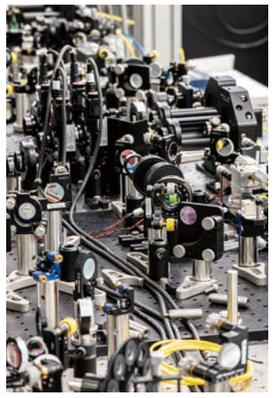
CONTENTS

NICT NEWS 2021 No.2 Vol.486

National Institute of
Information and Communications Technology

FEATURE

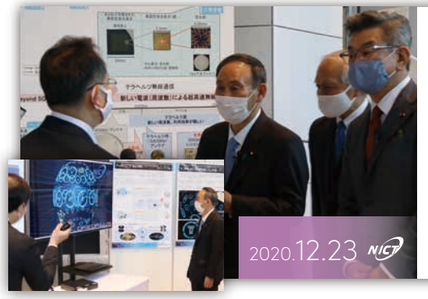
Special Issue on Quantum Technologies



Cover photo: Quantum key distribution equipment
The sender (left) and receiver (right) exchange photons and share the secret key for quantum cryptography. These devices are placed at two distant positions, between which the key is shared. They are housed in a server rack to serve as practical equipment. This equipment embodies the results of our long-term basic research using the quantum optical system built in our laboratory shown at the upper left of this page.

Interview

TOPICS



Special Column Prime Minister SUGA visited NICT headquarters to hear about the NICT's research on next-generation information and communications technology.

On Wednesday, December 23, 2020, Prime Minister SUGA Yoshihide visited the National Institute of Information and Communications Technology (NICT) headquarters located in Koganei City, Tokyo. Guided by Minister for Internal Affairs and Communications TAKEDA Ryoji and President of the NICT TOKUDA Hideyuki, he was shown around our research on next-generation information and communications technology.
The Prime Minister listened to the explanations of our researches including quantum cryptography, Beyond 5G, multilingual translation, and cybersecurity. After the tour, he commented to the press, "The NICT and the private sector are working hard on research and development toward the next-generation digitalization. I have got a strong belief that Japan will lead this field." Regarding Beyond 5G, he said, "It will become the social and industrial infrastructure in 2030 and beyond, and the government intends to boost research and development, and extend the outcomes to the world."

FEATURE Special Issue on Quantum Technologies

Interview

Future of Quantum ICT and Its Impact on Our Social Life

Research activities at NICT on quantum communication technologies

There is a growing trend towards the application of quantum mechanics, a science for describing the behavior of microscopic particles like photons and electrons, to engineering such as communication, computing, and sensing. IBM and Google are actively developing quantum computers. In Japan, Toshiba announced a practical quantum cryptography system that ensures the security of the core systems of the government and private companies. The NICT has a long history of research and development on quantum communication technologies, and has made significant contributions to the progress of quantum technology in Japan, including quantum cryptography. The heart of our research and development is the Quantum ICT Advanced Development Center. This article features an interview with the director, TAKEOKA Masahiro.

TAKEOKA Masahiro

Director, Quantum ICT Advanced Development Center, Advanced ICT Research Institute

He joined Communications Research Laboratory (currently NICT) in 2001 after receiving his Ph. D. degree. His current research area includes quantum optics, quantum information theory, and quantum cryptography. Ph.D. (Engineering).

——What is the situation of quantum technology in the world and in Japan?

TAKEOKA Looking back on the progress of research in quantum communication technology, research continued throughout the 1990s and the beginning of 2000s at the scientific level. However, around 2004-2010, Japan, Europe, and the United States succeeded in giving field demonstrations of quantum cryptography one after another, which were followed by practical research and development by private companies. In the mid-2010s, IBM and Google started full-fledged development of quantum computers, spurring the application of quantum physics, one of the most difficult-to-understand fields in physics, to engineering.

China invested heavily in quantum cryptography research, built a quantum cryptography network over 2,000 km long in 2017, and succeeded in an experiment with quantum cryptography between a satellite and the ground. It is considered that, in principle, quantum cryptography is unbreakable by any computer, and many nations including Japan are working hard on development. This is a new cryptographic technology and there are high hopes for both its social applications as well as national security.

