ISSN 1674-1056
http://cpb.iphy.ac.cn
http://iopscience.iop.org/cpb
中国物理 B
Chinese Physics
中国物理 Chinese Physics B

Realization of *t*-bit semiclassical quantum Fourier transform on IBM's quantum cloud computer

Xiang-qun Fu(付向群), Wan-su Bao(鲍皖苏), He-liang Huang(黄合良), Tan Li(李坦), Jian-hong Shi(史建红), Xiang Wang(汪翔), Shuo Zhang(张硕), Feng-guang Li(李风光)

Citation: Chin. Phys. B . 2019, 28(2): 020302. **doi:** 10.1088/1674-1056/28/2/020302
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

MatCloud, a high-throughput computational materials infrastructure: Present, future visions, and challenges

Xiaoyu Yang(杨小渝), Zongguo Wang(王宗国), Xushan Zhao(赵旭山), Jianlong Song(宋健龙), Chao Yu(虞超), Jiaxin Zhou(周嘉欣), Kai Li(李凯)
Chin. Phys. B . 2018, 27(11): 110301. **doi:** 10.1088/1674-1056/27/11/110301

Fabrication of Al air-bridge on coplanar waveguide

Zhen-Chuan Jin(金震川), Hai-Teng Wu(吴海腾), Hai-Feng Yu(于海峰), Yang Yu(于扬)
Chin. Phys. B . 2018, 27(10): 100310. **doi:** 10.1088/1674-1056/27/10/100310

Spin manipulation in semiconductor quantum dots qubit

Ke Wang(王柯), Hai-Ou Li(李海欧), Ming Xiao(肖明), Gang Cao(曹刚), Guo-Ping Guo(郭国平)
Chin. Phys. B . 2018, 27(9): 090308. **doi:** 10.1088/1674-1056/27/9/090308

Solid-state quantum computation station

Fanming Qu(屈凡明), Zhongqing Ji(姬忠庆), Ye Tian(田野), Shiping Zhao(赵士平)
Chin. Phys. B . 2018, 27(7): 070301. **doi:** 10.1088/1674-1056/27/7/070301

Realization of quantum Fourier transform over Z_N

Fu Xiang-Qun, Bao Wan-Su, Li Fa-Da, Zhang Yu-Chao
Chin. Phys. B . 2014, 23(2): 020306. **doi:** 10.1088/1674-1056/23/2/020306

Realization of t-bit semiclassical quantum Fourier transform on IBM's quantum cloud computer*

Xiang-Qun Fu(付向群)[1,2], Wan-Su Bao(鲍皖苏)[1,2,†], He-Liang Huang(黄合良)[1,2], Tan Li(李坦)[1,2], Jian-Hong Shi(史建红)[1,2], Xiang Wang(汪翔)[1,2], Shuo Zhang(张硕)[1,2], and Feng-Guang Li(李风光)[1,2]

[1] *Henan Key Laboratory of Quantum Information and Cryptography, Information Engineering University, Zhengzhou* 450004, *China*
[2] *Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026, *China*

(Received 9 July 2018; revised manuscript received 28 November 2018; published online 10 January 2019)

To overcome the difficulty of realizing large-scale quantum Fourier transform (QFT) within existing technology, this paper implements a resource-saving method (named t-bit semiclassical QFT over Z_{2^n}), which could realize large-scale QFT using an arbitrary-scale quantum register. By developing a feasible method to realize the control quantum gate R_k, we experimentally realize the 2-bit semiclassical QFT over Z_{2^3} on IBM's quantum cloud computer, which shows the feasibility of the method. Then, we compare the actual performance of 2-bit semiclassical QFT with standard QFT in the experiments. The squared statistical overlap experimental data shows that the fidelity of 2-bit semiclassical QFT is higher than that of standard QFT, which is mainly due to fewer two-qubit gates in the semiclassical QFT. Furthermore, based on the proposed method, $N = 15$ is successfully factorized by implementing Shor's algorithm.

Keywords: quantum cloud computation, quantum Fourier transform, semiclassical quantum Fourier transform, Shor's algorithm

PACS: 03.67.Lx, 03.67.–a **DOI:** 10.1088/1674-1056/28/2/020302

1. Introduction

The quantum algorithm[1,2] greatly threatens the current cryptography, especially public-key cryptography, whose security is based on the factorization and discrete logarithm,[3,4] which can be easily broken by Shor's algorithm. Considerable attention has since been paid to research on quantum computation.[5–12] Usually, the quantum algorithm is composed of different quantum transforms, where the quantum Fourier transform (QFT) is one of the most important transforms. It can be used not only to prepare the equal superposition state but also to increase the success probability of the quantum algorithms, such as Shor's algorithm. In 1994, Coppersmith[13] presented the circuit for the QFT over Z_{2^n}, which needs n qubits, n single-qubit gates, and $n(n+2)/2$ two-qubit gates. Thus, realizing the QFT over Z_{2^n} for larger n using this scheme is very resource-consuming.

