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.

---

**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 benchmark 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.

---

**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 transceivers. We are also in theanguard 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

Kevin Takeoka

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

Kevin 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 SCORATES, 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 a 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.

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

Kevin 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.

--- Could you talk about your efforts on satellite QKD?

Kevin Takeoka: From the technological viewpoint, quantum cryptography network is a communication network similar to telecommunication technology. It uses quantum states such as polarization, i.e., 0 or 1, as a carrier of information. Using this technology, we can establish a secure communication channel. QKD is considered to be a part of physics, mathematics, and 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 language. 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.

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

Kevin 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.

--- Could you talk about your research on international standardization?

Kevin 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 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 language. 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.

--- Can you talk about your research on satellite communications?

Kevin Takeoka: Communications satellites are used to provide international communication services, such as telecommunication, broadcasting services, and weather forecasts. The International Telecommunication Union (ITU) has established a number of international standards for satellite communications, but it is clear that these standards are not sufficient for the future needs of the industry. The ITU has been actively working towards the development of new satellite communication technologies, and NICT has been actively participating in these efforts. NICT has been working on a number of projects, such as the development of new satellite communication systems, the design of new satellite communication architectures, and the development of new satellite communication protocols. These efforts are aimed at ensuring that satellite communications can meet the needs of the future, including the needs of the growing number of users of emerging communication technologies, such as the Internet of Things (IoT) and the emerging 5G communication technology.

--- How do you see the future of quantum communication?

Kevin 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.

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

Kevin 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.
Development of Quantum Cryptography and Physical Layer Cryptography

The NICT has been conducting research and development of a technology for a cryptographic communication system that can 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 spaceborne implementation is also ongoing. This article introduces our efforts and 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 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 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 (quantum cryptography) 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.

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-enuring 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.

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-born 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.