In January 2020, the Integrated Innovation Strategy Promotion Council of the Japanese government announced the "Quantum Technology Innovation Strategy," which defined quantum technology as an important strategic technology, like AI. Also, a project for establishing a beachhead for quantum innovation has been started. The main applications of quantum technology include quantum computing, quantum sensing, and quantum communication. And through merging and collaboration with conventional technologies, quantum technology is expected to spawn unprecedented innovations in quantum AI, quantum life science, and quantum security, among others.

—— NICT has a long history of researching quantum cryptography technology.

TAKEOKA We collaborated with private companies including NTT, Mitsubishi Electric, NEC, and Toshiba, and universities to launch the Tokyo QKD Network in 2010. QKD stands for "quantum key distribution", and the Tokyo QKD Network is a testbed for conducting developments of practical quantum cryptography technologies. It is the longest-running testbed in the world. Through various experiments with private companies and universities, we have developed many technologies, and as a result, Japan is leading the world in terms of the performance of QKD tranceivers. We are also in the vanguard of application technologies such as controlling and managing networks, and how

Interview

Future of Quantum ICT and Its Impact on Our Social Life

Research activities at NICT on quantum communication technologies

to exploit QKD networks.

——Could you talk about your research on satellite QKD?

TAKEOKA In QKD, it is necessary to transmit photons, which are optical particles. However, photons scatter to some extent in a fiber, which restricts the distance they can reach. In contrast, space is a vacuum and so light does not scatter, meaning that in principle, we can transmit photons over long distances. To demonstrate this, we are working with the Wireless Networks Research Center to develop technology for QKD between a satellite and the ground. NICT has world-leading technology in satellite optical communication. Using this technology, we succeeded in a world-first basic experiment on using quantum communication to exchange information at the level of a single photon between a micro-satellite, what we call SOCRATES, and an optical ground station in 2017. The Chinese experiment used a large satellite weighing about 600 kg, but ours weighs just 50 kg. Micro-satellites are cheaper and therefore easier to commercialize. The development has been conducted as part of a five-year project by the Ministry of Internal Affairs and Communications (MIC). In fiscal 2020, we started new research and development involving collaboration among industry, academia, and government in Japan to create a global quantum cryptography network that integrates the ground networks and satellite QKD under a new MIC project.

Quantum research hubs

——What is the quantum research hub mentioned in the Quantum Technology Innovation Strategy of the Japanese government?

TAKEOKA Hubs are being established as strategic centers for research and development on major quantum technologies including quantum computing, quantum sensing, and quantum communication. The explicit intention is to attract players into this field of research. The NICT is in charge of the "quantum security hub," which pursues the commercialization and dissemination of new technologies created by combining quantum security technologies such as QKD, modern security technologies, as well as the cutting-edge communication technologies. Researchers and engineers from academia and industry gather here. The facility is the center of research and development, and also a place for nurturing human resources and social implementation.

Through collaboration between the government and private sector, we can clarify the vision for the practical stage of quantum cryptography. It also enables us to identify technology fields where we are weak, how the technology will be used, and how to make it more useful. For example, we are currently working with medical professionals to carry out demonstration experiments on protecting medical records and genetic information, which is important private information for patients. We also started collaboration with financial institutions and government organizations.

Japanese leadership in international standardization

——Could you talk about your efforts on international standardization?

TAKEOKA From the technological viewpoints, quantum cryptography network is a communication network similar to telephones and the Internet. If each country builds a network based on its own standard, it cannot connect to others. This is why we have to establish an international standard.

When building a standard across the globe, each country tries to take advantage of it by making it compatible with its own development. We have made a head start over others by launching the Tokyo QKD Network, and have gained practical experience through 10 years of development and operation. Another great advantage is the close ties between research institutions like the NICT and the manufacturers involved in actual operation. A network is not just a collection of equipment; its elements must be connected with each other and controlled in an integrated manner. Those nations that have acquired such techniques have an advantage.

