

Features on: Quantum Cryptography

01 Lead-off Interview

One More Step to Commercialization: Study of "Quantum Cryptography Network"

Masahide Sasaki

05 Tokyo QKD Network

Operating the Unconditionally Secure TV Meeting System

Mikio Fujiwara

07 Multichannel Superconducting Nanowire Single Photon Detector System

- The Best Performances in the World and Application to
Quantum Information and Communications -

Zhen Wang

09 Free-Space Optical Link and Its Application to Satellite QKD

Morio Toyoshima

11 International Conference on "Updating Quantum Cryptography and Communications" UQCC 2010

"Quantum Technology Pioneering
the Future Technologies Through
Visible and Tangible Approaches"





One More Step to Commercialization: Study of "Quantum Cryptographic Network"

High-Security Network Close at Hand to Replace Ongoing Cryptographic Technology

Masahide Sasaki

Group Leader, Quantum Group, New Generation Network Research Center

After completing the doctoral course at a graduate school, served at NKK (JFE Holdings at present), and in 1996, entered the Communications Research Laboratory (current NICT) to work on the research and development of quantum information and communications technology. Visiting Professor at Research Institute of Electrical Communication Tohoku University and Sophia University, Faculty of Science and Technology.

Ph.D. in Natural Science

In the fall of 2010, NICT conducted an extensive series of experiments of a network utilizing "quantum cryptography", the next-generation cryptographic technology. What is quantum cryptography which can realize higher level of security on existing optical fibers? In particular, it was shown that quantum communication could be used for realizing the ultimately secure cryptography, that is, quantum cryptography. The details of the interview on the quantum cryptographic network nearing its practical applications are described below:

Background of the birth of quantum cryptography

— Could you brief on the history of quantum communications and quantum cryptography?

Sasaki: Early in 1900, quantum mechanics was born, and half a century later in 1960, the concept of quantum communications was developed almost simultaneously with the invention of laser. Before that, communications normally were carried out by using radio waves. In fact, the energy of a single photon used for laser corresponds to about ten thousand degrees, when converting it to temperature. This led to the idea that using laser with that much energy would allow us to do communications with much larger infor-

mation capacity; the quantum communication has taken its way to develop at a slow pace. However, the optical fiber at that time was not at a commercial stage yet, and nothing beyond theoretical matters of physics was discussed.

In the 1980s, the quantum communication faced a significant turning point. Ideas of making use of quantum mechanics for new schemes of computation and communications were introduced. I was told that just a coincidence triggered the studies of implementing quantum cryptography. That is, when a physicist called Charles Bennett who was working on quantum mechanics at IBM in 1982 enjoying vacation in Puerto Rico happened to meet a scientist called Gilles Brassard of the University of Montreal who was specialized in cryptography at a poolside, and while they were casually chatting, the theory of quantum cryptography was born. The cryptographic protocol announced by them at an international conference held in 1984 has been referred to as BB84.

— Then, the study of quantum cryptography has been conducted extensively by an increasing number of researchers...

Sasaki: Well, not exactly. For a certain period of time in the beginning stage, people in related fields were saying, "Those sort of theories are conceivable"; the subject was studied little by little and nobody paid attention to the BB84. However, when Peter Shor of the Bell Laboratories in the United States presented a theory in 1994 that "when quantum computers

should be realized, most of the ongoing cryptographic schemes used in the Internet would be defeated", the quantum cryptography attracted interest and studies on the subject were initiated by a number of researchers.

The issue that the quantum computer technology would radically affect the infrastructure of modern society would be brought up to a national strategy level rather than scientific studies. In those times, the cold war ended and thus nuclear-based deterrence became less dominant than the information and communications technologies that would have decisive power in the survival of a nation. That's why every nation would strive for having quantum computers, or quantum cryptographic technologies with much higher level of security than those of any other nation. The movement was promoted as a national strategy in the United States and in Europe, and the numbers of papers were increased explosively from that time.

— How were the quantum cryptography studies going on at that stage in Japan?

Sasaki: In 1996, when I was employed as a doctoral researcher by the Communications Research Laboratory (currently, NICT), the studies of quantum studies evolved astonishingly in a matter of a year and so great a number of papers were presented that it was very hard for me to catch them up. On the contrary, studies on quantum communications in Japan were at a very moderate level.

— As compared with overseas activities, was the Japanese research-

ers circle rather subdued?

Sasaki: Not necessarily. Although the number of researchers engaged in that study was limited, theoretical studies were being carried out at a high enough level to compete with those in the States. The situation in Japan was not such that projects at national level were started in western countries, but that a total of 30 researchers organized a research society to discuss the subject up until 2000. When the Research Development Corporation of Japan (JRDC, currently, Japan Science and Technology Agency (JST)) adopted the project on quantum cryptography in 2000, it was considered to be the beginning of the study on quantum cryptography at a national level. In fact, since 1998 or so, the Ministry of Post, Telephone and Telegram held public hearing meetings with Nippon Telegraph and Telephone Corporation (NTT) and major universities to look at the feasibility of starting research on quantum communication. In 1999, we presented a research report, and in 2000, we organized a research society having Dr. Leona Esaki as the chairman. In 2001, a study group for which I was told to serve as the leader was established in NICT, and thus the study of quantum information technology with the main theme of communications was started.

— Please describe how plain texts are encrypted into the quantum cryptography.

Sasaki: The quantum cryptography com-

prises the two steps of quantum key distribution and encryption by using the key. In the quantum key distribution, a key consisting of a random number sequence of "0" and "1", which is shared by those concerned in such a way that nobody other than the sender and receiver would possibly be able to eavesdrop it (Figure 1). This is a very simple system of adding the key to data at the 'send' and further adding the key at the 'receive' to recover the original data. In the quantum cryptographic system, nobody can reproduce the original in the same state, and hence you can see if an eavesdropping is the case. This characteristic assures that it is indeed a secure cryptography.

While ongoing cryptographic technology employs a key, it is utilized not in the form of addition, but in a complicated system by means of prime factorization. That's why such a conventional cryptography cannot be normally deciphered, but when capabilities of a computer are enhanced, it may well be decoded. They say that an average life a cryptographic system is about 13 years. On the contrary, quantum cryptography has no such a problem theoretically.

What is quantum communication?

— Could you explain quantum communication in a simple way?

Sasaki: In a nutshell, it is the ultimate communication technology exhaustively

utilizing the characteristics and potential capability of light. The conventional optical communications can only control light as a flux of energy. The signals "0" and "1" represent whether or not a light pulse is issued. However, light is actually wave. So when a wave bumps with another wave, they mutually interfere and are made stronger or weaker. If we would use such a characteristic of light, we could transmit much more information than has been sent by conventional optical communications.

