Quantum computer

Tao Yang
Department of Physics
University of Oklahoma
440 W.Brooks, NH 100, Norman, OK 73019

November 22, 2010

Abstract

A brief introduction to quantum computer.

Contents

Chapter 1

Introduction

1.1 History of cryptography

Cryptography can date back thousands of years ago. Methods of secret communication were developed by many ancient societies, especially during the wartime. Spartans, the most warlike of the Greeks, employed a device called SCYTALE for military communications between commanders(1). This device was used to perform a transposition cipher. Another cipher called Julius Caesar's cipher, is a type of substitution cipher(2). Although invented thousands of years ago, these two basic methods of encryption - transposition and substitution are still used frequently until the two world wars, with the aid of physical devices. The Enigma machine, a family member of rotor machines, is widely used by German government from late 1920s(3). These physical implementations improve the cryptography a lot. However if eavesdroppers crack and rebuild these machines, or even just steal an original one, the cipher will turn out to be useless even harmful.

The revolution of classical computers has developed cryptography in an unprecedented way, which bring up the concerns of the protection of electronic transmission and digitally stored data. The algorithms for encrypting and decrypting can be revealed to anybody without compromising the security of a particular cryptogram(4). The key, a set of parameters for the ciphers, is supplied as an input to the encrypting algorithm or an input to the decrypting algorithm. Although the encrypting and decrypting algorithm are known to public, the security of the cryptogram depends on the secrecy of the key. One of the application of the classical ciphers is the Vernam cipher, invented in 1917 by the American AT&T engineer Gilbert

Vernam(5). In this cryptographic protocol, the key is the same as the the length of the message, which is input to the message to form an encoded message, and it cannot be decoded by any statistical methods. However, even if the randomization of the key can be fulfilled, there are two problems still comes up. Once the key is setup, we can send encrypted messages over a channel and they are vulnerable to eavesdropping. This step is safe since eavesdroppers do not have the key to decrypt the message. But how the two users initially share no secrecy can send the key over a reliable and secure channel? In the other way, a message can be "signed" using a privately held decryption key. This signature can be verified, but cannot be forged, and the signer cannot later deny the validity of the signature. As the advances in solving these problems, the public key cryptosystems were invented in the 1970s, and till today, some main public key cryptography techniques are in general use.

1.2 RSA cryptography

RSA (which stands for Rivest, Shamir and Adleman who first publicly described it), one of the public key cryptographic algorithms, is widely used for electronic commerce protocols(6). The main feature of the public key cryptographic algorithm is, it is very easy to compute in one direction but very difficult in the other direction, therefore it is called "trap-door one-way function(7)". The RSA algorithm can be represented as the following schematic

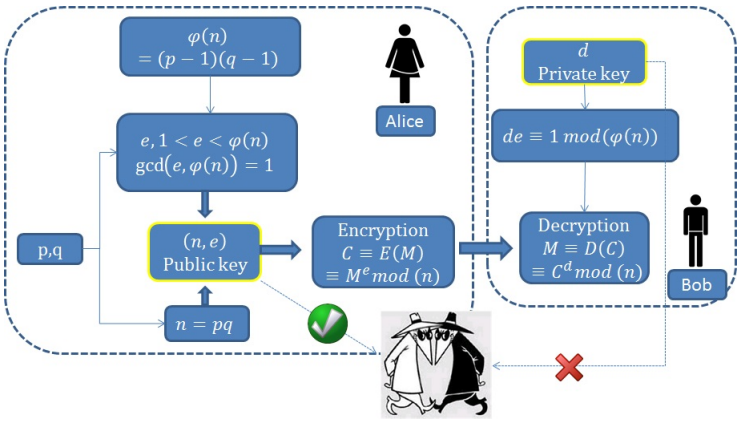

Figure 1.1: RSA algorithm schematic.