In October 2019, the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) published a recommendation labelled as Y.3800, the first international standard for QKD networks, at the initiative of Japan. Backed by our knowledge and experience accumulated through operating the Tokyo QKD Network, we were able to prepare a persuasive draft. The adoption of our proposal will bring significant advantages to Japanese industry when their QKDs are disseminated in worldwide commercial applications.

Educating "quantum natives"

——Do we have enough human resources for quantum ICT development?

TAKEOKA Because this field of technology is very new, we do not have enough human resources. Quantum science and technology such as quantum communication have been considered to be a part of physics, mathematics, and basic computer science. There has been little exchange between academia and industry on implementing communication and computing in the real world. Very few people understand both worlds. Since 2020, the NICT has been operating a project, NICT Quantum Camp (NQC), for educating "quantum natives," a new generation speaking quantum technology as native languages. This fiscal year, due to the spread of Covid-19, the main activities have been limited to online lectures with around 30 participants. However, we will expand the activities to include hands-on experiments and tours to research and development facilities, as well as lectures.

Most participants are graduate students interested in quantum technology, but there are also company employees and undergraduate students. In the future, we hope to develop human resources who will be involved in quantum technology as a business, not just as researchers.

——Are there any differences between the students studying quantum physics as cutting-edge physics and the people looking at engineering applications?

TAKEOKA Quantum physics itself is a broad field of study that cannot be fully explored in a lifetime. However, from the viewpoint of its engineering, it is not necessary to know everything. I think we will introduce a new form of study in which we start by efficiently acquiring only the essence of quantum mechanics required for engineering, then investigating the details when it is required. In fact, the basics can be understood with just knowledge of undergraduate-level linear algebra.

The future of quantum communication

——What future do you see for quantum communication technology?

TAKEOKA When Toshiba started introducing practical quantum cryptography last year, it marked the dawn of the industrialization of quantum communication technology in Japan. Other quantum-related technologies, such as quantum computing, have been attracting public attention, but these are new technologies with many issues to be solved. Rather than being swayed by the latest trends, we will take a practical approach and deliver what society really wants.

To make this happen, I think it is important to steadily nurture the existing technologies into practical forms. Another important approach is to think beyond the conventional frame of reference. We intend to conduct research and development while striking the best balance between these approaches.

In the 1960s, when several researchers started experiments on the first Internet, could they have imagined the services we enjoy today, such as online shopping and SNS? The early Internet was nowhere near as good as the telephone networks already in existence around the world at the time. Simply thinking beyond the conventional frame of reference and challenging new technologies led to the development of technologies that changed the world in 20 or 30 years. The same can be said for quantum network technology. Rather than keeping up with the latest trends, by continuing to tackle difficulties diligently and boldly, I believe we will be able to contribute to society in a completely new way.

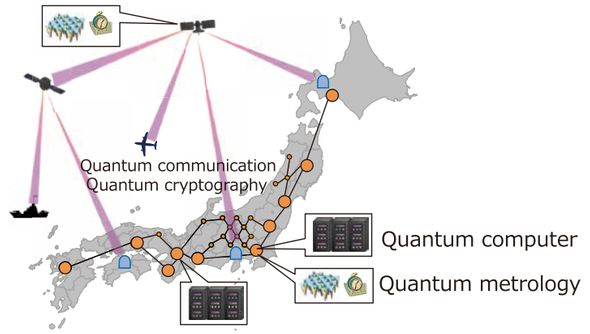


Figure 1 Overview of global quantum network

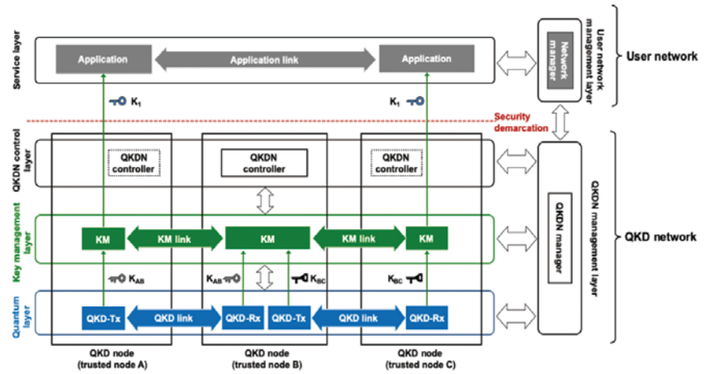


Figure 2 Basic configurations of the QKD network and user network specified in the international standard recommendation, ITU-T Y.3800

