National Institute of
Information and Communications Technology

NICT NEWS

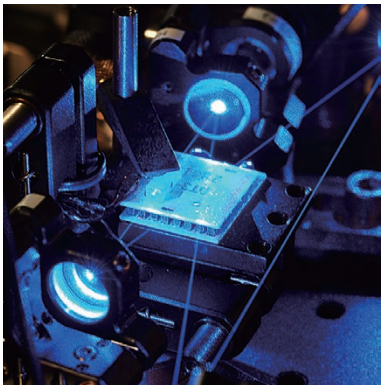
No.459 AUG 2016

FEATURE

New horizon of quantum-inspired ICT

NICT NEWS No.459 AUG 2016
National Institute of Information and Communications Technology

CONTENTS



FEATURE

New horizon of quantum-inspired ICT

1 Interview
The Vast and Fertile Field of ICT opened up by Quantum Technology
Masahide SASAKI

4 Quantum Info-Communications
Exploring the ultimate technologies of communication and measurement
Masahiro TAKEOKA

6 Developing quantum key distribution networks for absolutely secure communication
Mikio FUJIWARA

8 Frontiers of Research towards Quantum Communications Exceeding the Current Limits
Ultimate Control on Photons and Atoms Using Quantum Technologies
Kazuhiro HAYASAKA / Kentaro WAKUI

10 Quantum physics explored through superconducting circuits
Controlling interactions between light and matter at the single photon level
Kouichi SEMBA

TOPICS

12 Report on WIRELESS TECHNOLOGY PARK 2016
Report on Interop Tokyo 2016

13 Awards

Cover photo
An optical resonator, which stores laser light reflecting it back and forth between mirrors, and a nonlinear optical crystal placed at the center of the resonator. "Quantum entangled" photon pairs are generated by a nonlinear effect induced by the intense stored laser light.

INTERVIEW

The Vast and Fertile Field of ICT opened up by Quantum Technology

Masahide SASAKI
Distinguished Researcher
Advanced ICT Research Institute
NICT Fellow

After receiving B.S., M.S., and Ph.D. degrees in physics (high-Tc superconductivity), Masahide SASAKI worked for Nippon-Kokan Inc. (currently JFE Holdings). In 1996, he joined the Communications Research Laboratory, Ministry of Posts and Telecommunications (since 2004, National Institute of Information and Communications Technology (NICT), Ministry of Internal Affairs and Communications), working on quantum optics, quantum communication and quantum cryptography.

Quantum computers have computing power 100 million times faster than conventional computers. Quantum cryptography is mathematically proven to be unbreakable. Quantum phenomena will bring a revolution in information and communications technology and as such, are attracting much attention. How is quantum technology different from conventional technology? How can it be put to practical use? We spoke with Masahide SASAKI, Distinguished Researcher at the Advanced ICT Research Institute on these topics.

What does "quantum" mean, and what is "quantum ICT"?

—— Recently, "quantum" has come up more and more often as a new technology keyword. Can you tell us what "quantum" and "quantum ICT" mean?

SASAKI: A "quantum" is the smallest measurable unit of physical variables. For example, with electricity, in every-day use we measure current in Amperes, and voltage in Volts. However, when we create ultra-micro electronic devices, the voltages and currents involved are measured differently. As quantities get smaller, they change continuously to a certain point, but the behavior suddenly becomes discrete when they get very small and values change in steps. These steps are due to movement of electrons, which are "particles" that cannot be divided further.

Another example is with the light from a laser pointer. As the light is made very dim, eventually it starts to be intermittent, like raindrops, showing the scattered behavior of individual particles called photons.

In this way, the quantities that we use every day are all made up of particles that cannot be divided further. What is interesting is that these particles behave completely differently from objects we normally deal with. For example, if a pachinko ball is rolling on a particular path and encounters a branch, it will always take one or the other branch. In the quantum world, even if there is only one particle, it can be in a state where it "exists" in both branches. If that was the case for larger objects, there wouldn't be any point in a game like pachinko, because the basic rules of the game would change.

If these phenomena are used skillfully, however, great innovations can be made, completely different from computing and communications technologies built according to the classical rules. Quantum computers and quantum cryptography are such technologies typical of quantum ICT.

The goals of quantum ICT research

—— So this research holds the possibility of replacing conventional systems with completely new rules. Can you describe some of the prominent themes in this research?

SASAKI: There are two main issues with information and communications.

The first is the issue of transmission efficiency. Data traffic continues to increase, and how to process this increasing amount of information is a major issue. It is a matter of transmission efficiency; how to transfer more information with a smaller amount of energy. Within quantum ICT, quantum communication is the field that seeks to resolve this issue.

The second issue is security. With large amounts of important information being exchanged on networks, information leaks can lead to critical situations. Encryption is a practical measure for preventing leaks, and quantum cryptography performs encryption using quantum concepts. This is a particularly practical area, with quantum cryptography almost ready for practical use and some enterprises already beginning trial operation in user environments.

The key feature of quantum cryptography is that it is "unbreakable even against eaves-

INTERVIEW

The Vast and Fertile Field of ICT opened up by Quantum Technology

dropper who has unbounded ability". According to the uncertainty principle, each photon can carry information, and the action of measuring it changes the state of the photons. This makes it is possible to implement a function that will show definitively, whether an attempt to intercept the information has been made. This revolutionary new feature is impossible with conventional cryptography.

On the other hand, quantum communication uses the phenomenon mentioned earlier called superposition that a particle can exist in two states at the same time. This phenomenon is extremely delicate. The effect can only be gained under conditions with no noise, we have only recently reached a stage where we can handle it in laboratory conditions. If, in 10 or 20 years, we are able to build this extremely promising technology into receivers, it could provide transmission efficiencies of 1000, 10,000, or in cases even a million times that of today's technology. It will also be revolutionary for measurement standards technologies.

To summarize, our research is still at the laboratory level, but it includes both quantum communication, for which we are looking to the far future, and quantum cryptography, which has already almost reached practical implementation.

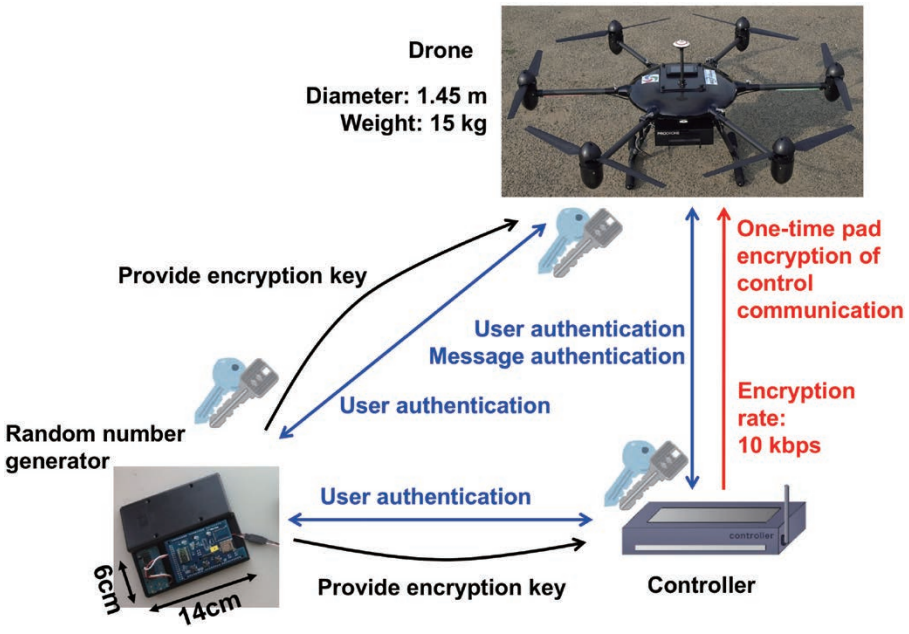


Figure 1 Secure drone communication. Random numbers are generated by a random number generator for encryption keys, which is shared with the drone and controller. Each control packet is encrypted. Encryption keys are only used once (one-time pad encryption). Random numbers are also used for user authentication and message authentication, ensuring the strongest security.

