Quantum Information Technology

Yoshiro Hirayama†

Abstract

Quantum mechanics and physics have become important sources for developing ultimately secure communication in the form of quantum cryptography and an extremely powerful computer called a quantum computer. Cutting-edge nanofabrication technologies, highly accurate measurements, and a deep understanding of quantum information science are necessary to control quantum systems arbitrarily and to advance the research on quantum information technology (QIT) toward quantum cryptography and quantum computers. This paper summarizes the present status and future expectations of QIT and describes some recent activities in NTT Laboratories.

1. Introduction

To transfer, store, and process information, we have used electrons and photons up to now. In current communication systems, they are manipulated by using several materials, including metals, semiconductors, and optical fibers. However, all these methods use the classical properties of electrons and photons.

Recent research on information technology has discovered a new and powerful source for information processing: quantum mechanics. Quantum mechanics was first developed at the beginning of the twentieth century and it has dominated many areas of physics, especially photonics and solid-state physics. Now, it has become an important source for guaranteeing "ultimately secure communication" that prevents all efforts of eavesdroppers and for making an extremely powerful "dream computer", which has vast parallelism based on quantum superposition [1].

Naturally the role of quantum mechanics has expanded to solid-state systems. Following Moore's law, the integration density of semiconductor circuits has increased dramatically every year, and semiconductor devices have developed from a single transistor to super computers. The size of structures inside semiconductor circuits is approximately 100 nm at present and it is decreasing rapidly. That means the structure size should become 20 to 50 nm by 2010. This scale is already close to that of the wavelengths of electrons in semiconductors. Therefore, quantum mechanical effects are expected to be significant in these future systems. Although it is not clear whether quantum effects will have good or bad effects on these cutting-edge supercomputers (which are still classical computers), using the quantum mechanical principle in computing systems has produced a new computer type, called the quantum computer.

The quantum computer will be more powerful than any existing or future classical computer because the superposition principle allows an extraordinarily large number of computations to be performed simultaneously. It promises to have tremendous potential for efficiently solving some of the most difficult problems in computational science, such as integer factorization and discrete logarithms, which are intractable on any present or future conventional (classical) computer. Other examples of the potentially great impact are quantum modeling and simulation, as first mentioned by Feynman [2]. Although many physical phenomena are now successfully described in quantum mechanics, we have simulated quantum mechanical systems by using a classical computer. Therefore, it might not be surprising if a quantum simulation is more effective than a classical one for representing quantum mechanical systems.

Quantum mechanics is also revolutionizing com-

† NTT Basic Research Laboratories
Atsugi-shi, 243-0198 Japan
E-mail: hirayama@will.brl.ntt.co.jp

munication systems. Any eavesdropping action leaves traces when quantum mechanics is used for information transfer processes. Therefore, in a quantum cryptography scheme where we utilize the uncertainty principle of quantum mechanics, we can confirm that communication has run completely securely without any eavesdropping. As discussed below, we can implement this quantum cryptography by placing information on a series of photon pulses. In other words, quantum cryptography is based on the quantum properties of a single photon not on photon-photon interaction. Therefore, quantum cryptography will be in actual use much earlier than the quantum computer, which uses the entanglement of many quantum particles. A test kit for quantum cryptography is already commercially available [3]. However, many issues remain to be solved before quantum cryptography becomes practical.

Taking into account the huge impact that QIT will have on future communication systems, we have accelerated research toward "ultimately secure communication" and "the dream computer" in NTT, especially in NTT Basic Research Laboratories. In this introductory paper, I summarize the status of quantum cryptography and quantum computers including developments in NTT. Our activities lead the field in some aspects of QIT as discussed in more detail in the following papers.

2. Quantum cryptography

Research for quantum cryptography has been progressing rapidly. Although using the macroscopic coherence of laser beams has been proposed, we have developed a more comprehensible method, which uses the quantum features of a single photon, *e.g.*, the circular and linear polarization of a single photon [4], [5]. Figure 1 illustrates a typical setup for quantum cryptography communication. The polarization characteristics of a single photon are used to share the cryptographic key between Alice and Bob. Because of the uncertainty principle of quantum mechanics, any eavesdropping can be detected, so Alice and Bob can share the key with the assurance of no eavesdropping. After the key has been successfully distributed, Alice sends information to Bob over a conventional communication line using the shared cryptographic key. Quantum mechanical theory confirms that the persons who know the key are limited to only Alice and Bob. Therefore, the communication is guaranteed to be ultimately secure.

