\rangle(|0\rangle+e^{\frac{\pi i}{2}}|1\rangle)+|00\rangle(|0\rangle-|1\rangle)+|10\rangle(|0\rangle+|1\rangle)]\\
&\xrightarrow{CT_{13}} \frac{1}{\sqrt{6}}[|01\rangle(|0\rangle+e^{\frac{\pi i}{2}}|1\rangle)+|00\rangle(|0\rangle-|1\rangle)\\
&\quad+|10\rangle(|0\rangle+e^{\frac{\pi i}{4}}|1\rangle)]\\
&\xrightarrow{H_2} \tfrac{1}{2\sqrt{3}}[|0\rangle(|0\rangle-|1\rangle)(|0\rangle+e^{\frac{\pi i}{2}}|1\rangle)+|0\rangle(|0\rangle+|1\rangle)]\\
&\quad(|0\rangle-|1\rangle)+|1\rangle(|0\rangle+|1\rangle)(|0\rangle+e^{\frac{\pi i}{4}}|1\rangle)]\\
&\xrightarrow{CT_{12}^2} \frac{1}{2\sqrt{3}}[|0\rangle(|0\rangle-|1\rangle)(|0\rangle+e^{\frac{\pi i}{2}}|1\rangle)+|0\rangle(|0\rangle+|1\rangle)\\
&\quad(|0\rangle-|1\rangle)+|1\rangle(|0\rangle+e^{\frac{\pi i}{2}}|1\rangle)(|0\rangle+e^{\frac{\pi i}{4}}|1\rangle)]\\
&\xrightarrow{H_1} \frac{1}{2\sqrt{3}}[(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)(|0\rangle+e^{\frac{\pi i}{2}}|1\rangle)+(|0\rangle+|1\rangle)\\
&(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)+(|0\rangle-|1\rangle)(|0\rangle+e^{\frac{\pi i}{2}}|1\rangle)(|0\rangle+e^{\frac{\pi i}{4}}|1\rangle)]\end{aligned}$$

We also give the BQC protocol similar to above BQC protocols of GHZ entangled states. For four-qubit states, we have the similar analysis. For example, $|0001\rangle \xrightarrow{\mathrm{QFT}} (|0\rangle-|1\rangle)(|0\rangle+e^{\frac{\pi i}{2}}|1\rangle)(|0\rangle+e^{\frac{\pi i}{4}}|1\rangle)(|0\rangle+e^{\frac{\pi i}{8}}|1\rangle)$, the server only needs to perform CT_{1k}^t where t is a integer and k=2,3,4. The server also performs other operations such as rotation operators of X, H gates. By the principle,, we have the similar results for multi-qubit QFT.

IV. PROOFS OF BLINDNESS AND CORRECTNESS

In BQC protocol, the client needs to keep quantum inputs, algorithms and outputs private for servers, so we show the blindness of these BQC protocols. However, the analysis and proof of correctness are also essential in BQC protocols. Therefore, we will mainly consider the two aspects.

Quantum inputs are generated by the trusted center unknown to Bob. And in every round, Alice only sends one qubit or two qubits to Bob such that Bob cannot get anything since he dare not to measure. If eavesdroppers do not know which GHZ state in the transmission of qubits, since the density matrix is

$$\begin{aligned}&\frac{1}{8}(|GHZ_{000}^+\rangle\langle GHZ_{000}^+|+|GHZ_{000}^-\rangle\langle GHZ_{000}^-|\\ &+|GHZ_{001}^+\rangle\langle GHZ_{001}^+|+|GHZ_{001}^-\rangle_{001}\langle GHZ_{001}^-|\\ &+|GHZ_{010}^+\rangle\langle GHZ_{010}^+|+|GHZ_{010}^-\rangle\langle GHZ_{010}^-|\\ &+|GHZ_{011}^+\rangle\langle GHZ_{011}^+|+|GHZ_{011}^-\rangle\langle GHZ_{011}^-|=\frac{I}{8}\end{aligned} \tag{4}$$

This shows that they are independent of $|GHZ_{000}^+\rangle$, $|GHZ_{000}^-\rangle$, $|GHZ_{001}^+\rangle$, $|GHZ_{001}^-\rangle$, $|GHZ_{010}^+\rangle$, $|GHZ_{010}^-\rangle$, $|GHZ_{011}^+\rangle$ and $|GHZ_{100}^-\rangle$ respectively.