Also broadly expanding existing fields

—— Does the research seem to be getting farther away from existing technologies?

SASAKI: No, not at all.

If individual particles can be controlled, they behave according to a new set of rules, but when many particles are gathered together, they behave according to the classical rules. Researchers in this field look at both of these aspects. In that sense, we consider ourselves to be taking the broadest perspective on conventional ICT systems and our research encompasses all of conventional ICT to date.

In fact, quantum ICT work leaps beyond fields like conventional cryptography and networking technology, expanding them and turning out original new papers and patents.

In a recent example, random number generation techniques developed for quantum cryptography were used successfully to demonstrate secure drone communication. Drones are beginning to be used for various applications, but security of control and data communication has been inadequate, so establishing security has become a big issue. Our technology is a lightweight implementation that uses one-time pad encryption with random numbers, realizing the theoretical maximum-strength encryption for drones (Figure 1). Even when we issue a press release, people don't expect it to be from our team, and we get inquiries directed to, for example, the wireless networking field (smiles).

Quantum ICT research investigates the basic principles of information and communications, and in that process, can reveal new knowledge and discoveries regarding conventional technologies like cryptography and networking. Such results are written in the language of electromagnetics, information theory or cryptography, and while they may not be based on quantum properties, they are new technologies that improve aspects of conventional networks, like connectivity or safety.

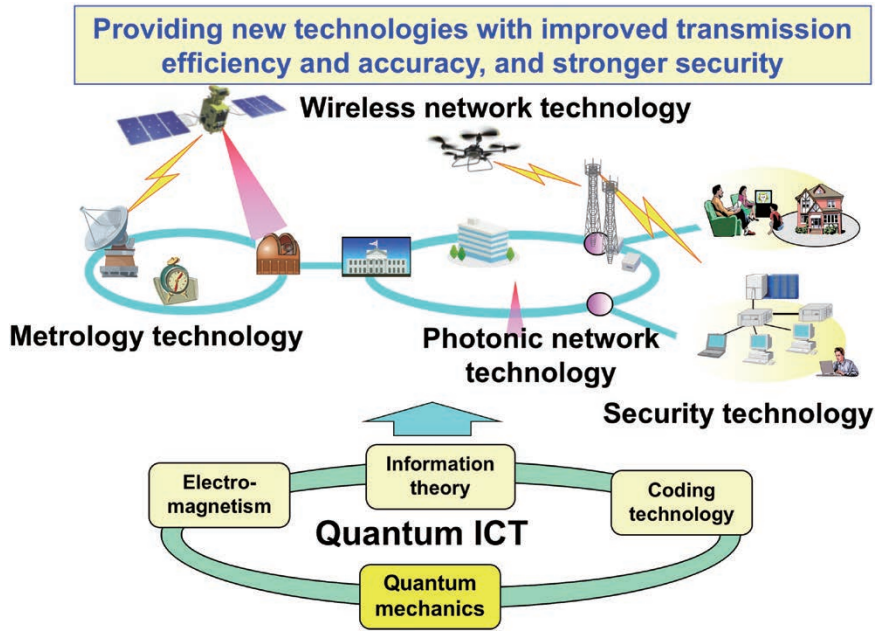


Figure 2 **Quantum ICT incorporates electromagnetism, information theory, coding technology, and quantum mechanics, opening up new horizons in security, network, and metrology technologies.**

We are working to dig deeper on such issues, and extend them using the language of quantum technology. Beyond that, the vast and fertile field of ICT is opened up, and we are cultivating new horizons not seen before (Figure 2). These areas of quantum ICT have been very exciting for us recently.

—— There is research on quantum ICT, but also developments in existing fields. It seems to be very broad and worthwhile research.

SASAKI: Sometimes people question whether our results have anything to do with quantum technology, but they still lie on the frontiers of technology, whether they deal with quantum ICT or conventional ICT. In fact, physical layer cryptography, which is a hybrid of existing technologies and quantum communication concepts, will bring a revolution in future networks, and will result in practical new technologies much more quickly than quantum communications.

ICT research from a "quantum perspective" is very dynamic and evokes very exciting responses. Recently, some enterprises that are giants in networking have begun putting all of their efforts into building new networks using satellites and drones. It seems that they are prioritizing the connectivity and convenience, but they will have to address security issues as well. As a forerunner in this area, we intend to contribute by producing results, both academic and practical, that will be useful in this area too.

COLUMN

R&D on Physical Layer Cryptography for Building a Global Secure Network

Till now, R&D on quantum communication, with the goal of optimal transmission efficiency, and that on quantum cryptography, with the goal of perfect security, have been conducted independently. To achieve strong confidentiality, additional bandwidth and coding is necessary for encryption, so no matter the case, some transmission efficiency must be sacrificed. Quantum communication realizes the maximum transmission rate while quantum cryptography enables perfect security. They are two extreme schemes of communication technologies. Physical layer cryptography is a technology that skillfully combines the strengths of both of them. The method optimizes the balance between transmission efficiency and security according to the channel characteristics, and the technology is generic enough to be used with light as well as other electromagnetic frequency bands. In particular, it is a core technology that will be used in building new, global, and secure networks using satellites and drones. In 2014, we built the Tokyo Free-Space Optical Communication testbed (Tokyo FSO testbed) and we are conducting R&D to demonstrate physical layer cryptography.

NICT Terminal (on the roof of building 3) in the Tokyo Free-Space Optical communication testbed (Tokyo FSO testbed). And the main R&D team members. It is a container system equipped with communications as well as an all-weather scanner that can also be used for sensing. It has an 8 km optical link with the optical terminal, located at The University of Electro-Communications, and conducts R&D on physical layer cryptography and new sensing technologies.

Quantum Info-Communications

Exploring the ultimate technologies of communication and measurement

Masahiro TAKEOKA
Director
Quantum ICT Advanced Development Center, Advanced ICT Laboratory

Joined Communications Research Laboratory (currently NICT) in 2001 after receiving his Ph. D. degree. His current research areas include quantum optics, quantum information theory, and quantum cryptography.

Current information and communications technology was designed based on physical laws established in the 19th century, and issues regarding transmission capacity and security of encryptions are prompting concern that we will reach the limits of these laws in the future. To overcome such limitations, NICT is conducting R&D on quantum information and communication technology, new technology based on quantum mechanics, the ultimate physical laws, and applications of this technology. We give an overview of this work below.

Quantum information and communications

The development of modern information and communication technology is remarkable, with advances continuing, even today. However, the possibility that performance limits will be met when extending current technologies has also been identified. For example, there are physical limits to the power of lasers that can be input to an optical fiber, and signals weaken until they cannot be received reliably as communication distances are extended in space. On the topic of communication security, the danger that currently common encryption methods used for communication will be decoded as computing technology advances in the future has also been identified.

On the other hand, there are predictions that if information technology can be implemented using quantum mechanics, the latest physics of the microscopic world of atoms, electrons and photons; a drastic technology revolution is possible. "Quantum cryptography" will achieve security impossible with conventional technologies, and "quantum computers" will be capable of rapid computations that would require tens of thousands of years using current computers. Since the beginning of the 21st century, there has been extensive R&D on such quantum ICT around the world.

NICT has established and is conducting R&D on two particular research themes related to communication, called "quantum photonic network technology" and "quantum node technology". Overviews of these technologies are shown in Figures 1 and 2.