Moreover, while the light has the characteristics of waves, it has also the characteristics of particles. When we are able to make use of the characteristics of the particles of light, namely, photon, we could realize quantum cryptography that can detect any fact of eavesdropping if it is the case. The act of eavesdropping means extracting a photon; the spot where a photon is taken away remains when the data is received, and thus the eavesdropping can be found out very easily.

And when such a technology that can yield maximum amount of information from each photon is created, the signal with same energy as before can convey much more information than before. In other words, the ultimate communications technology that can be allowed by the laws of physics is the quantum communication.

— How much information can we transmit in communications?

Sasaki: The more the energy is input, the more the information can be transmitted in a communication. However, the existing optical fibers have a limit in regard to the amount of energy to be carried. An optical fiber is made of glass with several tens of a hair width and its transparency is higher than that of the atmosphere, being capable of sending light much farther than the atmosphere does. However, it can only pass light with a power of 10 watts or so. If more energy is fed through an optical fiber, the glass melts down. Therefore, it is an issue in communications as to how much information can be transmitted with a limited amount of energy. There are various problems such as noise. After considering them, the communication capacity that can be achieved by using all the available technologies has been theoretically found. At present we know

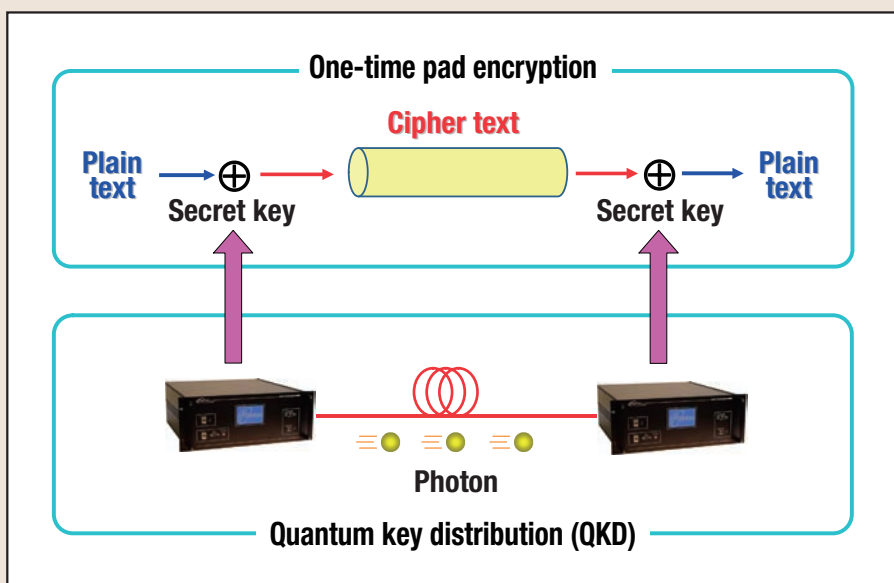


Figure 1 ● Outline of Operations of Quantum Cryptographic System Encryption
Even if a piece of data could have successfully been intercepted, it cannot be deciphered in its original form.

at what transmission rate we can communicate by using what sort of optical fiber at an energy level of 10 watts. Nevertheless we must face the problem how it should be implemented.

While we cannot send infinite amount of information with limited energy, it has at least been already proved that "this much can be achieved". Within another half a century, new materials and technologies will be created to achieve this upper bound of communication capacity. Then to increase the capacity of communications, there would be no other way than to increase the number of optical fibers. In such a situation, however, the lifestyle of mankind itself should have to change. There are quite a few barriers in the real life, although they are discussed in the theories of quantum communications.

Quantum cryptography is already in use.

— In quantum communications, theories are ahead of other activities...

Sasaki: Not only in quantum communications, in the fields of information technology, theories have always been in advance than practice. The mobile telephone sys-

tem now used by everyone originates from the "information theory" for sending video images and sounds by means of "0" and "1", proposed by Claude Shannon back in 1948. At that time, how to implement the theories in the real world was not known. It is only recently that the communications performance predicted by Shannon has been achieved. Thus, it took about half a century for the reality to catch up with the theory.

— Do you mean that it would be further ahead when quantum communications will be in reality?

Sasaki: Yes, I guess it will take another half a century. Nevertheless, while most of predictions of quantum communications are not yet in practical use, quantum cryptography is already being used. There are two directions in quantum communications, namely, toward infinite capacity and absolute security. Currently, the direction of security is more or less advanced in such a way that quantum cryptography is being commercialized. In western countries, products of quantum cryptography are actually marketed. While they are mostly purchased by research organizations, I hear that some of them are also delivered to banks.

— Is there any particular reason why quantum communications are not yet commercialized in Japan?

Sasaki: Presumably, while the enterprises selling those units in the United States and Europe are small venture companies. I think there is no such a company in Japan. In the past, there was actually a venture company who wanted to handle quantum cryptography, but as the national project was not yet initiated in the 1990s, the attempt subsided because of bad timing. Since 2001, in Japan, NEC Corporation (NEC), Mitsubishi Electric Corporation (MELCO), and NTT have been developing quantum cryptographic systems, being commissioned by NICT. However, no product has so far been commercialized because of significant barriers such as quality assurance issues.

Quantum cryptographic communications just before the start of commercialization

— At NICT, what types of studies are carried on?

Sasaki: Since October 2010, we have been conducting experiments on the long-term operation of the systems developed by NEC, MELCO, and NTT that are in-