In 1996, Griffiths and Niu[14] presented the single-bit semiclassical QFT over Z_{2^n}, which requires only one qubit and 2 single-qubit gates. Thus, in their scheme, not only the quantum computational resources but also the implementation difficulty has been reduced (two-qubit controlled gate is more difficult to realize than single-qubit gate in experiments). In addition, Chiaverini *et al.*[15] experimentally implemented this kind of single-bit semiclassical QFT over Z_{2^3} on the ion-trap system in 2005, which demonstrated the feasibility of the semiclassical QFT. In 2000, based on the single-bit semiclassical QFT, Parker *et al.*[16] presented a circuit with $n+1$ qubits for factorization problem. While, based on the QFT, $3n+O(\log N)$ qubits is needed[17] (N is an integer and $n = \lceil \log_2 N \rceil$). Thus, the single-bit semiclassical QFT is a candidate solution to implement the large-scale QFT, with which Shor's algorithm may be applied to break the public-key cryptology (*e.g.*, Rivest–Shamir–Adleman (RSA) and elliptic-curve cryptography (ECC)) under the condition of limited computation resources.

Although the single-bit semiclassical QFT over Z_{2^n} needs less quantum computation resources than the QFT over Z_{2^n}, the implementation speed is slower. To overcome this drawback, t-bit semiclassical QFT over Z_{2^n} is presented,[18] which can balance the tradeoff between quantum resource and speed in the implementation of QFT. Thus, how to realize this method on a quantum computer is worth studying.

In this paper, we realize the t-bit semiclassical QFT over Z_{2^n}. To explore the actual performance of QFT, we realize the 2-bit semiclassical QFT over Z_{2^3} on IBM's quantum cloud quantum computer. This method may provide a feasible route to realize the QFT over Z_{2^n}.

2. The QFT over Z_{2^n}

Definition 1 The quantum Fourier transform (QFT)[17] on an orthonormal basis $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ is defined to be a

*Project supported by the National Basic Research Program of China (Grant No. 2013CB338002) and the National Natural Science Foundation of China (Grant No. 61502526).

†Corresponding author. E-mail: 2010thzz@sina.com

© 2019 Chinese Physical Society and IOP Publishing Ltd

linear operator $U_{\rm F}$ with the following action on the basis states:

$$U_{\rm F}:|j\rangle \mapsto \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\omega_N^{jk}|k\rangle. \tag{1}$$

So, the action on an arbitrary state can be written as

$$U_{\rm F}:\sum_{j=0}^{N-1}x_j|j\rangle \mapsto \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\sum_{j=0}^{N-1}x_j\omega_N^{jk}|k\rangle, \tag{2}$$

where $\mathrm{i}=\sqrt{-1}$, $\omega_N=\mathrm{e}^{2\pi\mathrm{i}/N}$, and the symbol "$\mapsto$ " stands for that the transform is invertible.

When $N=2^n$, the QFT $U_{\rm F}$ on the state $|a\rangle$ is given as

$$U_{\rm F}|a\rangle=\bigotimes_{j=0}^{n-1}\left|p(\phi_j)\right\rangle, \tag{3}$$

where $U_{\rm F}$ is also called the QFT over Z_{2^n}, $a=\sum_{j=0}^{n-1}a_j2^j$ in the binary representation (a_j is 0 or 1), $|p(\phi)\rangle=(|0\rangle+\mathrm{e}^{2\pi\mathrm{i}\phi}|1\rangle)/\sqrt{2}$, and $\phi_j=\sum_{k=0}^{n-j}a_k2^{j+k-n-1}$ for $j=0,1,\ldots,n-1$.

The QFT is a usual transform in quantum algorithms, which can be applied to prepare the superposition state. The circuit for the QFT over Z_{2^n} needs n qubits, n single-qubit gates, and $n(n+2)/2$ two-qubit gates, which is designed by Coppersmith,[13] and the circuit is called standard QFT.

Based on the standard QFT, the QFT over Z_{2^n} cannot be realized within existing technology for larger n. In 1996, Griffiths and Niu[14] presented a method that only required one qubit and 2 single-qubit gates to implement the QFT, which was called single-bit semiclassical QFT over Z_{2^n}.

