4

Trends in Research and Development of the Quantum Computer

TETSUYA YAMAZAKI
Information and Communications Research Unit

4.1 Introduction

It was announced in “Nature,” a British science magazine, on December 20, 2001 that a research group of MIT (Massachusetts Institute of Technology) and IBM had succeeded in a fundamental experiment to make a simple factorization using a quantum computer. The actual calculation used in this experiment was very simple; 15 = 3 x 5. Why does this topic have such an important meaning as to be taken up in Nature? Because this calculation was made by a computer incorporating a completely different theory from ordinary computers currently being used.

Semiconductor devices based on the Si processing technology and ordinary computers using these semiconductor devices have evolved quickly according to Moore’s Law. However, it is said that the limit will soon be reached due to problems of minuteness and generation of heat. It is said that even if the technology can break through the issue of minuteness by around 2010, it will in the end face the problem of heat generation by around 2020. Nanodevices and molecular devices are in the spotlight as means to break through this problem.

Ordinary computers currently available have several other limits. Factorization of large numbers is one of them. With current computers, the calculation may take a vast amount of time, making it practically impossible to do. For instance, the fastest computer currently available may take several hundred million years to make a factorization of a number with 200 digits. In the last 10 years, the calculation speed of a computer has improved by about 200 times. Even if the development progresses at the same pace and the speed improves again by 200 times in 10 years from now, it may take several million years to do the same calculation, making it still impossible to do practically. However, the quantum computer operating at a clock speed of around 100 MHz may be able to calculate a factorization of a number with 200 digits within several minutes.

The level of difficulty of the factorization is a foundation of security for the public key cryptosystem (RSA cryptosystem), which is now widely used on the Internet. If the quantum computer is put to practical use, the security of the public key cryptosystem will be lost. In 1994, Mr. P. Shor announced a factorization algorithm using the quantum computer and logically indicated that factorization could be made quickly. With this as a momentum, quantum computer research activities have become active.

Thus, the quantum computer can make certain calculations outstandingly faster than computers currently available (they are referred to as the classic computer in contrast with the quantum computer). Since the required energy to operate a quantum is very small and its time is so short, the quantum computer can theoretically be a low-heat-generation, super-high-speed computer, the same as nanodevices. However, in order to put it to practical use, it may take a lot of time and there are many problems that must be solved.

In this report, I examine the future evolution to put the quantum computer to practical use, while explaining about the theory of the quantum computer as well as the trends of research and development activities.

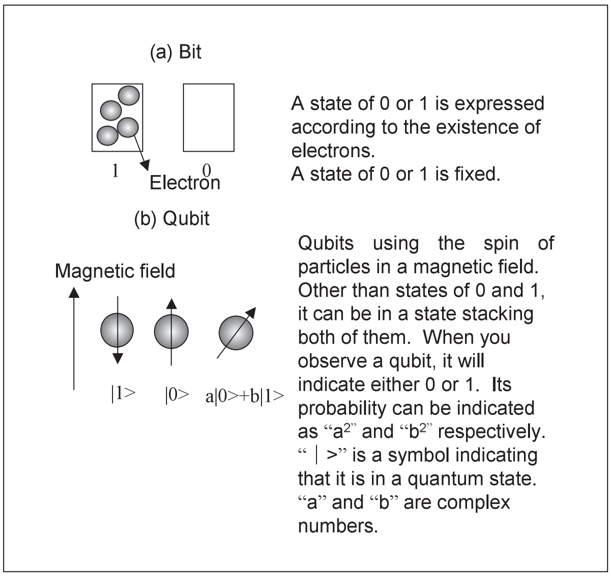
4.2 What is a quantum computer?

4.2.1 Differences between the quantum computer and the classic computer

A classic computer is composed of bits (memories) storing data and logic gates (combinations of transistors) operating the bits. The bits are basically capacitors and the state of 0 or 1 will be decided according to conditions of whether the bit has a charge or an electron. A single bit indicates either 1 or 0, so then n pieces of bits express a binary value with n digits.