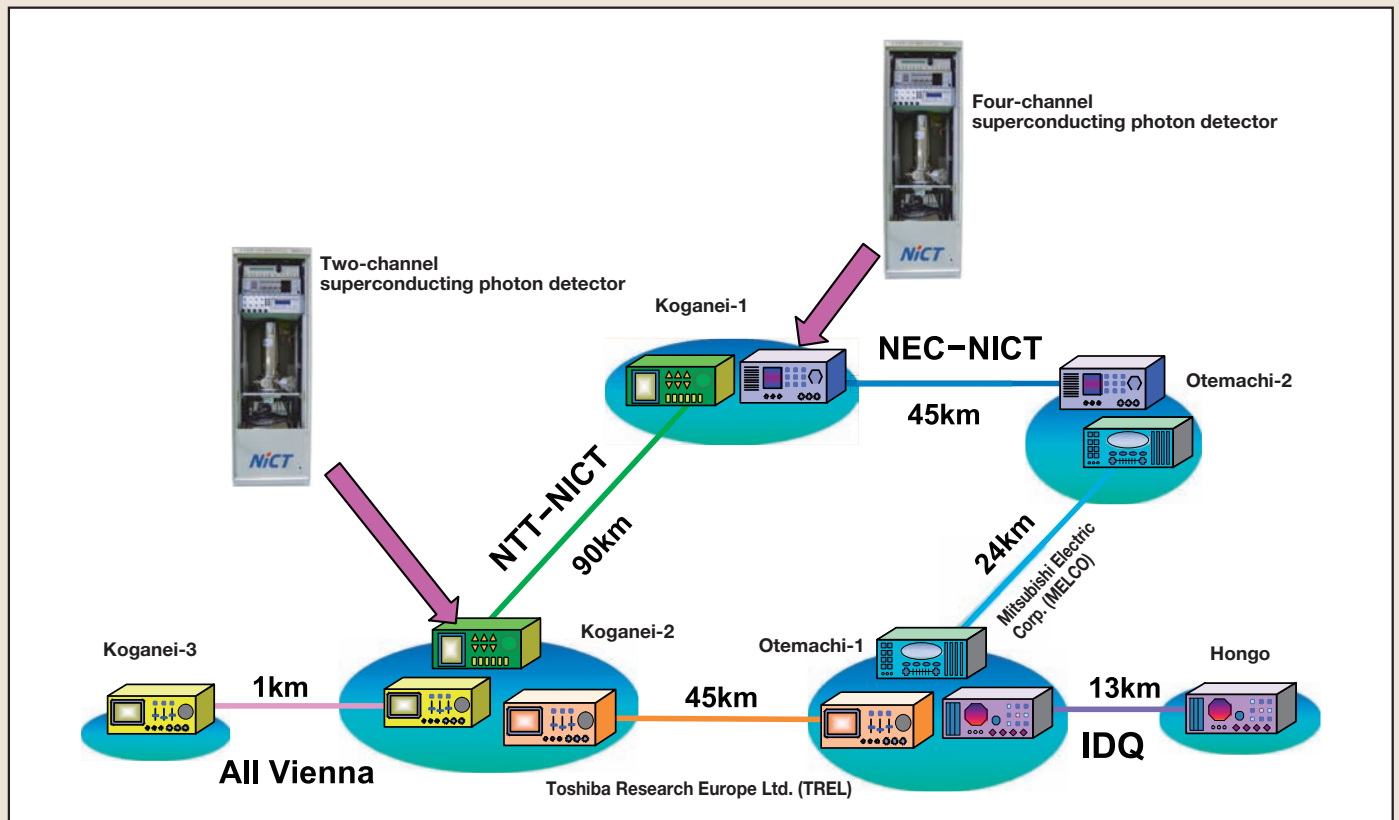


Figure 2 ● An Experiment Conducted in October 2010
The quantum cryptographic apparatus assigned to each node is linked with existing optical lines.

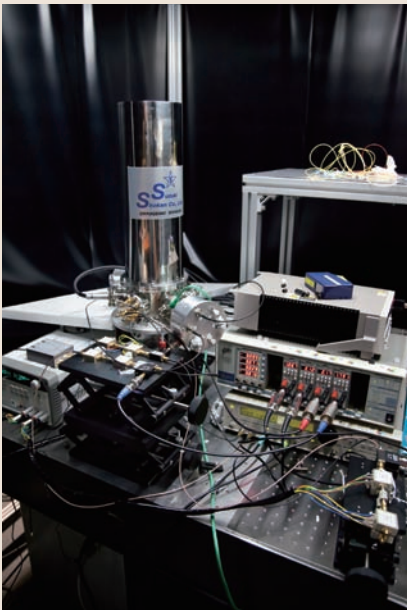


Figure 3 ● Testing Equipment of Quantum Cryptography
The entire equipment is installed in an area covered with dark screens to minimize noise and avoid any stray light.

incorporated into the cryptographic network designed by us (Figure 2). Operating such a system for a long term would inevitably give rise to various problems. For example, when the system was allowed to keep running during the New Year's leave period, it was found that operation stopped during that period. Our troubleshooting revealed that one of the variables of the program exceeded the predetermined capacity in 4 days, which may well have happened normally. Besides, we came across a problem in which the systems picked up such a minute level of noise that would never be a concern in conventional types of equipment because the equipment used for quantum cryptography is of extremely high precision.

— **Is any quantum cryptography network being built up?**

Sasaki: We have built up an experimental environment by combining the existing Internet facilities in current use with optical fibers laid along roads and the quantum cryptographic systems (Figures 3, 4 and 5). The stations located in Koganei and Otemachi that are 45 km apart are linked with an optical fiber and the generation of cryptographic key and encryption can be conducted at a transmission rate of 100 kbps. Although the system is not altogether of a large capacity and high-speed communication, its performance and security level are at the highest level ever realized in quantum cryptography com-



Figure 4 ● Superconducting Photon Detector
The use of superconducting photon detector enhances photon detection efficiency and reduces noise level. This is an indispensable apparatus for long-distance and high-speed quantum cryptography.

munications.

In a series of experiments carried out in 2010, we established a quantum cryptographic network linking the six stations and also implemented a high level of intercepting unit on a path. Then, we conducted repeated tests to determine if an eavesdropping can be detected, and when it is the case, if we could quickly reroute a secure path, and if the transmitted data was not interrupted.

— **So, perfectly secure network is already in place, right?**

Sasaki: Yes, the highest possible level of cryptographic technology is now working in field testbed. Nevertheless we must still continue tests to verify whether the system should never be eavesdropped. In other words, there is no way to implement a system perfectly as prescribed by theories, and thus we should be aware that any error and imperfection beyond our design may often occur. Furthermore, we always have problems regarding attacks via side channels and how we should take an eavesdropper away when it is detected. They are actually matters of the cryptographic technology as a whole rather than a specific concern of quantum cryptography.

— **When will quantum communications be commercialized in Japan?**

Sasaki: We are going to conduct field tests and will then move onto prototype commercial test in 5 years from now.



Figure 5 ● Monitoring Equipment of Quantum Cryptography Network
For general market penetration, its size reduction is required.

During this period, whether or not the Japanese government will formally approve quantum cryptography would be the decisive issue for the commercialization. However, for general users to benefit from quantum cryptography, it might take 10 years to solve such problems as may be found in transmission distance and transmission rate.

— **Thank you very much for your elaboration today.**

Terminology

* **Side channel**

In a cryptographic system, besides the plain text and cipher text attacks, eavesdropping information from the leaking electromagnetic waves and consumed power and subsequent decryption may occur. Thus, even if a protocol itself is secure, there always exist a means for accessing information on a cryptographic system, which is called "side channel", when the system is implemented incompletely or surrounded by additional peripheral apparatus.

Tokyo QKD Network Operating the Unconditionally Secure TV Meeting System



Mikio Fujiwara

Senior Researcher, Quantum ICT Group, New Generation Network Research Center

Dr. Fujiwara joined the Communications Research Laboratory, Ministry of Posts and Telecommunications (currently NICT) in 1992, where he was engaged in the development of Ge:Ga far-infrared photoconductors. Since 2000, he has been a member of the quantum information technology group. His current interests include GaAs JFETs and InGaAs pin photodiodes for the development of ultra-sensitive photodetectors in the telecom bands.