Here, M is the message need to be encrypted. For the simplicity we break

it into a series of blocks, and represent each block as an integer. p and q are large-bit(more than 1000 bits) randomly chosen prime numbers, which are of similar bit-length; e has a short bit-length but can not be so short. After these certain parameters have been chosen, we take e-th power of M modulo n and have the remainder as the ciphered information. For the decryption process, by using Modular multiplicative inverse Extended Euclidean algorithm we choose d as the private key to decrypt the encrypted message, in association with the public key (n,e). In the schematic, Bob send out the public key that everyone including eavesdroppers can get it. Alice get one, encrypt the message and send it back to Bob. Finally, Bob use his private key, which can not be obtained by the eavesdroppers, to decrypt the ciphered text. The problem is, can the eavesdroppers can calculate the private key d?

By examining this problem, we can do a sample test on this algorithm.

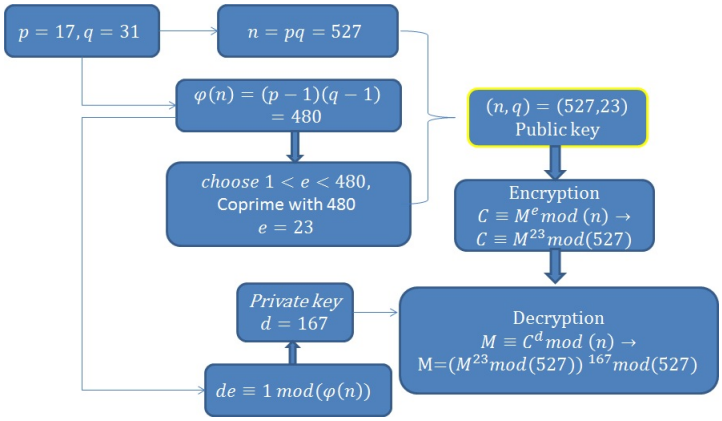

Figure 1.2: Sample test of RSA algorithm

In order to find out d, we need to compute $\varphi(n)$, which is equivalent to factorize n(at least 1000-bit length) to two prime numbers *(p,q)*. How hard is it to factorize a 1000-bit integer using our contemporary computers? The scientists reported in December 2009 that they factored 768-bit integer utilizing hundreds of machines over a span of 2 years(8). Especially, the semiprimes, the product of two prime numbers, will be super hard to factorize even for super fast computer and super efficient factorization algorithms, providing both of the primes are large enough, randomly chosen, about the same size. However, efforts by the scientists show that factoring a large integer in a limited time scale is not a problem for quantum computers! What make quantum computer such a special implementation for factoriza-

tion than the classical computer? What kind of revolution it will bring to the classical cryptography? Now let's explorer the modern computer in the quantum world.

Chapter 2

Quantum computer basics

Many people associate the birth of quantum computation and quantum computer with the talk given by Richard Feynman at MIT in 1981(9). He pointed out the difficulties of simulating quantum systems using classical computers, so the conjecture of a machine using quantum effects would effectively simulates quantum systems. Decades after that, in 2001 and after, IBM (10) and D-wave (11) (12) claimed to have build quantum computers. IBM claimed to have factorized 15 into two prime numbers with a seven qubit quantum computer, while D-wave build a 28-qubit quantum machine supposed to be available on-line in future for applications such as pattern-matching and searching. Before we want to build the tower of the quantum computer, we need to study its basic blocks.

