Quantum Cryptography: A Reliable Security Guard!

"Ultimate encryption" quantum mechanics guarantees security

Mr. Akio TAJIMA
Assistant Manager
System Platforms Research Laboratories

Dr. Akihisa TOMITA
Principal Researcher
Fundamental and Environmental Research Laboratories

It has been widely considered that "There is no humanly produced encryption that is not decipherable." Even if a cipher that is based on factorization theory such as the current RSA encryption is not decipherable, it is because "It takes too much time using a currently available computer" and not because it is indecipherable in principle. However, when a code based on the "uncertainty principle" of quantum mechanics is applied, it is reported that an encrypted communication is realized that is absolutely impossible to be decrypted. This is the "ultimate encryption," which is a research topic that is presently more advanced than the "quantum computer" research in the field of practical quantum-based research. NEC now stands as a world leader in this research, with successes at the highest level in terms of length and speed of successive cryptographic key generation, under practical conditions. This achievement is a very interesting theme. In this article, we interviewed two researchers in this field who are working in different departments.

* * * * * * * * *

Quantum cryptography that "Cannot be broken unless the system is physically destroyed"

Today, commercially based cryptography is actively employed on the Internet and for other communications systems. But it is impossible for the current technology to prevent "bugging" completely. The "public key encryption methods" based on factorization theory (such as RSA) are said to be "undecipherable," but this presupposes the use of "principles that are inherent in the currently employed computers." It is almost axiomatic to say that, once the "quantum computer" becomes widely available (see the article on page 248 of this issue), it will become possible to factorize a 200-digit number in a few minutes and even a 10,000-digit number could be factorized in a few hours or days.

The breakthrough against such a threat is possible only by exploring the lowermost constraint of the information communication layer model, that is to say the physical layer. For example, in the case of optical fiber

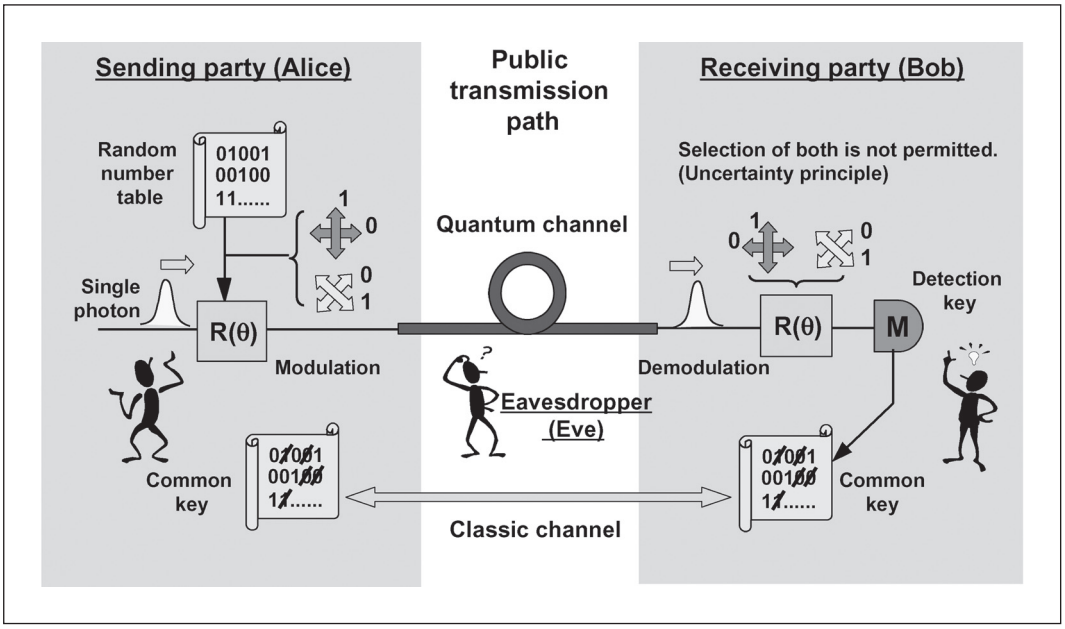

Fig. 1 Example of quantum key distribution.

communication, this corresponds to the use of "photons." Every photon can be transmitted and detected individually. In the detection of bugging, there is the notion of monitoring whether or not each photon is captured during its transmission path in terms of the classical understanding of photon behavior. Although this strategy is logical, it is still inadequate. If the villain is equipped with a perfect detector and generator and retransmits the signal, it is no longer possible to identify the bugging. The conclusion is that no system is certain except for the quantum cryptography method which, "cannot be broken unless the system is physically destroyed." This is an idea proposed in 1984.

"Quantum cryptography is also called the quantum key distribution system. This system consists of the sharing of a random number sequence, or a secret key, by two remote parties connected through an optical fiber. The "secret key" is also one of the keywords of the current symmetric-key encryption systems," Dr. Tomita of the NEC Fundamental and Environmental Research Laboratories began the explanation.