One factor has already been proved, then we will consider that whether the algorithm QFT is blind or not. The QFT is blind when Bob obtain all the classical information in the protocol, the conditional probability distribution of Bob's rotation operators is equal to the priori probability distribution of Bob's rotation operators. That is, according to Bayes' theorem, we get

$$\begin{aligned}&p(R_y(\frac{\pi}{4})_j \mid \Omega_j=j,\mathrm{QFT}_j)\\ &=\frac{p(\Omega_j=j\mid \mathrm{QFT}_j,R_y(\frac{\pi}{4})_j)p(R_y(\frac{\pi}{4})_j,\mathrm{QFT}_j)}{p(\Omega_j=j,\mathrm{QFT}_j)}\\ &=\frac{p(\Omega_j=j\mid \mathrm{QFT}_j,R_y(\frac{\pi}{4})_j)p(R_y(\frac{\pi}{4})_j)p(\mathrm{QFT}_j)}{p(\Omega_j=j,\mathrm{QFT}_j)p(\mathrm{QFT}_j)}\\ &=p(R_y(\frac{\pi}{4})_j).\end{aligned}$$

where the conditional probability distribution of $R_y(\frac{\pi}{4})_j$, i.e. Bob's knowledges about Alice's rotation angles, is given by QFT_j and $\Omega_j=j$. The equation proves $R_y(\frac{\pi}{4})_j$, QFT_j and $\Omega_j=j$ are completely independent such that $R_y(\frac{\pi}{4})_j$ is unknown to Bob.

At last, we present the outputs are unknown to Bob by the following equation.

$$\begin{aligned}&p(\mathrm{QFT}_j \mid \Omega_j=j,R_z(\frac{\pi}{4})_j)\\ &=\frac{p(\Omega_j=j\mid \mathrm{QFT}_j,R_z(\frac{\pi}{4})_j)p(\mathrm{QFT}_j,R_z(\frac{\pi}{4})_j)}{p(\Omega_j=j\mid R_z(\frac{\pi}{4})_j)p(R_z(\frac{\pi}{4})_j)}\\ &=\frac{p(\Omega_j=j\mid \mathrm{QFT}_j,R_z(\frac{\pi}{4})_j)p(\mathrm{QFT}_j)p(R_z(\frac{\pi}{4})_j)}{p(\Omega_j=j\mid R_z(\frac{\pi}{4})_j)p(R_z(\frac{\pi}{4})_j)}\\ &=p(\mathrm{QFT}_j).\end{aligned}$$

That is, the conditional probability distribution of the final output quantum states is equal to the priori probability distribution of the final output quantum states. It shows that QFT is unknown to Bob as follows. By the same method, for gates $\mathrm{T},\mathrm{Z},\mathrm{CT},\mathrm{CZ},\mathrm{H}$, we have the same conclusions. Therefore, these BQC protocols are blind by analyzing the three points.

In the end, the correctness of these BQC protocols is as follows.

1) For state $|\mathrm{GHZ}^{\pm}_{000}\rangle$, we have

$$\begin{aligned}|\mathrm{GHZ}^{\pm}_{000}\rangle &= \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle)_{123} \\ &\xrightarrow{QFT} \frac{1}{4}[(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \\ &\quad \pm(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{3\pi i}{2}}|1\rangle)(|0\rangle + e^{\frac{7\pi i}{4}}|1\rangle)]_{123}.\end{aligned}$$

Equivalent to

$$\begin{aligned}|\mathrm{GHZ}^{\pm}_{000}\rangle &\xrightarrow{\mathrm{H_2H_3}} \frac{1}{2\sqrt{2}}[|0\rangle(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \pm |1\rangle \\ &\quad (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)]_{123} \\ &\xrightarrow{\mathrm{CT}^{10}_{12}} \frac{1}{4}[|0\rangle(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \pm |1\rangle(|0\rangle + e^{\frac{3\pi i}{2}}|1\rangle) \\ &\quad (|0\rangle - |1\rangle)]_{123} \\ &\xrightarrow{\mathrm{CT}^{11}_{13}} \frac{1}{4}[|0\rangle(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \pm |1\rangle(|0\rangle + e^{\frac{3\pi i}{2}}|1\rangle) \\ &\quad (|0\rangle + e^{\frac{7\pi i}{4}}|1\rangle)]_{123} \\ &\xrightarrow{\mathrm{H_1}} \frac{1}{4}[(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \pm (|0\rangle - |1\rangle) \\ &\quad (|0\rangle + e^{\frac{3\pi i}{2}}|1\rangle)(|0\rangle + e^{\frac{7\pi i}{4}}|1\rangle)]_{123}.\end{aligned}$$