Introduction

Since the encryption system on a computer normally encrypts important information on the Internet, an eavesdropping attack does not necessarily mean the loss of information, and thus the security will not be totally damaged all at once. Nevertheless, since the cryptographic system in current use has recourse to such a mathematical problem that requires a huge amount of computation as the basis of security, whenever an epoch-making decrypting method is discovered in the future, the security will not function any longer. That is, even if those eavesdropped data cannot be decoded in the present time, they may be deciphered with innovative technology in the future. Thus, we may sooner or later confront security risk if we continue to pursue economy and convenience of the Internet simply counting on the currently available security measures. Against such a threat, now we can obtain a cryptographic system that can relieve us of anxiety for the future. The quantum cryptography is the system, which is described here. The quantum cryptography is the ultimate cryptographic technology that cannot logically be deciphered by any technology. The cryptographic method is such that each of the sender and receiver is provided with a quantum key distribution apparatus to share by way of an optical line the absolutely secure common key that is perfectly protected from eavesdropping. Then, the data to be transmitted are encrypted on a one-time pad by using the key.

Unconditionally secure communication TV System

In the quantum key distribution, the sender modulates photons (adding information to them) and transmits. If modulated signals at a photon level are subjected to a measuring operation, the trace of the operation infallibly remains (Heisenberg uncertainty principle), and cannot be reproduced without changing the state of a single photon (no-cloning theorem). Use of such a principle or theorem allows us to detect an eavesdropping. The receiver determines the condition of each single photon to exclude any bit that may be eavesdropped (so-called secure key distillation) and allow both the sender and receiver share the absolutely secure key (random number sequence for encryption).

In decrypting on a one-time pad, the length of a piece of digital sent data is equilibrated with the common key (a bit array of 0 and 1) in exclusive logical sum for the encryption, and the reverse process is taken for the decryption. The term "pad" means a cryptographic key. Prohibiting the repeated use of a random number sequence that is used once is the rule on the one-time pad. A one-time pad is also called Vernam cryptography after its inventor, and the absolute impossibility of decrypting was proved by C.D. Shannon in 1949.

However, quantum key distribution is such an extremely sophisticated technology that its commercialization faces a number of problems and that in the projects of United States Department of Defense and European Union, the encryption of audio data was its limit and the transmission distance was limited to several tens of kilometers. Since 2001 in Japan, NICT has been carrying on an R&D project of industry, academy, and administration collaboration to establish the world's fastest quantum key distribution technology that will realize an unconditionally secure TV meeting system (Figure 1).

Last October, NICT, NEC Corporation, Mitsubishi Electric Corporation (MELCO), and Nippon Telegraph and Telephone Corporation (NTT) jointly established a quantum key distribution unit at each of four bases on the R&D network JGN2plus operated by NICT to build up a quantum cryptography network consisting of multiple line patterns ranging from 10 km to 90 km at the longest, and conducted a series of eavesdropping attack detecting tests and the trial operation of multi-spot, unconditionally secure TV meeting system. During the international conference on "Updating Quantum Cryptography and Communications" UQCC 2010 held at the ANA

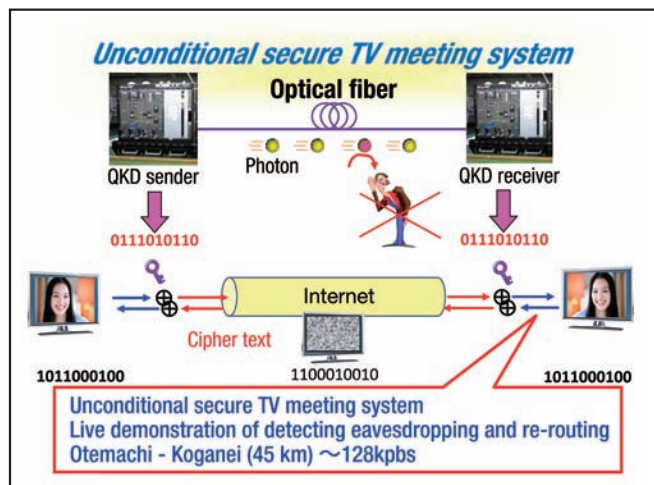


Figure 1 The Unconditionally Secure TV Meeting System Based on Quantum Cryptography

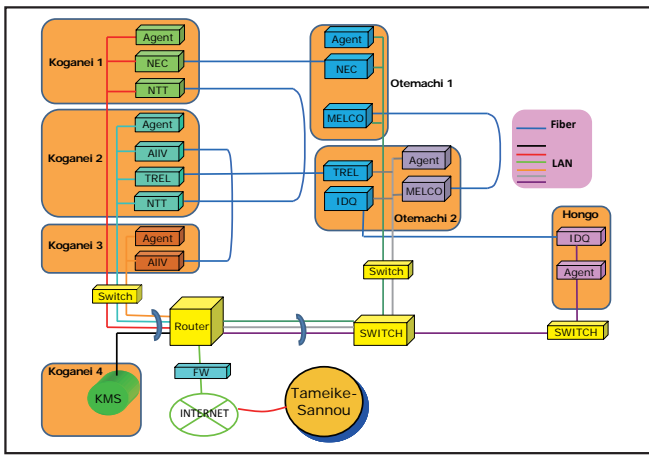


Figure 2 ● Deployment of Quantum Key Distribution Units and the Protocol Employed

Intercontinental Hotel Tokyo on Monday, October 18 to Wednesday, October 20, 2010, we performed a live demonstration of the unconditionally secure TV meeting system between Koganei and Otemachi. This is the first case in the world of implementing video image transmission by means of quantum cryptography with an optical fiber line laid in a 50 km zone.

This quantum cryptography network, which is also called Tokyo QKD (Quantum Key Distribution) Network, consists mainly of the Test Bed Network JGN2plus, in which this specific network refers to the four bases including a separately provided Hongo base in addition to the Otemachi, Koganei, and Hakusan covered by the JGN2plus. In reference to the origin of Otemachi, Koganei base is located about 45 km in the west, Hakusan about 12 km away in the north-north-west, and Hongo about 13 km in the north. The generation rate of the common key is approximately 100,000 bit per second in the optical fiber line laid between Koganei and Otemachi, which are 45 km apart, and thus this rate was proved to be the highest in the actual environment in the world. Concurrently, we conducted experiments of two-way link exchanges with the systems of Toshiba Research Europe Ltd. (TREL) and other European research organizations such as ID Quantique S.A. (IDQ in Switzerland) and All Vienna (Austria).