Development of Quantum Cryptography and Physical Layer Cryptography

FUJIWARA Mikio

Research manager, Quantum ICT Advanced Research Center, Advanced ICT Research Institute

He joined the Communications Research Laboratory, Ministry of Posts and Telecommunications (currently NICT) in 1992. He has been engaged in research on satellite-mounted far-infrared detectors, photon number classifiers, cryogenic electronics, and quantum key distribution. Ph.D. (Science).

ENDO Hiroyuki

Researcher, Quantum ICT Advanced Research Center, Advanced ICT Research Institute

After completing doctorial course, he joined NICT in 2017. He has been engaged in research on physical layer cryptography, quantum random number generation source. Ph.D. (Science).

The NICT has been conducting research and development of a technology for a cryptographic communication system that can not be broken even with the most advanced computers in the future, or a quantum cryptography network that ensures information-theoretically secure communication, as well as a technology for building a distributed storage on the network that is also theoretically secure. We have been operating a quantum cryptography network, Tokyo QKD Network, covering an area within 100 km from the center of Tokyo since 2010, and research on space-borne implementation is also ongoing. This article introduces our efforts and the progress towards global deployment.

Background

RSA and DH are currently the most popular public key cryptography, and are used in cryptographic communication through TLS and digital signatures. However, they are known to be breakable in polynomial time using a quantum computer, and so there is an urgent need to make them stronger. In August 2015, the National Security Agency (NSA) announced a migration to post-quantum cryptography based on a mathematical algorithm resistant to quantum computers. Then, in February 2016, the National Institute of Standards and Technology (NIST) released a plan for standardizing post-quantum cryptography, which is now in its third round as of December 2020. The migration is expected to start in around 2025. However, the post-quantum public key cryptography, which is used to exchange encryption keys, is only computationally secure, which does not guarantee that it will remain unbreakable in the future. Communication that is considered secure today could be broken someday. If genomic information that is encrypted today is decrypted in 30 years, it would cause serious damage, and so it is vital to take measures against information leakage today. A quantum cryptography technology frees us from the threat of decryption and is readily available. However, it has some technical issues such as the transmission distance and key generation rate. It is being implemented in society, along with research for overcoming the above weakness and introducing new functions.

QKD network

Quantum cryptography is a combination of two techniques: quantum key distribution (QKD) that enables sharing a secret key (random number) and Vernam's one-time pad (OTP) cipher that XORs the transmission data with a random number shared by the sender and receiver bit by bit. Based on the key distribution speed and distance of QKD as shown in Figure 1 (top), with typical optical fiber (having a transmission loss of 0.2 dB/km), a key generation rate of around 100 kbps to 1 Mbps is achievable over a distance of 50 km (transmission loss of 10 dB). Since the service distance is limited with only a single link, the encryption key information is stored in a trusted node as classical information and the key is distributed by encapsulation relay to extend the key distribution distance, or service area (Figure 1 bottom). QKD links and trusted nodes comprise a network, which is defined as a QKD network. Since 2010, the NICT has been operating Tokyo QKD Network, which was developed to enable reliable key relay even between QKD links of different vendors. The skills acquired through the development led us to establish Y.3800, the first ITU-T recommendation in the field of QKD, and the following series of recommendations, seven in total, demonstrating Japan's initiative in standardization.

In Europe, the operation of a network with a similar size is starting. China has built a QKD network with a total distance of 2,000 km through key relay between Shanghai and Beijing.

Even though our QKD network is smaller than the Chinese one, it is world-leading in terms of the performance of the QKD equipment, and the reliability and applications of the network.