2) For state $|\mathrm{GHZ}^{\pm}_{001}\rangle$, we have

$$\begin{aligned}|\mathrm{GHZ}^{\pm}_{001}\rangle &= \frac{1}{\sqrt{2}}(|001\rangle \pm |110\rangle)_{123} \\ &\xrightarrow{QFT} \frac{1}{4}[(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle)(|0\rangle + e^{\frac{\pi i}{4}}|1\rangle) \\ &\quad \pm(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{3\pi i}{2}}|1\rangle)]_{123}.\end{aligned}$$

Equivalent to

$$\begin{aligned}|\mathrm{GHZ}^{\pm}_{001}\rangle &\xrightarrow{\mathrm{X_1X_3}} \frac{1}{\sqrt{2}}(|100\rangle \pm |011\rangle)_{123} \\ &\xrightarrow{\mathrm{H_3}} \frac{1}{2}[|10\rangle(|0\rangle + |1\rangle) \pm |01\rangle(|0\rangle - |1\rangle)]_{123} \\ &\xrightarrow{\mathrm{CT_{13}}} \frac{1}{2}[|10\rangle(|0\rangle + e^{\frac{\pi i}{4}}|1\rangle) \pm |01\rangle(|0\rangle - |1\rangle)]_{123} \\ &\xrightarrow{\mathrm{CT}^{10}_{23}} \frac{1}{2}[|10\rangle(|0\rangle + e^{\frac{\pi i}{4}}|1\rangle) \pm |01\rangle(|0\rangle + e^{\frac{3\pi i}{2}}|1\rangle)]_{123} \\ &\xrightarrow{\mathrm{H_2}} \frac{1}{2\sqrt{2}}[|1\rangle(|0\rangle + |1\rangle)(|0\rangle + e^{\frac{\pi i}{4}}|1\rangle) \\ &\quad \pm|0\rangle(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{3\pi i}{2}}|1\rangle)]_{123} \\ &\xrightarrow{\mathrm{CT}^{2}_{12}} \frac{1}{2\sqrt{2}}[|1\rangle(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle)(|0\rangle + e^{\frac{\pi i}{4}}|1\rangle) \\ &\quad \pm|0\rangle(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{3\pi i}{2}}|1\rangle)]_{123} \\ &\xrightarrow{\mathrm{H_1}} \frac{1}{4}[(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle)(|0\rangle + e^{\frac{\pi i}{4}}|1\rangle) \\ &\quad \pm(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{3\pi i}{2}}|1\rangle)]_{123}.\end{aligned}$$

3) For state $|\mathrm{GHZ}^{\pm}_{010}\rangle$, we have

$$\begin{aligned}|\mathrm{GHZ}^{\pm}_{010}\rangle &= \frac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle)_{123} \\ &\xrightarrow{QFT} \frac{1}{4}[(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle) \\ &\quad \pm(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle)(|0\rangle + e^{\frac{5\pi i}{4}}|1\rangle)]_{123}.\end{aligned}$$

Equivalent to

$$\begin{aligned}|\mathrm{GHZ}^{\pm}_{010}\rangle &\xrightarrow{\mathrm{H_3}} \frac{1}{2}[|01\rangle(|0\rangle + |1\rangle) \pm |10\rangle(|0\rangle - |1\rangle)]_{123} \\ &\xrightarrow{\mathrm{CT}^{2}_{23}} \frac{1}{2}[|01\rangle(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle) \pm |10\rangle(|0\rangle - |1\rangle)]_{123} \\ &\xrightarrow{\mathrm{CT}^{9}_{13}} \frac{1}{2}[|01\rangle(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle) \pm |10\rangle(|0\rangle + e^{\frac{5\pi i}{4}}|1\rangle)]_{123} \\ &\xrightarrow{\mathrm{H_2}} \frac{1}{2\sqrt{2}}[|0\rangle(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle) \\ &\quad \pm|1\rangle(|0\rangle + |1\rangle)(|0\rangle + e^{\frac{5\pi i}{4}}|1\rangle)]_{123} \\ &\xrightarrow{\mathrm{CT}^{2}_{12}} \frac{1}{2\sqrt{2}}[|0\rangle(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle) \\ &\quad \pm|1\rangle(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle)(|0\rangle + e^{\frac{5\pi i}{4}}|1\rangle)]_{123} \\ &\xrightarrow{\mathrm{H_1}} \frac{1}{4}[(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle) \\ &\quad \pm(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle)(|0\rangle - e^{\frac{5\pi i}{4}}|1\rangle)]_{123}.\end{aligned}$$

