NICT NEWS

National Institute of Information and Communications Technology

No.2 2021

Vol.486

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

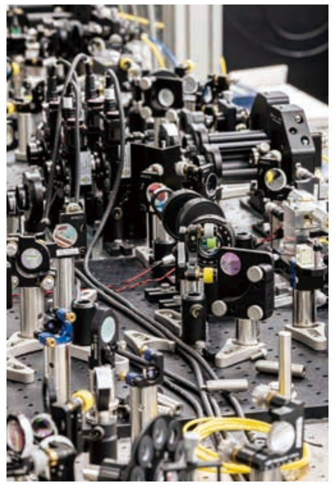
CONTENTS

National Institute of
Information and Communications Technology

NICT NEWS 2021 No.2 Vol.486

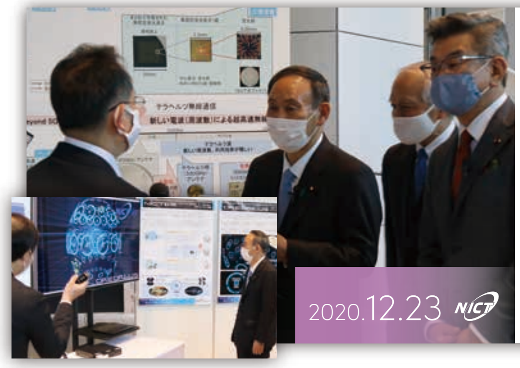
FEATURE

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



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."

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.

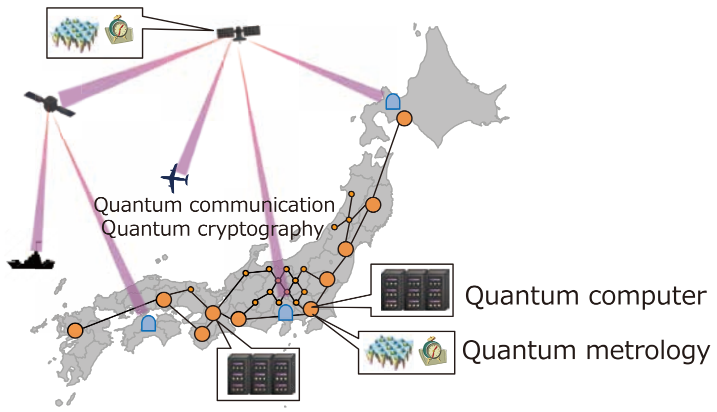


Figure 1 Overview of global quantum network

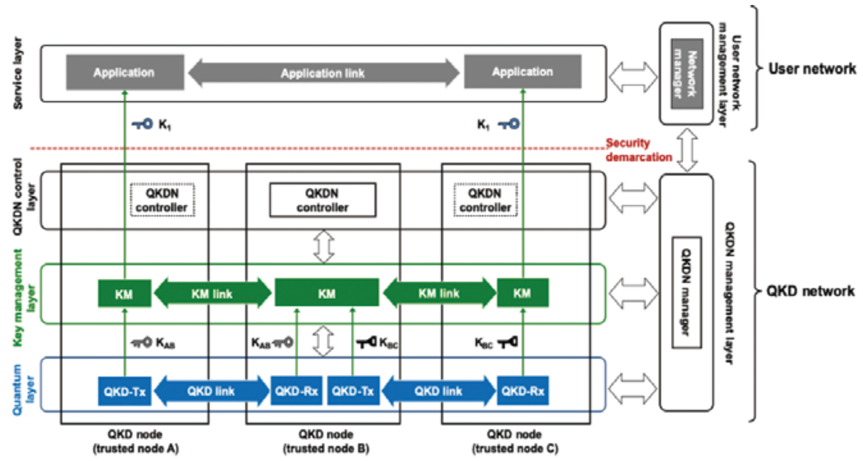


Figure 2 Basic configurations of the QKD network and user network specified in the international standard recommendation, ITU-T Y.3800

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.

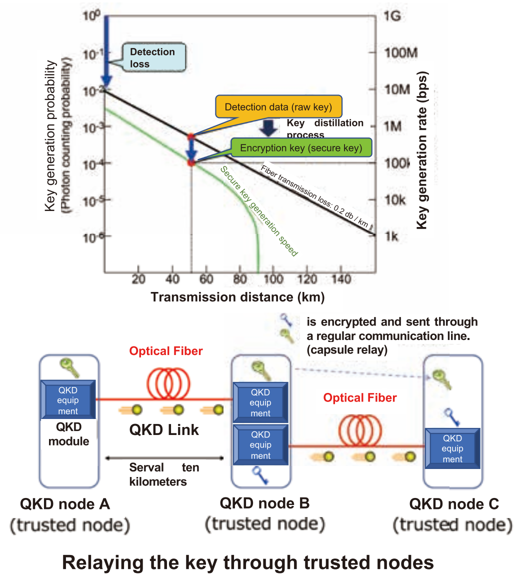


Figure 1 Performance of quantum key distribution (top) and key relay schematic (bottom)