Single-bit semiclassical QFT over Z_{2^n} transforms each basis state $|a\rangle=|a_{n-1},\ldots,a_0\rangle$ into $|c\rangle=|c_{n-1},\ldots,c_0\rangle$ with a measuring probability equal to that of QFT.[14] Thus, the single-bit semiclassical QFT over Z_{2^n} can realize QFT and $|a\rangle$'s input is from left to right by bit flipping. That is to say, single-bit semiclassical QFT over Z_{2^n} can carry out the parallel computing of 2^n inputs within n steps. Compared to standard QFT, single-bit semiclassical QFT over Z_{2^n} requires less quantum computation resources through measurement after transforming each bit. The 1 qubit can be applied cyclically to prepare $|a_{n-1}\rangle,\ldots,|a_0\rangle$,[16] and the quantum gate can also be cyclically used, which requires the preparation of superposition $(|0\rangle+|1\rangle)/\sqrt{2}$ n times. The measurement result of each qubit needs feedback to the next qubit, which is applied to control the quantum gate. However, the measurement result of the full QFT does not require feedback and the quantum gates on each qubit can run simultaneously. Thus, the full QFT has a higher implementation speed than the single-bit semiclassical QFT.

3. The t-bit semiclassical QFT over Z_{2^n}

3.1. The t-bit semiclassical QFT over Z_{2^n}

The standard QFT has a higher implementation speed but needs more quantum computation resources, whereas the single-bit semiclassical QFT needs less resources but has lower speed. To overcome the disadvantages of both methods, t-bit semiclassical QFT over Z_{2^n} is presented in Ref. [18], and its circuit is shown in Fig. 1.

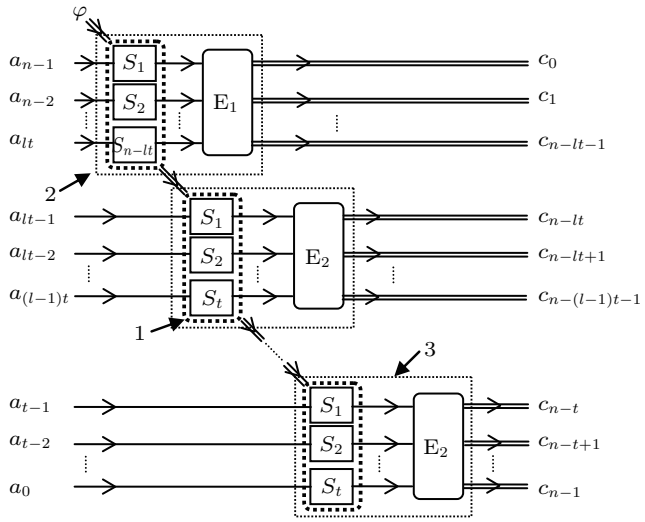


Fig. 1. The circuit for t-bit semiclassical QFT over Z_{2^n}.

The explanation of Fig. 1 is shown as follows:

(i) Each virtual box with a bold line denotes VB1 while the one with fine line which contains E_1 denotes VB2, and the one with fine line which contains E_2 denotes VB3, where E_1 is the QFT over $Z_{2^{n-lt}}$ and E_2 is the QFT over Z_{2^t}. The circuit for E_1 and E_2 can refer to Ref. [13];

(ii) VB2 outputs $c_{n-lt-1},c_{n-lt-2},\ldots,c_0$,

$$\varphi'=\frac{c_0}{2^{n-lt+1}}+\cdots+\frac{c_{n-lt-1}}{2^2};$$

If VB3 inputs $a'_{t-1},a'_{t-2},\ldots,a'_0$, it outputs $c'_{t-1},c'_{t-2},\ldots,c'_0$,

$$\varphi'=\frac{\varphi}{2^t}+\frac{c'_0}{2^{t+1}}+\cdots+\frac{c'_{t-1}}{2^2};\quad S_k=\begin{bmatrix}1 & 0\\ 0 & \mathrm{e}^{2\pi\mathrm{i}\varphi/2^{k-1}}\end{bmatrix}$$

for $k=1,2,\ldots,t$, where φ' is the input of the next VB1, and the initial value of φ is 0;

(iii) The final measurement c is $\sum_{j=0}^{n-1}2^jc_j$;

(iv) The single line represents quantum signal and double line represents classical signal.

3.2. Realization of t-bit semiclassical QFT over Z_{2^n}

In 2016, IBM opened the first 5-qubit quantum cloud computer.[19] We will study how to implement the QFT on IBM's quantum cloud computer, which provides limited quantum gates, as follows:

$$U_1(\lambda)=\begin{bmatrix}1 & 0\\ 0 & \mathrm{e}^{\lambda\mathrm{i}}\end{bmatrix},\quad U_2(\lambda,\varphi)=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -\mathrm{e}^{\lambda\mathrm{i}}\\ \mathrm{e}^{\varphi\mathrm{i}} & \mathrm{e}^{(\lambda+\varphi)\mathrm{i}}\end{bmatrix},$$

$$U_3(\theta,\lambda,\varphi)=\begin{bmatrix}\cos(\theta/2) & -e^{\lambda i}\sin(\theta/2)\\ e^{\varphi i}\sin(\theta/2) & e^{(\lambda+\varphi)i}\cos(\theta/2)\end{bmatrix},$$

$$\oplus=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix},\quad H=\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix},$$

$$S=\begin{bmatrix}1&0\\0&i\end{bmatrix},\quad \text{and}\quad T=\begin{bmatrix}1&0\\0&(1+i)/\sqrt{2}\end{bmatrix}.$$