In the optical Test Bed JGN2plus in the Koganei-Otemachi-Hakusan sections, multiple optical fiber lines are laid in parallel so that a variety of line forms can be configured. Figure 2 shows the layout and protocol of each participating company constituting the Tokyo QKD Network. Further, Figure 3 schematically illustrates the configuration of the quantum cryptography network employed in the trial operation of this time. In the bottom layer, called quantum key distribution (QKD) layer, the equipment belonging to each research team (NEC, Mitsubishi Electric (MELCO), NTT, TREL, IDQ and All Vienna) is installed in such a way that it faces one another. The QKD of NEC and NTT employs a high-performance superconducting single photon detector developed by NICT. Key distribution units of each team are grouped into a single node, and a total of six nodes (including Koganei 1, 2, and 3, Otemachi 1 and 2, and Hongo) have been installed. The common key generated through quantum key distribution is taken up by the key management (KM) agent in the key management layer at a higher level located physically in the same place. The KM agent constantly monitors the common key and

amount of keys of each link, and reports to the key management server (KM server) at a further upper layer on the amount of keys and the link status. On request of the user, the KM server issues instructions to two or more KM agents to establish a secure path even at a spot where no direct link is available through a suitable relay node so that required amount of keys can be transferred. The KM agent at a relay node performs a one-time pad encryption of the common key generated from one side of the adjoining QKD link by using the common key on the other side of the QKD link to proceed with the so-called key capsule relaying. In this process, the assumption is required that the relay node is physically secure. At the current technical level, the relay nodes for quantum key distribution must be installed at intervals of approximately 50 km. This distance depends on the loss in the optical fiber. Even at the current technical level, Tokyo and Osaka (a linear distance of 400 km) can be linked with eight or so relay nodes.

Future Perspective of Quantum Key Distribution

The quantum key management system thus developed has such a function that, when an eavesdropping is detected along a QKD link, the KM server immediately finds out another secure path, and by switching the paths, secure communications can be maintained without interruption. We will further improve the required facilities in order to apply the technology to the confidential communications at the national level, the protection of communications in the important infrastructure consisting of power grids, gas and water supply networks, the secure communications of financial organizations, etc. Furthermore, we will exert our R&D efforts to realize such a comprehensive operation technology that the next-generation cryptography enabling higher rate and longer distance transmissions can be integrated with the ongoing cryptography, so that advanced, secure networks can be built up on the existing optical fiber infrastructure, where flexible services satisfying needs and cost requirements can be offered.

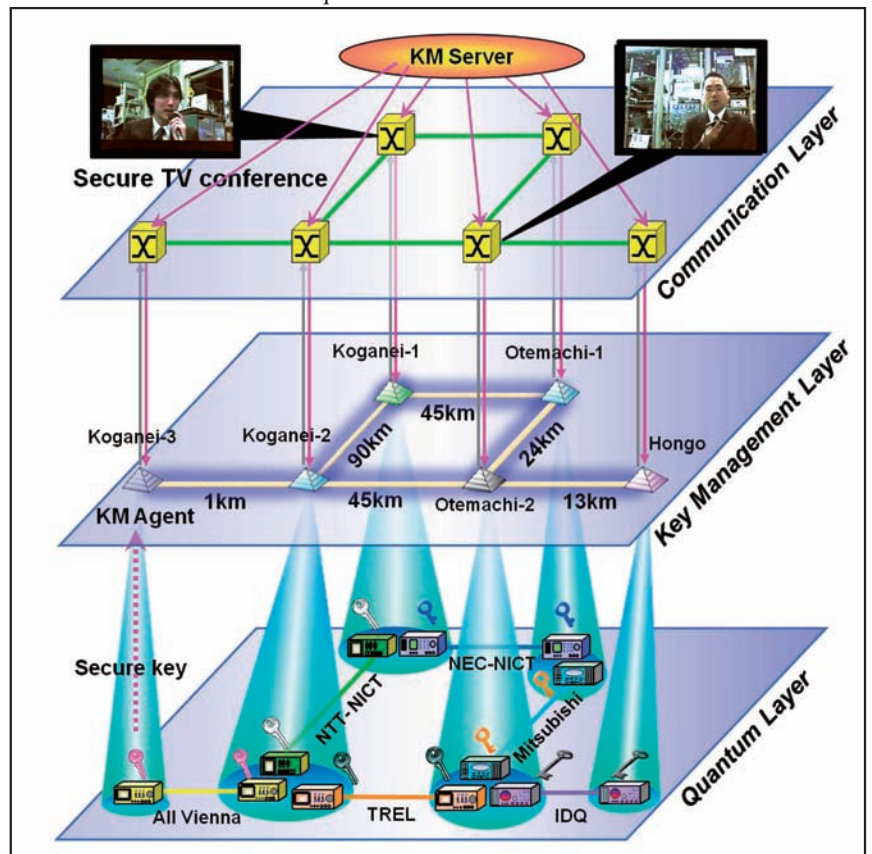


Figure 3 ● Configuration of Quantum Cryptography Network Layers

Multichannel Superconducting Nanowire Single Photon Detector System

- The Best Performances in the World and Application to Quantum Information and Communications -



Zhen Wang

Group Leader, Nano ICT Group, Kobe Advanced ICT Research Center

Joined Communications Research Laboratory (currently NICT) in 1991. Has been engaged in researches on superconducting electronics. Guest Professor of Osaka University, Nanjing University in China and Osaka Prefecture University. Visiting Fellow of Nanjing Purple Mountain Observatory, Chinese Academy of Sciences. Ph.D. of engineering.

Background of the Study

The development of high-sensitivity, high-speed, and low noise photon detectors is called for as a key technology for quantum cryptography and quantum information and communications technology. As a photon detector, photomultiplier tube (PMT) and avalanche photodiode (APD) consisting of semiconductors such as Si and InGaAs/InP have already been developed and in the communication wavelength band (wavelength: 1,550 nm), InGaAs/InP-based APD is mainly used. However, since semiconductor APDs have limited detecting efficiency and operating rate depending on the material and detecting principle, a certain breakthrough is required to establish the quantum information and communications technology. Accordingly, since 5 years ago, we have been carrying on the research and development on superconducting nanowire single photon detectors (SNSPD) that can normally operate by using the materials and the principles that are substantially different from those of semiconductor APDs.




Superconducting Nanowire Single Photon Detectors

Since superconducting nanowire single photon detectors are based on macroscopic quantum phenomena pertaining to

superconductors and can operate at cryogenic temperatures, they have high potential capabilities far exceeding the performance of PMTs and semiconductor APDs in the communications wavelength band. Table 1 compares the performance of three different type of photon detectors. The performance index that indicates total performance of SNSPD is already 100 times elevated, and thus suggests that the performance will be improved further higher.