In this quantum cryptography scheme, important

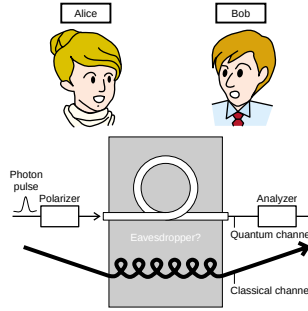

Fig. 1. Schematic diagram of quantum cryptography communication.

factors determining the performance of the quantum key distribution are a single-photon emitter and detector. The device characteristics and performance of the quantum key distribution system are summarized in Table 1. The emission efficiency of a single-photon emitter and the dead time, jitter and detection efficiency of a single-photon detector determine the maximum speed of quantum key distribution. The dark current of the detector is an important factor for determining the reliability of the system. Photon number fluctuation is also very important and reducing it improves the maximum transmission distance of the system. In a conventional system, a single-photon source is obtained by simply attenuating laser light. In such systems, the photon number fluctuates according to the Poisson distribution and there always remains a possibility that one pulse includes two or more photons. Developing technologies that could lead to an ideal single-photon source is really challenging. Quantum dots in a microcavity and turnstile devices may be good candidates for a future single-photon emitters. Recently, NTT, in collaboration with Stanford University, has demonstrated long-distance quantum key distribution using a quantum-dot single-photon emitter [6].

A highly sensitive photon detector is also in strong demand. The highly sensitive avalanche photodetector, the unicarrier photodetector, and the quantum dot photodetector may all be potential candidates for a single-photon detector. An efficient detector has been

Table 1. Device characteristics and performance of quantum key distribution system.

Device	Characteristics	Performance of key distribution system
Single-photon emitter	Photon number fluctuation Emission efficiency Higher temperature operation	Distance Speed Convenience
Single-photon detector	Dark count Dead time Jitter Detection efficiency Higher temperature operation	Reliability Speed Speed Speed Convenience

Wavelengths: 1.5 μm for an optical fiber system
0.8 μm for a short distance system, satellite system

developed for the 0.8-μm wavelength band, but not for the 1.5-μm band, which is necessary for quantum cryptography using optical-fiber communication systems. Meanwhile, the 0.8-μm band is useful as a test bed for quantum cryptography. This band is also applicable to short-distance secure communication systems and satellite communication.

3. Quantum computer

Research on the quantum computer has also progressed very rapidly. The Advanced Research and Development Activity (ARDA) predicts in its quantum computer roadmap that by 2012 we will be developing a suite of viable quantum computer technologies of sufficient complexity to function as quantum computer test beds, where architectural and algorithmic issues can be explored. This will require on the order of 50 physical quantum bits (qubits). Although the report claims that this development is not a prediction but a desired outcome, it suggests that the development in the quantum computer field will be fast and very competitive.

Developing a quantum computer is a basic endeavor in science today and a fault-tolerant quantum computer on a small scale could be made within the next decade. A quantum computer consists of qubits. In contrast to classical bits, $|0\rangle$ or $|1\rangle$, qubits can represent a superposition of $|0\rangle$ and $|1\rangle$, *i.e.*, $\alpha|0\rangle + \beta|1\rangle$ (where $\alpha^2 + \beta^2 = 1$). Therefore, a large number of qubits can represent a vast superposition and this huge parallelism makes it possible to solve some of the most difficult problems. For example, the time required for integer factorization increases exponentially as a function of the number of digits in a classical computer. However, in a quantum computer, Shor's algorithm [7] turns the integer factorization into an easy problem, where the processing time increases approximately linearly with the number of digits.

The necessary conditions for a practical quantum computer were first shown by DiVincenzo [8]. His criteria are:

1. a scalable physical system of well-characterized qubits;
2. the ability to initialize the state of the qubits to a simple fiducial state;
3. long (relative) decoherence times;
4. a universal set of quantum gates (for example a rotation gate and a controlled NOT (CNOT) gate); and
5. a qubit-specific measurement capability.