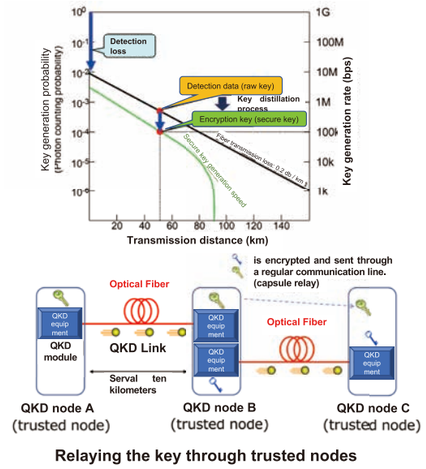


Figure 1 Performance of quantum key distribution (top) and key relay schematic (bottom)

Quantum secure cloud technology

A quantum secure cloud is defined as a QKD network and a distributed storage built on a quantum cryptography network that enables secure communication using the QKD network (Figure 2). The distributed storage is based on a protocol called secret sharing, which enables information-theoretically secure data storage. Secret sharing converts the original data into several pieces of data called "share" and transmits them through communication secured with quantum cryptography to distant places, where they are stored. The owner of the data can restore the original data by collecting a predefined number (threshold) of shares. If a number less than the threshold of shares is obtained by someone, the information in the original data is never leaked, which is mathematically guaranteed. The concept of secret sharing was first proposed in 1979. However, the secure transmission of shares was merely an assumption. The information-theoretically secure distributed storage of data, which does not rely on hand delivery, became available only after the advent of a quantum cryptography network. In secret sharing, it is also possible to implement a secure computation function that calculates statistical information about the stored data while maintaining its security. This means that secure transmission, storage, and secondary use of data are guaranteed. We are also conducting research and development of various other functions such as user authentication and integrity-ensuring technology. With these technologies, we succeeded in demonstrating the distributed storage of genome analyses, electronic health records (EHR), and biometrics data. Experiments using actual data are underway.

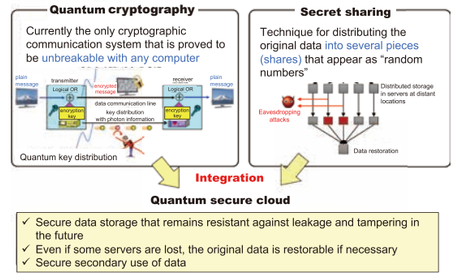


Figure 2 Concept of quantum secure cloud

Figure 3 Schematic of ground-satellite integrated global quantum secure cloud

Future prospects —Towards globalization—

With only a QKD network and a quantum cryptography network using an optical fiber network, it is too costly to cover the whole of Japan, let alone the entire world. Considering the above quantum secure cloud technology as a function like a database, accessing the cloud with an encryption key transmitted by satellite would dramatically expand the service area. Since 2018, the NICT has been participating in the "Research and Development of Quantum Cryptography Technology in Satellite Communication," a research directly controlled and commissioned by the Ministry of Internal Affairs and Communications, and proceeding with the development of small-satellite-borne equipment and portable ground stations. QKD is designed to be secure even against eavesdroppers by using a quantum computer or quantum memory, in a trade-off with restrictions on throughput. On the other hand, in line-of-sight communication such as that between a satellite and the ground, eavesdroppers in the communication channel can be identified by various means. The attacks available to an eavesdropper can be rationally restricted to passive tapping. We distinguish the technology for securely sharing an encryption key in such a communication channel from QKD and call it "physical layer cryptography." Research and development is under way on technology for sharing an encryption key at speeds that are orders of magnitude higher than that of QKD. Assuming that either QKD or physical layer cryptography will be used depending on the target, efforts will focus on developing practical technology. It is considered possible to build an information-theoretically secure global network using this technology (Figure 3). We are the only organization in the world which is conducting comprehensive research on a globalization strategy and killer applications, based on feedback from those involved in the NICT with various backgrounds. To achieve social implementation, we will strive to develop this technology into a truly meaningful art, not just a technique for dealing with quantum technology.