SNSPDs perform photon detection by referring to the sharp change of resistance that occurs when the superconducting nanowire undergoes transition from superconducting state to normal conducting state. Key technologies improving their performance include the preparation of high-quality, ultrathin superconducting films, extremely fine fabrication of nanowires, and the high-efficiency coupling of an incident photon with the devices. Concurrently, the development of multichannel detecting system is absolutely required for the commercialization. We have successfully prepared the nanowire single photon detecting device having a thickness of 5 nm maximum with a line width of 80 nm to 100 nm by fully utilizing NICT's unique high-quality superconducting film fabricating technology and the nanofabrication technology that has been accumulated in the fundamental research phase. Similarly, in order to couple the incident photon through an optical fiber with the detecting device

Table 1 ● Performance Comparison of Communication Band Photon Detectors

Wavelength: 1,550 nm				
Detector	Detecting efficiency (%)	Dark count rate (Hz)	Count rate (MHz)	Performance index $\times 10^3$
 PMT	2	2×10^5	10	1
 InGaAs/InP APD	20	10×10^3	100	2
 SNSPD (NICT)	20	100	100	200

Performance index = Detecting efficiency \times Count rate / Dark count rate

at high efficiency, we have developed the optical fiber coupled packing technology to enable coupling the optical fiber and the device at micrometer order precision. Further, with the aim of commercialization, we have developed the multichannel SNSPD system using a compact, mobile, and non-coolant Gifford-McMahon (GM) refrigerator that can be energized with 100-volt household power supply (Figure 1). In the developed system, six optical fiber-coupled SNSPD packages are installed so that six-channel photon simultaneous detection can be performed. Table 2 gives the specifications and performance of the system. At current stage, the system has achieved the highest performance indicators in the world, including a quantum detecting efficiency of 20%, an

operating rate of 100 MHz, and a dark count rate* of 100 count/s. This system was used for the live demonstration of the recent Tokyo QKD Network (Page 5), and was proved to be competent for its commercial use and effectiveness.

Future Perspective

The single photon detecting technology that employs SNSPDs and occupies the core position of supporting the future quantum information and communications technologies has phased in the commercialization R&D stage only recently. Now the system shows its performance already exceeding semiconductor APDs, and by improving the devices and optimizing the systems configuration, further improvement in performance can be expected. As an ultimate photon detector, the multichannel SNSPD system will be able to find market in the near future not only in the field of quantum information and communications, but also in a variety of fields such as quantum optics, space physics, live substance mass analysis, new drugs development, and low-energy particles detection.

Table 2 ● Specifications and Performance of the Multichannel SNSPD System

Number of channels	Six channels
System detection efficiency	20%
Dark count	<100 counts/s
Response rate	100 MHz
Jitter	100ps
Bias current	10-50 μ A
Power supply	AC 100 V, 15 A
Operating temperature	2.9 K
Size	H 1,750×W 570×D 650 (mm)

Terminology

*** Dark count rate**

Indicates the number of photons detected when incidental photon is zero. The ideal count is 0.

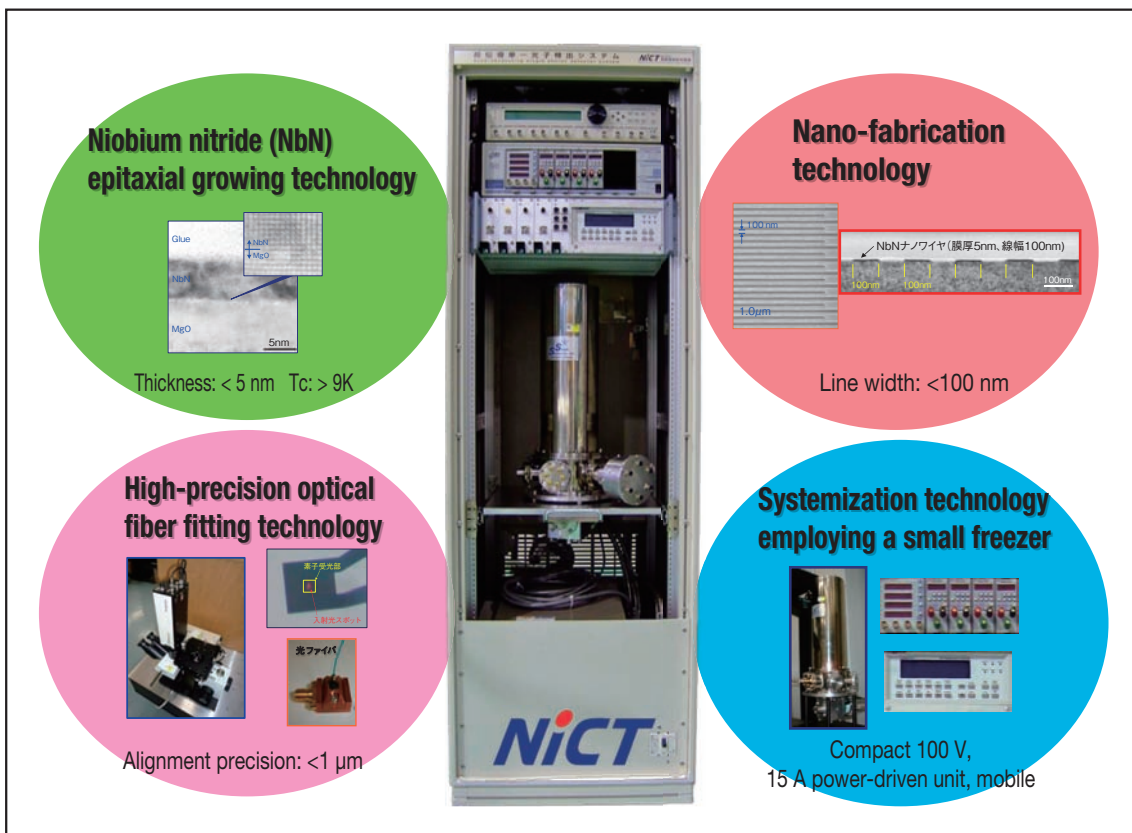


Figure 1 ● The Multichannel Photon Detecting System Realized by NICT's Technology

Free-Space Optical Link and Its Application to Satellite QKD



Morio Toyoshima

Senior Researcher, Space Communications Group, New Generation Wireless Communications Research Center

Joined the Communications Research Laboratory (presently NICT) in 1994. Performed optical communication experiments using the ETS-VI satellite. Was temporarily transferred to JAXA, followed by research abroad at the Vienna University of Technology. Conducted the Kirari optical communication experiment. Presently develops the Small Optical TrAnsponder (SOTA) for micro-satellites.

Ph.D.

Introduction

Terrestrial communication lines with ever increasing transmission rate are predicted to be totally replaced with optical fibers that will establish a complete link network in the near future. Such information and communicating technology employing "light" will be extensively used for space communication network and the communications both in the space and on the ground will be linked with "light". While radio waves and light waves are included in the group of electromagnetic waves, since the light has such high carrier frequencies in the order of several hundred terahertz, antennas and apparatuses can be made compact and lightweight permitting the effective use of resources. Besides, legal restrictions are rather lenient. While the data transmission rates from observation satellites and other spatial facilities are assumed to be higher than 20 Gbps in 2015, the high-speed, large-capacity communications beyond radio waves can only be realized by optical communications. With the remarkable development in optical technologies in recent years, the era of using laser for space communications has come.