The controlled-S_j gate is one of the most important gates used in Fig. 1(a). However, $\oplus$ is the only two-qubit gate on IBM's quantum cloud computer. Thus, we design a circuit for controlled-S_j gate according to the circuit for arbitrary controlled-U gate by single-qubit gate and $\oplus$ gate in Ref. [17], which is shown in Fig. 2.

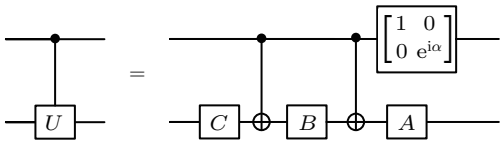


Fig. 2. The circuit for controlled-U gate.

Note that in Fig. 2, α, A, B, and C satisfy $U=e^{i\alpha}AXBXC$ and $ABC=I$, where A, B, and C are all single-qubit gate, $X=\left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right]$, and $I=\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]$.

Take controlled-S_4 gate as an example, which can be realized by $U_1(\pi/32)$, $U_1(-\pi/16)$, $U_1(\pi/32)$, and $\alpha=\pi/16$ (based on Matlab software). The circuit is shown in Fig. 3.

When the input state is $|00\rangle$, the running result of Fig. 3 is shown in Fig. 4. To quantitatively evaluate the performance, we use the squared statistical overlap[20] of experimental data with the ideal values, which is defined as $\gamma=\left(\sum_{y=0}^{3}\sqrt{m_y e_y}\right)^2$, where m_y and e_y are the measured and expected output-state probabilities of the state $|y\rangle$, respectively. From the data in Fig. 4, we find $\gamma=0.956$, which indicates a near-perfect experimental accuracy. Thus, the circuit in Fig. 3 can realize the controlled-S_4 gate.

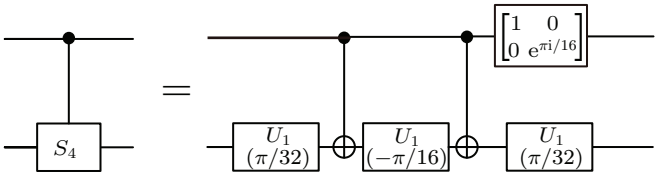


Fig. 3. The circuit for the controlled-S_4 gate on IBM's quantum cloud computer.

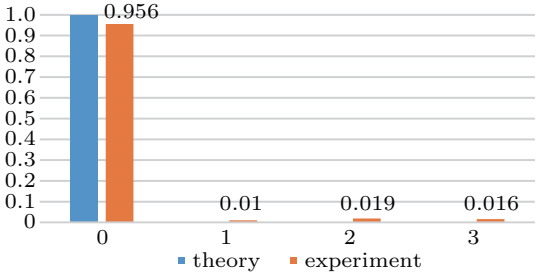


Fig. 4. The running result of the controlled-S_4 gate. The horizontal axis represents the measurement result, and the vertical axis represents the measuring probability.

Based on the circuit in Fig. 3, we design the method to realize it on IBM's quantum cloud computer, which verifies the feasibility (taking 2-bit semiclassical QFT over Z_{2^3} as an example).

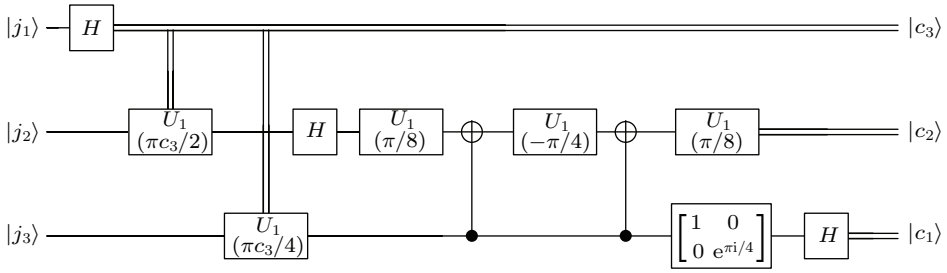


Fig. 5. The circuit for 2-bit semiclassical QFT over Z_{2^3} on IBM's quantum cloud computer.