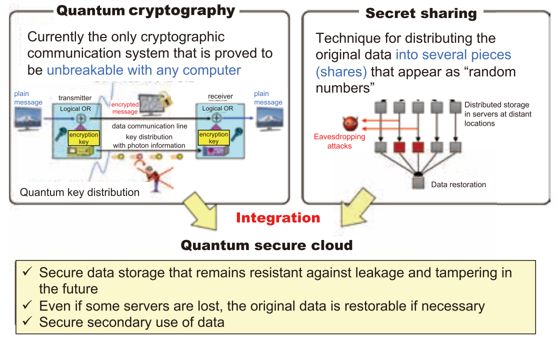


Figure 2 Concept of quantum secure cloud

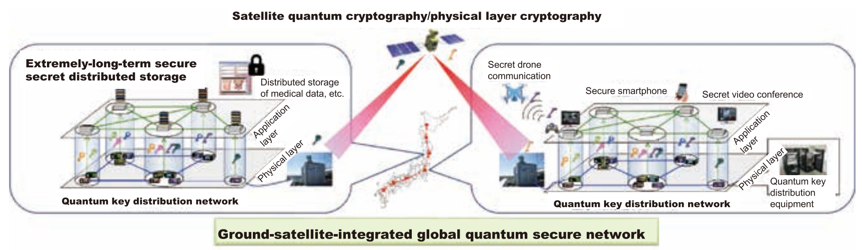


Figure 3 Schematic of ground-satellite integrated global quantum secure cloud

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-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.

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.

Research and Development of Photonic Quantum Technologies

TSUJIMOTO Yoshiaki

Researcher (Tenure-Track), Quantum ICT Advanced Development Center, Advanced ICT Research Institute

After getting his Ph.D. in Physics, he joined NICT in 2017. He is engaged in developing entangled photon pair sources and experimental demonstration of the quantum protocols. Ph. D. (Science).

A quantum network is the ultimate network which aims to connect quantum devices such as quantum computers in order to derive the maximum functionality based on the principles of physics. This network uses a correlation specific to quantum mechanics called "quantum entanglement" as a resource to realize a protocol that is not attainable with conventional technology based on classical physics. This article explains the latest results of our research and development on the fast generation and application of entangled photon pairs that have such a quantum correlation, and a proof-of-principle experiment of the quantum protocol made possible using those entangled photon pairs.

Creating a quantum network

The Internet has brought new values to society by connecting people and things. Similarly, the concept of a quantum network is a network that connects quantum devices such as quantum computers and quantum sensors. Distributed/blind quantum computing and ultra-precise time synchronization and various other protocols using quantum networks have been proposed, and many other applications will emerge in the future. However, much technical development remains to attain the benefits that are expected of quantum networks. NICT has been conducting research and development on technologies for generating and controlling entangled photon pairs, which will provide a basic resource for quantum networks.

Entanglement

Entanglement is a quantum correlation that cannot be explained by classical physics. Before exploring quantum entanglement, let's look at a classical correlation by taking the polarization of photon pairs as an example. Here, we have a device that generates photon pairs polarized vertically or horizontally, which is selected at random. By distinguishing whether each photon is polarized vertically or horizontally using a polarization filter, a correlation in which one photon is vertically (horizontally) polarized and the other photon is also vertically (horizontally) polarized, should be observed. However, if we replace the filter to distinguish between clockwise and counter-clockwise circular polarization, no correlation is detected. A correlation obtained by only a specific polarization is called a classical correlation. On the other hand, if we use entangled photon pairs, both the measurement that distinguishes between vertical and horizontal polarization and the measurement that distinguishes between clockwise and counter-clockwise circular polarization will detect a correlation. This behavior cannot be explained using the concepts of classical physics. A quantum network exploits such a quantum correlation.

Development of a source of ultra-fast entangled photon pairs

NICT has been developing a high-brightness / high-quality entangled photon pair source using non-linear optical effects called spontaneous parametric down-conversion (SPDC). Since SPDC generates photon pairs with a probability proportional to the intensity of a pumped laser, it should be possible to raise the brightness by increasing the intensity of the pumped laser. However, it is known that the higher the intensity of a pumped laser, the larger the probability of generating two or more photon pairs in a single pulse, or an error event, which degrades entanglement. One way to avoid this trade-off is to raise the pulse repetition frequency of the pumped laser. This decreases the energy per pulse, which increases the rate of generating entangled photon pairs without an increase in error events. We have succeeded in developing a