Establishment of the Satellite-To-Ground Optical Link

In 1994, the Space Communications Group of NICT successfully conducted the ground-to-geostationary satellite optical communications link test by using the Engineering Test Satellite VI "Kiku 6" (ETS-VI) for the first time in the world. Later, since 2001, the European Space Agency (ESA) has been availing the optical communications links twice a day between the geostationary satellite ARTEMIS and the French SPOT 4 optical Earth observation satellite. The Optical Inter-orbit Communications Engineering Test Satellite (OICETS, customarily called "Kirari") developed by the Japan Aerospace Exploration Agency (JAXA) was put in the sun-synchronous orbit at an altitude of 610 km in August 2005. In December 2005, the two-way optical communication experiment between the Kirari and ARTEMIS satellites was conducted on an international collaboration basis. At that time, the writer was sent to JAXA for the development of the optical communication mission payload, then returned to NICT, and in 2006 through 2009, we carried out the ground-to-low Earth orbit optical communications test above the NICT optical space communications ground station (hereafter called "NICT Optical Ground Station", Figure 1) located in

Koganei City, Tokyo (Figure 2). The successful actual measurement of atmospheric turbulence on the ground-to-low earth orbit optical links for the first time during the course of this communications test not only indicates its academic significance but also suggests that the technology can be expected to realize a broad scope of applications such as optical communications between buildings in urban areas, optical communications between aircraft or other flying objects and the ground, and optical wireless technology fields.

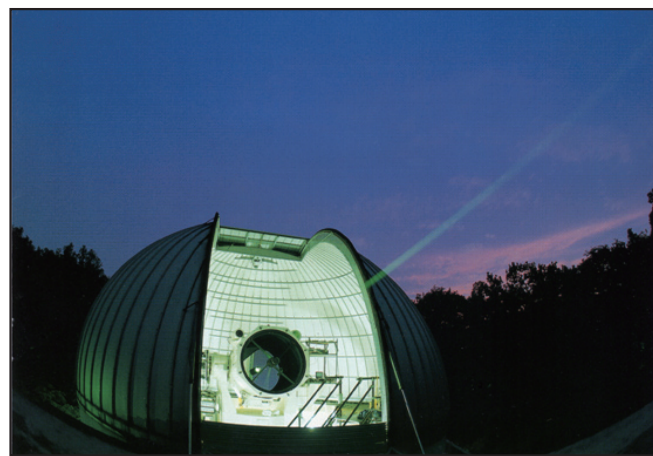


Figure 1 ● Telescope of NICT Optical Ground Station

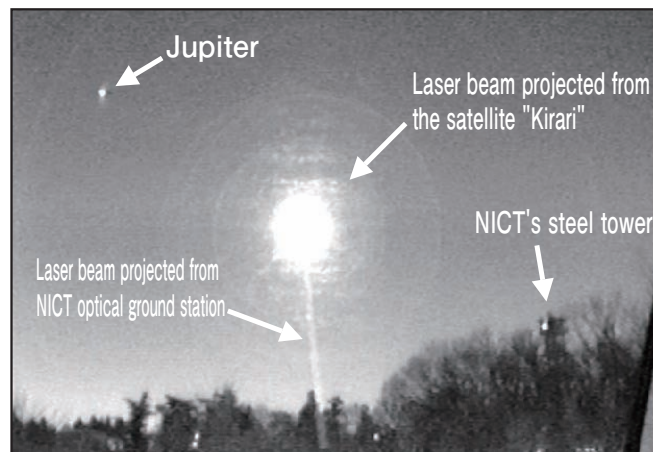


Figure 2 ● Experiment of the World's First Optical Communications Between the Low-Earth-Orbit Satellite and Ground Station

Application to Free-space Quantum Key Distribution

In the information and communications technology fields, the demand for information security technologies to prevent information leakages and illegal accesses is ever on the increase and thus cryptographic technologies are gaining importance against the ever-sophisticating eavesdropping technologies. Since the quantum cryptography system employs photon as the transmission medium for quantum signals, it has a very high affinity with optical communications. The optical transmission used for quantum key distribution at current stage is limited in its transmission distance to 150 km or so because of the loss in the fiber, and consequently intercontinental transmission cannot be performed. In contrast, any free space permits much further transmission, and when a low-Earth-orbit satellite is utilized, the quantum key distribution can reach anywhere on the Earth. In many cases of quantum key distribution, polarized light is employed. In the optical communications test with the satellite "Kirari", we obtained the satellite-to-ground polarized light characteristics for the first time in the world, and successfully quantified the influences on quantum key distribution. NICT developed a prototype model of verifying the implementation of quantum key distribution system for space transmission, and

performed the demonstration test of quantum key distribution between buildings within a distance of approximately 1.37 km during the International Conference on Updating Quantum Cryptography and Communication (UQCC) held in October 2010 (Figure 3).

Future Perspective

The Space Communications Group is now contemplating the space demonstration test of optical communications with the use of the Small Optical TrAnsponder (SOTA) on an orbit by seizing an opportunity of launching a small satellite. We are currently developing the flight model of SOTA, and it will be installed onto a small satellite of 50-kg class. It will have a weight of 5 kg, and an optical antenna with a diameter of 4.5cm will be equipped on it (Figure 4). SOTA will be equipped with two laser units, each capable of emitting non-orthogonal polarized light, and the photon measurement experiment at a photon counting level will be conducted on a ground station. This setup will allow us to obtain fundamental data required for quantum key distribution. These optical technologies are expected to play important roles in the transmission of a wide variety of environmental and disasters observation data collected by Earth observation satellites and to serve as the infrastructure to support social reliance and security in the provision of high-security communication lines.



Figure 3 ● A View of Inter-Building Quantum Key Distribution Demonstrated at the UQCC

Keyword Optical Inter-orbit Communications Engineering Test Satellite (OICETS, "Kirari")

Satellite "Kirari" (OICETS) is an engineering test satellite. On August 24, 2005, it was installed on the Dnieper rocket and launched from the Baikonur Cosmodrome, Republic of Kazakhstan, with the primary objective of conducting the demonstration test for communications with the Advanced Relay and Technology Mission Satellite "ARTEMIS" of the European Space Agency (ESA). In the optical communications between a low-Earth-orbit satellite and a ground station, since the optical intensity level of received light significantly varies with the time under the atmospheric turbulence, an extremely high-precision tracking technology is required to maintain laser transmission to a ground station while flying at a high speed. As introduced on this page, NICT and JAXA have succeeded in the joint operation of optical communications between the above-mentioned satellite and a ground station. Such a success in optical communications between a low-Earth-orbit satellite and an optical ground station is indeed for the first time in the world, and thus the results have proved the high technological capabilities of Japan.