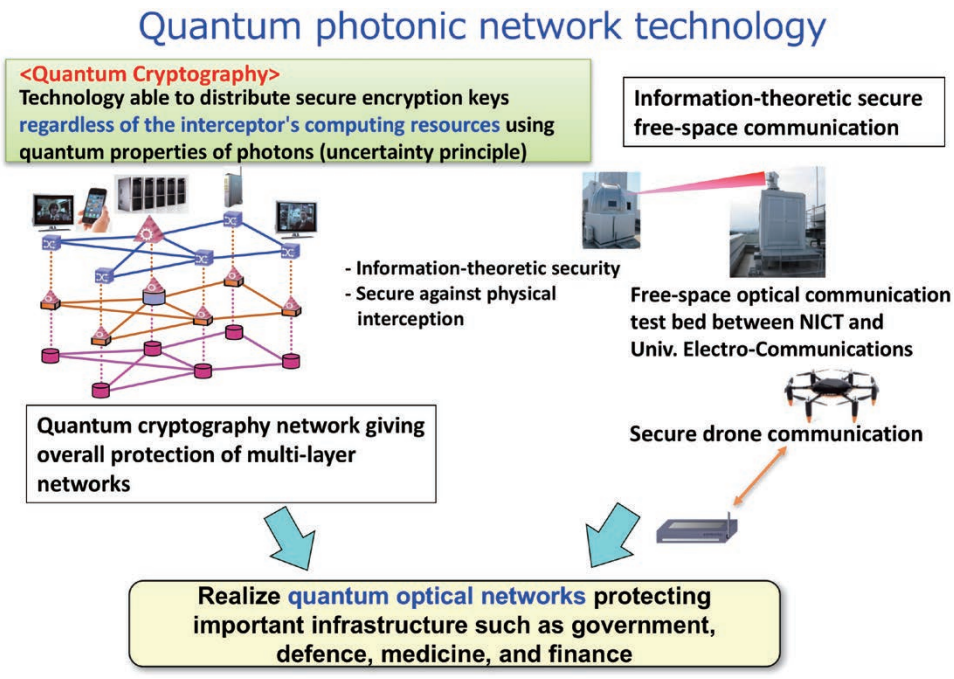


Figure 1 Overview of quantum photonic network technology

Quantum photonic network technology

Cryptography is currently used in various scenarios in society, but there is a danger that it will be decoded using future innovations in computing technology. This is a major issue for communication of confidential data such as government or medical information. For a radical solution to this issue, NICT is advancing R&D focused on quantum cryptography, which will provide the ultimate cryptographic solution. The main strengths of quantum cryptography over conventional cryptography are that it provides information-theoretically secure free communication, guaranteeing security that is not breakable regardless of advances in computing capabilities, and guaranteed security against any type of physical interception attack (such as tapping an optical fiber and stealing part of the signal). A quantum cryptography network would implement this using the quantum mechanical properties of light. Please see other articles in this issue for more specific details. NICT is also conducting R&D in areas other than quantum cryptography to implement information-theoretic secure communication using physical noise in various applications in the real world, such as optical free-space communication for drones, satellites, and other unmanned vehicles.

Quantum node technology

This area is more basic, long-term R&D. To extract the ultimate performance from optical communication, information must be carried on the very faint signals of individual photons and detected from them reliably. To do so, the ability to detect and control particular quantum mechanical phenomena without destroying them is essential. These quantum mechanical properties are extremely delicate, however, and several technical breakthroughs are still needed to achieve this.

"Node" refers to a relay point within a communications network. For this research theme, we take a broad perspective on the word, studying various ultimate technologies necessary to quantum-mechanically receive and process light signals at relay points. In particular, we focus on three research problems: "quantum optical control technology," to control the quantum state of light, "quantum metrology," which applies control of individual atoms or ions to quantum communication and frequency standards technologies, and "superconducting quantum circuit technology," which uses superconducting circuits, which are micro-sized artificial atoms, to accurately control single photons using interactions between light and matter. Details are discussed in other articles in this issue, but all are future pioneering technologies in quantum physics and are challenging problems that no one has fully realized yet.

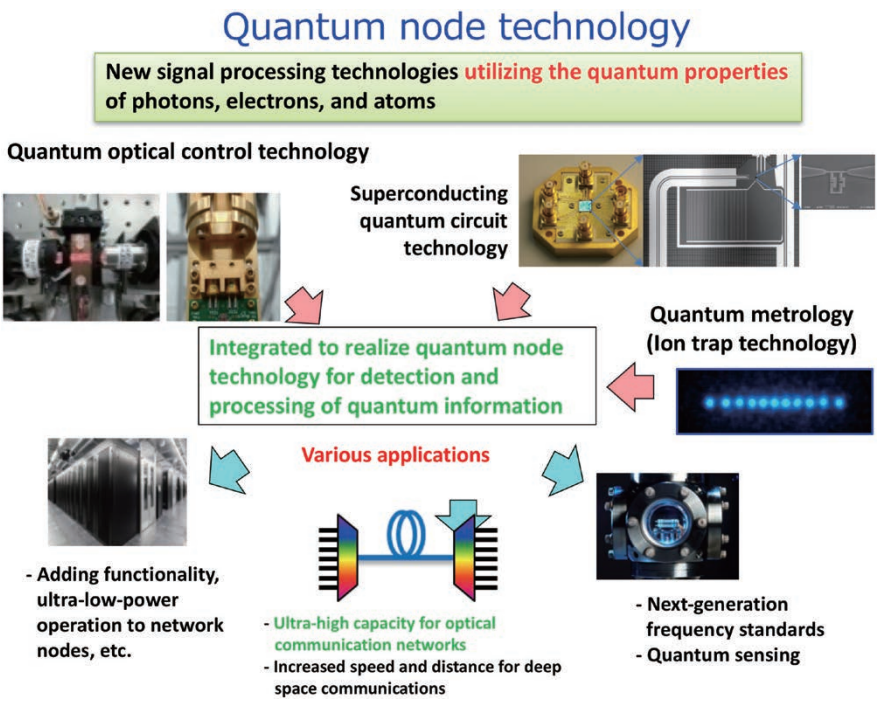


Figure 2 Overview of quantum node technology

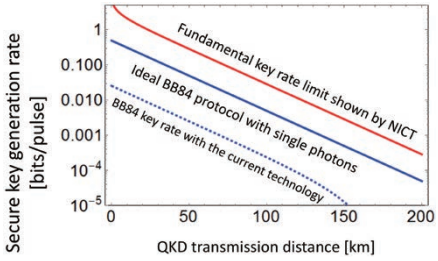


Figure 3 Fundamental limit of secure key generation rate in quantum key distribution.
BB84 is the current standard for quantum key distribution. The theoretical limit that we have shown will not be exceeded regardless of what new point-to-point protocols are conceived in the future.

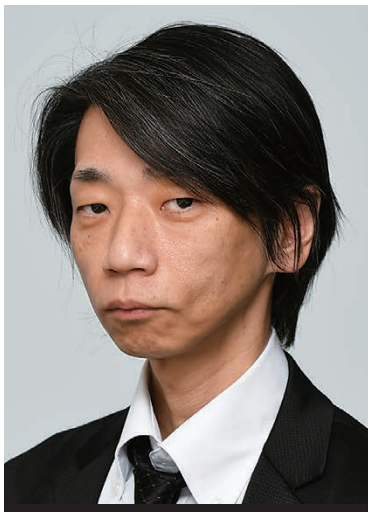
Conclusion

Theoretical research is also important for advancing quantum information R&D. Development of current digital communications technology is approaching the theoretical limits and capabilities shown by Shannon in 1948. Quantum ICT must be systematized into a new theory that incorporates quantum mechanics into Shannon's information theory, but this is still in progress. On the other hand, it is an extremely interesting research field, with technology and basic theory advancing together. We recently established the fundamental limit of secure key generation rate in quantum key distribution, which is a primitive of quantum cryptography, by applying information theory and quantum mechanics (Figure 3). This sort of basic theory is not only important as science, it also provides important guidelines for future technical development, giving benchmark levels of performance to strive for and levels that will be unattainable even with yet-to-be-discovered quantum key distribution protocols or even with the optimal design of real equipment. The theoretical outcome has been published in the journal Nature Communications*.