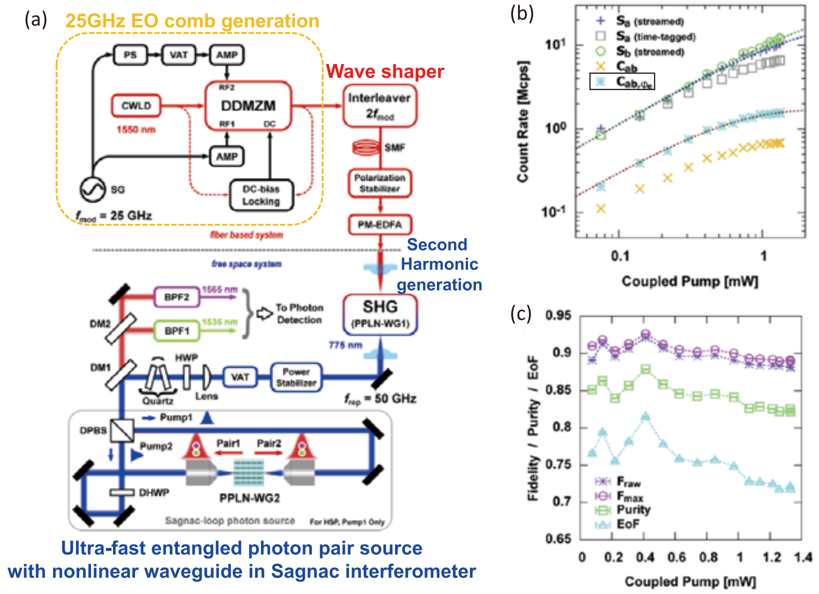


Figure 1 a) Configuration of ultra-fast entangled photon pairs: The entangled photon pairs are emitted from the waveguide-type nonlinear crystal. The pump beam is obtained by doubling the frequency of the high-speed optical pulses generated by electro-optical modulation (EOM).
b) Relationship between the detection rate of entangled photon pairs and pumping power
c) Relationship between the quality of entangled photon pairs and pumping power

new ultra-fast entangled photon pair source by combining a frequency comb source and a high-efficiency waveguide-type non-linear crystal (see Figure 1(a)). In this frequency comb source, the repetition frequency can be varied up to 50 GHz. As Figure 1(b) shows, the maximum detection rate of entangled photon pairs was 1.6 MHz, which was approximately a hundred times higher than the rate obtained in a previous experiment conducted by the Quantum ICT Advanced Development Center. In addition, as shown in Figure 1(c), we achieved high levels of fidelity, purity, and entanglement of formation (EoF), which represents the quality of quantum entanglement.

Quantum protocol demonstration experiment

A protocol that uses such entangled photon pairs as a resource is device-independent quantum key distribution (DIQKD). DIQKD is a next-generation QKD protocol that can obtain the secret key without any knowledge of the QKD device by monitoring the degree of quantum correlation between entangled photon pairs. The quantum correlation can be evaluated with the correlation parameter S, which is obtained from measurement, and if S exceeds two, the security of the private key is guaranteed. However, when performing DIQKD using entangled photon pairs generated with SPDC, the average photon number that maximizes S has not been clearly known. Using the experimental setup illustrated in Figure 2(a), we experimentally confirmed that S takes the maximum in a region of the average photon number that is significantly higher than conventionally thought (Figure 2 (b)). In addition, we experimentally demonstrated that long-distance DIQKD is possible by using a technique called entanglement swapping. The experimental setup shown in Figure 3(a) forms a long-distance quantum entanglement by generating two pairs of entangled photons and concatenating them. We applied entanglement swapping after adding the loss corresponding to a 50 km-long optical fiber to entangled photon pairs. The final state estimated from the result indicated that S > 2 (Figure 3(b)).

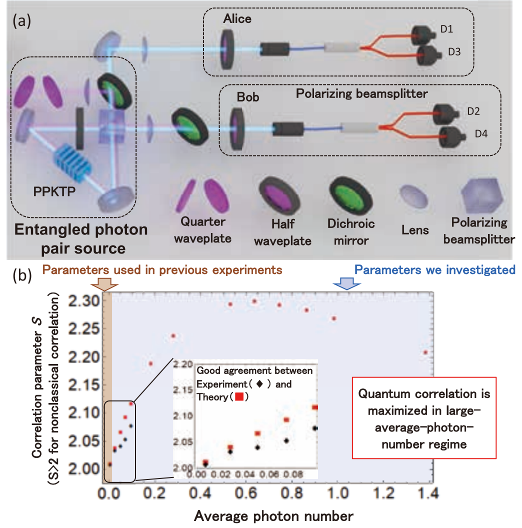


Figure 2 a) Schematic of the experiment system to measure the correlation parameter, S, of entangled photon pairs
b) Relationship between the average photon number of entangled photons and S

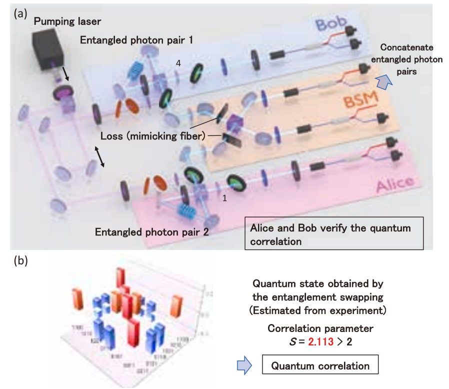
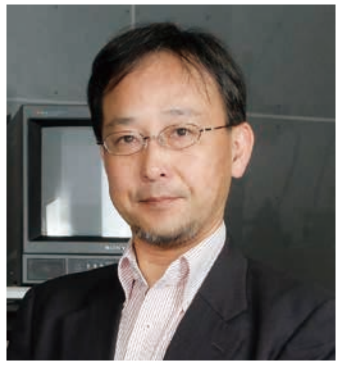


Figure 3 a) Schematic of the experiment system
b) Quantum state obtained by entanglement swapping

Future prospects

The research done so far has shown the possibility of fast generation of entangled pairs, and a quantum protocol such as DIQKD can be demonstrated by properly controlling and measuring generated photons. To create a quantum network, it is essential to mutually exchange quantum information by linking matter quantum memory and entangled photon pairs, as well as to sophisticate the above optical quantum control technology. This will require the research and development of various elemental technologies including quantum memory and a quantum media converter. The Quantum ICT Advanced Development Center will continue to study these technologies from various perspectives.