On the other hand, the quantum computer is also composed of bits (called quantum bits or qubits) and mechanisms operating and observing the qubits. Two quantum-mechanical states are used for expressing 1 or 0. (A quantum computer using three or more states is also possible.) In the qubit, various kinds of systems can be used, which include spin directions of electrons or nucleuses, energy levels of electrons of quantum dots, polarization of photons, directions of quantized magnetic fluxes, and the ground/excitation states of the electron orbits of atoms. Operating methods of them also depend on the qubit. Although the explanation about qubit as shown in Figure 1. (b) is often used for convenience, knowledge of expression with wave functions based on quantum mechanics is required to correctly understand the qubit (Figure 1).

Figure 1: Differences between bits and qubits



A state of 0 or 1 is expressed according to the existence of electrons.
A state of 0 or 1 is fixed.

Qubits using the spin of particles in a magnetic field. Other than states of 0 and 1, it can be in a state stacking both of them. When you observe a qubit, it will indicate either 0 or 1. Its probability can be indicated as "a^2" and "b^2" respectively. " | >" is a symbol indicating that it is in a quantum state. "a" and "b" are complex numbers.

Source: Author's compilation on the basis of "The quantum computing" of C. P. Williams et al., and so on

The following four basic characteristics of quantum mechanics are important for the quantum computer.

(a) Stack

This is to send photons or electrons one by one so that they will go through 2 slits at the same probability, and observe where the particles passed through will arrive. Although they must be observed at points corresponding to the respective slits, according to the classic theory, we can observe similar patterns of interference fringes of waves. This indicates not that the respective particles have gone through either one of the slits, but that states where particles have gone through both of the slits are stacked each other provide the same phenomena as the interference of waves.

(b) Convergence of wave packets

In the above-mentioned experiment, quantum mechanics foretells only that particles will be observed at a certain probability corresponding to the intensity of an interference fringe at a certain position. It is impossible to predict where the respective particles will be observed. However, you will know the positions of where the respective particles are detected if you actually observed them. This means that wave functions spread in a form of an interference fringe before observation have been converged at a certain point by the observation.

(c) Uncertainty

In classic mechanics, positions and momentums of particles can be observed at the respective arbitrary accuracies. However, in quantum mechanics, positions and momentums of particles cannot be decided indivisually; for instance, when you attempt to decide a position, a momentum will be uncertain, and when you attempt to decide a momentum, a position will be uncertain.

(d) Entanglement

This is a phenomenon where a special interrelation takes place among multi qubits. In terms of the direction of spin (magnetization) of two electrons, this is a state where probabilities to turn toward either one of the directions are equal but when one of them turns toward one direction, the other one always turns toward the reverse direction. When this state is expressed as a wave function, wave functions of two separate qubits are not independent but they can be expressed by a stacked wave function. Particles that have been in the entangle state once, will not loose their characteristics. However, there is a possibility that this interrelation will be lost due to disturbance. This is referred to as decoherence.

For the quantum computer, characteristic (a) as mentioned above is particularly important. With the stack characteristic, a qubit can be in both(or intermediate) state of 0 and 1 in the same time. A difference from the analog computer is the fact that an answer obtained when you observe this qubit is either 0 or 1.

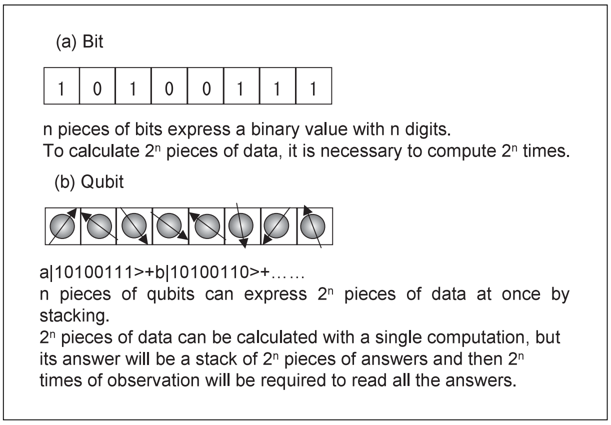
When this stack characteristic is expanded to n pieces of qubits, it is possible to express 2^n pieces of binary values with n digits simultaneously. Calculating with this qubit group, you can obtain 2^n pieces of answers in a single calculation. This is referred to as quantum parallel computation. This is one of the advantageous points of the quantum computer in comparison with a classic computer (Figure 2).