4) For state $|\mathrm{GHZ}^{\pm}_{100}\rangle$, we have

$$\begin{aligned}|\mathrm{GHZ}^{\pm}_{010}\rangle &= \frac{1}{\sqrt{2}}(|010\rangle \pm |101\rangle)_{123} \\ &\xrightarrow{QFT} \frac{1}{4}[(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle)(|0\rangle + e^{\frac{3\pi i}{4}}|1\rangle) \\ &\quad \pm(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)]_{123}.\end{aligned}$$

Equivalent to

$$\begin{aligned}|\mathrm{GHZ}^{\pm}_{010}\rangle &\xrightarrow{\mathrm{X_1X_3}} \frac{1}{\sqrt{2}}(|110\rangle \pm |001\rangle)_{123} \\ &\xrightarrow{\mathrm{H_2H_3}} \frac{1}{2\sqrt{2}}[|1\rangle(|0\rangle - |1\rangle)(|0\rangle + |1\rangle) \\ &\quad \pm|0\rangle(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)]_{123} \\ &\xrightarrow{\mathrm{CT}^{6}_{12}} \frac{1}{2\sqrt{2}}[|1\rangle(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle)(|0\rangle + |1\rangle) \\ &\quad \pm|0\rangle(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)]_{123} \\ &\xrightarrow{\mathrm{CT}^{3}_{13}} \frac{1}{2\sqrt{2}}[|1\rangle(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle)(|0\rangle + e^{\frac{3\pi i}{4}}|1\rangle) \\ &\quad \pm|0\rangle(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)]_{123} \\ &\xrightarrow{\mathrm{H_1}} \frac{1}{4}[(|0\rangle - |1\rangle)(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle)(|0\rangle + e^{\frac{3\pi i}{4}}|1\rangle) \\ &\quad \pm(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)]_{123}.\end{aligned}$$

In a word, we successfully prove the blindness and correctness of all BQC protocols.

V. CONCLUSION

In this paper, we propose a new blind quantum computation protocol of quantum Fourier transform performed on multi-qubit states. The quantum Fourier transform can be composed of $R_y(\frac{\pi}{4})$ and $R_z(\frac{\pi}{4})$ completely, this reduces the kinds of gates for Bob. We analyze and construct the BQC protocols of three-qubit QFT performed three-qubit states, where the three-qubit states with GHZ state and W state as a simple example to clearly express the QFT. After that, we immediately extend them to multi-QFT performed on multi-qubit states, the relevant BQC protocols are given similarly. In the end, we prove blindness and correctness of all BQC protocols. Since all protocols are implemented crossways, only a unified proof of blindness is given, but the correctness is proved respectively.