Quantum ICT is new technology at the boundaries between fields including physics, device engineering, communications engineering, security technology, and information theory. In our research group at NICT we have various backgrounds collaborating to advance this R&D. We are also actively collaborating with other research institutes and companies, domestically and internationally. These frontier technologies, which manipulate light, atoms, superconducting artificial atoms, and information, also hold great promise for development in various fields beyond quantum ICT, such as time/frequency standards and sensing technologies.

∗ Title: Fundamental rate-loss tradeoff for optical quantum key distribution
Author: Masahiro Takeoka, Saikat Guha, and Mark M.Wilde
Document number: Nature Communications 5:5235 (2014)
DOI: 10.1038/ncomms6235

Developing quantum key distribution networks for absolutely secure communication



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

Joined the Communications Research Laboratory, Ministry of Posts and Telecommunications (currently NICT) in 1992, where he was engaged in the development of Ge:Ga far-infrared photoconductors. Since 2000, he has been a member of the quantum information technology group. His current interests include GaAs JFETs, InGaAs pin photodiodes for the development of photon-number-resolving detectors in the telecom bands, and quantum key distribution. Ph.D. (Science).

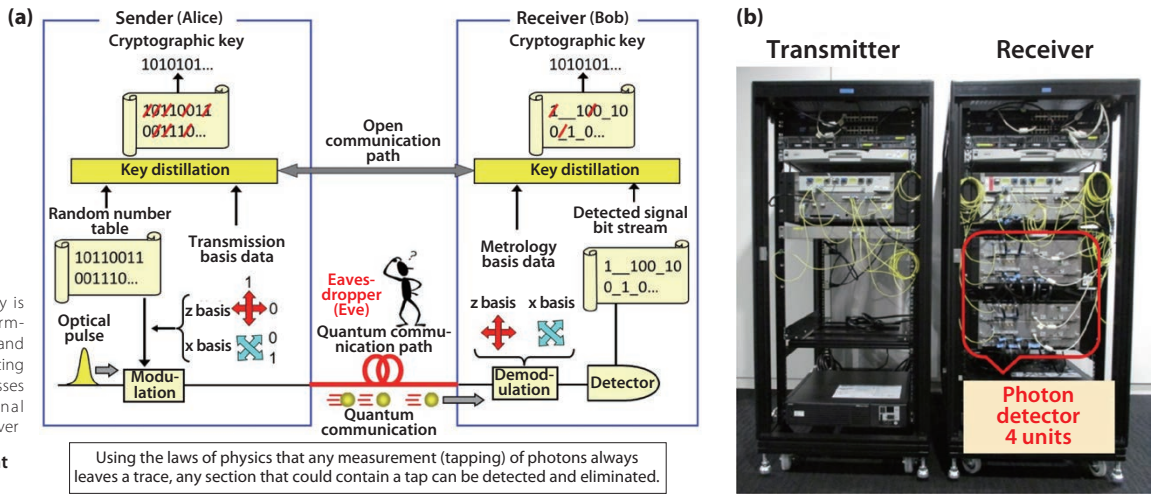
NICT is conducting research on quantum key distribution (QKD) links capable of absolutely secure communication, and networks composed of them. The security of QKD is guaranteed by the laws of physics, enabling unconditionally secure communication, regardless of the computing devices that may be developed in the future. Operating them in a network will not only allow for expanded service areas, it will also expand the range of applications. This article introduces the principles of this technology and related network architecture.

Background

The information leaked* by former NSA/CIA agent Edward Snowden has been widely reported, and some of the encryption used on the Internet may already have been cracked. A huge amount of capital is also being invested overseas in development of quantum computers, which will be able to decrypt public key encryption instantaneously. Highly confidential information is already being exchanged over the Internet in our daily lives, and there still seems to be little awareness of the danger of information leaks. Personal information such as genome data, which ought to be kept secure even after death, was never handled in the past, but ways to transmit such information, which needs to be kept confidential for long periods of time, now need serious consideration. Data such as confidential government information or genome data could result in problems even if it is disclosed 30 years later, so to transmit it safely will require development of safe encryption methods that are convenient and will not be affected by increases in computing performance.

Overview of Quantum key distribution

From its 2nd medium term target period (2006-2010), NICT has been working toward absolutely safe communications and advancing research on QKD, a technology that can share a random number as a cryptographic key between two parties in an absolutely safe manner. The QKD protocol, called BB84, was proposed by Dr. Charles Bennett and Prof. Gilles Brassard in 1984, more than 30 years ago, but QKD testing did not become common until this century. QKD is able to share a random number between sender and receiver, using photons as the information medium and sending one bit of information per photon using two non-orthogonal bases (Figure 1). The quantum state of a single photon is extremely fragile, so if an eavesdropper detects and resends the photon, there is a finite possibility that the quantum state will change. To detect such a change,



Using the laws of physics that any measurement (tapping) of photons always leaves a trace, any section that could contain a tap can be detected and eliminated.

Figure 1 **(a) Principles of quantum key distribution**
A cryptographic key is generated by performing error correction and other security reinforcing key distillation processes on the optical signal delivered to the receiver

(b) QKD Equipment photograph

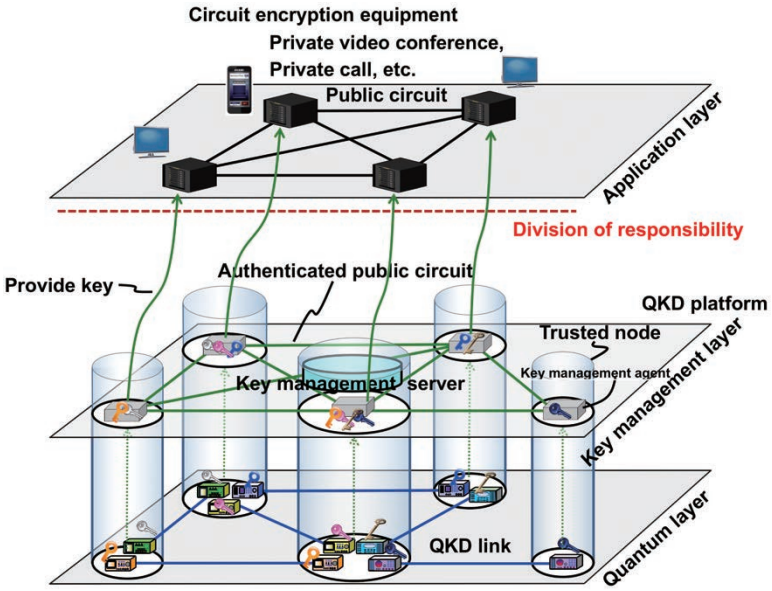


Figure 2 QKD platform overview
Quantum layer composed of QKD links from various vendors
Key management layer
Key management server: Constantly monitors overall network state and manages rerouting, etc.
Key management agent: Arranges and records cryptographic key formats and provides them according to user requests

the legitimate sender and receiver publish and check a part of the shared random number stream. An error in the responses indicates some sort of eavesdropping has occurred. The sender and receiver can use a random number for which eavesdropping has not occurred as an encryption key. Changes in physical state are absolute as long as quantum mechanics (specifically, the no cloning theorem) is correct, so we can say the safety of the protocol is guaranteed by the laws of physics. In 1948, one of the giants of information theory, Dr. Claude Shannon, proved that if a cryptographic key was shared in this way, it would be possible to implement absolutely secure communication that would not be decodable regardless of future increases in computing performance using one-time-pad encryption. One-time-pad encryption is an information-theoretically secure encryption scheme (not decryptable even with infinite processing capability) which uses exclusive OR operations on a cryptographic key shared between sender and receiver and uses different random numbers each time. The QKD link we have developed in Japan through collaboration among industry, academia, and government is the most advanced in performance and safety in the world today.