2.1 Qubit and quantum register

In general, a quantum computer with n qubits can be in an arbitrary superposition of up to 2^n different states simultaneously, where a qubit in quantum computer is the analogue to a bit in classical computer. Qubits can be fundamentally chosen with the particles with two spin-1/2 states: "up" and "down", usually written as $|0\rangle$ and $|1\rangle$. Based on the normalized and orthogonal properties of this two-level system, we can represent a general qubit state in this basis as

$$|q\rangle = c_0|0\rangle + c_1|1\rangle \tag{2.1}$$

where c_0 andc_1 are complex numbers. Generally, in a larger quantum system with numerous two-level subsystems (such as the cluster of the electrons),

it can be represented as

$$|q\rangle = e^{i\eta}(\cos(\frac{\theta}{2})|0\rangle + e^{i\varphi}(\frac{\theta}{2})|0\rangle) \tag{2.2}$$

We can clearly see a qubit can exist as a any combination of $|0\rangle$ and $|1\rangle$, while a bit can only be either 0 or 1. In another way, if we expand to a system which is described by n orthogonal eigenstates, a general state in this system is

$$|\psi\rangle = \sum_{i=0}^{n-1} c_i * |x_i\rangle \tag{2.3}$$

We all know that the processor register are crucial to a computer, and registers are normally measured by the information they can hold. As the top of the memory hierarchy, registers provide the fastest way for a CPU to access data. Therefore, the capacity of the register will determine the power of the computation significantly. As an analogue to the classical register, quantum register has several interesting features. By its mathematical description, an n-qubit quantum register can be described as an element $|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots |\psi_n\rangle$ in the tensor product Hilbert space $H = H_1 \otimes H_2 \otimes \cdots H_n$. From Equ.(2.3), any state can be expresses as a combination of n base qubit states, therefore, there are 2^n ways of combination for the any state to be. If we want to store 2^n states in a classical register, we need 2^n bits to hold them! In some sense, we can store an exponentially increasing amount of information in a quantum register.

There are several ways for storage quantum information, one of which is using a disorder magnet(13). Researchers demonstrates that measurements of nonlinear magnetic dynamics in the low-temperature liquid reveal the alignment of coherent spins, in contrast with the behavior of similar materials. Labeled with frequency and controlled by the external magnetic field, these excitations can perform in the encoding of information at multiple frequencies simultaneously.

Some other ways help us from a dilemma when we choose the candidates for quantum qubits. In an analogue to a classical register, the qubit should be easily read and written, and its quantum nature will endure enough long for processing. The problem is, a good quantum qubit will be not only well isolated from the noisy world outside in order to be kept processing, but also need to be easily read and written. Like in a drama we have a pair

Operation name	Formula
Hadamard	$H(c_0\|0\rangle + c_1\|1\rangle) = \frac{1}{\sqrt{2}}[(c_0 + c_1)\|0\rangle + (c_0 - c_1)\|1\rangle]$
Not	$\sigma(c_0\|0\rangle + c_1\|1\rangle) = (c_0\|1\rangle + c_1\|0\rangle)$
Phase shifter	$\Phi(c_0\|0\rangle + c_1\|1\rangle) = e^{-i\varphi/2}(c_0\|0\rangle + c_1 e^{i\varphi}\|1\rangle)$
Two-qubit	$\|c\rangle_1\|x\rangle_2 \Rightarrow \|c\rangle_1 U_c\|x\rangle_2$

Table 2.1: Several examples of one-qubit and two-qubit quantum gates

of twins to behave different, we can also put two physical objects into the qubits, one for reading and writing and the one for interacting. The team in Yale University find a good way to solve this dilemma(14). They achieved the coupling of the electrons by placing the crystals,which are impure, next to tiny superconducting cavities that resonate at a specific microwave frequency. When the energy of the flip in the electron spins induced by the external magnetic field matches the energy of the microwaves in the cavity, the spins will flip back and forth which can help exchange the photons between the electrons and the superconducting cavity.

We can see from the above two experiments that the external magnetic field is popularly used, which hints that a electro-magnetic field controlled quantum processor might be possible.

2.2 Quantum gate

In classical digital circuits, logic gates play important roles in signal processing. Similar to classical logic gates, quantum circuits are composed of a sequence of quantum gates, and a quantum gate operates on a small number of qubits. There are many ways to realize quantum gates, which will be discusses in next chapter. The following are some basic single-qubit and two-qubit quantum gates

Take The Hadamard gate for example. This gate acts on a single qubit, and it turns the basis state $|0\rangle$ to $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|1\rangle$ to $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, which can be expressed as a matrix $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$.