Trapped-ion Optical Clock and Quantum Network



HAYASAKA Kazuhiro

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

Joined Communications Research Laboratory (currently NICT) in 1990 after finishing his graduate studies. His research activities cover quantum optics with trapped ions. He is a specially appointed associate professor at Graduate School of Engineering Science of Osaka University. Ph.D. (Science).

TANAKA Utako

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

Joined Communications Research Laboratory (currently NICT) in 1994 after finishing her graduate studies. In 2003, she started working on quantum metrology with trapped ions at Graduate School of Engineering Science of Osaka University and she was appointed to an associate professor in 2006. In 2017, she was appointed to the current position under the cross-appointment system. Ph.D. (Science).

An ion trap is a device for capturing ions in a closed space with controlled magnetic fields. In combination with the laser cooling technique, it can keep ionized atoms stationary in a space. In addition, optical clocks, which are atomic clocks using optical frequencies, and quantum computers are known to be feasible by controlling the quantum states inside the atoms and of motion. This article introduces the research and development of a trapped-ion optical clock conducted by the NICT and the prospects for its application to a quantum network of optical clocks.

Background

Quantum mechanics textbooks introduce many thought experiments that involve manipulating the quantum states of each atom. However, even E. Schrödinger, one of the fathers of quantum mechanics, stated in the 1950s that experiments on an individual atom are unrealistic. However, in the late 1970s, it became possible to observe the quantum states of each ion in an ion-trap experiment. In 1982, a single-ion optical clock with a frequency accuracy of 18 digits was proposed. Then, based on the quantum state control technology of a single-ion optical clock, an ion-trap quantum computer was proposed in 1995. These technologies have translated into the recent realization of 19-digit frequency accuracy optical clocks and 32-qubit quantum computers.

Trapped-ion optical clock

The NICT has been conducting research and development on ion-trap technology since the 1990s. We have been leading the world, creating a calcium ion optical clock in 2008 and an indium ion optical clock based on sympathetic cooling in 2017. A single-ion optical clock generates an accurate optical frequency with the clock transition of an ion as the reference frequency. However, it takes a long time to determine the precise frequency due to the weak signal from a single ion. This issue was solved by an optical lattice clock that uses atomic ensembles. In this clock, ten thousand or more atoms are arranged in optical lattices, which are generated by light with a specific wavelength that cancels frequency fluctuations, to amplify the signal. Attempts have been made to use many ions in trapped-ion optical clocks, but the situation is different from a neutral atom that has no charge. In the conventional ion trap, frequency fluctuations called electric quadrupole shifts differ between ions, which leads to a different transition frequency by each ion, lowering the advantage of the use of many ions (Figure 1). While working to overcome this problem, the NICT has discovered a trap potential at which all ions generate the same transition frequency. Following the practice of calling the optical wavelength that suppresses the frequency fluctuations in an optical lattice clock a magic wavelength, we call this trap potential a magic potential. However, with the conventional ion trap, it is not possible to generate a magic potential due to the limited degree of freedom of controlling the potential.

On-chip ion trap

Since the conventional ion trap has the electrode arranged in three dimensions, it is not easy to generate arbitrary trap electric fields. This problem can be solved by an on-chip ion trap. In this ion trap, the electrodes approximate a flat shape and are placed on the same plane. By dividing these electrodes and applying different voltages, it is possible to generate a trap potential with a high degree of freedom (Figure 2). With this feature, on-chip ion traps are also widely used for quantum computers. In collaboration with Osaka University, the NICT created a prototype ion trap with 13 pairs of electrodes, and tried to generate a magic potential. As a result, we confirmed that a magic potential could be generated with 35 ions (Figure 3). Moreover, collaboration within the Advanced ICT Research Institute accomplished the in-house manufacturing of an on-chip ion trap with a superior surface accuracy and voltage resistance (Figure 4). In addition, we verified signal enhancement by several ions in an emulator with a conventional ion trap, and came close to creating a multi-ion optical clock using an on-chip ion trap.

Figure 1 Conventional ion trap (left) and trapped calcium ion (right)
It is recognized from the uneven intervals of the ions that the electric quadrupole shifts are not uniform.