QKD Network Technology Improving Convenience

QKD is able to guarantee extremely strong security, but since the medium for transporting data is individual photons, many are lost during transmission. Some loss is acceptable because key generation can be done using just the arriving photons, but the key generation rate degrades rapidly as the transmission distance increases. Even on the most advanced QKD links, key generation rates only range between 100 kbps and 1 Mbps. It has been shown that transmission rates can be improved using wavelength multiplexing, but to develop technology to increase transmission distances there are still many technical issues to overcome, and more research is needed before quantum relay technology can be implemented. As a practical solution, a key information relay scheme is used, stringing QKD links together and temporarily storing information conventionally at intermediate points. For example, suppose that key K1 is generated on the QKD link between A and B, and K2 is generated on the link between B and C. To share keys between A and C, the disjunction (exclusive OR) of the keys (K1⊕K2) can be sent as classical data from B to C. Then K2 can be used at C to recover K1. In this case, there is a risk that key data could leak at nodes where it is stored as classical data, so key data must be managed with strict security. Such nodes are called "trusted nodes" and perform an important role in networking QKDs. This technology is essential for expanding usage area, applications, and availability for QKD link networks. Some important technologies for network connectivity include key format regulation, reliable key relay implementation, and reliable key sharing. The QKD network architecture proposed by NICT defines a layered structure with central monitoring. A quantum layer is formed by the QKD link set and a key management layer stores and manages keys as classical data. The key management layer has an interface for passing keys safely and reliably to the various users and applications. These two layers together are called the QKD platform and a QKD network (Tokyo QKD Network) is being operated using installed optical fiber with the cooperation of JGN-X and the Information and Communication Systems Office (Figure 2). With this testbed, we are conducting research to increase the reliability of the QKD platform, experimenting on long-term stability, rerouting when incidents occur, and other issues. We are also supplying cryptographic keys to communication devices on layers 2 to 4 of the OSI model, to enable expansion for various applications. In particular, sharing keys on mobile telephones will enable not only secure calling, but also applications such as personal authentication devices. We are also researching provision of keys to promising devices to be implemented in the IoT society, such as drones.

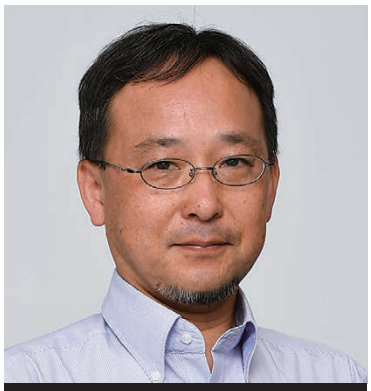
Future development

We are conducting R&D on QKD equipment and networks that use it to implement absolutely secure communication. We are also researching applications beyond just transmission, including distributed storage systems that can store data with information-theoretic security. As microbiologist Louis Pasteur said, "Chance favors the prepared mind." In the future, threats to current encryption techniques could be found at any time, so we are advancing our research so that when the need for unbreakable encryption becomes urgent, we will be able to provide a solution immediately.

＊ http://www.fortinet.co.jp/security_blog/130906-NSAs-and-GCHQ-Decryption-Capabilities.html
https://agilecatcloud.com/2015/10/20/researchers-claim-to-have-solved-nsa-crypto-breaking-mystery/

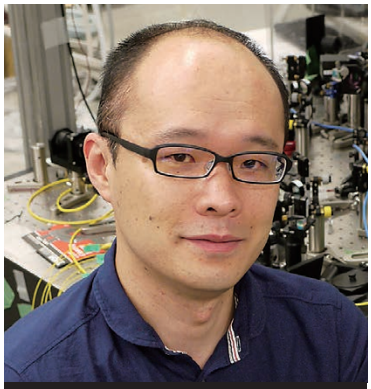
Frontiers of Research towards Quantum Communications Exceeding the Current Limits

Ultimate Control on Photons and Atoms Using Quantum Technologies



Kazuhiro HAYASAKA
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 guest associate professor at Graduate School of Engineering Science of Osaka University. Ph.D. (Science).



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

Worked for Fujitsu Laboratories Ltd. after finishing his Ph. D. He joined NICT in 2009. His research activities cover quantum optics and nonlinear optics. Ph.D. (Engineering).

On most data network nodes in the future, so-called "quantum node" technology will be needed for optimal quantum control of the light signals traveling on backbone networks. To achieve this, the ultimate control technology for quantum systems of photons and atoms will be essential, and such a technology will also have many applications beyond quantum nodes. This article introduces photon and laser-cooled ion quantum state measurement, which is one aspect of quantum node technical development being done at the Quantum ICT Advanced Development Center.

Background

With the spread of smartphones and the Internet, the issue of transmitting large amounts of information reliably and efficiently is becoming rapidly more pressing and familiar. According to the latest results in quantum information theory, it will be necessary to decode received signal pulses using quantum computation in order to achieve optimal transmission capacity on backbone networks. This involves being able to generate, control, and measure quantum superposition states, like the famous "Schrödinger's cat," within the decoding circuits. Quantum superposition is a quantum mechanical property that we do not observe in normal life, in which "the cat is both alive and dead at the same time." To control such states requires quantum node technology, which requires creating extreme environments in the main data network nodes, able to control interference and losses at the photon or atomic level, and performing optimal quantum control on the optical signals traveling over backbone circuits. Technology to measure and control quantum systems such as photons and atoms is essential for implementing quantum node technology.

Entanglement swapping using photons

Quantum mechanics allows two particles separated by an unlimited distance to be correlated in a remarkable way that enables them to appear to exchange information. A pair of photons that have this quantum correlation are called a quantum-mechanically entangled photon pair. Applications of entangled photon pairs include safe communication (quantum signals) not possible with laser light, high-speed computation (quantum computation), and even highly accurate optical measurements. However, specific crystals and driving lasers must be developed for entangled photon sources, and it is difficult to generate and detect entangled photon pairs rapidly. R&D on these issues is currently advancing around the world.

Among communication protocols using entangled light sources, a protocol called entanglement swapping is fundamental to extending distances for quantum signals and for networking quantum computation devices. The entanglement swapping scheme is shown in Figure 1. First, separate entangled photon