However, an answer will also be a stack of 2^n pieces of answers. Due to the convergence of wave packets as mentioned in the above (b), this stack will be converged at a certain value by observing the answer. Since it is arbitrarily decided at this moment which answer in the stack will be obtained, it is necessary to examine an algorithm so that wave packets will be converged at the required answer with a high probability. Furthermore, at the same time when stacked answers will be converged on a value, stacked input values will also be converged on a value corresponding to the answer. This is one of the characteristics of the quantum computer that this interrelation between input and output values is always maintained with the entanglement (a stack of wave functions) as mentioned in the above (d). If explained in a very simplified way; the quantum computer will stack up numerous wave functions composed of multi qubits, and pick up a wave function that will be an answer by operating the stack.

Other than the quantum computer, the above (c) is a basic theory of the quantum cryptosystem and the above (d) is used in quantum communications referred to as quantum teleport.

In order to actually operate qubits on the quantum computer, quantum gates must be configured. There are two types of quantum gates; namely, the phase shifter (it is also called the phase gate) and the control NOT gate, which corresponds to AND and NOT (or OR and NOT), the basic logic gate of current computers (Figure 3). If these two gates can be materialized, the

Figure 2: Stack of qubits



(a) Bit

1	0	1	0	0	1	1	1

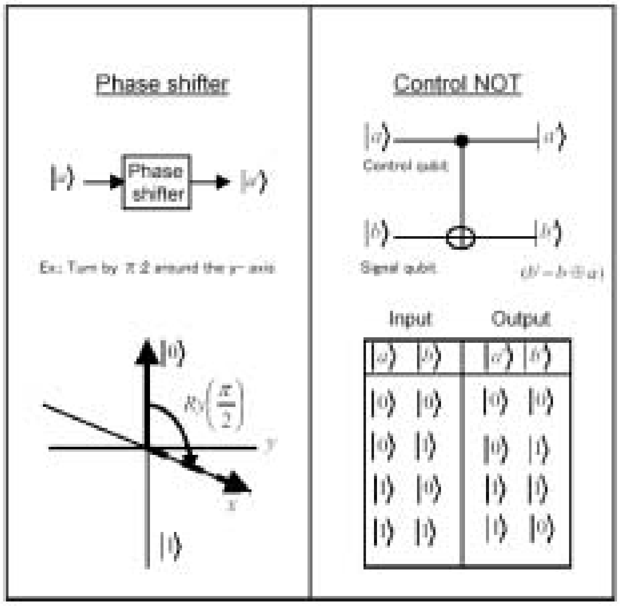
n pieces of bits express a binary value with n digits.
To calculate 2^n pieces of data, it is necessary to compute 2^n times.

(b) Qubit

a|10100111>+b|10100110>+……
n pieces of qubits can express 2^n pieces of data at once by stacking.
2^n pieces of data can be calculated with a single computation, but its answer will be a stack of 2^n pieces of answers and then 2^n times of observation will be required to read all the answers.

Source: Author's compilation on the basis of "The quantum computing" of C. P. Williams et al., and so on

Figure 3: Quantum gates

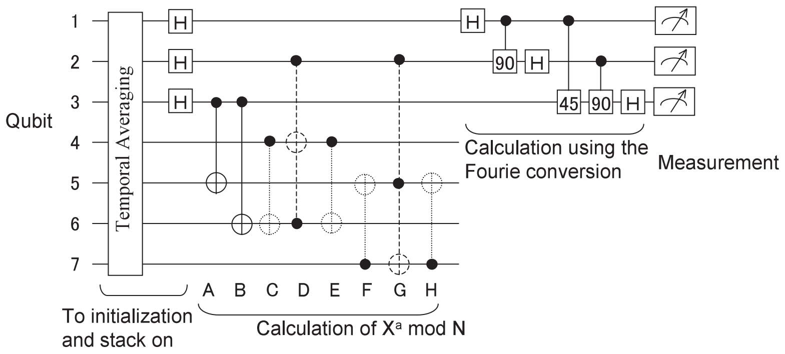


$\lvert a\rangle$	$\lvert b\rangle$	$\lvert a'\rangle$	$\lvert b'\rangle$
$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$	$\lvert 0\rangle$
$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$
$\lvert 1\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 1\rangle$
$\lvert 1\rangle$	$\lvert 1\rangle$	$\lvert 1\rangle$	$\lvert 0\rangle$

The phase shifter is used for expressing a stack of quantum states. The control NOT appears the same as a logic circuit of 0/1, but there is a difference that the control NOT can accept a stack state.

