

$t$-bit semiclassical quantum Fourier transform

FU XiangQun, BAO WanSu*, ZHOU Chun & SONG Zhen

Institute of Electronic Technology, The PLA Information Engineering University, Zhengzhou 450004, China

Received June 13, 2011; accepted July 21, 2011

Because of the difficulty of building a high-dimensional quantum register, this paper presents an implementation of the high-dimensional quantum Fourier transform (QFT) based on a low-dimensional quantum register. First, we define the $t$-bit semiclassical quantum Fourier transform. In terms of probability amplitude, we prove that the transform can realize quantum Fourier transformation, illustrate that the requirement for the two-qubit gate reduces obviously, and further design a quantum circuit of the transform. Combining the classical fixed-window method and the implementation of Shor’s quantum factorization algorithm, we then redesign a circuit for Shor’s algorithm, whose required computation resource is approximately equal to that of Parker’s. The requirement for elementary quantum gates for Parker’s algorithm is $O\left(\frac{\log N}{t}\right)$, and the quantum register for our circuit requires $t-1$ more dimensions than Parker’s. However, our circuit is $t^2$ times as fast as Parker’s, where $t$ is the width of the window.

Quantum computing has a strong ability for parallel computing, which poses a great challenge to the security of the modern cipher. In 1994, Shor [1] presented a polynomial-time quantum algorithm for factorization. Apparently, the emergence of this algorithm greatly threatens the public-key cryptography, such as RSA cryptography, whose security is based on factorization and a discrete logarithm. In 1996, Grover [2] presented a quantum searching algorithm that reduces the computational complexity of current exhaustive search attacks from $O(2^n)$ to $O(2^{n/2})$. To overcome this problem, scholars [3–11] in China and abroad have since intensively investigated quantum computation and quantum cryptology.

Although the correctness of quantum computation and Shor’s algorithm has been proved to hold true [12], it is still difficult to break 2048-bit RSA or 191-bit ECC in the case of the quantum computer for the reason that the kilobit quantum computer does not exist. Thus, how to reduce the computation resource required for Shor’s algorithm is an issue of common concern.

In 1996, Vedral et al. [13] published a circuit with a 7$n+1$-dimensional quantum register and $O(n^3)$ elementary gates for modular exponentiation (where $n$ denotes the length of the integer to be factorized). It has been mentioned that the quantum register requirement can be reduced to $4n+3$ if unbounded Toffoli gates ($n$-controlled NOT gates) are available. Also in 1996, Beckman et al. [14] presented an extended analysis of modular exponentiation, with a circuit of a 4$n+1$-dimensional quantum register if unbounded Toffoli gates are available. In 1998, Zalka [15] described a method for factorization with a 3$n+O(\log N)$-dimensional quantum register using only elementary gates. However, these achievements are the optimization of Shor’s algorithm, which is based only on reducing the dimensions of the quantum register.

Generally speaking, in the implementation of the quantum Fourier transform (QFT), the $n$-bit quantum state is once inputted into a $n$-dimensional quantum register and the circuit needs $n^2/2$ two-bit quantum gates and $n$ one-bit quantum gates in total [16]. To date, for larger $n$, there is no
implementation method for the \( n \)-dimensional QFT within existing technology. In 1996, Griffiths et al. [17] presented the single-bit semiclassical QFT. Since the transform’s input is from bit flipping, the transform only needs a one-dimensional quantum register and one one-bit quantum gate, and the QFT can thus be implemented without a two-bit quantum gate. In 2000, on the basis of the single-bit semiclassical QFT, Parker et al. [18] presented a circuit of the \( n+1 \)-dimensional quantum register for factorization. Thus, the single-bit semiclassical QFT provides a solution for implementing a high-dimensional QFT, with which Shor’s algorithm can be used to break public-key cryptography (e.g., RSA and ECC) under the condition of limited computation resources.

The QFT, compared with the single-bit semiclassical QFT, has higher implementation speed but needs more quantum computation resources. Considering that a two-bit quantum gate is more difficult to implement than a one-bit quantum gate, the two-bit quantum gate should be avoided as much as possible in a quantum computation circuit. To replace the QFT with a single-bit semiclassical QFT is a good choice. However, it is at the expense of implementation speed. Because of the difficulty of realizing a high-dimensional quantum register, how to balance the tradeoff between the quantum resource and speed in the implementation of the QFT (e.g., how to implement a high-dimensional QFT based on a low-dimensional quantum register) requires further study.