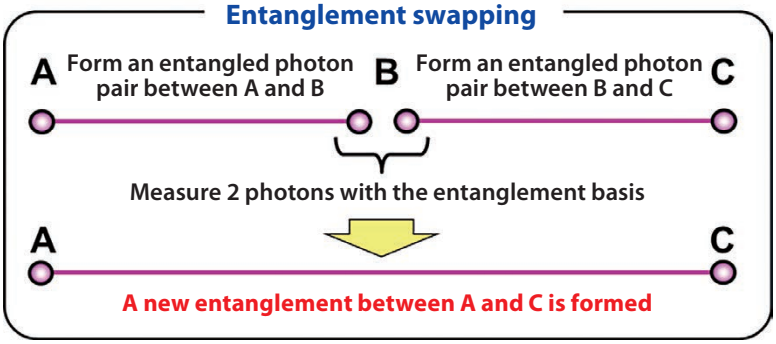


Figure 1 Entanglement swapping procedure

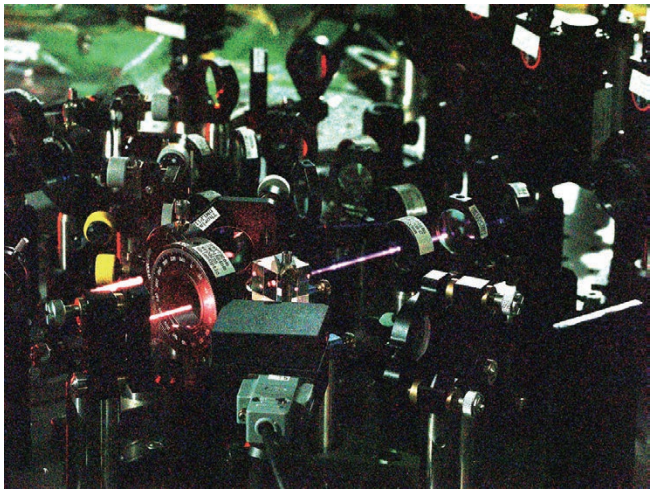


Figure 2 Experimental equipment used for entanglement swapping

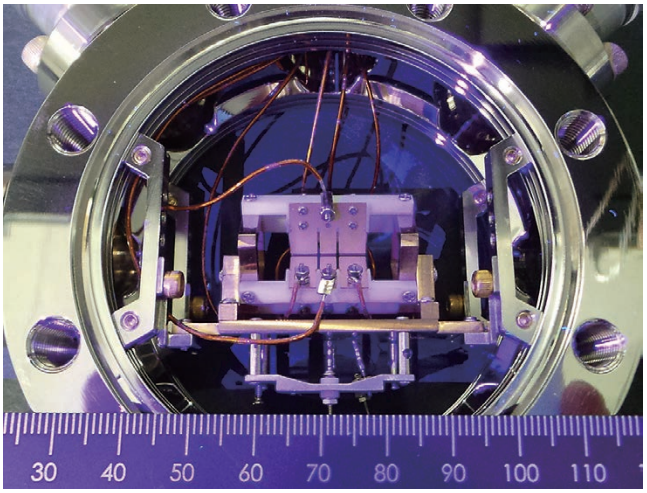


Figure 3 Ion trap equipment

pairs are shared between points A and B, and between points B and C. Initially, the photon pairs between A and B, and between B and C have no correlation. Then, a special measurement is performed at B to determine whether a photon has arrived. This measurement captures a photon, masked such that whether the photon came from A or C cannot be determined, which forms a new entanglement between A and C. The actual experimental system is shown in Figure 2 and uses special optical elements (such as mirrors that are highly reflective for specific wavelengths), lasers of various colors, and highly efficient photon detectors.

NICT has developed an original technology that is able to generate entangled pairs of photons efficiently, at wavelengths that are important for fiber-optic communications (near 1,550 nm). We have also successfully achieved entanglement swapping using multiple entangled photon pairs generated this way, with much greater performance than was possible earlier. Various research facilities are conducting research on entanglement swapping, but with our accumulation of technical improvements, including our search for special optical crystals and highly efficient photon detectors, we have recently verified entanglement swapping success rates more than 1,000 times higher than other leading research.

Measuring ion quantum state

While photons are being considered for transmitting quantum state, atoms are considered suitable for quantum computation and quantum state memory. Atoms that have lost an electron are called ions. Their motion can be controlled by an electric field and they can be isolated and held still using a technique called laser cooling. Figure 3 shows equipment called an ion trap, which is able to capture ions, and Figure 4 shows calcium (Ca^+) and indium (In^+) ions laser cooled in the ion trap. Quantum computation using ions like this with several quantum bits has been demonstrated and reported .

Quantum mechanics shows that atoms are only able to absorb light of specific transition frequencies determined by their internal structure. An optical frequency standard, which emits the same frequency accurately no matter where it is in the world, can be created by controlling a laser frequency to match these specific transition frequencies. The transition frequency from a laser-cooled ion in the ion trap does not fluctuate due to motion or collisions, so it is promising as an optical frequency standard. R&D on such standards is being conducted using several different ion species. We are conducting R&D on the ultimate metrology technology, using In^+ as an optical frequency standard, which will improve accuracy by two orders of magnitude. Laser cooling and measuring the quantum state of In^+ ions requires a light wavelength of 159 nm, but since it is difficult to generate light at such short wavelengths, new methods had to be developed. We developed a method called "sympathetic cooling" for cooling an In^+ ion to its vibrational ground state, which is the lowest energy state allowed by quantum mechanics. The ion is cooled indirectly by two laser-cooled Ca^+ ions. Figure 4 shows the arrangement of Ca^+ and In^+ ions, captured using an image-intensified CCD camera. To measure the quantum state of an In^+ ion fixed in this way, we developed a quantum logic spectroscopy method that uses a weak transition of the In^+ ion and transfers the quantum state of the In^+ ion to a Ca^+ ion, which is then measured. We have also transferred several of these technologies to the time-space standards laboratory, which has demonstrated operation of an In^+ optical frequency standard.

Future prospects

Realizing entanglement swapping at wavelengths suitable for high-speed fiber-optic communication will enable it to be integrated with inexpensive, high-performance optical communication components. This should contribute to increased performance of quantum cryptography and other quantum communication techniques. By increasing the operating speed of entanglement swapping equipment, we hope to realize various quantum node technologies in the future, including quantum computation using entanglement and high-precision optical measurements.

The current ion trap system weighs over 100 kg, so it is not suitable for applications in data network nodes. New R&D on an integrated ion trap has begun, with the goal of a device size that will fit in a standard instrumentation rack. This should bring us one step closer to implementing quantum node technologies. Greatly increased optical communication capacity can also be expected by applying increases in optical frequency stability to communication lasers.

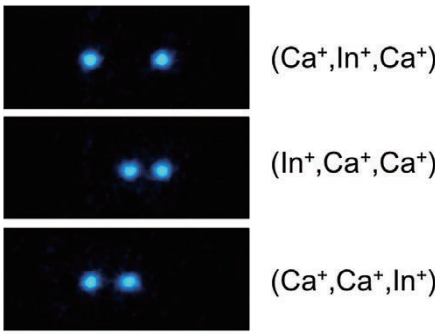


Figure 4 Arrangement of calcium ions (Ca^+) and indium ions (In^+) observed using an image-intensified CCD camera. The In^+ ions cannot be observed directly.

Quantum physics explored through superconducting circuits

Controlling interactions between light and matter at the single photon level

Kouichi SEMBA
Principal Investigator, Macroscopic Quantum Physics Project, Frontier Research Laboratory, Advanced ICT Research Institute

Prior to joining NICT, Dr. Semba engaged in research on superconducting quantum electronics at NTT Basic Research Laboratories, NTT Corporation, and at the Global Research Center for Quantum Information Science of the National Institute of Informatics. Ph.D. (Engineering).

The Macroscopic Quantum Physics Project team conducts research on accurately measuring and controlling the interactions between light and matter at the single photon level. To represent matter, we use macroscopic quantum systems such as superconducting circuits (artificial atoms), which are fabricated using semiconductor nano-fabrication techniques and have properties similar to atoms and electron-spin ensembles in semiconductor crystals. We use these artificial atoms because the light-matter interactions are orders of magnitude stronger than those using ordinary atoms, making it easier to observe and control the interactions between light and matter at the single photon level. By understanding physical phenomena that only appear with these types of macroscopic quantum systems, we hope to pioneer certain quantum technologies that will be useful for information and communications in the future.