Specifically, there is one kind of quantum cotrolled gates useful for performing selective state copying, called quantum controlled-NOT gate. This

2-qubit quantum controlled gate performs NOT operation on the second qubit when the first qubit is $|1\rangle$. And the operation is expressed as

$$(\alpha|0\rangle_1 + \beta|1\rangle_1)|0\rangle_2 \longrightarrow \alpha|0\rangle_1|0\rangle_2 + \beta|1\rangle_1|1\rangle_2 \tag{2.4}$$

Here we can see this performance deposits the quantum information α, β in both systems.Actually, most of the quantum gates can operate on one qubit or two qubits, just like the common classical logic gates. If we denote the qubit in Dirac notation, we can find out these quantum gates can be viewed as 2×2 or 4×4 unitary matrices, such as Hadamard gate matrix and 2-qubit controlled-NOT gate matrix. People initially want to find a quantum gate to handle three-qubit operation, but it turned out to be very hard(15). Fortunately, scientists showed that all the quantum gates can be decomposite to one set of universal quantum gates, which are all of the one-qubit quantum gates and the two-qubit Controlled-NOT quantum gates(16). Therefore, constructions of quantum computational networks are not impossible with the universal quantum gates. The problem is how can we realize these quantum gates in physical systems, which will be discussed in the next chapter.

2.3 Quantum processor

In 2007 D-wave announced they have built 28-qubit quantum computer by using the technology "adiabatic quantum computing", based on superconducting electronics. Experts are skeptical if it is a classical computer which decoheres qubtis acting like random classical bits. Leaving the debates alone in 2009, NIST demonstrated a two-qubit "universal" programmable quantum processor(17). Although there are infinite number of programs available for two-qubit quantum system, they perform 160 programs on this quantum processor, which are large and diverse enough that the authors believe the processor is universal. However, theoretical evidences showed that it is impossible to "build a fixed, general purpose quantum computer which can be programmed to performed an arbitrary quantum computation" (18). They used a linear number of gates to reach an exponentially small probability of result. A more efficient programmable array of quantum gates are needed and the ways to increase the probability of desired measurement results are top issues for constructing a quantum computer. Perhaps quantum entanglement may provide a alternative way to execute quantum programs.

Chapter 3

Physical realizations of quantum computer

In the previous chapter, we show the theories how to create the building blocks of the quantum computer. Now we need to choose the what the material of the building blocks. Quantum logic gates are the basic controls of the quantum computation, and there are many ways to build quantum gates using physical systems. Here we will talk about the physical realization of quantum controlled-NOT gate, since it is an important gate in constructing the set of universal quantum gates.

One of the practical implementations of the quantum controlled-NOT gate is the selective driving of optical resonance of two subsystems undergoing a dipole-dipole interaction(19). Here we do not anticipate this will be a universal quantum controlled NOT gate, which is a practical consideration in real quantum computer.

The qubits in this dipole-dipole interaction can be one of the magnetic dipoles and electric dipoles. In the article the researchers take single-electron quantum dots for example. A quantum dot is a semiconductor whose excitons are confined in all three spatial dimensions. We can treat the quantum dot as confining the electron is a box(20). Two single-electron quantum dots separated by a distance R are imbedded in a semiconductor. Let's take the first quantum dot, with resonant frequency $\omega_1\rangle$, acts as the control qubit, while the second quantum dot with resonant frequency ω_2 acts as the target qubit. Due to the quantum-confined Stark effect(21), the charge distribution of the two levels will shift to the other directions, shown in Figure (3.1).