In this paper, we define the \( t \)-bit semiclassical QFT. In terms of the probability amplitude, we prove that the transform can realize quantum Fourier transformation, illustrate that the requirements for the two-bit and one-bit quantum gates are respectively reduced to \( 1/l^2 \) and \( 2/l \) times those of the QFT (where \( n \) denotes the dimension of the QFT; if \( t \) divides \( n \) exactly, \( l=n/t \), otherwise \( l=[n/t] \)), and clarify that the speed of the \( t \)-bit semiclassical QFT increases to \( t \) times that of the single-bit case. Finally, combining the classical fixed-window representation and the implementation method for Shor’s algorithm, we design a circuit for Shor’s quantum factorization algorithm based on the \( t \)-bit semiclassical QFT, whose computation resource is approximately equal to that of Parker’s. However, our circuit is \( t^2 \) times as fast as Parker’s, where \( t \) is the width of the window representation.

1 QFT and single-bit semiclassical QFT

**Definition 1** (Quantum Fourier transform) [16] The QFT on an orthonormal basis \( |0\rangle, |1\rangle, \ldots, |N-1\rangle \) is defined to be a linear operator \( U_F \) with an action on the basis states described by

\[
U_F : |j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \alpha_n^j |k\rangle.
\]

Therefore, the action on an arbitrary state may be written as

\[
U_F : \sum_{j=0}^{N-1} \alpha^j |j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \alpha^j \alpha_n^k |k\rangle.
\]

where the symbol “\( \mapsto \)” stands for an invertible transform and \( \alpha_n^j = e^{2\pi i j/N} \).

If \( N = 2^t \), the QFT \( U_F \) acting on the state \( |a\rangle \) can be written as

\[
U_F |a\rangle = \prod_{j=0}^{2^t-1} |p(\phi_j)\rangle.
\]

(1)

\( U_F \) is also called the \( n \)-dimensional QFT, where \( a = \sum_{j=0}^{2^t-1} a_j 2^j \) is the binary representation of \( a \), \( a_j \) is 0 or 1, \( \phi_j = \sum_{j=0}^{2^t-1} a_j 2^{j-t-1} \) for \( j = 0, 1, \ldots, 2^t-1 \) and \( |p(\phi)\rangle = (|0\rangle + e^{2\pi i \phi} |1\rangle)/\sqrt{2} \).

It has been pointed out [16] that the circuit of the QFT requires a \( \lfloor \log N \rfloor \)-dimensional quantum register. In 1996, Griffiths et al. presented a method that only required a one-dimensional quantum register and one-bit gate to implement the QFT, which was called single-bit semiclassical quantum Fourier transform [17]. Its circuit is illustrated in Figure 1.

Figure 1 is explained as follows.

1. Each box, standing for an oracles, performs the operations

\[
\begin{align*}
|0\rangle &\mapsto (|0\rangle + |1\rangle)/\sqrt{2} \\
|1\rangle &\mapsto e^{2\pi i \phi} (|0\rangle - |1\rangle)/\sqrt{2}.
\end{align*}
\]

(2)

2. A single line represents a quantum signal and a double line represents a classical signal.

3. The outputs of each box are two classical signals, one of which is the result of the measurement and the other represents the phase \( \phi' = \phi/2 + c/4 \); \( \phi' \) is the input of the next box, whose initial value is zero.

4. The final measurement result is \( c = \sum_{k=0}^{2^t-1} 2^k c_k \).

The single-bit semiclassical QFT carries each basis state
The 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 the two methods, we design a new QFT to balance the tradeoffs of the quantum resource and speed.

**Definition 2** Suppose \( t \) is a positive integer and

\[
l = \left\lfloor \frac{n}{t} \right\rfloor \quad \text{and} \quad l = \left\lfloor \frac{n}{t} \right\rfloor - 1, \quad \text{then} \quad \{a\} = \{a_{n-1}, a_{n-2}, \ldots, a_0\} \quad \text{is an arbitrary orthonormal state with orthonormal basis} \quad \{0\}, \{1\}, \ldots, \{N-1\}.\]

