1 Intoroduction

Masahide SASAKI

The real form of information running through smartphones, PCs and the Internet is a series of a vast amount of electric and photon pulses in the form of digital signals of 0 and 1. The information concept that uses these binary digits (bit) was established in 1948 as “Information Theory” by Shannon. Around the same time, in 1950, Gabor suggested that communication channel capacities may be increased beyond the Shannon limit by combining Shannon’s theory with quantum mechanics to control electromagnetic waves at the level of photons which are the smallest unit of electromagnetic energy. This is how the concept of quantum communication was born. The new era of lasers began in 1960 when Maiman succeeded in laser oscillation. The frequency of a laser is 100,000 times greater than that of a radio frequency wave. The temperature of a photon at that frequency is equivalent to 10,000°C, which is much higher than thermal noise. Hence, the particle nature of electromagnetic waves, namely the quantum nature as “photons” can be clearly observed. The technology to achieve quantum communication became a real possibility and basic theoretic research has been performed since then.

In 1982, a physicist named C. H. Bennett and a cryptographer named G. Brassard met by chance and had dialogue poolside at a hotel in Puerto Rico. Quantum cryptography, often referred to as quantum key distribution (QKD), was born from this conversation. On 1985, D. Deutsch developed multi-universe cosmology. He introduced the idea of the “quantum bit,” which can be both 0 and 1 simultaneously, to formulate quantum computing. The idea replaced the conventional 0 and 1 concept. In 1994, P. Shor discovered a quantum calculation computing to solve discrete logarithm problems at high speed. He demonstrated that quantum computers, if realized, may decrypt modern cryptography in several minutes. Since then, many papers on quantum communication, quantum cryptography and quantum computing have been published that have led to the emergence of quantum information science.

At around that time, research on quantum communication started at the Communication Research Laboratory (CRL, predecessor of NICT). In the Laboratory of Optical Data Processing, theoretical research on quantum communication started at that time. Since 1999, research on quantum info-communication technology (quantum ICT) to unite quantum communication, QKD, and quantum computing started. This project was supported by the Ministry of Posts and Telecommunication. The industry, university and government collaborate to design research and development strategies in Japan. In 2001, the Laboratory of Quantum Information Technology was established and full-fledged efforts to research and develop quantum ICT began in coordination with the commissioned research on QKD funded by the Telecommunications Advancement Organization of Japan (TAO).

1 The First Medium-Term Plan (FY2001-2005)

The first study performed by the laboratory was on a basic principle of quantum communication, which is a demonstration experiment of coding technology that realizes ultimate communication efficiency. As a background, the quantum communication field faced a major turning point in 1995. That is, the US-UK joint theoretical study team led by Schumacher convincingly proved the conjecture of the Holevo limit on the capacity of quantum communication and the existence of communication that

exceeds the Shannon limit. However, the team showed only the theorem of such existence, and concrete means to exceed the Shannon limit and to reach the Holevo limit were still unknown.

We started the study by extracting important points to construct a model to perform experiments. In 1996, the author met Prof. Holevo for the first time at an international conference held in Hakone and spent a week with him after the conference, observing him study the generalization of the capacity theorem. Discussion with him gave the author an idea about a mechanism enabling exceeding the Shannon limit. The principle is to generate quantum interference between the states of code words by quantum computing during the process of decoding in order to improve the distinguishability of signals. The effect can be expressed easily (when the amount of communication resource doubles, the capacity of transmitted data increases more than twice: super-additive coding gain). By the conventional theorem, the capacity of transmitted information increases twice at maximum. A principle demonstration experiment of super-additive coding gain succeeded in 2003. However, it became clearer that the practical application of the theorem was more difficult than expected.

On the other hand, since 2000, full-fledged experiments in QKD started in various countries. In 2005, a project funded by the Defense Advanced Research Project Agency (DARPA) of the Department of Defense (DoD) in the USA succeeded in a field experiment by constructing a QKD network between three points in the Boston area. In Europe, a project of the European Union, SECOQC, was established in 2004 and research by a team consisting of 41 teams from 12 countries started. At the same time, NICT was developing basic technologies for a prototype of QKD by outsourcing to Mitsubishi Electric Corporation, NEC and the University of Tokyo.

In the field of quantum metrology standards, the technology to improve the assurance of frequency standards and technology for controlling the generation of single photons were developed by controlling a single ion freely by enclosing it in a cavity.

2 The Second Medium-Term Plan (FY2006-2010)

In the experiment to prove super additive coding gain performed in 2003, a specific signal format called polarization of single photons and path modulation coding was used. However, it is necessary to use quantum computing to treat states of laser light (coherent state) for practical application. In the Second Medium-Term Plan, full-fledged development of technology to control quantum bits consisting of a coherent state started. A quantum bit in a coherent state is known as the paradox of Schrodinger's cat, and the generation of it had been a dream in quantum physics. In NICT, we had been trying to realize it. In 2004, a group of Laboratoire Charles Fabry in France published a paper on basic technology, from which we knew for the first time the existence of a competitor for the same goal. In fall of 2005, we received news that the state of Schrodinger's cat was generated in the Niels Bohr Institute in Denmark. And in December, we came to know that Laboratoire Charles Fabry submitted a paper on generation of Schrodinger's cat to Science.

We stood up again from the discouragement of falling behind the competition and made progress in improving our unique experiment apparatus. In the summer of 2006, we succeeded in generating a high-purity Schrodinger's cat state that was greatly advanced from the previous experiments in quality. After that, new technologies such as for amplifying the cat's state (amplitude of wave) and for freely controlling the weight of odd and even photons in the cat's state have been developed one after another by using the technology and foundations for new ICT have been established by exploiting new aspects in quantum optics. The achievements were accepted by the most famous international journal in the field of physics and optics.