ACKNOWLEDGMENTS

This work was supported by National Key R&D Plan of China (Grant No. 2017YFB0802203), National Natural Science Foundation of China (Grant Nos. U173620045, 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), Natural 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, Special Program for Applied Research on Super Computation of the NSFC-Guangdong Joint Fund (the second phase), under Grant No.U1501501, 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] C. Greganti, M. C. Roehsner, S. Barz, T. Morimae, P. Walther, Demonstration of measurement-only blind quantum computing, New J. Phys. 18 (2016) 013020.
[3] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, P. Walther, Demonstration of blind quantum computing, Science 335 (2012) 303–308.
[4] T. Morimae, K. Fujii, Secure entanglement distillation for double-server blind quantum computation, Phys. Rev. Lett. 111 (2013) 020502.
[5] L. Qin, C. W. Hong, W. Chunhui, W. Zhonghua, Triple-server blind quantum computation using entanglement swapping, Phys. Rev. A 89 (2014) 040302.
[6] Y.-B. Sheng, L. Zhou, Deterministic entanglement distillation for secure double-server blind quantum computation, Sci. Rep. 5 (2015) 7815.
[7] T. Morimae, K. Fujii, Blind topological measurement-based quantum computation, Nat. Commun. 3 (2012) 1036.
[8] T. Morimae, V. Dunjko, E. Kashefi, Ground state blind quantum computation on aklt states, Quantum Inf. Computat. 15 (2015) 200–234.
[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. Koshiba, T. Morimae, Ancilla-driven universal blind quantum computation, Phys. Rev. A 87 (2013) 060301.
[13] T. Morimae, Verification for measurement-only blind quantum computing, Phys. Rev. A 89 (2014) 060302.
[14] M. Hayashi, T. Morimae, Verifiable measurement-only blind quantum computing with stabilizer testing, Phys. Rev. Lett. 115 (2015) 220502.
[15] A. Gheorghiu, E. Kashefi, P. Wallden, Robustness and device independence of verifiable blind quantum computing, New J. Phys. 17 (2015) 083040.
[16] J. Fitzsimons, E. Kashefi, Unconditionally verifiable blind quantum computations, arXiv:1203.5217v3.
[17] M. Hajdusek, C. A. Pérez-Delgado, J. Fitzsimons, Device-independent verifiable blind quantum computation, arXiv:1502.02563v2.
[18] K. Fujii, M. Hayashi, Verifiable fault-tolerance in measurement-based quantum computation, arXiv:1610.05216v1.
[19] T. Morimae, Measurement-only verifiable blind quantum computing with quantum input verification, Phys. Rev. A 94 (2016) 042301.
[20] A. Broadbent, How to verify a quantum computation, arXiv:1509.09180v3.
[21] V. Dunjko, E. Kashefi, Blind quantum computing with two almost identical states., arXiv:1604.01586.
[22] C. A. Pérez-Delgado, J. F. Fitzsimons, Iterated gate teleportation and blind quantum computation, Phys. Rev. Lett. 114 (2015) 220502.
[23] Y.-B. Sheng, L. Zhou, Blind quantum computation with noise environment, arXiv:1609.08902v1.
[24] Y. Takeuchi, K. Fujii, R. Ikuta, T. Yamamoto, N. Imoto, Blind quantum computation over a collective-noise channel, Phys. Rev. A 93 (2016) 052307.
[25] T. Kapourniotis, V. Dunjko, E. Kashefi, On optimising quantum communication in verifiable quantum computing, arXiv:1506.06943.
[26] Y. Takeuchi, K. Fujii, T. Morimae, N. Imoto, Practically verifiable blind quantum computation with acceptance rate amplification, arXiv:1607.01568.
[27] E. Kashefi, P. Wallden, Optimised resource construction for verifiable quantum computation, J. Phys. A Math. Theor. 50.
[28] K. Honda, Publicly verifiable blind quantum computation, arXiv:1604.00116.
[29] A. Mantri, C. A. Pérez-Delgado, J. F. Fitzsimons, Optimal blind quantum computation, Phys. Rev. Lett. 111 (2013) 230502.
[30] V. Giovannetti, L. Maccone, T. Morimae, T. G. Rudolph, Efficient universal blind quantum computation, Phys. Rev. Lett. 111 (2013) 230501.
[31] V. Dunjko, E. Kashefi, A. Leverrier, Blind quantum computing with weak coherent pulses, Phys. Rev. Lett. 108 (2012) 200502.

[32] Z. Sun, J. Yu, P. Wang, L. Xu, Symmetrically private information retrieval based on blind quantum computing, Phys. Rev. A 91 (2015) 052303.

[33] 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.

[34] S. Aaronson, A. Cojocaruy, A. Gheorghiuz, E. Kashefix, On the implausibility of classical client blind quantum computing, ArXiv:1704.08482v1.

[35] 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.

[36] 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.

[37] J. F. Fitzsimons, Private quantum computation: an introduction to blind quantum computing and related protocols, npj Quantum Information 3 (2017) 1–11.

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

[39] Y. Gao, H. Zhou, D. Zou, X. Peng, J. Du, Preparation of greenberger-horne-zeilinger and w states on a one-dimensional ising chain by global control, Phys. Rev. A 87 (2013) 032335.

[40] J. Chen, H. Zhou, C. Duan, X. Peng, Preparing greenberger-horne-zeilinger and w states on a long-range ising spin model by global controls, Phys. Rev. A 95 (2017) 032340.

[41] Y. S. Nam, R. Blümel, Robustness of the quantum fourier transform with respect to static gate defects, Phys. Rev. A 89 (2014) 769–772.

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

[43] C. Moore, D. Rockmore, A. Russell, Generic quantum fourier transforms, Journal ACM Transactions on Algorithms (TALG) 2(4) (2006) 707–723.