If \( U_{F_{t}} \) transforms a block of bits of \( \{a\} \) entering on the left to one leaving on the right through

\[
|a_{n-1}, a_{n-2}, \ldots, a_{0}\rangle \mapsto \frac{1}{2^{(n-t)/2}} \sum_{c=-0}^{2^{(n-t)/2}} \omega_{2^{n-t}} (t) e^{i \sum_{a'_{i}=0}^{2^{(n-t)/2}} 2^{a'_{i}} c_{n-1} + \sum_{a_{n-t}^{(n-t)/2}}^{2^{(n-t)/2}} 2^{a_{n-t}^{(n-t)/2}} c_{n-t} \ldots c_{0}} \langle c_{n-1}, c_{n-2}, \ldots, c_{0} | \wedge 12 = 0, 1, \ldots, N/2 \).
\]

where

\[
a'_{i} = \sum_{r=0}^{\infty} 2^{-t} a_{r}, \quad a'_{i} = \sum_{r=0}^{\infty} 2^{-t} a_{r}, \quad c'_{j} = \sum_{r=0}^{\infty} 2^{-t} c_{n-1} + \sum_{a_{n-t}^{(n-t)/2}}^{2^{(n-t)/2}} 2^{a_{n-t}^{(n-t)/2}} c_{n-t} \ldots c_{0} \]

and

\[
\phi_{k} = \frac{c_{0}}{2^{0}} + \frac{c_{2}}{2^{1}} + \frac{c_{4}}{2^{2}} + \ldots + \frac{c_{2k}}{2^{k}} \quad (j = 1, \ldots, l, \quad k = 2, \ldots, l), \quad \text{then} \quad U_{F_{t}} \quad \text{is called the} \ t \text{-bit semiclassical Fourier transform.}
\]

In essence, \( U_{F_{t}} \) is a block transform. That is to say, \( \{a\} \) is transformed from left to right in blocks, the first of which is \( n-\lfloor n/t \rfloor \) bits and the other is \( t \) bits.

**Theorem 1** Suppose \( \{0\}, \{1\}, \ldots, \{N-1\} \) is an orthonormal basis, \( U_{F} \) is the QFT and \( U_{F_{t}} \) is the \( t \)-bit semiclassical QFT. \( U_{F} \) carries \( \{a\} = \{a_{n-1}, a_{n-2}, \ldots, a_0\} \) into \( \{c\} = \{c_{n-1}, c_{n-2}, \ldots, c_0\} \), whose probability is equal to that for \( U_{F_{t}} \).

**Proof:** To prove the theorem, we only need to prove that \( U_{F} \) carries \( \{a\} = \{a_{n-1}, a_{n-2}, \ldots, a_0\} \) into \( \{c\} = \{c_{n-1}, c_{n-2}, \ldots, c_0\} \), whose amplitude is equal to that for \( U_{F_{t}} \).

From Definition 2 and \( e^{2\pi i} = 1 \), we obtain

\[
\frac{\omega_{2^{n-t}} (t)}{2^{(n-t)/2}} e^{i \sum_{a'_{i}=0}^{2^{(n-t)/2}} 2^{a'_{i}} c_{n-1} + \sum_{a_{n-t}^{(n-t)/2}}^{2^{(n-t)/2}} 2^{a_{n-t}^{(n-t)/2}} c_{n-t} \ldots c_{0}} = e^{i \sum_{a'_{i}=0}^{2^{(n-t)/2}} 2^{a'_{i}} c_{n-1} + \sum_{a_{n-t}^{(n-t)/2}}^{2^{(n-t)/2}} 2^{a_{n-t}^{(n-t)/2}} c_{n-t} \ldots c_{0}} \quad \text{where} \quad \omega_{2^{n-t}} (t) = e^{i \sum_{a'_{i}=0}^{2^{(n-t)/2}} 2^{a'_{i}} c_{n-1} + \sum_{a_{n-t}^{(n-t)/2}}^{2^{(n-t)/2}} 2^{a_{n-t}^{(n-t)/2}} c_{n-t} \ldots c_{0}}.
\]

Therefore, the amplitude of \( \{c_{n-1}, c_{n-2}, \ldots, c_0\} \) is

\[
\frac{1}{2^{(n-t)/2}} e^{i \sum_{a'_{i}=0}^{2^{(n-t)/2}} 2^{a'_{i}} c_{n-1} + \sum_{a_{n-t}^{(n-t)/2}}^{2^{(n-t)/2}} 2^{a_{n-t}^{(n-t)/2}} c_{n-t} \ldots c_{0}}.
\]
From Definition 1, we obtain $$U_r |a\rangle = \frac{1}{\sqrt{2^n}} \sum_{c=0}^{2^n-1} \omega_2^c |c\rangle.$$ Then, after $U_r$ acts on $|a\rangle$, the amplitude of $|c\rangle = |c_{n-1},c_{n-2},\cdots,c_0\rangle$ is $$\frac{1}{2^n} \omega_2^c.$$ We thus obtain Theorem 1.