Source: Infromation-teconology Promotion Agency's investigation report, "Investigation on the research and development of the quantum computer."

Figure 4: An example of an algorithm for the quantum computer (Shor's factorization algorithm made by Chuang et al.)


Qubit
1
2
3
4
5
6
7
Temporal Averaging
H
90
45
Calculation using the Fourie conversion
Measurement
A B C D E F G H
To initialization and stack on
Calculation of X^a mod N

$\boxed{H}$ is the generation of a stack state, and $\boxed{45}$ and $\boxed{90}$ indicate phase shifts at the respective angle. The dotted lines indicate calculations omitted by optimization, and the dashed lines indicate calculations that were converted to simpler operations.

Source: Author's compilation on the basis of the reference [5]

quantum computer will be able to calculate any algorithm that can be calculated (Figure 3).

An example of algorithms for the quantum computer is shown in Figure 4.

4.2.2 History of the quantum computer

The possibility of the quantum computer had been pointed out a relatively long time ago. However, practical research activities started in the 1970s. The research started from a study on what would happen if the size of the current LSI were reduced up to where the quantum effect would be dominant. In the 1970s to 1980s, it had been indicated that all the logic gates available in a current computer could be materialized with the quantum computer logically. However, the activities declined in the later half of the 1980s, due to the difficulties in materializing hardware and no advantageous points in comparison with current computers, etc.

The quantum computer gained the spotlight again in 1994, when Mr. P. Shor of AT&T (present Lucent) Bell Laboratories logically verified that the quantum computer could calculate a factorization of a high number within a reasonable time, which a current computer could not do practically. The difficulty of the factorization is a foundation of security for the public key cryptosystem (RSA cryptosystem), which is now widely used on the Internet. If the quantum computer is materialized, the public key cryptosystem will be broken easily. Through this research, the quantum computer became widely recognized as a useful item, and, as such, many researches related to it have been conducted positively all over the world. At the same time, various kinds of research activities related to communications technologies based on quantum mechanics progressed as well, such as the quantum cryptosystem and quantum communications, and, as a result, new technology fields namely the quantum information theory and quantum information technology (QIT) have shown up.

4.3 Examples of the quantum computer

4.3.1 Hardware

Five conditions required for configuring the quantum computer are cited as follows.

(1) Qubits can be practically materialized as a physical system and integrated. (5,000 pieces of qubits are required for factorizing a number with 1,000 bits.)

(2) The respective qubits can be measured.

(3) The respective qubits can be operated. (Computation of basic qubits must be possible.)

(4) The time for interaction among qubits (the decoherence time) must be sufficiently longer than the calculation time (time for operating a qubit once x the number of operations). (It is said that the decoherence

time must be at least 1,000 to 10,000 times longer than the calculation time. For factorization of a number with 1,000 bits, 5 x 10^{11} times of operations are required.)

(5) Qubits can be initialized.

Table 1 shows the candidates of quantum computers now being researched that satisfy the above-mentioned conditions. All of them are now on the basic research level. Among them, the method combining organic molecules and NMR, which is now being developed by a group led by IBM, is the most progressed. However, it is very difficult for this method to support multi qubits and it is said that there is a wall at around 10 qubits. Other methods also have merits and demerits, and various ideas are now being proposed for further breakthroughs. There is also a proposal to use a molecular device itself for the quantum computer.

4.3.2 Algorithm

As mentioned above, if two basic quantum gates can be materialized, the quantum computer can calculate any kind of algorithm by combining these two gates. However, if the same algorithms as the ones used in current computers are utilized, it is not necessary to be the quantum computer. Under existing circumstances, there are roughly three algorithms (and some other problems similar to them) where the quantum computer can make overwhelmingly more efficient calculations than a classic computer as follows.