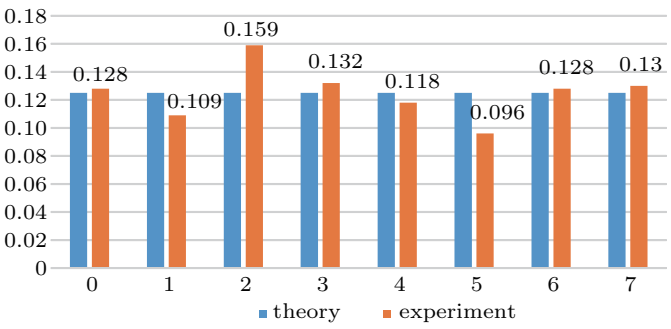


Fig. 6. The running result of 2-bit semiclassical QFT over Z_{2^3}. The horizontal axis represents the result $c=\sum_{k=1}^{3}2^{3-k}c_k$, and the vertical axis represents the measuring probability.

When the input state is $|j_1j_2j_3\rangle=|000\rangle$, the running result of the above circuit is shown in Fig. 6. The squared statistical overlap of experimental data with the ideal values is $\gamma'=0.9952$, indicating a near-perfect experimental accuracy. Thus, the circuit in Fig. 5 can realize 2-bit semiclassical QFT over Z_{2^3}, *i.e.*, t-bit semiclassical QFT over Z_{2^n} can be applied to realize the QFT over Z_{2^n}. And 2-bit semiclassical QFT over Z_{2^3} requires two qubits and two $\oplus$ gates.

And t-bit semiclassical QFT over Z_{2^n} is theoretically superior to the QFT over Z_{2^n}. For the sake of comparison, we realize the standard QFT over Z_{2^n}. The circuit for the standard QFT over Z_{2^3} can be designed as Fig. 7, which can be implemented on IBM's quantum cloud computer.

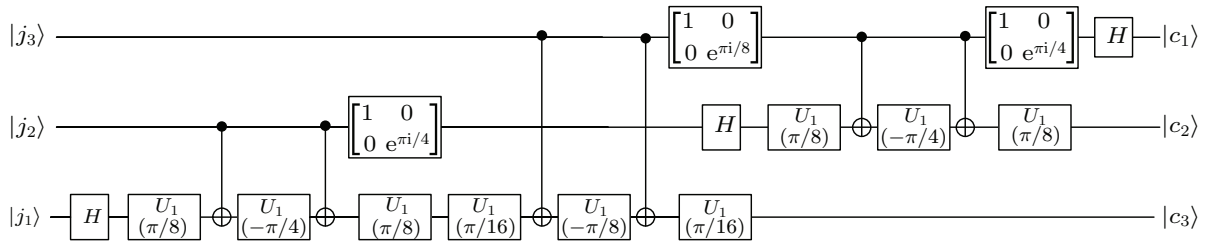


Fig. 7. The circuit for the standard QFT over Z_{2^3} on IBM's quantum cloud computer.

When the input state is $|j_1 j_2 j_3\rangle = |000\rangle$, the running result of the above circuit is shown in Fig. 8. The squared statistical overlap of experimental data with the ideal values is $\gamma' = 0.9355$, indicating a near-perfect experimental accuracy. The standard QFT over Z_{2^3} requires 3 qubits and 6 $\oplus$ gates.

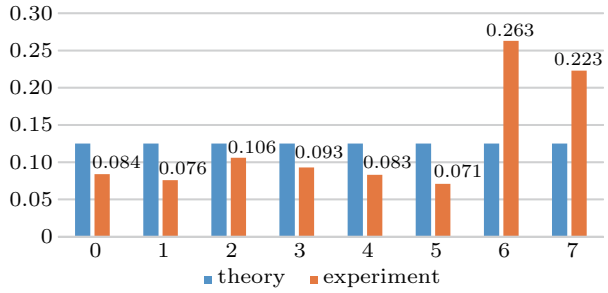


Fig. 8. The running result of the standard QFT over Z_{2^3}. The horizontal axis represents the result $c = \sum_{k=1}^{3} 2^{3-k} c_k$, and the vertical axis represents the measuring probability.

3.3. Advantage of t-bit semiclassical QFT over Z_{2^n}

According to Subsection 3.2, we can obtain Table 1.

Table 1. The comparison of 2-bit semiclassical QFT over Z_{2^3} and standard QFT over Z_{2^3}.

	2-bit semiclassical QFT over Z_{2^3}	Standard QFT over Z_{2^3}
Qubit	2	3
$\oplus$ gate	2	6
Squared statistical overlap of experimental data with the ideal values	0.9952	0.9355

Compared with the standard QFT over Z_{2^3}, 2-bit semiclassical QFT over Z_{2^3} requires less qubits and $\oplus$ gates. The fidelity and squared statistical overlap of 2-bit semiclassical QFT is also higher (the fewer the two-qubit gate is needed, the higher the fidelity is). Thus, 2-bit semiclassical QFT is superior to the standard QFT, and it may be more suitable for realizing the QFT.