According to Theorem 1, the $t$-bit semiclassical QFT can realize quantum Fourier transformation. The circuit of the transform is illustrated in Figure 2.

Figure 2 is explained as follows.

1. Each bold virtual box denotes VB1, while the fine virtual box containing $E_1$ denotes VB2 and that containing $E_2$ denotes VB3, where $E_1$ is the $n-L$-dimensional QFT and $E_2$ is the $t$-dimensional QFT. The circuits of $E_1$ and $E_2$ are detailed in [16].

2. The outputs of VB2 have $n-L+1$ values, namely $c_{n-L-1}c_{n-L-2}c_{n-L-3}c_0$, $\varphi' = \frac{c_0}{2^{n-L+1}} + \cdots + \frac{c_{n-L-1}}{2^{t}}$. If VB3 enters as $a_{t+1}a_{t+2}a_{t+3}$, it leaves as $t+1$ values, namely $c_{t+1}c_{t+2}c_{t+3}c'_0$, $\varphi' = \frac{c'_0}{2^t} + \cdots + \frac{c'_{t-1}}{2^2}$. $R_j = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i j/2^t} \end{bmatrix}$ for $j = 1, 2, \cdots, t$, where $\varphi'$ is sent to the next VB1, $\varphi$ is the input of VB1, and the very first VB1 uses $\varphi = 0$.

3. $c = \sum_{j=0}^{t-1} 2^j c'_j$ is the final measurement.

We now analyze the required resources of the circuit of the $t$-bit semiclassical QFT.

Figure 2 shows that the $t$-bit semiclassical QFT requires $t$-dimensional quantum registers. Since the $n$-dimensional QFT needs $n^t/2$ two-bit gates and $n$ one-bit gates [16], our circuit in Figure 2 needs $t^t/2$ two-bit gates and $t$ one-bit gates to realize $t$-dimensional quantum Fourier transformation. It also needs $t$ one-bit gates to realize $R_j$ ($j = 1, 2, \cdots, t$). Therefore, the two-bit gates and one-bit gates for the $t$-bit semiclassical QFT are respectively $1/t^t$ and $2/t$ times as many as those of the $n$-dimensional QFT. It is obvious that the $t$-bit semiclassical QFT requires the preparation of superposition $\frac{1}{2^{t^t}} \sum_{c=0}^{2^t-1} |c\rangle$ once and that of $\frac{1}{2^{t^t}} \sum_{c=0}^{2^t-1} |c\rangle$ $t'$ times while the single-bit semiclassical QFT requires preparation of superposition $|0\rangle+|1\rangle)/\sqrt{2}$ $L$ times. Therefore, the running speed of the $t$-bit semiclassical QFT is $t$ times that of the single-bit semiclassical QFT.

3 Parker’s circuit of Shor’s quantum factorization algorithm

In 2000, Parker et al. presented a circuit of Shor’s quantum factorization algorithm, which is illustrated in Figure 3 [18].

In Figure 3, $H$ is a Hadamard gate [16]. $R_j = \begin{bmatrix} 1 & 0 \\ 0 & \phi_j \end{bmatrix}$, where $\phi_j = e^{-2\pi i n_j / 2^m}$. $U_d$ is the operation $U_d : |r\rangle|x\rangle \rightarrow |r\rangle|a^r \mod N\rangle$ controlled by one bit. $c = \sum_{m_i \leq 2^t} 2^{t-m_i} m_i$ is the final measurement result, where $L = 2[\log N] + 1$ and $[\log N]$ is the minimum integer greater than $\log N$. The quantum state $|0\rangle+|1\rangle$ is $\frac{1}{\sqrt{2}} (|0\rangle+|1\rangle)$, which can be obtained by the Hadamard transform acting on $|0\rangle$.