(1) Factorization (Shor's algorithm)
(2) Database retrieving (Glover's algorithm)
(3) Traveling salesman problem (given a finite number of "cities" along with the road of travel between some pair of them, find the shortest way to visit all the cities once and return to your starting point)

Table 1: Candidates of quantum computers being researched and their features

Method	Qubit	Advantages	Disadvantages	Current situation
Ion trap	Vibration mode of the gravity center of an ion fixed by an electromagnetic field under vacuum	The decoherence time is long.	It is difficult to support multi qubits. It will operate only under a vacuum condition.	The entanglement with 4 qubits has been confirmed.
NMR (Nuclear Magnetic Resonance)	Nucleus spin of organic molecules in a solution (a single molecule is a quantum computer)	It can operate at normal temperature. It can measure many molecules (quantum computers) at once. It can be materialized with the NMR equipment.	It is difficult to support multi qubits. (Designing of molecules is required.) If the number of qubits increases, it will be difficult to analyze the measured results.	Shor's algorithm has been materialized with 7 qubits.
	Nucleus spin of a crystal or an atomic line	It is relatively easy to support multi qubits. The decoherence time is long (?)	It is difficult to analyze the measured results. It will operate only at an extremely low temperature. It is difficult to provide elements.	The element is under development.
Quantum dot	Spin of an electron kept in a quantum dot	It is relatively easy to support multi qubits. The decoherence time is long (?)	It will operate only at an extremely low temperature. It is difficult to provide elements.	The element is under development.
Superconducting element	Magnetic flux or cooper pairs generated on a superconductor	It is relatively easy to support multi qubits. The decoherence time is long.	It will operate only at an extremely low temperature.	The entanglement with 2 qubits has been confirmed.
Photon	Polarization state of photons, etc.	The decoherence time is long. It can operate at a normal temperature.	The interaction between quanta is not sufficiently strong. It is difficult to support multi qubits.	An experiment with 3 qubits.

Source: Author's compilation on the basis of the Information-technology Promotion Agency's investigation report, "Investigation on the research and development of the quantum computer," etc.

These problems are basically issues for choosing one among numerous candidates. In these problems, a feature of the quantum computer, i.e., capability to make a large amount of calculations with a few steps by using quantum parallel computation, can be effectively used. However, since the calculation results will also be observed in a stack state, it is necessary to at least converge them on a few numbers of wave functions, which can be analyzed to choose a wave function to be an answer. This is one of the most difficult points of algorithms for the quantum computer. (Refer to the supplemental explanation.)

It is theoretically impossible to reduce to zero the probability of the quantum computer observing an incorrect answer. Since the stack among qubits is also arbitrarily destroyed (decoherence), there is a possibility of calculation errors. Thus, it is necessary to reduce the error rates by performing more than one calculation or to provide some type of error correction means. Then, it is required to maintain the efficiency of the algorithms within a reasonable range even if these extra works are included.

Conversely speaking, at present, the quantum computer can be applied to only these three areas (and some other similar problems), and it is expected that algorithms supporting a wider range of problems will be developed. It is also important to develop efficient error correction algorithms.

4.4 Current situations of research and development activities for the quantum computer in the respective countries

The quantum computer is often developed not only as a future computer technology but also as a part of quantum data communications technologies including the quantum cryptosystem and quantum communications, or nanotechnologies. In this section, I take up several projects relatively concentrating on the quantum computer.

4.4.1 U. S.

In the U. S., there are many big names involved in this field, including IBM famous for the NMR quantum computer, Bell Laboratory (AT&T to Lucent) of algorithms for quantum computing, NIST of the qubits using Ion trap and Los Alamos Laboratory of the qubits using the quantum dot. As governmental projects, the quantum computer has been taken up for the first time in the annual budgetary request of the U. S. Information Processing and Communications Policy (Blue Book) FY1997 (issued in November 1996) and in the implementation plan (issued in January 1997) as a part of the High End Computing and Computation (HECC) program. In these documents, the quantum computer is treated as a future technology of which research activities must be supported by the government, along with the bio computer and the optical computer. This point has not changed in the budgetary request for FY2002 as well. Meanwhile, it was proposed that the research and development of quantum information communications technology be promoted as a fundamental information and communications technology in the IT^2 Plan announced in 1999.

Core institutes in the field of HECC are NSF, DARPA, NIST, NSA, DOE, NOAA, NASA and so on. Among these institutes, NSA, maintaining a watch on decipherment of cryptosystems with the quantum computer and the quantum cryptosystem, leads projects related to the quantum computer. The first phase of the project was jointly executed among more than 9 universities and companies, and governmental institutes such as DARPA and NIST from 1994 to 1999. The second phase is now being executed successively. The budget amounts of the individual projects are unknown, but the total amount of the budget for HECC of NSA is around $20 to $25 million/ annually.