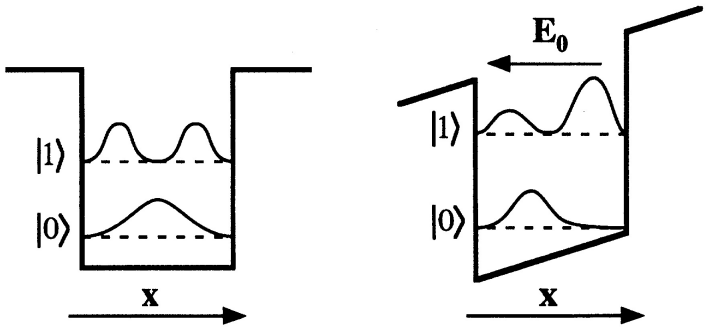

Figure 3.1: Charge density redistributed due to the quantum-confined Stark effect, with the quantum well on the right side in the biased electric field. Produced from(19)

For simplicity, we do not take into account holes in the valence band of the semiconductors. As we see, the charge distribution of the quantum dot will shift to opposite directions for the ground state and the first excited state, therefore, we can utilize the external field to control the control qubit. Since it is a confined two-electron system under the perturbation of external electric field, we can write the Hamiltonian

$$\hat{H} = \hat{H}_1 + \hat{H}_2 + \hat{V}_{12} \tag{3.1}$$

Here, the interaction term $\hat{V}_{12}$ is diagonal in the four-dimensional state space spanned by eigenstates $|\epsilon_1\rangle, |\epsilon_2\rangle$ of the Hamiltonian $\hat{H}_1 + \hat{H}_2$. The we have

$$(\hat{H}_1 + \hat{H}_2)|\epsilon_1\rangle|\epsilon_2\rangle = \hbar(\epsilon_1\omega_1 + \epsilon_2\omega_2)|\epsilon_1\rangle|\epsilon_2\rangle \tag{3.2}$$

$$\hat{V}_{12}|\epsilon_1\rangle|\epsilon_2\rangle = (-1)^{\epsilon_1+\epsilon_2}\hbar\bar{\omega}|\epsilon_1\rangle|\epsilon_2\rangle \tag{3.3}$$

where

$$\bar{\omega} = -\frac{d_1 d_2}{4\pi\epsilon_0 R^3} \tag{3.4}$$

Shown in Figure(3.2), if we set state of the first quantum dot as the control qubit, the transition frequency is $\omega_2 - \bar{\omega}$ when the control qubit is $|0\rangle$. If control qubit is $|1\rangle$, the transition frequency becomes $\omega_2 + \bar{\omega}$. This is a similar situation for state of the seconde quantum dot to be the control qubit. We can conclude that in the dipole-dipole interaction, the transition frequency of one quantum dot between $|0\rangle$ and $|1\rangle$ depends on the state of its neighboring dot. Some other models, including the method based on cavity

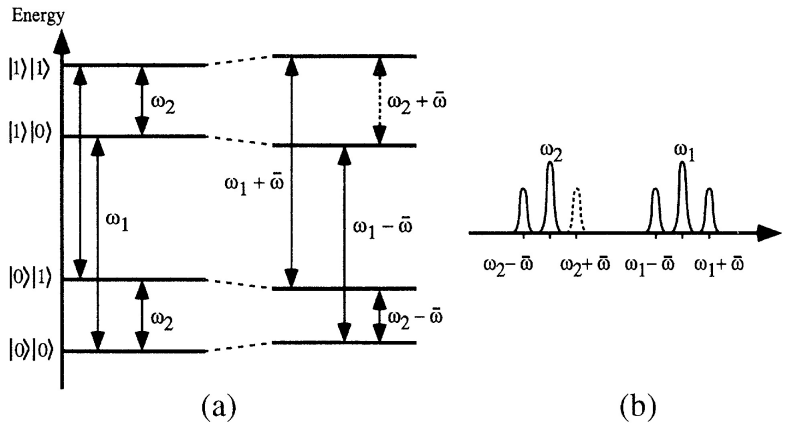

Figure 3.2: (a) Energy levels distribution before and after applying the external field; (b) Resonance spectrum of the two quantum dots. Produced from(19)

quantum electrodynamics(22), selective excitation of trapped ions(23), etc. Once these models can be implemented, it will easier for the quantum gates to be integrated into the complex quantum circuits, which is anxiously required in the quantum information processing.