Parker’s circuit needs a $\lceil \log N \rceil + 1$-dimensional quantum register and $O(\lceil \log N \rceil)$ elementary gates [18]. Furthermore, it has been pointed out that the circuit requires $nL$ addition operations (the addend length being $n = \lceil \log N \rceil$) when $a \mod N, a^2 \mod N, \cdots, a^{2^t} \mod N$ are precomputed classically [19].

4 Circuit of the Shor algorithm based on the window method and analysis

In the circuit of Shor’s algorithm, the modular exponential-
Addition operations when \( \alpha^k \mod N \) is the most time-consuming calculation [16]. In classical computation, there are two methods to accelerate implementation of modular exponentiation; i.e., the modified representation of integer \( k \) and increasing the precomputation amount. The window method [20] can accelerate the implementation of modular exponentiation by space for time, and its general concept is expressed as follows.

According to some rules, \( k \) can be represented as
\[
k = \sum_{i=0}^{n} 2^i \alpha_i,
\]
where \( 0 \leq k \leq 2^v - 1 \) and \( 0 \leq i < v - 1 \). If \( \alpha, \alpha^2, \alpha^3 \), \( \alpha^{2^i} \) are precomputed, the time taken by the addition operation can be reduced in modular exponentiation and \( u_i \) has already been inputted before each operation. If the classical fixed-window method is combined with the implementation of Shor’s algorithm, all bits of \( u_i \) should be inputted once.

Employing the window method and \( t \)-bit semiclassical QFT, we design a quantum circuit of Shor’s algorithm as presented in Figure 4.

The explanation of Figure 4 is as follows:

1. \( c = \sum_{i=0}^{n} 2^i \) is the final measurement; if \( t \) divides \( L \) exactly, \( l' = [L/t] \), otherwise \( l' = [L/t] - 1 \).
2. The structures and above outputs of VB2 and VB3 are the same as in Figure 2; the inputs of VB2 and VB3 are \( L - l't \) and \( t \) bits respectively; the initial value of \( \phi \) is zero.
3. If the left input of the black box \( U^2 \alpha^u \) is \( A \), then the output is \( A \cdot \alpha^{2^i} \mod N \), where \( \alpha^{2^i} \mod N \) is precomputed classically and \( u_i = \sum_{j}^{t} 2^i u'_{ij} \) (\( u_0, u_1, \ldots \) are the above inputs of the black box \( U^2 \alpha^u \) from right to left).
4. The quantum state \( |0\rangle + |1\rangle \) is actually \( \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \), which can be obtained from the Hadamard transform acting on \( |0\rangle \).
5. The lengths of \( |1\rangle \) and \( |0\rangle \) are \( \log N \) bits and 1 bit respectively.

From Figure 4, \( \alpha^k \mod N \) can be computed by the black box \( U^2 \alpha^u, U^2 \alpha^{2^i} \mod N, \ldots, U^2 \alpha^{2^n} \), and the output result is \( \alpha^k \mod N \) \( u_i \) is the above input of black box \( U^2 \alpha^u \) with \( \sum_{i}^{L} u_i 2^i \) just being \( k \)'s window representation, where \( t \) is the width of the window. Therefore, the width of the window is the same as the dimension of the input of the \( t \)-bit semiclassical QFT.

The circuit needs a \( \log N + t \)-dimensional quantum register. \( O(1) \) elementary quantum gates are needed for \( R_i \) running once. The QFT needs \( O(t^3) \) elementary quantum gates. Therefore, VB2 and VB3 running once both need \( O(t^3) \) elementary quantum gates. Since modular exponentiation running once needs \( O(\log N^3) \) elementary quantum gates, the new circuit needs \( O(\log N^3) \) elementary quantum gates in all. Comparing with the circuit in [18], both need \( O(\log N^3) \) elementary quantum gates, but the quantum register for the former requires \( t-1 \) dimensions more than the latter.

The runtime of the circuit of Shor’s algorithm can be depicted in terms of modular exponentiation and quantum Fourier transformation [15]. Modular exponentiation running once needs \( n \) addition operations [19] and the new circuit needs \( l' + 1 \) modular exponentiations. Therefore, the new circuit needs \( (l' + 1)n \) addition operations when \( \alpha^{2^i} \mod N, \alpha^{2^2} \mod N, \ldots, \alpha^{2^{t-1}} \mod N \) are precomputed classically (\( j = 0, 1, \ldots, l' \)). The circuit of Shor’s algorithm in [18] needs \( nL \) addition operations.