Since FY2001, DARPA has started a series of research and development activities for the next generation technologies including the quantum computer, with the title of "Beyond Silicon," under the "Microelectronic Device Technology" project. The "Beyond Silicon" activity was upgraded to project status in FY2002. Among the themes of the "Beyond Silicon" project, "The Quantum Information Science and Technology" is directly related to the quantum computer and quantum

<Supplement>

Method of factorization using the quantum computer

In the case of factorization, the simplest algorithm is as follows. A number "N" to be factorized will be divided by "a" that is any integer of 2 or more and $N^{1/2}$ +1 or less. The quantum computer will execute this calculation as follows.

1) To store "N" in the 1st quantum memory and a stack of integers of 2 or more and $N^{1/2}$ +1 or less in the 2nd quantum memory, respectively.
2) To divide the 1st memory by the 2nd memory, and store the residual of this division in the 3rd quantum memory.
3) The number indicated in the 2nd memory when the observed result in the 3rd memory is zero (the 2nd memory will be converged by the observation of the 3rd memory), will be one of the desired factors.

In this method, the dividing operation can be made with a single step due to the stack of qubit and quantum parallel computation, but the probability for reading numbers other than zero in the 3rd memory will be overwhelmingly high. Consequently, the number of observations repeated in the 3rd memory until observing zero will be almost the same as the number of steps for repeating the dividing operations in the classic computer. (If the "N" is a number of the order of 10,000 and a product of 2 pieces of prime numbers, there is only one case of which the residual is zero among stacks of $N^{1/2}$ (around 100). In this case, the probability for observing zero during the repeats up to 100 times is only 63%. On the other hand, it is certainly possible to obtain an answer by repeating the dividing operation up to 100 times in the classic computer.)
Thus, the following characteristic of integers is used in the Shor's algorithm.

1) x^a mod y ("x^a mod y" is a function for finding a residual after dividing "x^a" by "y") is a periodic function of "a" relative to integers x and y, which are prime numbers each other (they don't have any common measure other than 1).
2) If a period "r" satisfying x^{nr} mod y = 1 ("r" will be an integer, "n" will be 0, 1, 2, 3 …) under the condition the above 1) exists and "r" is an even number, its equation will be as follows.

$$(x^r -1) \bmod y = \{(x^{r/2} - 1)(x^{r/2} + 1)\} \bmod y = 0$$

Then, either one of $x^{r/2} - 1$ or $x^{r/2} + 1$ at least, and y will have common measures other than 1.

The actual calculation will be as follows.

1) To choose an integer "x" (N > x) that is a prime number relative to an integer "N" to be factorized at random.
2) To choose an appropriate integer "q" satisfying $N^2 < q < 2N^2$
3) To calculate $y = x^a$ mod N (a = 0, 1, 2, … q-1) for all "a" by using quantum parallel calculation. If you obtain a value "k" as observing "y" on this stage, "a" will be a stack of an integer h + nr ("h" is an integer, "r" is a period, and n = 0, 1, 2, …) satisfying x^{h+nr} mod N =k, but "r" cannot be found since all "h", "r" and "n" are unknown.
4) To make Fourie conversion for "a". The details of the process will be omitted. The value to be obtained will be a stack of mq/r (m = 0, 1, 2, … r-1).
5) To find a single value of "c" satisfying $c = m_0\, q/r$ (m_0 = 0, 1,2, … r-1) as a result of observation of the above 4).
6) If "m_0" and "r" are prime numbers each other, "r" can be calculated by reducing "c/q" (both of them are known). It is possible to increase the probability for that "m0" and "r" are prime numbers each other by repeating the calculation.
7) If "r" is a even number, you can find the greatest common measure between $x^{r/2} - 1$, $x^{r/2} + 1$ and y.

Source: Author's compilation on the basis of the reference [1, 2] and [5]

Table 2: The number of research projects related to the quantum computer approved by NSF

Year	The number of approved projects	Total amount ($)	Amount / project	Term
1995	23	4,930,629	214,375	1 - 4 years
1996	20	5,851,012	292,551	2 - 4 years
1997	23	5,923,848	257,559	0.8 - 4 years
1998	25	6,504,615	260,185	2 - 4 years
1999	22	4,808,112	218,551	2.8 - 4 years
2000 (Note)	6	1,361,800	226,967	3 years
Total	119	29,380,016	246,891	0.8 - 4 years
Programs under execution	61	15,435,106	253,035	

Note: Data for 2000 is as of April 2000.