Furthermore, from Figs. 1 and 5, we can see that it takes only two qubits to realize the QFT over Z_{2^n} based on 2-bit semiclassical QFT. That is, t-bit semiclassical QFT over Z_{2^n} is a candidate solution of implementing a large-scale QFT. The QFT over Z_{2^n} can be realized on IBM's quantum cloud computer by t-bit semiclassical QFT over Z_{2^n}, where $t \leq 5$. Thus, the method shows a good scalability.

How to reduce the required quantum resource, especially the qubit, is a popular research question. The semi-quantum model can also reduce the quantity of qubit.[21,22] The most important reason is that the quantum algorithm can be realized by a set of individual genuine quantum computers with a small amount of qubits. There are two differences between the semi-quantum computing model and the semiclassical method.

(i) In the semi-quantum computing model, the quantum algorithm is divided into multiple tasks that can be processed in parallel. Each task is not intended to solve a whole algorithmic problem but is just a part, a subroutine, consistent with their supported number of qubits and coherence time. In the semiclassical method, the quantum transform is divided into multiple steps that can be processed serially. The number of steps is polynomial, *i.e.*, it will not increase the computation complexity of the quantum algorithm.

(ii) In the semi-quantum computing model, the final measurement result of each task does not require feedback to control any quantum gate. In the semiclassical method, the final measurement result should be feedback to control the quantum gate of the next step.

Thus, the semi-quantum computing model is intrinsically different from the semiclassical method. In this manuscript, the semiclassical method is applied to realize the QFT. However, the QFT is also one important transform in the semi-quantum computing model.[23] The semiclassical QFT may be applied in the semi-quantum computing model, and the required qubits for realizing quantum algorithm will be further reduced.

4. Realization of Shor's quantum algorithm

In this section, based on t-bit semiclassical QFT, we realize Shor's algorithm, which can further demonstrate the feasibility of the method. The application process of Shor's algorithm may be accelerated under the condition of limited computation resources.

Shor's algorithm was presented in 1994, which can break the RSA public-key crypto. The strategy for quantum factoring a composite number $N = pq$, with both p and q being odd primes, is as follows.[1]

First, we choose x, which is coprime to N.

Next, two registers of qubits are used: the first register with $n = 2\lceil \log_2 N \rceil$ qubits and the second with $l = \lceil \log_2 N \rceil$ qubits, which are initialized in the quantum state $|0\rangle^{\otimes n} |0\rangle^{\otimes l}$. The first register becomes $\frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} |j\rangle |0\rangle$ after applying QFT over Z_{2^n}.

Next, by computing modular exponential function $x^j \bmod N$ in the second register, it will become $\frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} |j\rangle \left|x^j \bmod N\right\rangle$.

Then, applying QFT over Z_{2^n} on the first register, we can obtain

$$\frac{1}{2^n} \sum_{j=0}^{2^n-1} \sum_{c=0}^{2^n-1} \mathrm{e}^{2\pi \mathrm{i} jc/2^n} |c\rangle \left|x^j \bmod N\right\rangle.$$

Finally, we observe the machine. We will then obtain c solely in the first register.

Shor proved that period r can be obtained by using a continued fraction expansion of $c/2^n$; when

$$\left| \frac{c}{2^n} - \frac{d}{r} \right| \leq \frac{1}{2^{n+1}},$$

period r is the smallest positive satisfying $x^r \bmod N = 1$ and $d = [rc/2^n]$. Based on this period r, at least one nontrivial factor of N can be given by the greatest common divisor (GCD) of $(x^{r/2} \pm 1) \bmod N$ with probability greater than $1/2$.[17]

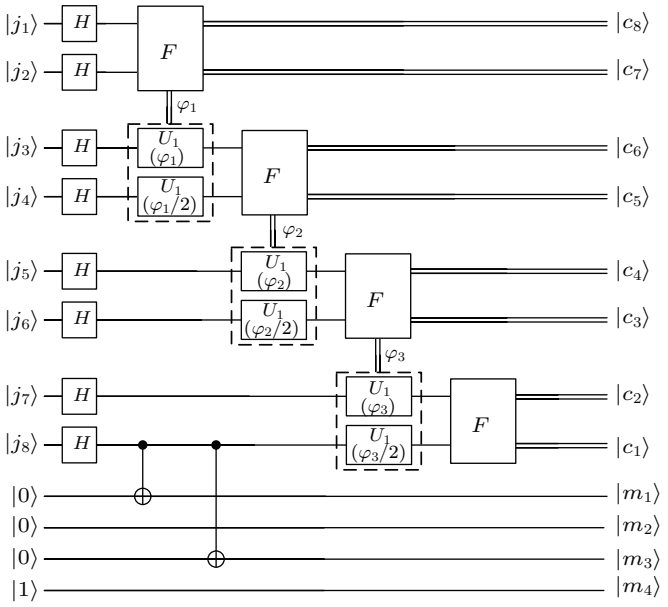


Fig. 9. The circuit for Shor's quantum algorithm based on the t-bit semiclassical QFT.