Chapter 4

Shor's algorithms

4.1 overview of Shor's algorithm

Determining if a problem is computable is to find out if it can be resolved by a computer in a reasonable mount of time. Within a finite steps of computation, an algorithm can be characterized by the number of operations, the amount of memory and the input program, which determines the algorithm complexity. According to Cobham-Edmonds thesis, the computational problems can be feasibly computed on some computational device only if they can be computed in polynomial time, while in the way of computation complexity, the problems lie in the complexity class P. For example, the quicksort sorting algorithm on n integers requires at most AN^2 operations for some constant. This algorithm runs in time $O(n^2)$ and is a polynomial algorithm. These polynomial-time computable algorithms are generally deemed to be "tractable". On the other hand, problems which require more than polynomial time are usually considered to be "intractable", one of which is the determination of the prime factors of a large number.

However, as we see from the other chapters, quantum register demonstrates greater advantages over the classical register, showing that an n qubit register can store 2^n qubit states, and this hints that it may be tractable for the exponentially-time-solved problems on a quantum computer, providing a good quantum algorithm.

Most of the quantum algorithms are very famous for the better efficiency of solving problem than the classical algorithm. A well-known example is Shor's Algorithm. The list of all quantum algorithms can be viewed through

this link Quantum Algorithm Zoo.

Factoring larger integers is crucial for quantum cryptography, and it has been proven that this can be achieved on a classical computer in exponential time, even for conjectured classical deterministic or randomized computers. Shor's algorithm can factorize a large number n in $O((\log n)^2 * \log\log n)$, or in polynomial time.

4.2 Period-finding and Quantum Fourier Transform

The essence of Shor's algorithm is to find the period of some sequence. Suppose we want to find factors of number $N > 1$. Randomly choose some integer $a \subset 2, ..., N-1$. If the greatest common divider(gcd) of a and N is larger than 1, then a is the factor what we need to find. If $\gcd(a, N) = 1$, consider the following sequence

$$1 = a^0 \ mod \ N, a^1 \ mod \ N, a^2 \ mod \ N, ... \tag{4.1}$$

We can find a least r which satisfy both of the following equation

$$1 = a^r \ mod \ N \qquad 0 < r \leq N \tag{4.2}$$

This r is called the period of this sequence. For simplicity, r is even, so we can have

$$a^r \ mod \, N = 1 \rightleftharpoons (a^{\frac{r}{2}}+1)(a^{\frac{r}{2}}-1) \ mod \, N = 0 \rightleftharpoons (a^{\frac{r}{2}}+1)(a^{\frac{r}{2}}-1) = kN \tag{4.3}$$

Here $k > 0$ because both $a^{\frac{r}{2}} + 1 > 0$ and $a^{\frac{r}{2}} - 1 > 0$ ($x > 1$). Therefore, $a^{\frac{r}{2}} + 1 > 0$ OR $a^{\frac{r}{2}} - 1 > 0$ will share a factor with N. Accordingly, if we have r then we can compute $\gcd(a^{\frac{r}{2}} + 1, N)$ and $\gcd(a^{\frac{r}{2}} - 1, N)$ effectively(in $O((\log n)^2 * \log\log n)$ steps), and both of the two gcds will be nontrivial factors of N. If we choose an x that does not give a factor, a few more attempts can be made to obtain random x which gives a high probability of finding a factor.