"The transmitter prepares a random bit sequence composed of <0> and <1> (random number sequence) and transmits this by expressing it by means of a 'polarization' of photons. The sets of the photon polarization states used here include the 'horizontal polarization (0°)' and 'vertical polarization (90°)' of '+basis' and '+45°' and '–45°' states of the 'x basis' and the basis may be selected randomly. Similarly, the receiver decides randomly on the basis used for the polarization state detection of each photon, and determines the bit value. After the transmission, the sender and the receiver exchange the basis information used for each photon detection. They keep only the bits where the receiver used the same basis as the sender, and forget about others. The above procedure leaves identical random bit sequences on the both parties. Bugging on the photons affects the polarization states, and results in errors in the shared random bit sequence, that is, the obvious proof of bugging (**Fig. 1**)."

Photon reception system based on scientific fundamentals achieves major breakthrough

Dr. Tomita continues to expand this theme, but the understanding of the interviewer reaches its limit. We decided to return to the original aim of the interview and asked him, "After all, what exactly is the contribution made by NEC through this research into quantum cryptography?"

Dr. Tomita then showed us **Fig. 2**.

"First of all, we conceived a new operation principle of the 'photon receiver,' which features the

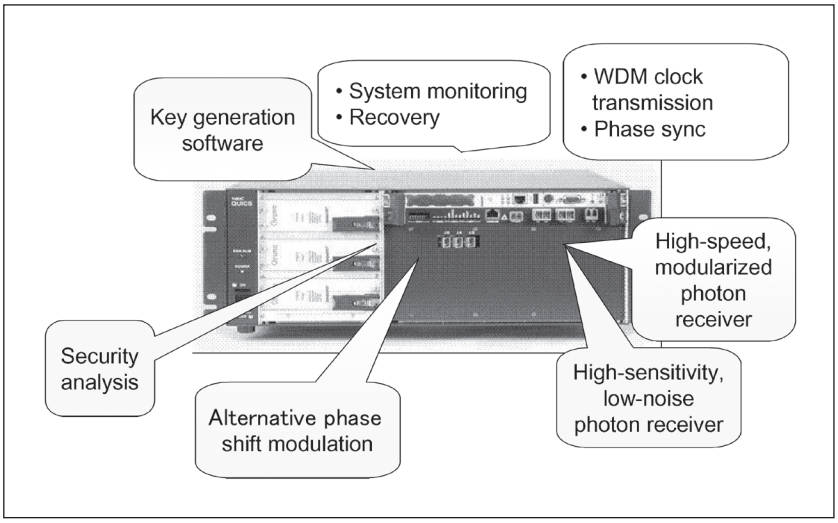

Fig. 2 Contribution made by NEC Fundamental and Environmental Research Labs. and System Platforms Research Labs.

highest sensitivity yet achieved, and implemented it. Secondly, we invented the 'alternative phase shift modulation system' that employs a fiber loop circuit using a polarized beam splitter, a system that ensured independent polarization rotation from the changes in the ambient temperature. We demonstrated the superiority of our technology. Thirdly, we established the synchronization technology that can absorb the effects of delay fluctuations in the transmission path. Fourthly, we developed key generation software that can generate the key concurrently with the photon transmission. Fifthly, we packaged all of the components, including the photon receiver, in a desktop sized cabinet and operated it successfully. These are the factors that allowed us to achieve successive final key generation in a practical environment."

The explanation was continued by Mr. Tajima of the NEC System Platforms Research Laboratories.

"The work assigned to my department was the demonstration, development and packaging of the system. The system has the official name of the "quantum cryptosystem." As is widely known, we have developed a "quantum cryptosystem" and succeeded in two-way quantum key communication over 16.3km of commercial fiber optic cable that is actually installed outdoors. More specifically, we conducted a demonstrative experiment 24 hours a day for more than 14 days, and achieved the world's highest final key generation average speed of 13kbps, and also performed encrypted communication of various data using the generated final key (**Fig. 3**). Prior to this experiment, we also succeeded in an experiment for single photon transmission over 150km and 100kbps raw key generation at 40km transmission. The reason that we selected outdoor operation in this experiment was because there had been concern that climate changes, including the differences between the daytime and nighttime temperatures would vary the cable length and thereby affect the photon bit synchronization. Naturally, we concede that there is the necessity of additional considerations concerning the handling of the sync signal, so we applied the WDM (Wavelength Division Multiplexing) transmission method, which transmits the quantum signal and sync signal through a single fiber

Photo 1 External view of quantum cryptosystem.