It is apparent that Shor's factorization algorithm needs $3\lceil \log_2 N \rceil$ qubits, where the QFT needs $2\lceil \log_2 N \rceil$ qubits. For $N = 15$, the QFT over Z_{2^8} in Shor's algorithm cannot be realized on IBM's 5-qubit quantum cloud computer. Luckily, the QFT can be realized by the t-bit semiclassical QFT, and then Shor's factorization algorithm can be realized. The circuit is designed as Fig. 9, where $x = 11$ and $t = 2$.

The explanation of Fig. 9 is shown as follows:

i) $\varphi_1 = (c_8/4 + c_7/2)\pi$, $\varphi_2 = (c_8/16 + c_7/8 + c_6/4 + c_5/2)\pi$, and $\varphi_3 = (c_8/64 + c_7/32 + c_6/16 + c_5/8 + c_4/4 + c_3/2)\pi$.

ii) The circuit of $11^a \bmod 15$ is quoted from Refs. [24] and [25], which only requires two qubits.

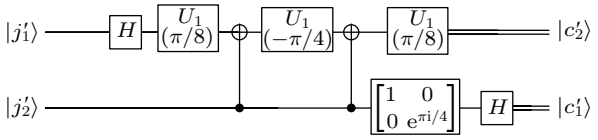


Fig. 10. The circuit for F.

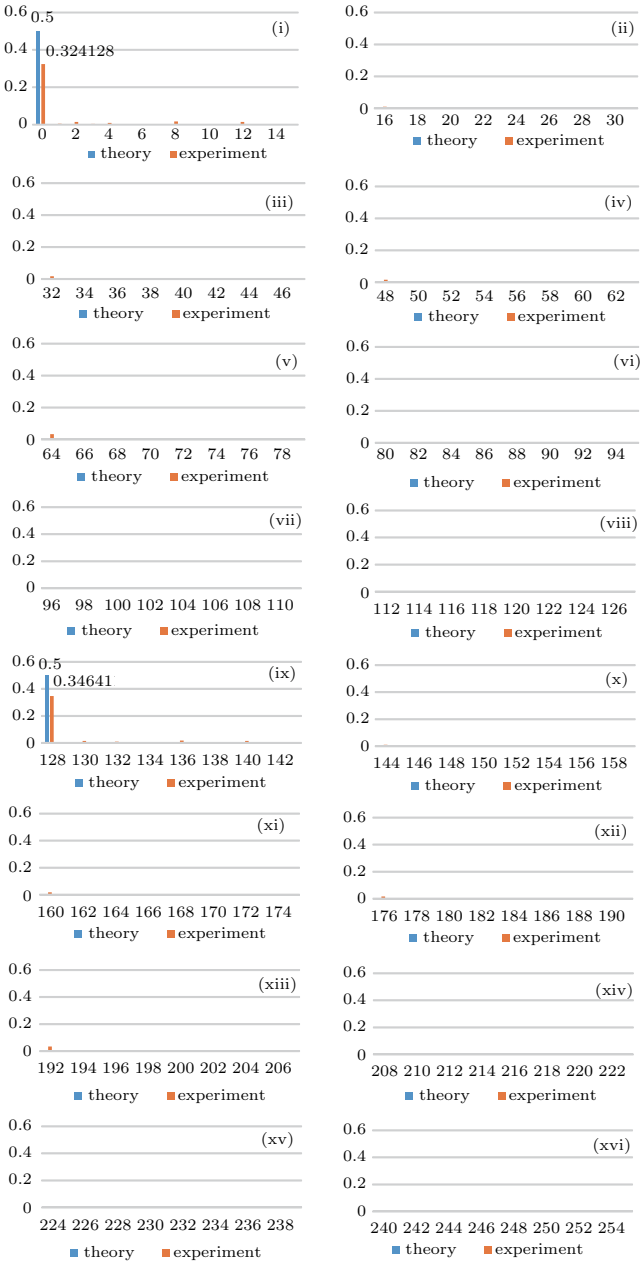


Fig. 11. The running result of Shor's quantum algorithm based on the t-bit semiclassical QFT. The horizontal axis represents the result $c = \sum_{k=1}^{8} 2^{8-k} c_k$, and the vertical axis represents the measuring probability.

iii) Like the single-bit semiclassical QFT, two qubits can be applied cyclically to prepare $|j_1 j_2\rangle, \ldots, |j_7 j_8\rangle$. That is to

say, the circuit can be implemented in 4 steps. The first three steps respectively need two qubits, and the last step needs four qubits.

iv) The circuit for F is shown in Fig. 10.

The experimental result is shown in Fig. 11.