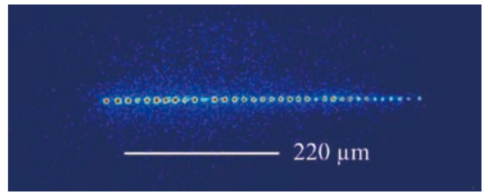


Figure 3 35 calcium ions trapped by the magic potential

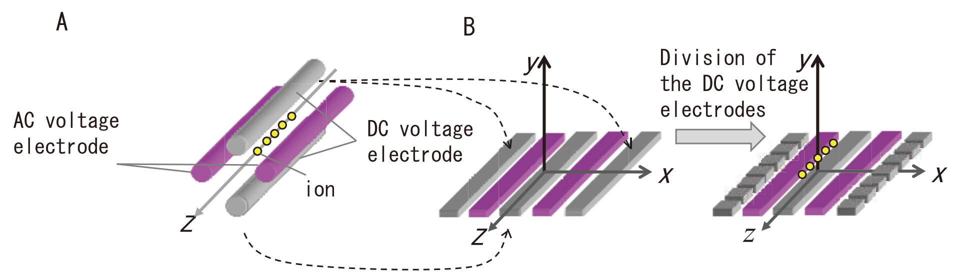


Figure 2 Configuration of ion-trap electrode
(A) Conventional ion-trap (linear trap) and (B) On-chip ion trap

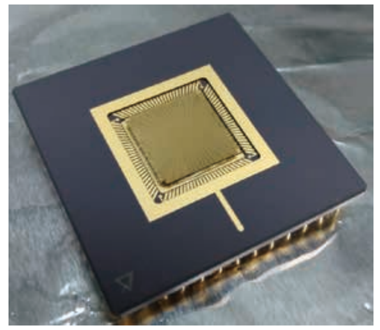


Figure 4 On-chip trap manufactured by the NICT
Manufactured by the Frontier Research Laboratory using the NICT's in-house facility

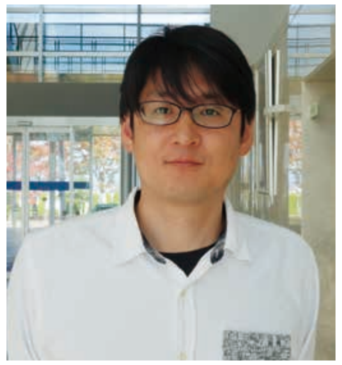
Quantum networks with ion traps and photons

When ions generate photons, the quantum states of the ions and photons produce a correlation called "quantum entanglement." While an ion has a mass and cannot be transported, photons can be transported over long distances in free space or through an optical fiber with relative ease. It is thought that by using ion traps and photons, we can attain quantum clock synchronization that quickly determines time by connecting optical clocks quantum-mechanically, and also create a photonically interconnected quantum computer by connecting quantum computers. The NICT has focused on quantum networks with ion traps and photons since an early stage, and, by teaming up with the Max-Planck-Institute of Quantum Optics, in 2004 succeeded in generating a single photon source with controlled time waveforms from a single ion. The wavelength of these photons was 866 nm, which limited the length of transmission through an optical fiber. However, in 2018, in collaboration with the University of Sussex and Osaka University, we demonstrated transmission through a 10-km optical fiber by converting these photons into photons having a wavelength for optical communication while preserving the quantum mechanical properties of the original photons. This achievement brought us much closer to the realization of a quantum network with ion traps connected through optical fibers.

Future prospects

Forming a network of optical clocks is expected to improve time-space information and the sensing of local gravity fluctuations, which will lead to the deployment of fiber links in Japan and other nations. A quantum network should reduce the time required for distributing and sensing time-space information obtained from such a network to the limit allowed by quantum mechanics. In addition to ion-trap technology, the NICT is conducting research and development on many element technologies required for quantum networks, such as optical frequency reference technology and micromachining technology, with the aim of pioneering the realization of these technologies.

Deepening of Superconducting Photon Detection Technology



MIKI Shigehito

Senior Researcher, Frontier Research Laboratory, Advanced ICT Research Institute

After Completing doctorial course, he became a researcher of JST. Joined NICT in 2005. He has been engaging in research of superconducting single photon detectors. Ph. D. (Engineering).

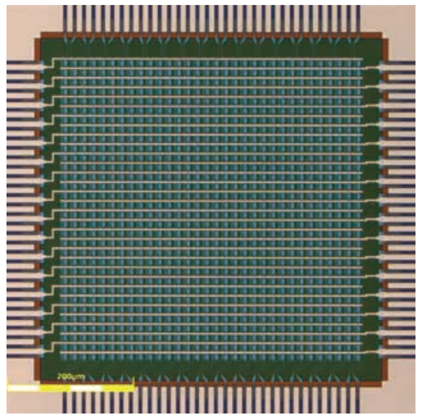


Figure 1 Optical microscopic photo of a prototype 1024-pixel SSPD

Photon detection is a basic technology in various fields such as quantum communication, very long-distance laser communication, laser ranging, and fluorescence correlation spectroscopy. For more than 10 years, the NICT has been conducting research and development of superconducting-nanowire single photon detectors (SSPDs) that outperform other types of detectors by using a superconducting material. Following past technological revolutions which delivered outstanding performance, work has started on refining the technology further.

Our research was introduced in the December 2013 issue of the NICT news under the title "Revolution of superconducting photon detection technology."* An SSPD is formed with superconducting nanowire with a thickness of several nm (nanometers) and a width of 100 nm or less. Our research project at that time succeeded in forming optical resonance structures above and below these nanowires, which boosted the detection efficiency at the communication wavelength band (wavelength of 1550 nm) from 20% to 80%. Then, the employment of a new structure further improved the performance. The detection efficiency of our SSPDs is now close to 90%. The dark count rate (number of misdetections per unit time), which is an important performance index of an SSPD, is 10 counts per second, which is much better performance than other types of detector.