"Schrödinger's cat" and superconducting artificial atoms

About 100 years ago, at the beginning of the 20th century, it gradually became clear that the physical laws governing the microscopic world of atoms are very strange compared with the physical laws we experience intuitively in everyday life. For example, when we go to work or school in the morning, we have to choose a method of transportation, e.g., train, bus, or walking. In the world of atoms, we could take all of them at once, in arbitrary proportions. We could be in a (superposition) state where we are "mostly walking, riding the train a little, and maybe on the bus too." Similarly in the world of atoms, given only one umbrella and one raincoat, I could use one while my brother uses the other or vice versa, or we could be in an (entangled) state with any combination of these two states. In fact, being noticed (observed) by anyone would result in only one of these states. These extremely weird properties of quantum states like superposition and entanglement are collectively called "quantum resources."

There is an experiment called Young's double-slit experiment (Figure 1). In this experiment, light from a light source appears as interference fringes on a screen when passing through a double slit. Here, individual photons, which are the smallest unit of light, have a strange property—they appear to interfere with an "alternate history" of which slit they passed through when traveling from the light source through the double slit to be observed on a screen. Thus, in some places the light weakens due to interference and almost no photons are observed while in other places it strengthens, and many are observed. In this way, as a result of a large number of single photon interference events, we observe a striped pattern.

Why then do we not observe states like superposition or entanglement for the objects we deal with everyday, which are composed of atoms? Or, what is the largest size of an object for which a superposition can occur? These are questions that anyone would have. These questions, which are still not completely understood today, were first raised by Schrödinger in 1935, using his famous thought experiment involving a cat, as follows. Suppose there is a device with a bottle of deadly poison that will break in accordance with the radioactive nuclear decay of an atom, which occurs on average, once per hour. What will happen if a cat is placed in this device and left for one hour before being ob-

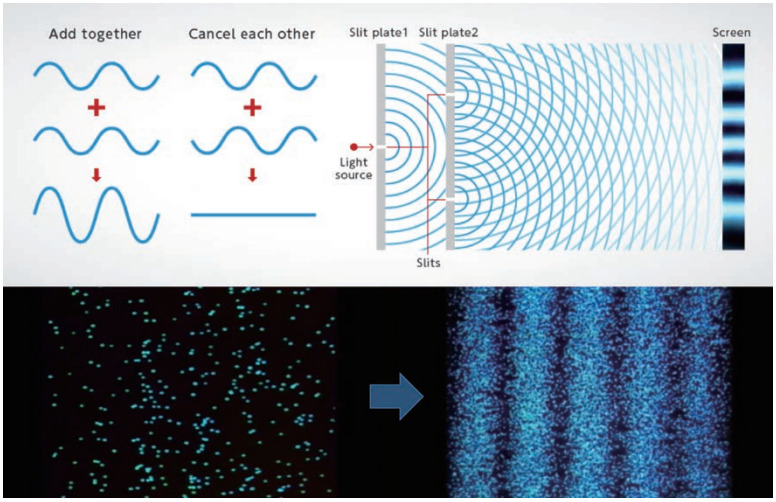


Figure 1 Young's double-slit experiment with extremely weak light (The source: Hamamatsu Photonics, "Photon terrace")

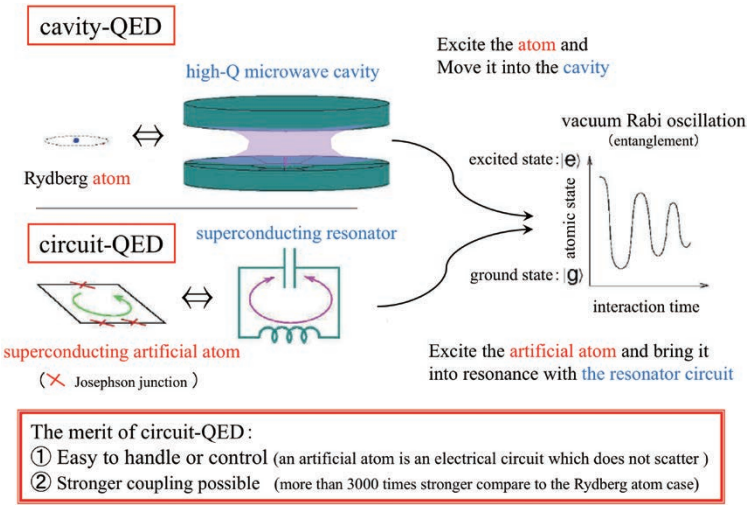
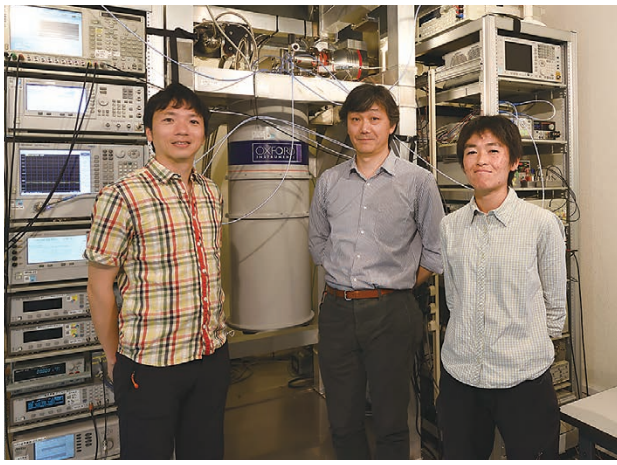


Figure 2 Comparison of a cavity-QED using an atom and a cavity resonator; circuit-QED using on-chip superconducting circuits



Circuit-QED experimental setup and Macroscopic Quantum Physics Project members (from left), Senior Researcher Fumiki YOSHIHARA, Kouichi SEMBA, and Senior Researcher Tomoko FUSE;

Web page introducing Macroscopic Quantum Physics Project research: http://www.nict.go.jp/en/frontier/mqp/index.html

served? Will a superposition of states with the cat both living and dead be realized? Hypothesizing how the physical laws of the microscopic world can affect macroscopic entities in this way leads to contradictions with classical, biological, and other irreversible phenomena and to paradoxical states, as clearly indicated by this thought experiment. This landmark experiment demonstrated the limited understanding of macroscopic quantum phenomena at that time and pointed out the challenges that persist almost 100 years later.

Today, more than 80 years later, macroscopic quantum phenomena can be studied and researched using superconducting artificial atoms, which are electronic circuits cooled to very low temperatures. These are still much smaller than a cat, but they can be seen with a microscope. In our research, we are able to produce arbitrary superpositions of two states in the laboratory, with currents of several hundred nanoamperes traveling both clockwise and counterclockwise within superconducting electronic circuits formed of aluminum superconductors. We can thus control and measure these states.

Reinforcing interactions between light and matter — Circuit-QED

Handling fundamental interactions between light and matter at the single photon level has conventionally been done using quantum electrodynamics in a resonator, or "cavity-QED," involving photons in a single-mode cavity oscillator with a high Q value, combined with an atom having a pair of energy levels resonant with the photon energy. Around 2001, it was theoretically proposed that similar experiments could be performed by replacing the atom with a superconducting artificial atom and the cavity resonator with a superconducting resonator circuit (see Figure 2). This was then verified in successive experiments from 2004 onward. Furthermore, it was found that interactions between microwave photons and superconducting artificial atoms can be made thousands of times stronger than those between microwave photons and atoms. As a result, it has become possible to measure changes in quantities due to a single microwave photon, such as a change in the energy levels in an artificial atom or a shift in phase of a probe microwave. In this way, circuit-QED experiments using superconducting circuits made on a silicon substrate are basically able to reproduce, in terms of quantum state control, what was possible with earlier methods using atoms and molecules. Also, since such control is much easier, quantum resources such as quantum simulators and quantum computers run and can be controlled systematically, and R&D on devices is advancing around the world. When they are completed, surely "Schrödinger's cat" will appear as well!