The first condition means a well-defined quantum superposition, *i.e.*, qubit formation, and the possibility to increase the number of qubits. The physical resource requirements, including gate operation steps, must scale linearly, not exponentially, with the number of qubits if the approach is to be a candidate for a large-scale quantum computer. The second condition describes the preparation of the initialization stage for many qubits, such as that of the $|000 - - - 0\rangle$ state. The third condition is essential for a practical quantum computer. All gate operations should be done maintaining the coherence of the system. This means that the decoherence time should be much longer than the gate operation time. The fourth condition is a universal set of gate operations for implementing several kinds of quantum calculation. Any kind of quantum calculation can be implemented by using only two gate operations: a rotation gate of one qubit and a CNOT gate for two qubits. The fifth condition is necessary for a successful readout of the calculated results.

Table 2 summarizes the statuses of proposed quantum computer systems from the viewpoint of DiVincenzo's criteria. Nuclear spin resonance (NMR) has been studied widely for the structural analysis of molecules and a coherent pulse technique has been devel-

Table 2. QC roadmap: development status.

	Single qubit operation	Two-qubit quantum gate operation	#1 Scalability	#2 Initialization	#3 Long decoherence	#4 Set of quantum gates	#5 Measurements
Solution NMR	◎	◎	?	○	◎	◎	○
Ion/atom trap	◎	◎	○	◎	○	◎	◎
Optical	◎	?	○	○	◎	○	○
e-helium	○	○	○	◎	○	○	○
Solid state	◎	○	○	◎	○	○	○

◎ = A potential approach has been successful with sufficient proof of principle.
○ = A potential approach has been proposed, but the principle has not been sufficiently proved.
? = No viable approach has been proposed.

oped. Therefore, at present, solution NMR is the leading technique for realizing a quantum computer system [9]. Shor's factorization algorithm has been implemented with a seven-qubit molecule using solution NMR techniques and has successfully identified the factors of 15 as 3 and 5 [10]. However, a chemical synthesis of special macromolecules is necessary for large qubit systems. Furthermore, solution NMR utilizes an advantage of solutions, and the energy separation of the nuclear spins of the $|0\rangle$ and $|1\rangle$ states is much smaller than the solution temperature, so the initialization of many qubits is very difficult. Therefore, this system may be inappropriate for a large-scale quantum computer, although it will be useful for testing some basic features of quantum computation.

An ion/atom trap is also an ideal test bed for quantum coherent control. However, the scalability of this system is also questionable. Optical systems are interesting because photons can easily form entangled pairs, which are used to confirm the principal aspects of entanglement [11]. However, the nonlinearity of the photon-photon interaction is not strong enough to achieve a viable two-qubit operation. Although implementing a quantum computer by using only linear optical systems has been proposed [12], its scalability may remain a problem. Although using electrons on the surface of liquid helium [13] is a new and interesting idea for implementing many qubits, solid-state qubits are considered the most suitable for future scalable quantum computers.

For many kinds of solid-state qubit systems, the initialization is rather easy and operations for one- and two-qubits have already been demonstrated. The most serious and challenging problem is how to get a long decoherence time in a solid-state system where decoherence is caused by several interactions, such as those with phonons and background charge fluctuation. Once the decoherence problem has been removed, the number of qubits in a solid-state system will increase, like the development from a single transistor to present-day large-scale integration. NTT is also focusing on developing solid-state qubits because they are expected to have scalability and because NTT Laboratories have excellent backgrounds for semiconductor and material science.

The present statuses of solid-state qubits are summarized in Table 3. Trial solid-state qubits can be roughly divided into three categories: superconductor qubits, quantum-dot qubits, and nuclear-spin qubits. For a superconductor qubit, we can use a charge (Cooper pair) [14] or flux [15] to implement a quantum two-level system. One-qubit operation was demonstrated earlier and two-qubit operation was achived recently [16]. A superconducting system has a macroscopic coherence with a superconducting gap so we can expect a rather long decoherence time. A cutting-edge experiment for a superconductor flux qubit has been done in NTT including single-shot readout [17].

Semiconductor quantum dots are extremely interesting nanostructures for realizing quantum two-level systems. A small quantum dot at a low temperature can provide an ideal system where a single electron or exciton is precisely controlled. Quantum-dot charge qubits have been demonstrated in NTT using coherent control of a single electron in a coupled quantum-dot system [18], [19]. This is the first demonstration of a fully electrical semiconductor qubit, and the electrical method has the advantage of local controllabil-

Table 3. QC roadmap: status of solid-state QC.