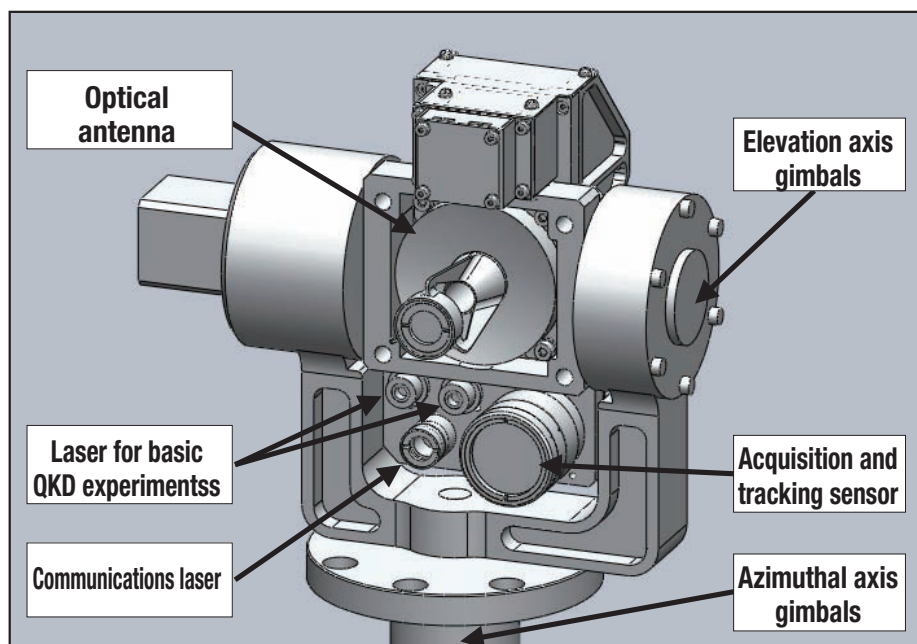


Figure 4 ● Small Optical TrAnsponder (SOTA) flight model onboard Micro-Satellites Being Developed

International Conference on "Updating Quantum Cryptography and Communications" UQCC 2010 "Quantum Technology Pioneering the Future Technologies Through Visible and Tangible Approaches"

Masahiro Takeoka, Former Senior Researcher and Mikio Fujiwara, Senior Researcher of the Quantum ICT Group,
New Generation Network Research Center

NICT held Updating Quantum Cryptography and Communications" UQCC 2010

by the co-sponsorship with National Institute of Advanced Industrial Science and Technology (AIST) and Information-technology Promotion Agency, Japan (IPA).

Date/venue October 18(Mon.) -20(Wed), 2010/ANA Intercontinental Hotel Tokyo

Organizer: NICT, IPA, and AIST

Co-organizer: Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry

Participants: Total 324 attendees. (including ICT-affiliated companies, financial related companies, universities, etc.)

UQCC 2010, Updating Quantum Cryptography and Communications, is the conference based on Updating Quantum Cryptography (UQC) held in 2007 and 2008 and the field of quantum communications. The objective of this conference is to introduce recent trends of the quantum cryptography and quantum communications that have just been put in practical use to not only researchers, but also people in the public sectors and private enterprises in a readily comprehensible way so as to allow those people to discuss upcoming problems and strategies for cross-field collaboration. In the morning session of the opening day, we succeeded the live demonstration for the unconditionally secure communication (the one-time pad encryption by using a shared key via quantum key distribution) of sending animated films in the world's first urban constructive environment (45 km) using the quantum key distribution network (Tokyo QKD Network) which was structured on the Optical Test Bed JGN2plus (Koganei-Otemachi-Hakusan) by NICT and contractors (NEC Corporation, Mitsubishi Electric Corporation and Nippon Telegraph and Telephone Corporation). Five organizations in EU including Toshiba Research Europe Ltd. (TREL) contributed excellent technologies to this demonstration. The afternoon sessions included an honor lecture and two keynote lectures. The first honor lecture given by Professor Tomonori Aoyama of Keio University (NICT Program Coordinator) introduced the vision of the new generation network. For the subsequent keynote lectures, Professor Adi Shamir of the Weizmann Institute of Science, one of the inventors of RSA cryptography presented the current status analysis and future problems in the technology of quantum cryptography, and then Professor Gisin of the University of Geneva gave a lecture on the current status of quantum cryptography and future directions. The following three principal issues in the progress of quantum cryptography were pointed out in the course of enthusiastic discussion:

1. Not only mere performance improvement but also simplifying systems and operations stabilization is extremely important in the developmental efforts.
2. Not only security of the equipment itself but also peripheral environment (risk of side channel attacks) must be taken into consideration in conducting the system design for enhancing the total cryptographic system.
3. To implement the technology on an actual network, the standardization of the interfaces between apparatuses is the urgent task.

Against these alluded points, the quantum key distribution apparatuses and quantum network management technology so far developed by the contractors have been materialized in the operation stability through optical fibers fitted in the urban area, the integration with TV meeting systems, the implementation of unconditionally secure TV meeting, and the two-way link with the apparatuses of the participating European organization. These achievements were exhibited at the live demonstration, and thus the high performance and the far-reaching capabilities were substantiated. It should be added that the superconducting single photon detector developed by NICT was employed in quantum key distribution apparatuses manufactured by NEC Corporation and Nippon Telegraph and Telephone Corporation (NTT), and its high performance and stabilized operation were verified. Domestic and foreign concerned parties placed the expectation on the Ministry of Internal Affairs and Communications and NICT take the initiative in the issues pointed out at the conferences as regards development of future quantum cryptography, namely, not only the standardization but also the extensive equipment improvement and network deployment.

We wish to thank the people of government ministries and sponsoring companies for their immense support and cooperation in the organization and operation of this conference as well as publicity of the subsequent results.



Greeting speech by NICT President Hideo Miyahara



A scene at the UQCC lecture meeting



Q&A session after the live demonstration



Banquet speech by Mr. Hirobumi Miyabe, NICT Vice President, Member of the Board of Director

Information for Readers

The next issue will cover a wide variety of subjects including monitoring variation of the atmospheric environment, multilanguage automatic translation technology, 3-D video images, biological safety against radio wave from mobile telephone units, and so on.

NICT NEWS No.401, February 2011

ISSN 1349-3531

Published by
Public Relations Office, Strategic Planning Department,
National Institute of Information and Communications Technology
<NICT NEWS URL> <http://www.nict.go.jp/news/nict-news.html>

4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan
Tel: +81-42-327-5392 Fax: +81-42-327-7587
E-mail: publicity@nict.go.jp
<NICT URL> <http://www.nict.go.jp/index.html>

Editorial Cooperation: Japan Space Forum