The photon number resolving detector that correctly identifies the photon number in a pulse is indispensable to realize quantum ICT as well as Schrodinger's cat state. The photon number resolving detector must be low noise and its efficiency to transform input photons to electric signals (quantum efficiency) must be almost 100%. In order to develop such a high performance photon number resolving detector that meets these requirements, we commissioned research and development of a superconductive transition edge sensor to the National Institute of Advanced Industrial Science and Technology, Nippon University and the National Institute for Materials Science, and they have developed the highest level photon number resolving detector in the world.

The field of QKD entered into field experiments and NTT also joined the collaboration following Mitsubishi Electric Corporation and NEC in Japan. The Second Medium-Term Plan started in NICT in 2006. In Europe, the SECOQC project started, establishing a QKD network between multi-stations. On October 8th in 2008, the field

experiment by the SECOQC was inaugurated in the presence of researchers and press in Vienna. The average transmission distance was 30 km, and the speed of key generation was 1 kbps. The performance was sufficient to encrypt voice data. In Japan, in October 2010, NICT succeeded in encryption of video data transmission by QKD by establishing the most advanced quantum cryptography network "Tokyo QKD Network". Toshiba Research Europe Ltd., ID Quantique, Austrian Institute of Technology and the University of Vienna as well as NICT, NEC, Mitsubishi Electric Corporation and NTT participated in the experiment. The transmission distance extended to 50 km, almost twice that of the SECOQC, and the speed of encryption improved almost 100 times after only two years since the experiment of the SECOQC. Also, we have developed an advanced application interface for interconnection of QKD devices with different specification of each institute. We stimulated various know-how by operating the network.

In the field of quantum metrology, a technology to measure frequency with high accuracy was developed by improving the assurance of frequency standards by cooling two kinds of ions in a cavity together.

3 The Third Medium- to Long-Term Plan (FY2011-2015)

During the Third Medium-to Long-Term Plan, we took on the challenge of developing a quantum receiver which is a basic component in quantum communication, using the world's top-level photon resolving detector. This is a receiver that performs quantum computing for single optical signal pulse and realizes the minimum bit error rate. NICT succeeded in verifying the principle of a quantum receiver for the first time in the world in 2011. Also, in 2013, we verified our original idea of "quantum amplification transmission" that transmits an input optical signal a far distance by noiseless amplification, that was an applied technology of the cat's state generation. However, the performance of these technologies is still limited to certain conditions such as in a laboratory. The practical application of super Shannon limit communication is still a very difficult technology so that a drastic and new technology needs to be developed. Actually, it is limited to realizing it using only optical elements. It may be necessary to adopt a superconductive device to realize stronger non-linear interaction. In the latter of the Third Medium-to Long-Term Plan, a new study on strong coupling of magnetic quantum bits and microwave quanta on a superconductive device was started.

In the field of quantum cryptography, we took on the challenge of developing a new security application that works on the Tokyo QKD Network. At first, the technology that supplies a cryptographic key generated by quantum cryptography to IP routers of two hubs to completely conceal each IP packet and to authenticate to prevent falsification was developed. This technology enables freely constructing a private network that is completely concealed between hubs for important communication through an open system on the internet. Also, a technology to completely conceal wireless communication by supplying a cryptographic key to smartphones or drones was developed.

The technology of quantum cryptography was transferred to the related divisions of NEC and Toshiba. In 2015, test operation started within areas of users' condition in Tokyo and Sendai city. Experiments to confirm reliability have been performed continuously.

In the field of quantum measurement standards, quantum theory spectroscopy was developed that controls or transcribes information between ions of time transition and ions of co-cooling and readout.

4 The Fourth Medium- to Long-Term Plan (FY2016-2020)

The research and development of quantum ICT in NICT is the history of appearance of and development in this field. Since the establishment of the laboratory in 2001, we have boldly moved to verify the new principles of quantum ICT and to research and develop practical use of it, which are two main axes of basic and applied research. Basic research has been heading to the next research phase in which we investigate new phenomena of integrated systems of several physical systems such as light, ions and superconductivity and to exploit applications in ICT. In the future, it will be possible to overcome the limit of conventional transmission capacity or measurement standards by introducing such integrated systems to nodes of a network and forming a "quantum node." However, there still remain many problems for practical use so that long-term basic research is needed. Applied research is spreading wide and merger of quantum cryptography and present cryptography and application of elemental technology to moving bodies is progressing, exploiting new faces in the fields of cryptography and network technology. Especially, from the research conducted in order to overcome the limit of distance or speed of quantum cryptography came a new region

of "physical layer cryptography" that integrates information theory and the technology of cryptography. This enables the construction of a new global secure network that is based on optical space communication. On the basis of these new trends, a new and excellent network with safety and high transmission efficiency that covers from ground optical fiber networks to satellites is called a "quantum optical network." This and the "quantum node" were set as the main themes of the Fourth Medium-to Long-Term Plan.

The framework in which information is expressed by bit sequences of 0s and 1s based on Shanon's theorem is now being fully reconstructed by including the bottom layer of physics of "quanta" (the quantum layer). The quantum layer viewpoint most widely captures ICT systems, thereby bringing new knowledge to science and innovating ICT itself. This special issue presents our latest efforts on this subject.

Masahide SASAKI, Ph.D

Distinguished Researcher, Advanced ICT Research Institute
Quantum communication, Quantum cryptography