	Preparation of qubit states	Readout of qubit states	Coherent oscillation	Long decoherence	Two-qubit quantum gate operation	Multiple-qubit quantum gate operation
Superconductor charge qubit	◎	◎	◎	?	○	?
Superconductor flux qubit	◎	◎	◎	?	?	?
Quantum-dot charge qubit	◎	○	◎	?	?	?
Quantum-dot spin qubit	○	○	○	?	?	?
Quantum-dot exciton qubit	◎	○	◎	?	○	?
Nuclear spin in solid-state	○	○	○	◎	?	?

◎ = Sufficient experimental demonstration
○ = Preliminary experimental demonstration, but further work is required
? = No experimental demonstration

ity of the qubits. Using electron spin is also a plausible method for semiconductor qubits, although electrically controlling the electron spin is not easy. Coherent oscillation of electron spin has been studied widely in optical pump and probe experiments [20], and a gate control of coherent oscillation has been demonstrated recently [21].

A semiconductor quantum dot also operates as a quantum two-level system, whether an exciton is located in the dot or not. All-optical qubits have been realized by using this type of coherent control of the exciton population with ultrafast optical pulses [22], [23]. NTT currently leads this field and details are discussed in the following paper [24].

Nuclear spin has a very long decoherence time and it is one ideal system for future quantum computers [25], [26]. A fully electrical control of the nuclear-spin polarization in semiconductors has been shown experimentally [27], and coherent oscillation has been detected electrically [28]. However, ideal control of nuclear spin, *i.e.*, manipulating a single nuclear spin, is very challenging and, over a certain time period, we should develop a method that coherently controls a group of nuclear spins.

Figure 2 shows how the physical number of qubits has increased every year. Several qubits have been demonstrated in solution NMR and in ion/atom traps. One- or two-qubit operations have been demonstrated in many solid-state systems within the last two years. In this sense, the twenty-first century is the dawn of the solid-state qubit. It is noteworthy that the slope in Fig. 2 shows that the number of bits has increased by nearly 2.7 times over three years, which corresponds to Moore's law for logic circuits. The increase in solution NMR qubits and ion/atom trap qubits really does fall on this line except for a small shift in the horizontal direction. Although the number of solid-state qubits is too small to agree with the slope, the optimistic expectations of ARDA (10 physical qubits in 2007 and 50 qubits in 2012) do fall on it. This means that quantum computer development is really a rapidly growing field and highly competitive, comparable with that of cutting-edge Si integrated circuits. The goals set by ARDA are ambitious, but they may be attainable through the collective efforts of NTT Laboratories in cooperation with outside organizations.

On the other hand, a practical quantum computer with about 10,000 qubits will only be demonstrated after 2025, even with this rapid progress. This clearly indicates the need to take a long-term view for quantum computer research. At present, a diverse range of experimental approaches from a variety of scientific disciplines are pursuing different routes to meet the requirements for a scalable quantum computing system. It is too soon to attempt to identify which ones may be successful. This is because the ultimate technology may not have been invented yet. We should remember the history of semiconductor devices where the first successful transistor was made of Ge, but Si is now the established material. Therefore, we need to be careful in comparing different materials, including superconductors and semiconductors. In addition, several qubit gate designs exist. In some electrical and optical manipulations, the quantum logic gate operation is intrinsically limited to opera-

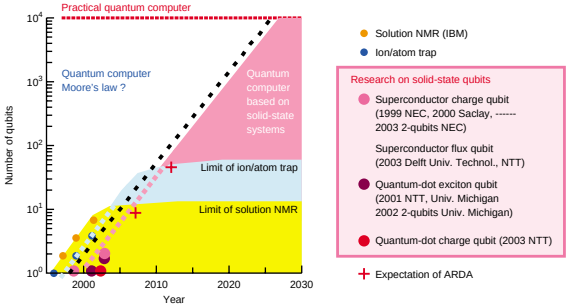

Fig. 2. Road map of quantum computers. Only some examples are plotted here.

tions between nearest-neighbor qubits. This type of logic operation, however, would allow parallel operation within a quantum computer. On the other hand, other approaches are capable of acting as logic gates between widely separated qubits, but they are limited to serial operations. Therefore, for both materials and implementation methods, we should develop various different systems in parallel for the time being.

4. Conclusion

Quantum mechanics was an important aspect of science in the twentieth century and a lot of physics, especially solid-state physics, was explained using it. Quantum mechanics will now become the key to ultimate communication and computer technologies. Quantum cryptography and quantum computers are fascinating examples of quantum information technology (QIT). Although we do not know if quantum computers will offer computational advantages over conventional computers for general-purpose computation, they are clearly extremely powerful tools for performing certain calculations.