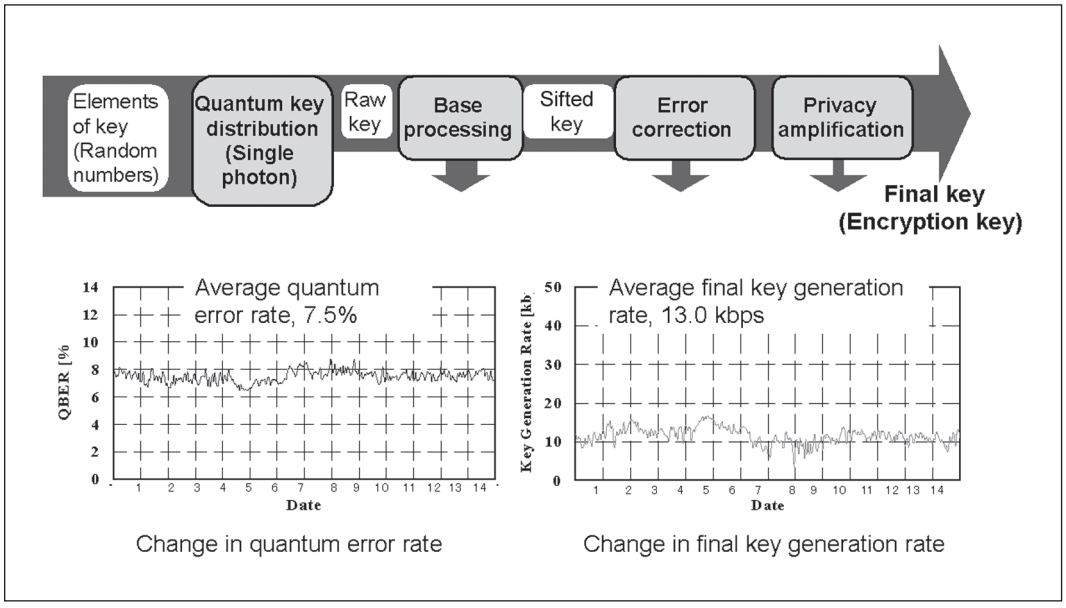

Fig. 3 Successive final key generation.

optic cable by multiplexing their wavelengths."

An experiment may always encounter unexpected events. One of the results obtained from this particular experiment was the fact that "even very low, previously ignored noise is captured because the energy level is so low." But each and every problem was solved one by one, and a significant result was achieved. Through these results we were awarded by the Ministry of Internal Affairs and Communications.

What are the next issues to be challenged?

We returned to question Mr. Tajima, who said, "Quantum cryptography research has now moved from the phase of proving the principles of photon transmission to the phase of system packaging."

"We have already begun to challenge more advanced topics. These can roughly be classified into three topics. The first topic is to improve the stability, speed and long-distance capability further, and the key to this may lie in the application of the PLC (Planar Light-wave Circuit) technology. The second is to package an application and perform a thorough verification of the encryption system from the viewpoint of system. And the third is to verify the unconditional security of quantum cryptography, which has already been confirmed theoretically, also in the field tests."

Listening to Mr. Tajima, Dr. Tomita explained about the topics from his own viewpoint.

"Past experiments employed an optical fiber cable connecting two points directly, but we also need to perform the transmission in a complicated network environment. This is the "quantum key distribution network." The design of repeaters is also an important topic and in any case, we have to study these systematically, by beginning from theoretical matters."

For the allotment of work, Dr. Tomita is to establish the fundamental principles and Mr. Tajima is to implement the system by considering its practical use and commercialization in the future.

"Q-Gov. (Quantum Government)" could be the next topic to come after "quantum cryptography"

We asked how it was that two laboratories with such different bases were able to develop such excellent cooperation.

According to Dr. Tomita, "Our lab began the study covering both 'quantum' and 'communication' in around '98, but it was in 2003 that we