Problem is how can we find r? Before that let's warm up by the concept of the quantum fourier transform. Let $Z_q = 0, ..., q-1$, for each $a \in Z_q$ we define a function $\chi_a : Z_q \rightarrow C$ by

$$\chi_a(b) = e^{2\pi i \frac{ab}{q}} \tag{4.4}$$

The set of basis states $|a\rangle|a \in Z_q$ is called standard basis. An alternative basis is the set $|\chi_a\rangle|a \in Z_q$, called Fourier basis, can be defined by

$$|\chi_a\rangle = \frac{1}{\sqrt{q}} \sum b \in Z_q \chi_a(b)|b\rangle \tag{4.5}$$

The quantum fourier transform(QFT) is the unitary transformation that maps the standard basis to the Fourier basis

$$QFT : |a\rangle \rightarrow |\chi_a\rangle \tag{4.6}$$

It is proved that if q is smooth(meaning all factors of q are $O(\log q)$, such us $q = 2^i$), then the QFT can be implemented on the quantum computer.

4.3 Two steps to factorize with Shor's algorithm

Now let's see how the whole factorization process occurs with Shor's algorithm.

The first step is transferring the factoring problem to the problem of order-finding. Based on what we have in the previous section ,we have the flowing chart as follows

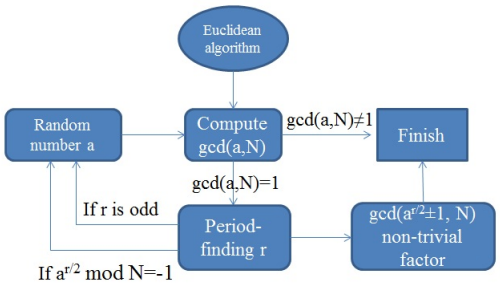

Figure 4.1: Flowing chart of first step of Shor's algorithm: reduction to period-finding

The second step is the subroutine of period-finding, which requires quantum computer to finish in a polynomial time. We need to mention that the

quantum circuits are different for each choice of a and N. Suppose we already have q quantum computer which can determine which type of sub-circuit will be chosen for different set of a and N. Pick some $Q = 2^q$ such that $N^2 < Q \leq 2N^2$. For input and output registers, they need to hold superpositions expanded from 0 to Q-1. After these prerequisites have been prepared, we can proceed the flowing chart Figure (4.2)

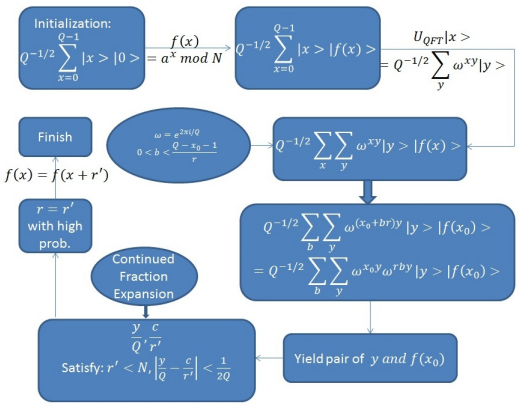

Figure 4.2: Flowing chart of second step of Shor's algorithm: period-finding

If we treat the quantum part: period-find part as the classical analogue, except we using the quantum register, we find that there is no exponential processing involve during these two steps. We clear demonstrate that the Shor's algorithm have a great advantage over the classical algorithms in factoring numbers into prime number, proving the existence of quantum computer.

Chapter 5

End of world?

Is that the end of the world? It seems that quantum computer will come out very soon and the public key distribution system will be broken down very soon! There is no secret in the e-commercial transactions, and the whole economy will fall into parts! Do not worry! Even if the quantum decryption algorithms will come out and be used for monitor the secrets of the world, the counterpart of quantum encryption algorithms will compete with these quantum eavesdroppers. We believe that science is always in harmony with the development of human-beings' nature. As long as people keep an objective and righteous attitude towards the applications of quantum computer, it can only help us to make a better and easier life.