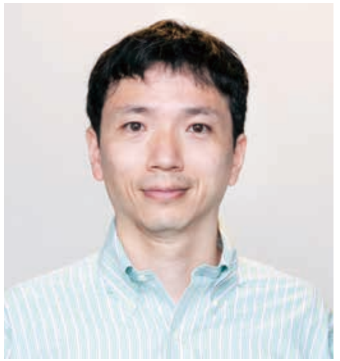
Development of SSPD array for deepening of the technology

The conventional SSPD can only detect the incidence of photons, but there is growing demand in various fields of advanced technologies for more sophisticated detection such as resolving the number of photons, their wavelength, and identifying the position of incidence. We believe that multi-pixelizing of the SSPD is the key technology to obtain such functions, and hence we are engaged in research and development. Since a large number of superconducting nanowires with a width of 100 nm or less have to be fabricated on a single chip, the difficulty of device fabrication technology increases dramatically. A technology for multiplexing the output signals from many SSPD pixels in a cryogenic environment (multiplexing signal processing) is also required. To solve these challenges, we have proposed SSPD multiplexed signal processing using a superconducting single-flux quantum (SFQ) circuit, and have demonstrated its operation. The SFQ circuit is a digital circuit, and so has flexibility in processing signals. With a multi pixel SSPD, the various functions mentioned previously can be implemented by combining a variety of circuits including multi-input logical OR, coincidence counting, address encoding, and so on. In addition, with the progress of technology for fabricating superconducting nanowires, starting from 4 pixels, we have succeeded in creating and demonstrating the operation of 8, 16, and 64-pixel SSPDs. We have also started to develop a prototype of a 1024-pixel SSPD as shown in Figure 1. Although it has not yet reached the stage of a complete operational demonstration, partial operation of the 1024-pixel SSPD has been confirmed, paving the way for a complete demonstration of a combination of SFQ circuits.

The number of pixels will continue to grow. Although many technological advances are still needed, we believe that a one million-pixel SSPD is no longer a dream.

* https://www.nict.go.jp/en/data/nict-news/NICT_NEWS_1312_E.pdf

Research and Development of Superconducting Quantum Circuits for Quantum ICT



YOSHIHARA Fumiki

Senior Researcher, Macroscopic Quantum Physics Research Project, Frontier Research Laboratory, Advanced ICT Research Institute

After completing his doctorial course of Nuclear Engineering, he worked at RIKEN as a researcher. He joined NICT in 2014. He has been engaged in research of quantum physics using superconducting quantum circuits. Ph.D. (Engineering).

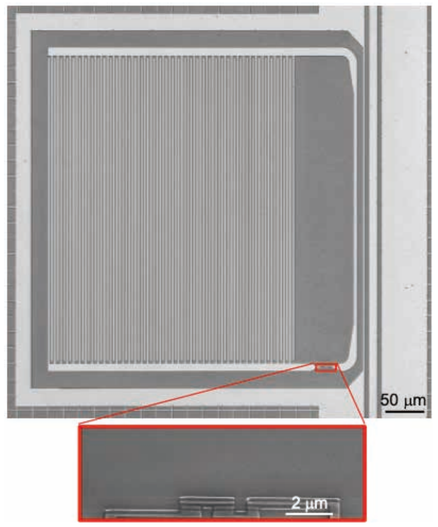


Figure Superconducting quantum bit (in the red rectangle) and a superconducting resonance circuit

In recent years, the research and development of quantum computers has gained momentum. About ten years ago, the feasibility of quantum computers was highly uncertain, but the number of qubits has grown rapidly in the last several years, and for specific problems, quantum computers have been demonstrated to offer faster processing speed than supercomputers.

The minimum building block of a quantum computer is called a qubit. It is the quantum version of a bit, which represents 0 or 1. A qubit can take a superposition of the 0 and 1 states. If there are two qubits, they can take a superposition of the state in which qubit A is 0 and qubit B is 0, and the state in which qubit A is 1 and qubit B is 1. In this state, the state of one qubit is determined by the state of the other qubit. Because of the strong correlation between the two qubits, this is called an entangled state. A quantum computer exploits superposition and entangled states specific to quantum mechanics to conduct quantum calculations. Such states are applicable to various types of quantum information processing, such as quantum communication, quantum measurement, and quantum simulation, as well as quantum computing.

Superconducting quantum circuits

Among the various physical systems for quantum information processing, a superconducting electric circuit is thought to be one of the most promising. When a superconducting electric circuit is in an ultra-low noise and very-low temperature (several tens of mK) environment, states specific to quantum mechanics such as superposition and entanglement appear. A superconducting electric circuit that shows phenomena specific to quantum mechanics is called a "superconducting quantum circuit." For a superconducting quantum circuit to operate, it must be cooled down to a very low temperature using a dilution refrigerator. However, a superconducting quantum circuit has the following advantages that more than offset the drawback of very-low operation temperature. A superconducting qubit formed on a superconducting quantum circuit has a size of several µm to several hundreds of µm, which is far larger than many other qubits. Therefore, it is possible to establish a very strong coupling between superconducting qubits and between a superconducting qubit and another circuit element, which results in high-speed operation. Moreover, since a superconducting quantum circuit is an electric circuit, it can be integrated, providing an infinite degree of freedom in design. These advantages imply the unexplored potential of quantum information processing technology using superconducting quantum circuits.