A quantum computer consists of qubits. The development of solid-state qubits to build the first quantum computer has been slow, due to decoherence, which implies the breakdown of the quantum information-storing state within a qubit. But new designs based on superconductors, quantum dots, and nuclear spin systems have improved the quality of the individual qubit, and the next step, to connect qubits together, has been taken. On the other hand, the quantum features of photons have been used to realize ultimately secure communication in the form of quantum cryptography.

NTT has studied QIT and its advanced activities are shown in the following papers. In particular, NTT Laboratories have accumulated knowledge and technologies about nanostructures. They have been used to develop solid-state qubit systems, based on superconductors and quantum dots, as well as single-photon sources and highly sensitive photon detectors. These are firm foundations for developing QIT, but considerable efforts will be needed to make practical quantum cryptography for ultimately secure electronic banking and commercial systems and to develop a practical quantum computer for executing real quantum algorithms. Putting this potential into practice will require engineering and control of quantum-mechanical systems on a scale far beyond anything achieved in any physical laboratory so far. However, the activities in NTT Laboratories should provide enough potential to realize these goals. Collaboration with outside organizations is also important to enhance fundamental research.

Finally, I would like to add that the development of new quantum algorithms that have attractive applications is also important for quantum computer research. Quantum bit commitment, quantum teleportation, and other quantum information technolo-

gies are also core long-term interests. They are also being studied at NTT.

Acknowledgments

The studies on QIT in NTT Basic Research Laboratories have partly been supported by CREST-JST and NEDO projects. Collaboration with many outside organizations through these programs is helping our activities. I would like to thank H. Takayanagi, T. Fujisawa, H. Kamada, K. Shimizu, and Y. Tokura for their discussions about quantum information processing including recent experimental results. I also would like to thank M. Morita and S. Ishihara for their encouragement throughout these studies.