Source: The investigation report of the Ministry of Posts and Telecommunications (the present Ministry of Public Management, Home Affairs, Posts and Telecommunications), "For creating revolutionary quantum information processing and communications technologies in the 21st century."

communications technology. Its actual budget for FY2001 was about $14.3 million, and its requested budget for FY2002 is $23.8 million. It is planning to request a budget of $27.1 million for this project in FY2003. Other than this, technologies related to the quantum computer such as the quantum dot or the quantum algorithm, etc., have been taken up in the themes of “Materials Science,” which is a research project related to nanotechnology, or the “High Performance and Global Scale System” related to computer science.

Furthermore, laboratories under NIST are promoting research on the quantum computer and quantum communications. In particular, their research on the ion trap method is famous. Table 2 shows the number of projects related to the quantum computer, which NSF fosters.

4.4.2 Europe

EC has provided and executed its research plan (Framework) for the entire region every 4 years since 1984. The 5th Framework is now being executed. For information processing and communications technology including the quantum computer, research and development activities have been conducted as a part of the ESPRIT project in the 1st to the 4th Frameworks.

The 5th Framework (from 1998 to 2002) is classified into 4 vertical fields and 3 horizontal theme, and information processing and communications technology including the quantum computer is executed as a part of the IST (Information Society Technology research).

Programs in the IST are classified into 9 kinds: 5 kinds by technology field including 4 kinds of existing technologies and 1 kind of new technology; and 4 kinds by its activity formation mainly aiming to support research activities. Researches on quantum information processing and communications are executed in the Quantum Information Processing & Communications (QIPC) project in the Future and Emerging Technologies (FET) in the field of new technologies.

In the QIPC, there are 12 research projects (started in 1999 to the beginning of 2000, with terms of 3 to 4 years) invited in 1999, and additionaly, 4 projects (their terms are 1 to 3 years) are currently conducted through FET-OPEN, a system inviting research projects at any time. According to the “For creating revolutionary quantum information processing and communications technologies in the 21st century” (the investigation report of the Ministry of Posts and Telecommunications), the total amount of the research fund for QIPC is expected to be about 22.4 million Euro. Out of this, about 17.2 million Euro (about 77% of the total) will be borne by EC.

A feature of the research projects of EC is that many institutes from many countries participate. The IST has the “Network of Excellence” Program aiming to intensify cooperation among the participating research institutes and to pass back the research results to the industries more positively, and QIPC also has a network project that is referred to as The Physics of Quantum Information European Research Network (QUIPROCONE). Its term is for 3 years from July 2000.

In the 6th Framework starting from 2002 up to 2006, the IST and the QIPC will continue, and the 2nd invitation of research projects was conducted in March 2002.

Other than the programs of EC, research networks among universities in the countries in Europe, which are led by Oxford University in the U. K., have spread spontaneously since around 1995.

4.4.3 Japan

In Japan, theoretical researches done by certain research groups were main streams of research activities on the quantum computer up to around 1990. Since around fiscal 1994, researches related to the quantum computer had been conducted as parts of selective themes of the CREST (Core Research for Evolutional Science and Technology) and the ERATO (Exploratory Research for Advanced Technology) of the JST (Japan Science and Technology Corporation). In 1999, the

Table 3: Major research projects related to the quantum computer and quantum communications in Japan

Research and development scheme	Theme	Research institute (Term)	Remarks
Japan Science and Technology Corporation International joint research	Quantum transition project	The University of Tokyo Notre Dame University, University of California (For 5 years from 1994)	
Japan Science and Technology Corporation Core Research for Evolutional Science and Technology	Correlative electronics	NTT, The University of Tokyo, The Graduate University for Advanced Studies, Electrotechnical Laboratory (For 5 years from 1998)	
Japan Science and Technology Corporation International joint research	Quantum entanglement	Stanford University, CNRS (National Center for Scientific Research of France) (For 5 years from 1999)	Japan will bear ¥1 billon for 5 years
Japan Science and Technology Corporation Core Research for Evolutional Science and Technology	Dynamics control of quantum correlative functions	The Institute of Physical and Chemical Research (Started from 1999)	
Japan Science and Technology Corporation Core Research for Evolutional Science and Technology	Nucleus spin network Quantum computer	Osaka University (Started in 2000)	
Japan Science and Technology Corporation Exploratory Research for Advanced Technology	Imai quantum computing mechanism	The University of Tokyo (Started in fiscal 2001)	
Ministry of Public Management, Home Affairs, Posts and Telecommunications Invited research projects	Research and development of quantum information processing and communications technologies	Invited research projects started in fiscal 2001	Budget ¥250 million

Source: Author's compilation on the basis of the investigation report of the Ministry of Posts and Telecommunications (the present Ministry of Public Management, Home Affairs, Posts and Telecommunications), "For creating revolutionary quantum information processing and communications technologies in the 21st century."