Future prospects

The Macroscopic Quantum Physics Research Project is conducting research with the aim of elucidating the interaction between superconducting qubits and microwaves at the level of a single photon, using a superconducting quantum circuit, which is indispensable for quantum information processing. By fully exploiting the advantages of a superconducting qubit, a large size and infinite degree of freedom in design, we have obtained various results.[*1,2] We will continue our research and development on improving the coherence properties of qubits, the quality of the qubit-gate operations and the measurement of qubit state, and so forth, which are essential for quantum information processing based on superconducting quantum circuits.

*1 "Superconducting qubit-oscillator circuit beyond the ultrastrong-coupling regime,"
DOI：https://doi.org/10.1038/NPHYS3906
*2 "Inversion of qubit energy levels in qubit-oscillator circuits in the deep-strong-coupling regime,"
DOI：https://doi.org/10.1103/PhysRevLett.120.183601

NICT Quantum Camp

KASHIOKA Hideki
Managing Director, Strategic Program Produce Office, Social Innovation Unit, Open Innovation Promotion Headquarters

There are high expectations for quantum ICT epitomized by quantum computation and quantum communication as a technology that provides superior performance to conventional technologies. As an important technology for maintaining national security and economic competitiveness, research and development of basic technology, as well as trials and reviews of industrial applications have been conducted. Many well-funded projects are under way in various countries.

Although the field is drawing attention, human resources are scarce. The final report on the Quantum Technology Innovation Strategy compiled by the Cabinet Office indicates the importance of "quantum-natives." The NICT held the NICT Open Summit on the theme "Next-Generation Quantum Information Processing and Artificial Intelligence" in July 2019, which also pointed out the shortage of researchers working on quantum ICT. In response, and in view of the requirement for developing good instructional materials and a system for developing human resources, NICT President Dr. TOKUDA initiated a review on specific efforts for developing human resources in this field. The NICT has been conducting a human resource development program called "SecHack365," which aims to foster cyber security innovators. While capitalizing on the experience of this program to establish an implementation system, we are developing "quantum natives" by inviting specialists in a wide range of fields, not just those covered by the NICT, from universities and companies across Japan to serve as instructors. For details, please visit https://nqc.nict.go.jp/(in Japanese).

Under the policy above, we are conducting two programs. (See Figure below.)

1. "Hands-on Human Resource Development Program" with seminars and exercises on basic knowledge and practical skills concerning quantum ICT

The purpose of this program is to broaden the human resources involved in quantum ICT. In fiscal 2020, it was initially planned to recruit around 20 participants. However, among the many applicants, 30 people including technical college students, university students, graduate school students, and employees were selected and are receiving remote seminars and exercises. During breaks between seminars, interaction among the participants and instructors is promoted to encourage the exchange of various ideas. Even when describing the same technology, instructors with different backgrounds have different aspects in their scope. Through these seminars, the participants learn various views and aspects of the same subject, quantum ICT.

2. "Exploring/Problem-Solving-Type Human Resource Development Program" for fostering researchers

This program aids research and development on quantum ICT with the theme chosen by each participant. A person or group can propose a theme for investigation, development, or research, with a grant of 1 million yen available for each theme. The program is intended to develop world-leading researchers who will support the NICT. Research and development are now under way on the two themes selected in fiscal 2020.

The name of the quantum ICT human resource development program, NICT Quantum Camp (NQC), was chosen based on various ideas and visions of people at the NICT. The NQC participants are closely linked, sometimes helping each other, sometimes competing with each other. The NQC provides such a community space. This is the essence of the NQC.

KASHIOKA Hideki

Joined ATR after completing the doctoral course at a graduate school, then joined the NICT in 2006. After working as the Director of the Spoken Language Communication Laboratory and the Director of the Brain Networks and Communication Laboratory, appointed to current post. Ph.D.(Engineering).

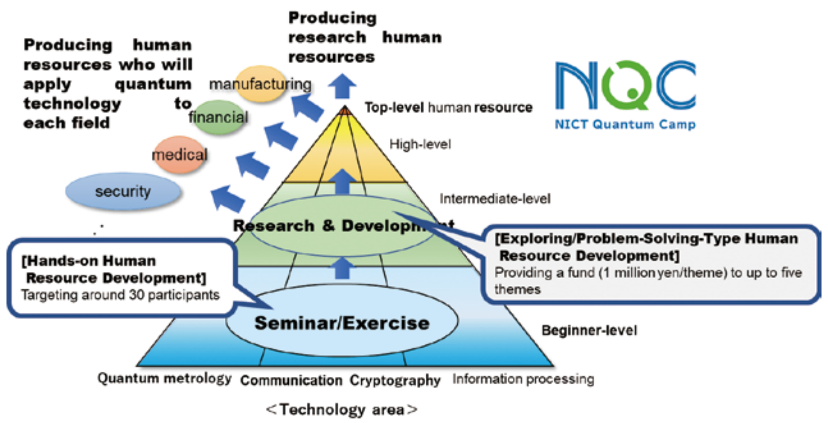
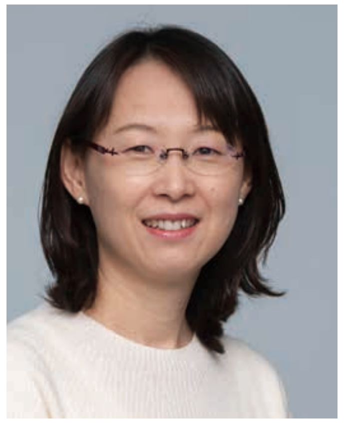