References

[1] D. Bouwmeester, A. Ekert, and A. Zeilinger "The Physics of Quantum Information," Springer, 2000.
[2] R. P. Feynman, "Simulating Physics with Computers," Int. J. Theor. Phys. 21, pp. 467-488, 1982.
[3] id Quantique; a spin-off venture company of the University of Geneva, http://www.idquantique.com.
[4] C. H. Bennett and G. Brassard, "Proc. IEEE Int. Conference on Computers, Systems and Signal Processing," IEEE, 1984.
[5] K. Inoue and K. Shimizu, "Quantum Cryptography–Quantum Mechanics Opens up a New Trend in Communication Security–," NTT Technical Review, Vol. 1, No. 3, pp. 24-30, 2003.
[6] Edo Waks, Kyo Inoue, Charles Santori, David Fattal, Jelena Vuckovic, Glenn S. Solomon, and Yoshihisa Yamamoto, "Secure communication: Quantum cryptography with a photon turnstile," Nature, Vol. 420, pp. 762-762, 2002.
[7] P. Shor, in Proc. 35th Annu. Symp. on the Foundations of Computer Science (ed. Goldwasser, S.) pp. 124-134 (IEEE Computer Society Press, Los Alamitos, California, 1994).
[8] D.P.DiVincenzo, "The Physical Implementation of Quantum ComputationX," Fortschr. Phys., 48, 771, 2000.
[9] Isaac L. Chuang, Lieven M. K. Vandersypen, Xinlan Zhou, Debbie W. Leung, and Seth Lloyd, "Experimental realization of a quantum algorithm," Nature, Vol. 393, pp. 143-146, 1998.
[10] Lieven M. K. Vandersypen, Matthias Steffen Gregory Breyta, Costantino S. Yannoni, Mark H. Sherwood, and Isaac L. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," Nature, Vol. 414, pp. 883-887, 2001.
[11] T. Yamamoto, M. Koashi, S. K. Ozdemir, and N. Imoto, "Experimental extraction of an entangled photon pair from two identically decohered pairs," Nature, Vol. 421, pp. 343-346, 2003.
[12] E. Knill, R. Laflamme, and G. J. Miburn, "A scheme for efficient quantum computation with linear optics," Nature, Vol. 409, pp. 46-52, 2001.
[13] M. I. Dykman, P. M. Platzman, and P. Seddighrad, "Qubits with electrons on liquid helium," Physical Review B, Vol. B67, 155402, 2003.
[14] Y. Nakamura, Yu. A. Pashkin, and J. S. Tsai, "Coherent control of macroscopic quantum states in single-Cooper-pair box," Nature, Vol. 398, pp. 786-788, 1999.
[15] I. Chiorescu, Y. Nakamura, C. J. P. M. Harmans, and J. E. Mooij, "Coherent Quantum Dynamics of a Superconducting Flux Qubit," Science, Vol. 299, pp. 1869-1871, 2003.
[16] Yu. A. Pashkin, T. Yamamoto, O. Astafiev, Y. Nakamura, D. V. Averin, and J. S. Tsai, "Quantum oscillations in two coupled charge qubits," Nature, Vol. 421, pp. 823-826, 2003.
[17] H. Takayanagi, "Reading Out Qubit States with a SQUID," NTT Technical Review, Vol. 1, No. 3, pp. 17-23, 2003.
[18] T. Hayashi, T. Fujisawa, H. D. Cheong, Y. H. Jeong, and Y. Hirayama, "Coherent oscillation of an electric dipole in a double quantum dot," Int. Symp. on Carrier Interactions and Spintronics in Nanostructures (CISN2003), Atsugi, Japan, 2003.
[19] T. Fujisawa, "Quantum Information Technology based on Single Electron Dynamics," NTT Technical Review, Vol. 1, No. 3, pp. 41-45, 2003.
[20] G. Salis, Y. Kato, K. Ensslin, D. C. Driscoll, A. C. Gossard, and D. D. Awschalom, "Electrical control of spin coherence in semiconductor nanostructures," Nature, Vol. 414, pp. 619-622, 2001.
[21] Y. Kato, R. C. Myers, D. C. Driscoll, A. C. Gossard, J. Levy, and D. D. Awschalom, "Gigahertz Electron Spin Manipulation Using Voltage-Controlled g-Tensor Modulation," Science, Vol. 299, pp. 1201-1204, 2003.
[22] T. H. Stievater, Xiaoqin Li, D. G. Steel, D. Gammon, D. S. Katzer, D. Park, C. Piermarocchi, and L. J. Sham, "Rabi Oscillations of Excitons in Single Quantum Dots," Phys. Rev. Lett., Vol. 87, 136603, 2001.
[23] H. Kamada, H. Gotoh, J. Temmyo, T. Takagahara, and H. Ando, "Exciton Rabi Oscillation in a Single Quantum Dot," Phys. Rev. Lett., Vol. 87, 246401, 2001.
[24] H. Kamada, "Quantum Computing with QD Excitons," NTT Technical Review, Vol. 1, No. 3, pp. 31-40, 2003.
[25] B. E. Kane, "A silicon-based nuclear spin quantum computers," Nature, Vol. 393, pp. 133-137, 1998.
[26] T. D. Ladd, J. R. Goldman, F. Yamaguchi, and Y. Yamamoto, "All-Silicon Quantum Computer," Phys. Rev. Lett., Vol. 89, 017901, 2002.
[27] K. Hashimoto, K. Muraki, T. Saku, and Y. Hirayama, "Electrically Controlled Nuclear Spin Polarization and Relaxation by Quantum-Hall States," Phys. Rev. Lett., Vol. 88, 176601, 2002.
[28] T. Machida, T. Yamazaki, K. Ikushima, and S. Komiyama, "Coherent control of nuclear-spin system in a quantum-Hall device," Appl. Phys. Lett., Vol. 82, pp. 409-411, 2003.

Yoshiro Hirayama
Executive Manager, Physical Science Laboratory, Group Leader, Quantum Solid State Physics Research Group and Group Leader, Photonic Nanostructure Research Group, NTT Basic Research Laboratories.
He received the B.E., M.E., and Ph.D. degrees in electrical engineering from the University of Tokyo in 1978, 1980 and 1983, respectively. He joined NTT Musashino Electrical Communications Laboratories in 1983. He was a guest scientist in Max-Planck-Institüt für Festkörperforschung, Stuttgart, Germany during 1990-1991. Since 1983 he has engaged in the study of semiconductor nanostructure fabrication, nanoscale characterization, and mesoscopic transport of semiconductor quantum systems. His current interests are transport properties of semiconductor layer and nanostructures especially putting emphasis on carrier interaction phenomena. From 1998 to 2001, he was a research coordinator of NEDO international joint research project (NTDP-98). He has also been a coordinator of a CREST research team for interacting carrier electronics since 1998. He is a member of the Japan society of Applied Physics, the Physical Society of Japan, and IEEE.