Quantum Information Technology Symposium was organized as a research society for a limited period under The Institute of Electronics, Information and Communication Engineers, so that a system for exchanging information and cooperating with research activities among researchers in various fields of science and engineering could be launched. In February 2000, the Information-technology Promotion Agency published "Investigation on the research and development of the quantum computer," and the Ministry of Posts and Telecommunications (the present Ministry of Public Management, Home Affairs, Posts and Telecommunications, MPHPT) published an investigation report titled "For creating revolutionary quantum information processing and communications technologies in the 21st century" in June 2000, respectively. Table 3 shows the on-going projects in Japan. For notes, The MPHPT's research projects are covering the entire quantum information processing and communications technology including the quantum cryptosystem and quantum communications.

4.5 Conclusion —For materializing the quantum computer

The direct, successive technologies of the current(classic) computer are the nano and molecule devices. With nano and molecule devices, it is expected that a computer having higher integration and extremely low power consumption will be materialized. Then, what is the position of the quantum computer?

The first thing we can think of is application as a subset of computers specialized in problems that can be solved efficiently with the quantum computer. However, for this, it is necessary to integrate a certain amount of qubits and materialize advantages in calculation speed that must be sufficiently faster than the classic computer, and it may take a lot of time. There is another problem in that fields where the quantum computer can be applied are too limited.

Thus, the transmitter/receiver and repeater equipment for quantum communications and the quantum cryptosystem are considered as the first application for the quantum computer. Becouse in which application, the quantum computer can be put to practical use even if the number of qubits is relatively few. The quantum cryptosystem is currently ready to be put to practical use except for its cost and limited communication distance. In particular, the photonic quantum computer is compatible with the quantum cryptosystem, in terms of hardware and technologies including the generating and detecting mechanism of single photon, etc.

On the other hand, there is a possibility for the quantum computer to be put to practical use quickly if completely new algorithms can be developed. As an idea, the quantum computer may be used for material development by simulating quantum states. While the classic computer requires peta flops class computing for simulating 1,000 pieces of atoms (see Science & Technology Trends, December 2001), it is considered that the quantum computer originally using the quantum state may calculate more efficiently. No practical result has been announced yet, but several research groups seem to be conducting relevant researches.

Thus, I think it is important to promote the quantum computer from an area where it can be put to practical use, such as seeking new fields where it can be applied and in technical breakthroughs.

On the other hand, the research field of the quantum computer and quantum information processing technology extend over a wide range covering from theoretical computer science, information theory, mathematics, physics, chemistry, and optics, and engineering such as materials and manufacturing technologies. It is possible to say that the research field is a boundary area having the potentiality to produce new ideas from various other research fields. Since it is a new research area, many attractive and untouched areas probably remain. In this sense, it may be required to introduce methods promoting many projects, taking in new concepts.

References

[1] C. P. Williams et al., "The quantum computing," Springer-Verlag Tokyo, 2000.

[2] Nishino, Tetsuro, "The quantum computer and

the quantum cryptosystem," Iwanami Shoten, 2002.

[3] Feature article,"The quantum information and the quantum computer," Mathematical Science No. 456, p. 5 (June 2001).

[4] Takeuchi, Shigeki, Magazine of the Institute of Electronics, Information and Communication Engineers,Vol. 84, No. 1, p. 17 (January 2001).

[5] L. M. K. Vandersypen et al., Nature, Vol. 414, p. 833 (2001.12.20).

[6] "Investigation on the research and development of the quantum computer," Information-technology Promotion Agency (February 2001).

[7] The investigation report of the Ministry of Posts and Telecommunications, "For creating revolutionary quantum information processing and communications technologies in the 21st century," (June 2001).

[8] 10th JST International Symposium "Quantum Computing"Abstracts (2002.3.12 – 14).

(Original Japanese version: published in April 2002)