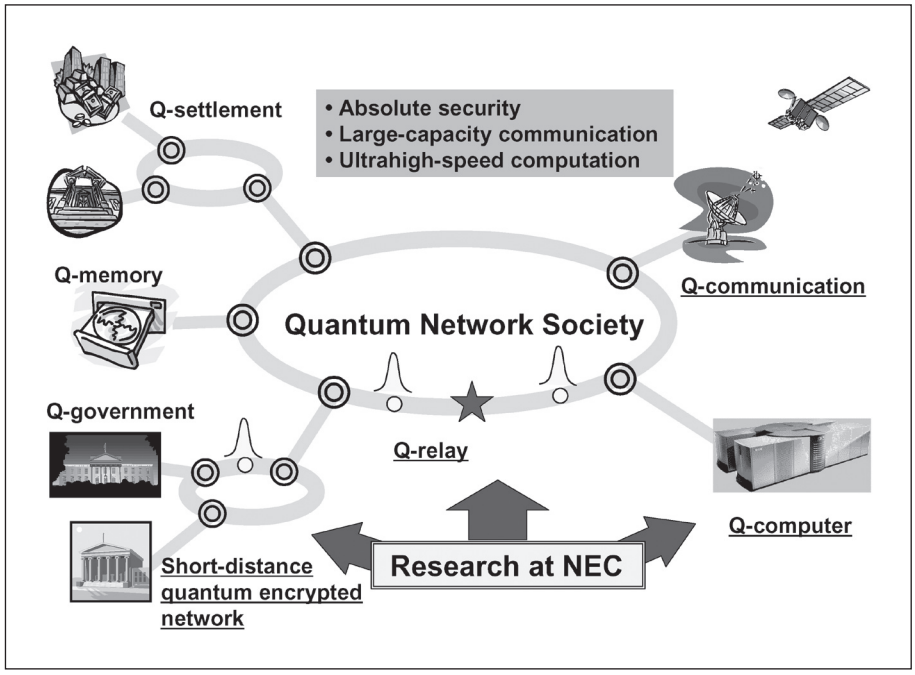

FIg. 4 Network society based on quantum information technology.

brought this subject to the System Platforms Research Laboratories where Mr. Tajima is working. There had been a gap of understanding between the two laboratories in the beginning, but we continued periodical exchanges of information by such means as the teleconference system. We sometimes spent very long hours talking on the phone. Thus, it has gradually become clear that the issue of 'sync' would be a significant bottleneck and that the 'alternative phase shift' modulation might be the key to a breakthrough."

On the other hand, Mr. Tajima says, "We have long been researching into optical communication, particularly the optical switch system. We also developed the optical Ethernet system since the lab was reorganized to emphasize practical implementation. When we had finished that work and felt as though we were in a vacuum, it was proposed to us to do the 'quantum cryptography.' But, when we considered the details, we felt that 'quantum' would be fairly difficult. The subject is hard to be understood, and no existing measuring instruments are usable (laughter). However, fortunately, our lab had a very large variety of staff members; some of them being strong in various fabrication techniques, some were strong in the field of photonics and some were capable of making objective judgments. So we came to think that we could all advance steadily by carefully allotting the work. And I am the kind of person who rather loves to mix with people with such strong individualities."

We also asked Dr. Tomita about his interests. "I originally majored in physics, but I tended to be interested in many things, often rather extensively but sometimes superficially. I have also been engaged in R&D of optical communication devices such as laser diodes and functional devices for photonics. But I felt like tackling something 'ultimate' for the physicists. This idea naturally led to the 'quantum,' and I selected the topic of 'quantum cryptography' thinking that it involved 'communication' which was a current trend."

We then asked this "trend-oriented" Dr. Tomita about the next topic to come after "quantum cryptography."

"We are today in the age of 'electronic government,' 'electronic payment,' 'electronic computers' and 'electronic memory." And I firmly believe that the time is near in which all of these adjectives 'electronic' are replaced by 'quantum.' Then, we will see the 'Q-government (quantum government),' and everything beginning with 'Q-' in place of 'E-' (laughter). When absolute security, large-capacity communication and

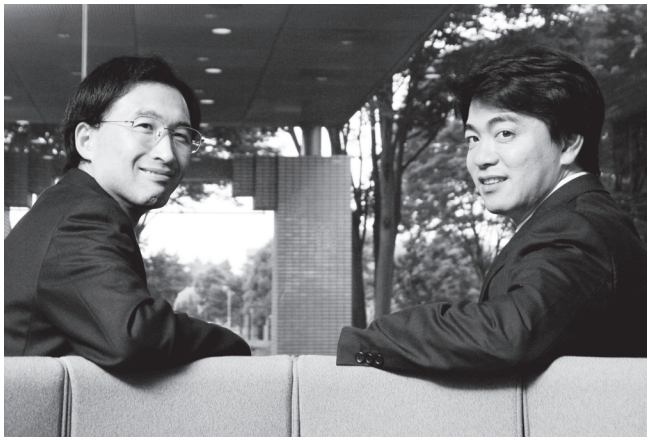

Photo 2 Dr. Tomita and Mr. Tajima in the lobby of NEC Tsukuba.

ultrahigh-speed computing backed by the theory of quantum mechanics come to be realized, will it not be evident that lifestyles and industries could be changed completely?" Saying this, Dr. Tomita showed us a panel of pictures attached to the door of his lab (**Fig. 4**). Mr. Tajima from his side seemed to be already aware of all this, saying, "private businesses are rather passive toward investment into security, but public organizations need the 'absolute security.' We should absolutely appeal to the government about the necessity of 'quantum government.' His words revealed to us how it is that their cooperation is going so well.

What kinds of effects will the synergy of these two personalities bring about, and how will they be developed commercially? The future leads us to expect much.

(Interviewed/compiled by Haruhito Tsuchiya)