Figure Overview of NICT Quantum Camp

Toward a Breakthrough in Quantum Technology through Research on Superconducting Nitride Qubits



KIM Sunmi

Researcher, Macroscopic Quantum Physics Research Project, Frontier Research Laboratory, Advanced ICT Research Institute
Ph.D. in Physics

Biography

1975	Born in Buyeo, Korea.
2003	After completing the Ph.D. course in the Graduate School of Sogang University (Korea), came to Japan and joined the National Institute for Materials Science (NIMS) as a postdoctoral fellow.
2006	Postdoctoral fellow at the Institute of Laser Engineering, Osaka University.
2009	Postdoctoral fellow at the NIMS.
2013	Postdoctoral fellow at the Institute of Industrial Science, The University of Tokyo, and since 2014, Project assistant professor.
2018	Joined the NICT as a researcher.

Awards, etc.

2020	NICT Excellence Award, "Successful fabrication of an all-nitride π-junction flux qubit"
2018	Best Poster Presentation Award, Advanced ICT Device Lab, NICT, "Fabrication of a superconducting quantum circuit with a π-junction qubit"

Q&As

Q What do you want to be in your next life?
A I want to be a doctor who saves people's lives.

Q What was the most difficult time in your life?
A During an invited talk at an international conference held in the U.K. in 2006, I got nervous and froze. I learned the importance of presentation practice.

Q Are you hooked on anything now?
A I am a frequent visitor to a new deep-fried chicken shop in my neighborhood.

I am working on nitride-based superconducting quantum bits (qubits) in a macroscopic quantum physics research group. Using nitride superconducting materials, I design and fabricate quantum circuits functioning as artificial atoms, and investigate their microwave properties at an extremely low temperature of 10 mK. By establishing the nitride-based qubits to have a long coherence time, we are trying to create a new material platform of superconducting quantum hardware, which is important for quantum information processing.

Recently, superconducting qubits have been developed for quantum information processing not only in academia but also by companies such as Google and IBM. The core part of the superconducting qubit is a Josephson junction (JJ), which is a superconductor/insulator/superconductor junction, mainly fabricated by the aluminum (Al) oxidation process. However, it has been pointed out that the coherence times of superconducting circuits based on Al-based JJs are fundamentally limited by energy and phase relaxation due to microscopic two-level systems (TLS) in the amorphous Al-oxide layers. To solve such problems, it is essential to consider alternative materials. In comparison to Al-based JJ, an epitaxially-grown nitride (NbN/AlN/NbN) JJ has high crystal quality, chemical stability against oxidization, and relatively high transition temperature (~16 K) of NbN, making it suitable for qubit applications. In collaboration with the group of Dr. TERAI Hirotaka in the Frontier Research Laboratory of NICT and Prof. YAMASHITA Taro of Nagoya University, I have successfully fabricated a superconducting nitride qubit. By employing a Si substrate with TiN buffer layer instead of a conventionally used MgO substrate to reduce dielectric losses and a structure of capacitively-shunted flux qubit to suppress charge fluctuations, we achieved a significant improvement in quantum coherence of epitaxially-grown NbN-based qubits (manuscript in preparation). Also, we are developing the NbN-based qubits with ferromagnetic JJs (so-called π-junction) which make them operate in a magnetic flux-free state. Through these investigations with nitride superconducting qubits, we would like to develop a new quantum hardware platform that can be a breakthrough in the field of quantum information processing.

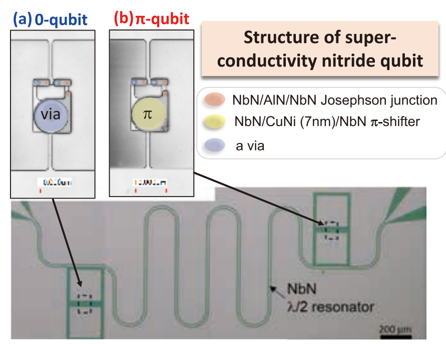


Figure Photograph of an NbN coplanar waveguide resonator coupled with a nitride flux qubits (a) without and (b) with π phase shifter

NICT NEWS 2021 No.2 Vol.486
Published by **Public Relations Department, National Institute of Information and Communications Technology**
Issue date: March 2021 (bimonthly)

4-2-1 Nukui-Kitamachi, Koganei, Tokyo
184-8795, Japan
TEL: +81-42-327-5392 FAX: +81-42-327-7587

URL: https://www.nict.go.jp/en/
@NICT_Publicity
#NICT

ISSN 2187-4050 (Online)