Bibliography

[1] Thomas Kelly, *The Myth of the Skytale*, Volume 22, Issue 3, pages 244 - 260, Cryptologia, July 1998.

[2] Murk, *The Caesar Shift*, September 2, 2004.

[3] *Enigma Machine: History And Development Of The Machine*.

[4] Artur K. Ekert and G. Massimo Palma, *Quantum cryptography with interferometric quantum entanglement*, Journal of Modern Optics, Vol.41, No. 12, 2413-2423 (1994).

[5] Gilbert Sandford Vernam, *Gilbert Sandford Vernam from wikipedia*, Last editied on 19 August 2010 at 03:46.

[6] R. L. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, Volume 21 Issue 2, Feb. 1978.

[7] Diffe, W., and Hellman, M., *New directions in cryptography*, IEEE Trans. Inform. Theory IT-22, (Nov. 1976), 644-654.

[8] Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K. Lenstra, Emmanuel Thom,Joppe W. Bos, Pierrick Gaudry, Alexander Kruppa, Peter L. Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev and Paul Zimmermann, *Factorization of a 768-bit RSA modulus*, February 18, 2010.

[9] Richard P. Feynman, *Simulating Physics with Computers* International Journal of Theoretical Physics, Vol. 21. Nos. 6/7, 1982.

[10] IBM's Test-Tube Quantum Computer Makes History 2001

[11] *D-Wave Demonstrates 28-Qubit Quantum Computer*, Nov. 2007.

[12] Dr. Geordie Rose, *AQUA@home* December, 2008.

[13] S. Ghosh, R. Parthasarathy,T. F. Rosenbaum and G. Aeppli *Coherent spin oscillations in a disordered Magnet*, Science 296, 2195 (2002).

[14] J. Majer, J. M. Chow, J. M. Gambetta, Jens Koch, B. R. Johnson, J. A. Schreier, L. Frunzio, D. I. Schuster, A. A. Houck, A. Wallraff1, A. Blais1, M. H. Devoret, S. M. Girvin and R. J. Schoelkopf, *Coupling superconducting qubits via a cavity bus*, Nature Vol 449, 27 September 2007.

[15] Dorit Aharonov, *Quantum Computation*, Annual Reviews of Computational Physics, World Scientific, vol VI, 1998.

[16] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin and H. Weinfurter, *Elementary gates for quantum computation*, Phys.Rev. A52 (1995)

[17] D. Hanneke, J. P. Home, J. D. Jost, J. M. Amini, D. Leibfried and D. J. Wineland Realization of a programmable two-qubit quantum processor, Nature Physics 6, 13 - 16 (2010).

[18] M. A. Nielsen and Isaac L. Chuang, *Programmable Quantum Gate Arrays*, Phys. Rev. Lett., Vol.79, No. 2, July 1997.

[19] Adriano Barenco, David Deutsch, Artur Ekert and Richard Jozsa, *Conditional quantum dynamics and logic gates*, Phys. Rev. Lett. 74, 4083C4086 (1995).

[20] Selvakumar V. Nair and Toshihide Takagahara, *Theory of exciton pair states and their nonlinear optical properties in semiconductor quantum dots*, Phys. Rev. B, Vol. 55, No. 8, Feb. 1997.

[21] Rajeev J. Ram, *Semiconductor Optoelectronics, Lecture 13: Quantum Confined Stark Effect*, MIT.

[22] M. Brune, P. Nussenzveig, F. Schmidt-Kaler, F. Bernardot, A. Maali, J. M. Raimond, and S. Haroche , *From Lamb shift to light shifts: Vacuum and subphoton cavity fields measured by atomic phase sensitive detection*, Phys. Rev. Lett. 72, 3339C3342 (1994).

[23] Dirk Bouwmeester, Artur K. Ekert and Anton Zeilinger, *The physics of quantum information:quantum cryptography, quantum teleportation, quantum computation*, Page 126-132,Springer, 2000.