According to Fig. 11, the experiments yield 128 with probability 0.346411, with $r = 2$ being determined by the continued fraction expansion of $128/256$, and the GCD$(11^{2/2} \pm 1, 15) = 3, 5$, giving a successful factorization. While, the experiments also yield 0 with probability 0.324128 and other values with probabilities very close to 0, corresponding to a failure.

Furthermore, the squared statistical overlap of experimental data with the ideal values is $\gamma''' = 0.6704$, which is lower than 1. The reason is that the probability distribution of the output results is not uniform. Only the theoretical measurement probabilities of 0 and 128 are non-zero. The number of the output results is 256. However, based on Figs. 9, 15 can be factorized with probability 0.346411, whose theory probability is 0.5. Thus, the experimental data is also accuracy.

In 2017, IBM announced that they have built the operational prototype 50-qubit processor,[26] which has a more powerful ability of implementing Shor's algorithm. Then, based on the t-bit semiclassical QFT, $N$with the maximum digit of 49 can be factorized for $t = 1$, however, the maximum digit of N is only 17 based on the standard QFT. Thus, the t-bit semiclassical QFT has significant advantage over the standard QFT, which may accelerate the application process of Shor's algorithm.

5. Conclusions

In this paper, we realize the 2-bit semiclassical QFT over Z_{2^3} on IBM's quantum cloud computer. The method can, in principle, be scaled to realize larger-scale QFT. Thus, this scheme may provide a candidate solution for implementing a large-scale QFT under the condition of limited computational resources. Based on this method, Shor's algorithm may be successfully implemented on IBM's quantum cloud computer.

Acknowledgment

The authors acknowledge the use of IBM's quantum experience for this work.

References

[1] Shor P W 1997 *SIAM J. Comput.* **26** 1484
[2] Grover L K 1996 *Proceeding 28th ACM Symposium on Theory of Computation*, May 22–24, 1996, New York, USA, p. 212
[3] Rivest R L, Shamir A and Adleman L M 1978 *Commun. ACM* **21** 120
[4] Diffie W and Hellman M E 1976 *IEEE Trans. Inform. Theor.* **22** 644
[5] Jordan S P, Lee K S M and Preskil J 2012 *Science* **336** 1130
[6] Wang H F and Zhang S 2012 *Chin. Phys. B* **21** 100309
[7] Wiebe N, Braun D and Lloyd S 2012 *Phys. Rev. Lett.* **109** 050505
[8] Long G L and Xiao L 2004 *Phys. Rev. A* **69** 052303
[9] Yu C H, Gao F, Wang Q L and Wen Q Y 2016 *Phys. Rev. A* **94** 042311
[10] Qu F M, Ji Z Q, Tian Y and Zhao S P 2018 *Chin. Phys. B* **27** 070301
[11] Huang H L, Zhao Q, Ma X F, Liu C, Su Z E, Wang X L, Li L, Liu N L, Sanders B C, Lu C Y and Pang J W 2017 *Phys. Rev. Lett.* **119** 050503
[12] Xu G L, Qiu D, Zou X and Gruska J 2018 *Reversibility and Universality* (Berlin: Springer) pp. 447–462
[13] Coppersmith D 2002 arXiv: 201067 [quant-ph]
[14] Griffiths R B and Niu C S 1996 *Phys. Rev. Lett.* **76** 3228
[15] Chiaverini J, Britton J, Leibfried D, Knill E, Barrett M D, Blakestad R B, Itano J D, Jost J D, Langer C, Ozeri R, Schaetz T, Winel and D J 2005 *Science* **308** 997
[16] Parker S and Plenio M B 2000 *Phys. Rev. Lett.* **85** 3049
[17] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (London: Cambridge University Press) pp. 216–247
[18] Fu X Q, Bao W S, Zhou C and Song Z 2012 *Chin. Sci. Bull.* **57** 119
[19] I B M 2016 http://www.research.ibm.com/quantum/
[20] Fuchs C A 1996 "Distinguishability and Accessible Information in Quantum Theory", Ph. D. Dissertation (Albuquerque: University of New Mexico)
[21] Ambainis A and Watrous J 2002 *Theor. Comput. Sci.* **287** 1
[22] Qiu D, Li L, Mateus P and Sernadas A 2015 *J. Comput. Syst. Sci.* **81** 359
[23] Li K, Qiu D, Li L, Zheng S and Rong Z 2017 *Inform. Process. Lett.* **120** 23
[24] Vandersypen L M K 2001 "Experimental quantum computation with nuclear spins in liquid solution", Ph. D. Dissertation (Palo Alto: Stanford University)
[25] Lu C Y, Browne D E, Yang T and Pan J W 2007 *Phys. Rev. Lett.* **99** 250504
[26] IBM 2017 http://www.research.ibm.com/ibm-q/