Figure 3 Parker’s circuit of Shor’s quantum factorization algorithm.

Figure 4 Quantum circuit of Shor’s algorithm based on the window method and \( t \)-bit semiclassical QFT.
Additionally, modular exponentiation in the new circuit is $t$ times as fast as that in [18]. As noted in section 2, the $t$-bit semiclassical QFT is $t$ times as fast as the single-bit semiclassical QFT. Thus, compared with the circuit in [18], the new circuit is $t^2$ times as fast, and the new circuit’s precomputation amount increases by a factor of $2^t/t$.

5 Conclusions

Because of the difficulty of building a high-dimensional quantum register, this paper presented an implementation of the high-dimensional QFT based on a low-dimensional quantum register. We defined the $t$-bit semiclassical QFT. The transform can balance the tradeoff of the quantum resources required and the speed of implementation of the QFT. Additionally, we design a quantum circuit for the transform. Combining the classical fixed-window representation with the implementation method for Shor’s algorithm, we design a circuit for Shor’s quantum factorization algorithm, which is $t^2$ times as fast as Parker’s, where $t$ is the width of the window.

1 Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Comput, 1997, 26: 1484–1509
2 Grover L K. A fast quantum mechanics algorithm for database search. In: Proceeding of the 28th ACM Symposium on Theory of Computation. New York: ACM Press, 1996, 212–219
3 Long G L, Xiao L. Parallel quantum computing in a single ensemble quantum computer. Phys Rev A, 2004, 69: 052303
4 Zhong P C, Bao W S. Quantum mechanical meet-in-the-middle search algorithm for triple-DES. Chin Sci Bull, 2010, 55: 321–325
5 Gao F, Guo F Z, Wen Q Y, et al. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication. Sci China Ser G-Phys Mech Astron, 2008, 51: 559–566
6 Chen W, Han Z F, Mo X F, et al. Active phase compensation of quantum key distribution system. Chin Sci Bull, 2008, 53: 1310–1314
7 Fang X M, Zhu X W, Hong M, et al. Realization of quantum discrete Fourier transform with NMR. Chin Sci Bull, 2000, 45: 1071–1075
8 He Y G, Sun J G. Complete quantum circuit of HAAR wavelet based MRA. Chin Sci Bull, 2005, 50: 1796–1798
9 Cao Y, Peng S G, Zeng C, et al. Quantum Fourier transform and phase estimation in qudit system. Commun Theor Phys, 2011, 55: 790–794
10 Wang X, Bao W S, Fu X Q. A quantum algorithm for searching a target solution of fixed weight. Chin Sci Bull, 2011, 56: 484–488
11 Zhou C, Bao W S, Fu X Q. Decoy-state quantum key distribution for the heralded pair coherent state photon source with intensity fluctuations. Sci China Inf Sci, 2010, 53: 2485–2494
12 Lieven M K V, Matthias S, Gregory B, et al. Experimental realization of Shor’s quantum factorization algorithm using nuclear magnetic resonance. Nature, 2001, 414: 883–887
13 Vedral V, Barenco A, Ekert A. Quantum networks for elementary arithmetic operations. Phys Rev A, 1996, 54: 147–153
14 Beckman D, Chari A N, Devabhatkuni S, et al. Efficient networks for quantum factoring. Phys Rev A, 1996, 54:1034–1063
15 Zalka C. Fast versions of Shor’s quantum factoring algorithm. Arxiv: quant-ph/980604v1, 1998
16 Nielsen M A, Chuang I L. Quantum Computation and Quantum Information. London: Cambridge University Press, 2000
17 Griffiths R B, Niu C S. Semiclassical Fourier transform for quantum computation. Phys Rev Lett. 1996,76: 3228–3232
18 Parker S, Plenio M B. Efficient factorization with a single pure qubit and logN mixed qubits. Phys Rev Lett, 2000, 85: 3048–3052
19 Fu X Q, Bao W S, Zhou C. Speeding up implementation for Shor’s factorization quantum algorithm. Chin Sci Bull, 2010, 55: 3648–3653
20 Kenji K, Yukio T. Speeding up elliptic cryptosystems using a signed binary window method. In: Proceeding of the 12th Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer-Verlag, 1993. 345–357

Open Access This article is distributed under the terms of the Creative Commons Attribution License which permits any use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.