Since it is possible to create much stronger couplings than with conventional methods using atoms and molecules, new areas of physics, which were previously difficult to achieve, can also be developed, such as super-strongly coupled states and super-radiant quantum phase transition. In our laboratory, we have achieved extremely strong interactions between aluminum superconducting artificial atoms and LC resonator circuits (Figure 3). We are now accumulating data from precise transmission spectrum measurements, indicating that coupled system states are in an unexplored region that has not yet been realized.

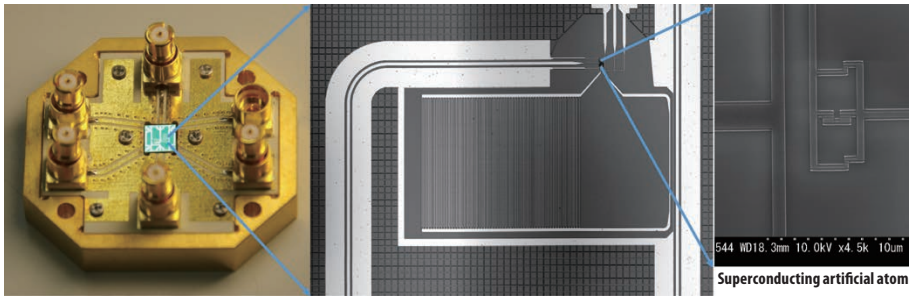


Figure 3 Circuit QED test sample using a superconducting artificial atom (white areas in photo are superconducting thin-film circuit made of aluminum)
Left: 3-mm sample chip mounted in sample holder for circuit QED experiment.
Center: Superconducting artificial atom and LC circuit coupled system.
Right: Superconducting artificial atom (4 μm × 8 μm)

Future developments

We are pioneering an unexplored region of physics by coupling macroscopic quantum systems (superconducting artificial atoms) with microscopic photons or electron spins. By understanding the resulting phenomena at the single photon level, and through precise control, we are searching for new resources and phenomena that will be useful for ICT in the future. Beyond quantum ICT, these resources also hold promise for development in other fields, such as improving the precision of time and frequency standards and enabling the development of quantum-enhanced sensors, quantum simulators, and quantum computers.

Exhibition and seminar focused on wireless networks playing important roles in business, industry, and social infrastructures

Report on WIRELESS TECHNOLOGY PARK 2016

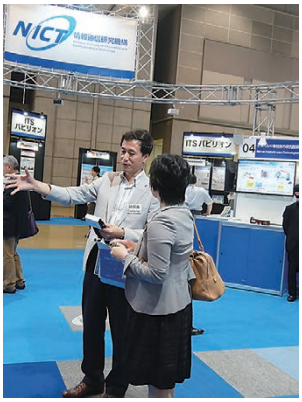
Planning Office, Wireless Networks Research Center

NICT, together with the YRP R&D Promotion Committee and YRP Academia Collaboration Network, held "Wireless Technology Park (WTP) 2016" on May 25-27, 2016, at Tokyo Big Sight.

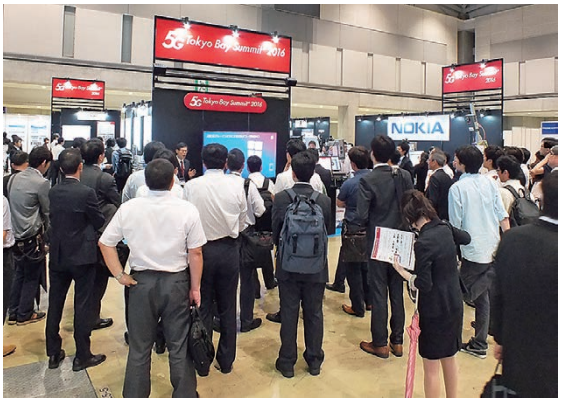
The exhibition featured 116 organizations, and 124 seminars were given covering 25 courses. Combined with concurrently held events, approximately 47,000 people attended, while WTP had approximately 11,000 attendees. This was 10% more than the previous year and the highest attendance ever. In particular, the pavilion and seminars under the theme of the 5th Generation Mobile Communication Systems (5G) attracted a lot of attention.

NICT presented 17 exhibits and 10 lectures on our latest results, mainly from our research center, and we received many questions and comments regarding implementation of the technologies from visitors.

We would like to thank all those who offered their cooperation with WTP 2016. We will work even harder to ensure that next year's exhibition (May 24-25, 2017) will be an even more interesting and attractive one.



Chief Senior Researcher Li introducing an IR-UWB indoor positioning system with high accuracy



The 5G Tokyo Bay Summit™ 2016 pavilion showing the latest 5G research results

Report on Interop Tokyo 2016

NICT exhibited at Interop Tokyo 2016, an event specializing in Internet and Digital Media, held at Makuhari Messe on June 8-10, 2016. The event was attended by 140,945 people, exceeding the number for the previous year.

NICT exhibited network and security technologies for the IoT era and introduced the finalist entrepreneurship companies from the Entrepreneurs' Expo. One of the lectures from NICT, "Next-generation cyber-attack countermeasures with the NICTER family of technologies," was so successful that an additional lecture was delivered, with over 150 attendees. Thank you to all who visited the NICT booth.

NICT booth

Awards

The Minister of Education, Culture, Sports, Science and Technology confers this award on individuals that have achieved remarkable results in R&D or advancing understanding in areas of science and technology. The Ichimura Prize is presented to a technical researcher or group, at a university or other research facility with research that has contributed to advancement in a technical field and has research achievements with practical applications.

Minister of Education, Culture, Sports, Science and Technology

Fiscal year 2016 The Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology

Development Category for Science and Technology

Seiho URATSUKA

Managing Director,
Applied Electromagnetic Research Institute

Comment from the recipient

We have advanced development of airborne synthetic aperture radar (Pi-SAR2) to rapidly grasp conditions after serious and wide ranging disasters such as earthquakes and volcanic eruptions, regardless of weather or sunlight condition.

Receiving this award shows that there is broad knowledge in society of the usefulness of this technology in times of disaster, and I share this honor with many who contributed their effort in developing it.

We continue to pray for realization of a society that is resilient in disaster, and hope that this technology can be widely used to this end.

data

- Date: April 20, 2016
- Description: For contributing to the safety and security of the population through R&D on Pi-SAR2, helping to assess disaster conditions quickly

The New Technology Development Foundation

The 48th Ichimura Prize in Science for Excellent Achievement

Miyako OHKUBO

Senior Researcher, Security Fundamentals Laboratory,
Cybersecurity Research Institute

Miyako OHKUBO (Center)

Comment from the recipient

This award is for proposing a novel concept called Structure-Preserving (SP) Cryptography, which enables simple yet secure design of information systems, and also for providing concrete instantiations such as SP digital signatures and commitments. It is a great honor for us to receive the award. Sincere thanks to all who collaborated with us in this research and supported our work explicitly or implicitly. We will continue to commit our efforts to this research field and help develop secure practical systems.

data

- Co-recipient: Masayuki ABE (Nippon Telegraph and Telephone Corporation)
- Date: April 25, 2016
- Description: For pioneering work on Structure-Preserving Cryptography for efficient and interoperable cryptographic system design

NICT NEWS No.459 AUG 2016
Published by
Public Relations Department,
National Institute of Information and Communications Technology
<NICT NEWS URL> http://www.nict.go.jp/en/data/nict-news/

4-2-1 Nukui-Kitamachi, Koganei, Tokyo
184-8795, Japan
TEL: +81-42-327-5392 FAX: +81-42-327-7587
E-mail: publicity@nict.go.jp
URL: http://www.nict.go.jp/en/
Twitter: @NICT_Publicity

ISSN 2187-4050 (Online)